Cisco Router and Security Device Manager Benutzerhandbuch

2.4.1

Firmenhauptsitz in den USA
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel.: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Kundenbestellnummer:
Dokumentnummer: OL-9961-04

DIE SPEZIFIKATIONEN UND INFORMATIONEN ZU DEN PRODUKTEN IN DIESEM HANDBUCH KÖNNEN SICH OHNE VORHERIGE ANKÜNDIGUNG ÄNDERN. ES WIRD DAVON AUSGEGANGEN, DASS ALLE DARLEGUNGEN, INFORMATIONEN UND EMPFEHLUNGEN IN DIESEM HANDBUCH KORREKT SIND, SIE WERDEN JEDOCH OHNE JEGLICHE GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH IMPLIZIERT, VORGELEGT. DIE BENUTZER TRAGEN DIE VOLLE VERANTWORTUNG FÜR DIE ANWENDUNG JEGLICHER PRODUKTE.

DIE SOFTWARELIZENZ UND EINGESCHRÄNKTE GEWÄHRLEISTUNG FÜR DAS BEGLEITENDE PRODUKT SIND IN DEM INFORMATIONSPAKET AUSGEFÜHRT, DAS DIESEM PRODUKT BEILIEGT, UND SIND DURCH DIESEN VERWEIS HIER AUFGENOMMEN. WENN SIE DIE SOFTWARELIZENZ ODER EINGESCHRÄNKTE GEWÄHRLEISTUNG NICHT FINDEN KÖNNEN, ERHALTEN SIE EIN EXEMPLAR BEI IHREM CISCO-REPRÄSENTANTEN.

Die Cisco-Implementierung der TCP Header-Komprimierung ist die Adaption eines Programms, das von der University of California, Berkeley (UCB) als Teil der öffentlichen Domänenversion von UCB des UNIX-Betriebssystems entwickelt wurde. Alle Rechte vorbehalten. Copyright © 1981, Regents of the University of California.

UNGEACHTET ALLER HIERIN ENTHALTENEN GEWÄHRLEISTUNGEN WERDEN ALLE DOKUMENTDATEIEN UND DIE SOFTWARE DIESER LIEFERANTEN IM VORLIEGENDEN ZUSTAND MIT ALLEN FEHLERN GELIEFERT. CISCO UND DIE OBEN GENANNTEN LIEFERANTEN SCHLIESSEN JEGLICHE GEWÄHRLEISTUNG, AUSDRÜCKLICH ODER IMPLIZIERT, EINSCHLIESSLICH, UNEINGESCHRÄNKT, JEGLICHER GEWÄHRLEISTUNG FÜR MARKTFÄHIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND WAHRUNG DER RECHTE DRITTER ODER SOLCHE GEWÄHRLEISTUNG, DIE AUS EINER GESCHÄFTS-, NUTZUNGS- ODER HANDELSPRAXIS ENTSTEHT, AUS.

CISCO ODER SEINE LIEFERANTEN HAFTEN IN KEINEM FALL FÜR INDIREKTE; SPEZIELLE; FOLGE- ODER BEGLEITSCHÄDEN, EINSCHLIESSLICH, OHNE BESCHRÄNKUNG, ENTGANGENE GEWINNE SOWIE DEN VERLUST ODER DIE BESCHÄDIGUNG VON DATEN, DIE AUS DER VERWENDUNG ODER UNFÄHIGKEIT DER VERWENDUNG DIESES HANDBUCHS ENTSTEHEN, AUCH WENN CISCO ODER SEINE LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN.

Die in diesem Dokument verwendeten IP (Internet Protocol)-Adressen sind frei erfunden. Alle im Dokument enthaltenen Beispiele, Befehlszeilenausgaben und Abbildungen dienen nur Darstellungszwecken. Die Verwendung tatsächlich vorhandener IP-Adressen in darstellenden Inhalten ist nicht beabsichtigt und zufällig.

Cisco Router and Security Device Manager 2.4 Benutzerhandbuch

INHALT

KAPITEL 1

Startseite

Auf der Startseite erhalten Sie allgemeine Informationen über Hardware, Software und Konfiguration des Routers. Diese Seite enthält die folgenden Abschnitte:

Hostname

Der konfigurierte Name des Routers.

Über Ihren Router

In diesem Abschnitt werden allgemeine Informationen über Hardware und Software des Routers angezeigt. Er enthält die folgenden Felder:

Hardware		Software	
Modelltyp	Zeigt die Modellnummer des Routers.	**IOS-Version**	Die Version der Cisco IOS-Software, die derzeit auf dem Router ausgeführt wird.
Speicher verfügbar/gesamt	Verfügbarer RAM/gesamter RAM.	**Cisco SDM-Version**	Die Version der Cisco Router and Security Device Manager (Cisco SDM)-Software, die derzeit auf dem Router ausgeführt wird.

Hardware		Software	
Flash-Kapazität gesamt	Flash und Webflash (sofern zutreffend).		
Funktionsverfügbarkeit	Die im Cisco IOS-Abbild verfügbaren Funktionen, die der Router verwendet, werden durch eine Überprüfung ermittelt. Cisco SDM führt eine Überprüfung auf folgende Funktionen durch: IP, Firewall, VPN, IPS und NAC.		

Mehr?

Über den Link **Mehr?** wird ein Popup-Fenster mit weiteren Details zu Hardware und Software angezeigt.

- Hardwaredetails – Zusätzlich zu den Informationen im Abschnitt „Über Ihren Router“ informiert diese Registerkarte über Folgendes:
  - Ob der Router vom Flash oder von der Konfigurationsdatei bootet
  - Ob der Router Beschleuniger hat, z. B. VPN-Beschleuniger
  - Ein Diagramm der Hardwarekonfiguration mit dem Flashspeicher und den installierten Geräten, wie z.B. USB-Flash und USB-Tokens.
- Softwaredetails – Zusätzlich zu den Informationen im Abschnitt „Über Ihren Router“ informiert diese Registerkarte über Folgendes:
  - Die im IOS-Abbild enthaltenen Funktionssätze
  - Die geladene Cisco SDM-Version.

Konfigurationsübersicht

Dieser Abschnitt der Startseite enthält eine Übersicht über die vorgenommenen Konfigurationseinstellungen.

Hinweis Wenn Sie Informationen zu einer Funktion, die in diesem Hilfethema erläutert werden, nicht auf der Startseite wiederfinden, wird die Funktion vom Cisco IOS-Abbild nicht unterstützt. Beispiel: Wenn der Router ein Cisco IOS-Abbild verwendet, das Sicherheitsfunktionen nicht unterstützt, sind die Bereiche Firewallrichtlinie, VPN und Intrusion Prevention auf der Startseite nicht enthalten.

Aktive Konfiguration anzeigen

Mit einem Mausklick auf diese Schaltfläche wird die aktive Konfiguration des Routers angezeigt.

Schnittstellen und Verbindungen	**Aktiv (*n*)**: Die Anzahl der aktiven LAN- und WAN-Verbindungen.	**Inaktiv (*n*)**: Die Anzahl der inaktiven LAN- und WAN-Verbindungen.	**Doppelpfeil**: Klicken Sie darauf, um Details ein- bzw. auszublenden.
Unterstütztes LAN gesamt	Die Gesamtzahl der LAN-Schnittstellen im Router.	Unterstütztes WAN gesamt	Die Gesamtzahl der von Cisco SDM unterstützten WAN-Schnittstellen im Router.
Konfigurierte LAN-Schnittstelle	Die Anzahl unterstützter LAN-Schnittstellen, die derzeit auf dem Router konfiguriert sind.	WAN-Verbindungen gesamt	Die Gesamtzahl der von Cisco SDM unterstützten WAN-Verbindungen im Router.
DHCP-Server	Konfiguriert/ Nicht konfiguriert		
DHCP-Pool (Detailansicht)	Wenn ein Pool konfiguriert ist, Start- und Endadresse des DHCP-Pools. Wenn mehrere Pools konfiguriert sind, Liste der konfigurierten Pool-Namen.	**Anzahl der DHCP-Clients (Detailansicht)**	Aktuelle Anzahl der Clients, die Adressen leasen.
Schnittstelle	**Art**	**IP/Maske**	**Beschreibung**
Name der konfigurierten Schnittstelle	Schnittstellentyp	IP-Adresse und Subnetzmaske	Beschreibung der Schnittstelle

Firewallrichtlinien	**Aktiv/Inaktiv**	**Vertrauenswürdig (*n*)**	**Nicht vertrauenswürdig (*n*)**	**DMZ (*n*)**
	Aktiv – Es ist eine Firewall eingerichtet. Inaktiv – Es ist keine Firewall eingerichtet.	Die Anzahl der vertrauenswürdigen (inneren) Schnittstellen.	Die Anzahl der nicht vertrauenswürdigen (äußeren) Schnittstellen.	Die Anzahl der DMZ-Schnittstellen.
Schnittstelle	**Firewallsymbol**	**NAT**	**Prüfregel**	**Zugriffsregel**
Der Name der Schnittstelle, der eine Firewall zugeordnet wurde.	Ob die Schnittstelle als innere oder äußere Schnittstelle angegeben ist.	Der Name oder die Nummer der NAT-Regel, die dieser Schnittstelle zugeordnet ist.	Die Namen oder Nummern der eingehenden und ausgehenden Prüfregeln.	Die Namen oder Nummern der eingehenden und ausgehenden Zugriffsregeln.

VPN	**Aktiv (*n*)**- Die Anzahl aktiver VPN-Verbindungen.		
IPSec (Site-to-Site)	Die Anzahl der konfigurierten Site-to-Site-VPN-Verbindungen.	**GRE over IPSec**	Die Anzahl der konfigurierten GRE over IPSec-Verbindungen (GRE: Generic Routing Encapsulation).
XAuth-Anmeldung erforderlich	Die Anzahl der Easy VPN-Verbindungen, die eine XAuth-Anmeldung erwarten. *Siehe Hinweis.*	**Easy VPN Remote**	Die Anzahl der konfigurierten Easy VPN Remote-Verbindungen.

VPN	**Aktiv (*n*)**- Die Anzahl aktiver VPN-Verbindungen.		
Anzahl der DMVPN-Clients	Wenn der Router als DMVPN-Hub konfiguriert ist, die Anzahl der DMVPN-Clients.	**Anzahl der aktiven VPN-Clients**	Wenn der Router als Easy VPN-Server fungiert, die Anzahl der Easy VPN-Clients mit aktiven Verbindungen.
Schnittstelle	**Typ**	**IPSec-Richtlinie**	**Beschreibung**
Der Name einer Schnittstelle mit einer konfigurierten VPN-Verbindung.	Der Typ der auf der Schnittstelle konfigurierten VPN-Verbindung.	Der Name der IPSec-Richtlinie, die mit der VPN-Verbindung verknüpft ist.	Eine Beschreibung der Verbindung.

Hinweis

- Einige VPN-Server oder -Konzentratoren authentifizieren Clients mit Extended Authentication (XAuth). Hier wird die Anzahl der VPN-Tunnel angezeigt, die eine XAuth-Anmeldung erwarten. Wenn ein Easy VPN-Tunnel eine XAuth-Anmeldung erwartet, wird ein separater Mitteilungsbereich mit der Schaltfläche **Anmeldung** angezeigt. Wenn Sie auf **Anmeldung** klicken, können Sie die Anmeldeinformationen für den Tunnel eingeben.
- Wenn XAuth für einen Tunnel konfiguriert wurde, wird er erst aktiviert, wenn die Anmeldeinformationen und das Kennwort angegeben wurden. Es gibt keine Zeitbegrenzung, nach der nicht mehr auf diese Informationen gewartet wird.

NAC-Regeln	**Aktiv oder Inaktiv**
Spalte Schnittstelle	**Spalte NAC Regelungen**
Der Name der Schnittstelle, auf welche die Regel anzuwenden ist. Z.B. FastEthernet 0 oder Ethernet 0/0.	Der Name der NAC Regel.

Routing		Intrusion Prevention	
Anzahl der statischen Routen	Die Anzahl der auf dem Router konfigurierten statischen Routen.	**Aktive Signaturen**	Anzahl der vom Router verwendeten aktiven Signaturen. Sie können integriert sein oder von einem Remote-Standort geladen werden.
Protokolle für dynamisches Routing	Liste der Protokolle für dynamisches Routing, die auf dem Router konfiguriert sind.	**Anzahl IPS-aktivierter Schnittstellen**	Die Anzahl der Routerschnittstellen, auf denen IPS aktiviert wurde.
		SDF-Version	Die Version der SDF-Dateien in diesem Router.
		Sicherheits-Dashboard	Ein Link zur IPS-Sicherheitskonsole, auf der die wichtigsten zehn Signaturen angezeigt und übernommen werden können.

KAPITEL 2

LAN-Assistent

Der Cisco Router and Security Device Manager-(Cisco SDM-)LAN-Assistent leitet Sie durch die Konfiguration einer LAN-Schnittstelle. Dieser Bildschirm listet die LAN-Schnittstellen im Router auf. Sie können beliebige im Fenster angezeigte Schnittstelle auswählen und auf **Konfigurieren** klicken, um die Schnittstelle als LAN-Schnittstelle zu verwenden und diese zu konfigurieren.

Dieses Fenster listet die Routerschnittstellen auf, die als innere Schnittstellen in der Startkonfiguration angegeben wurden, sowie die Ethernet-Schnittstellen und Switch-Ports, die nicht als WAN-Schnittstellen konfiguriert wurden. Die Liste umfasst Schnittstellen, die bereits konfiguriert wurden.

Wenn Sie eine Schnittstelle als LAN-Schnittstelle konfiguriert haben, fügt Cisco SDM die Beschreibung $ETH-LAN$ zur Konfigurationsdatei hinzu, sodass diese Schnittstelle künftig als LAN-Schnittstelle erkannt werden kann.

Schnittstelle

Der Name der Schnittstelle.

Konfigurieren

Klicken Sie auf diese Schaltfläche, um eine von Ihnen ausgewählte Schnittstelle zu konfigurieren. Wenn die Schnittstelle vorher noch nicht konfiguriert wurde, werden Sie von Cisco SDM zum LAN-Assistenten geleitet, der Sie bei der Konfiguration unterstützt. Wenn die Schnittstelle mit Cisco SDM konfiguriert wurde, zeigt Cisco SDM ein Fenster **Bearbeiten** an, in dem Sie die Konfigurationseinstellungen ändern können.

Die Schaltfläche **Konfigurieren** ist eventuell deaktiviert, wenn einer LAN-Schnittstelle eine Konfiguration zugewiesen wurde, die nicht von Cisco SDM unterstützt wird. Eine Liste solcher Konfigurationen finden Sie unter Ursachen, warum eine Ethernet-Schnittstellenkonfiguration schreibgeschützt sein kann.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Konfigurieren oder Bearbeiten einer LAN-Schnittelle oder eines LAN-Switch-Ports	Wählen Sie die VLAN-Schnittstelle oder den Switch-Port in der Liste aus, und klicken Sie auf **Konfigurieren**. Wenn die Schnittstelle vorher noch nicht konfiguriert wurde oder wenn Sie einen Switch-Port auswählen, werden Sie von Cisco SDM durch einen LAN-Assistenten geleitet, in dem Sie die Konfiguration der Schnittstelle vornehmen können. Wenn die Schnittstelle bereits konfiguriert wurde, oder wenn es sich nicht um einen Switch-Port handelt, können Sie auf **Konfigurieren** klicken, um ein Fenster **Bearbeiten** anzuzeigen, über das Sie Änderungen an der LAN-Konfiguration vornehmen können.
Erneutes Konfigurieren der IP-Adresse, der Maske oder der DHCP-Eigenschaften einer Schnittstelle, die bereits konfiguriert wurde	Wählen Sie eine Schnittstelle mit einer IP-Adresse aus, und klicken Sie auf **Konfigurieren**.

Aufgabe	Vorgehensweise
Ausführen bestimmter LAN-bezogener Konfigurationen für Elemente wie DHCP-Server- oder Maximum Transmission Unit-(MTU-)Einstellungen	Klicken Sie auf in der Cisco SDM-Leiste **Kategorie** auf **Schnittstellen und Verbindungen**, klicken Sie auf die Registerkarte **Schnittstellen und Verbindungen bearbeiten,** und führen Sie die Änderungen an der Konfiguration aus.
Informationen zum Ausführen verwandter Konfigurationsaufgaben	Lesen Sie eine der folgenden Vorgehensweisen: • Wie konfiguriere ich eine statische Route? • Wie zeige ich Aktivitäten in meiner LAN-Schnittstelle an? • Wie aktiviere oder deaktiviere ich eine Schnittstelle? • Wie zeige ich die IOS-Befehle an, die ich an den Router sende? • Wie starte ich die Wireless-Anwendung von Cisco SDM aus?

Sie können beliebig oft zu diesem Bildschirm zurückkehren, um weitere LAN-Schnittstellen zu konfigurieren.

Ethernet-Konfiguration

Der Assistent leitet Sie durch die Konfiguration einer Ethernet-Schnittstelle im LAN. Sie müssen folgende Informationen angeben:

- Eine IP-Adresse und Subnetzmaske für die Ethernet-Schnittstelle
- Einen DHCP-Adressen-Pool, wenn Sie DHCP in dieser Schnittstelle verwenden möchten
- Die Adressen der DNS- und WINS-Server im WAN
- Einen Domänennamen

LAN-Assistent: Schnittstelle auswählen

Wählen Sie die Schnittstelle aus, in der Sie die LAN-Verbindung über dieses Fenster konfigurieren möchten. Dieses Fenster listet die Schnittstellen auf, die Ethernet-LAN-Konfigurationen unterstützten können.

LAN-Assistent: IP-Adresse und Subnetzmaske

In diesem Fenster können Sie eine IP-Adresse und Subnetzmaske für die Ethernet-Schnittstelle, die Sie im ersten Fenster ausgewählt haben, konfigurieren.

IP-Adresse

Geben Sie die IP-Adresse für die Schnittstelle im durch Punkte getrennten Dezimalformat ein. Ihr Netzwerkadministrator kann die IP-Adressen der LAN-Schnittstellen ermitteln. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Diesen Wert erhalten Sie von Ihrem Netzwerkadministrator. Die Subnetzmaske ermöglicht es dem Router, zu ermitteln, zu welchem Teil die IP-Adresse zur Definition des Netzwerks und des Hostanteils der Adresse verwendet wird.

Wählen Sie alternativ die Anzahl der Netzwerkbits aus. Dieser Wert wird verwendet, um die Subnetzmaske zu berechnen. Sie erhalten die Anzahl der einzugebenden Netzwerk-Bits von Ihrem Netzwerkadministrator.

LAN-Assistent: DHCP-Server aktivieren

In diesem Bildschirm können Sie einen DHCP-Server in Ihrem Router aktivieren. Ein DHCP-Server weist automatisch den Geräten im LAN IP-Adressen zu, die erneut verwendet werden können. Wenn ein Gerät im Netzwerk aktiv wird, erhält es vom DHCP-Server eine IP-Adresse. Wenn das Gerät vom Netzwerk getrennt wird, wird die IP-Adresse in den Pool zurückgegeben, sodass sie von einem anderen Gerät verwendet werden kann.

So aktivieren einen DHCP-Server im Router:

Klicken Sie auf **Ja**.

LAN-Assistent: DHCP-Adressen-Pool

In diesem Bildschirm können Sie den DHCP-IP-Adressen-Pool konfigurieren. Die IP-Adressen, die der DHCP-Server zuweist, werden von einem allgemeinen Pool bezogen, den Sie konfigurieren, indem der Bereich für die Start-IP-Adressen und der Bereich für die End-IP-Adressen angegeben wird.

Weitere Informationen finden Sie unter DHCP-Adressen-Pools.

Hinweis Wenn keine zusammenhängenden Adressen-Pools im Router konfiguriert sind, sind die Start-IP- und End-IP-Adressenfelder schreibgeschützt.

Start-IP

Geben Sie den Beginn des IP-Adressenbereichs ein, den der DHCP-Server beim Zuweisen von Adressen an Geräte im LAN verwenden soll. Dies ist die IP-Adresse mit dem niedrigsten Wert im angegebenen Bereich.

End-IP

Geben Sie die IP-Adresse mit den höchsten Zahlenwerten im Bereich der IP-Adressen ein.

Felder „DNS-Server“ und „WINS-Server“

Wenn dieses Fenster die Felder **DNS Server** und **WINS Server** anzeigt, können Sie auf DHCP-Optionen klicken, um weitere Informationen dazu zu erhalten.

DHCP-Optionen

In diesem Fenster konfigurieren Sie DHCP-Optionen, die an Hosts im LAN gesendet werden, die IP-Adressen vom Router anfordern. Es handelt sich dabei nicht um Optionen für den Router, der konfiguriert wird, sondern um Parameter, die an die Hosts im LAN gesendet werden, die Adressen anfordern. Um diese Eigenschaften für den Router festzulegen, klicken Sie in der Cisco SDM-Leiste **Kategorie** auf **Zusätzliche Aufgaben**, klicken auf **DHCP**, und konfigurieren Sie diese Einstellungen im Fenster **DHCP-Pools**.

DNS-Server 1

Der DNS-Server ist üblicherweise ein Server, der eine Zuordnung eines bekannten Gerätenamens mit dessen IP-Adresse vornimmt. Wenn ein DNS-Server für Ihr Netzwerk konfiguriert ist, geben Sie die IP-Adresse für dieses Gerät hier ein.

DNS-Server 2

Wenn sich ein zusätzlicher DNS-Server im Netzwerk befindet, können Sie die IP-Adresse für diesen Server in dieses Feld eingeben.

Domänenname

Der DHCP-Server, den Sie in diesem Router konfigurieren, stellt Dienste für andere Geräte innerhalb dieser Domäne bereit. Geben Sie den Name dieser Domäne ein.

WINS-Server 1

Einige Clients erfordern eventuell den Windows-Internet-Namensserver (Windows Internet Naming Service, WINS) für eine Verbindung mit Geräten im Internet. Wenn ein WINS-Server im Netzwerk konfiguriert ist, geben Sie die IP-Adresse für diesen Server in dieses Feld ein.

WINS-Server 2

Wenn sich ein zusätzlicher WINS-Server im Netzwerk befindet, geben Sie die IP-Adresse für diesen Server in dieses Feld ein.

LAN-Assistent: VLAN-Modus

In diesem Bildschirm können Sie den Typ der VLAN-Informationen ermitteln, die über den Switch-Port übertragen werden. Switch-Ports können entweder für den Zugriffsmodus vorgesehen sein – in diesem Fall werden nur Daten weitergeleitet, die für das VLAN bestimmt sind, dem Sie zugewiesen wurden – oder sie können für den Trunk-Modus vorgesehen sein – in diesem Fall werden Daten weitergeleitet, die für alle VLANs bestimmt sind, einschließlich des VLANs, dem sie zugewiesen sind.

Wenn dieser Switch-Port mit einem einzelnen Gerät verbunden ist, wie beispielsweise einem PC oder IP-Telefon, oder wenn das Gerät mit einem Port oder einem Netzwerkgerät verbunden ist, wie beispielsweise einem anderen Switch, der als Zugriffsmodusport fungiert, wählen Sie die Option **Einzelgerät**.

Wenn dieser Switch-Port mit einem Port in einem Netzwerkgerät, wie einem anderen Switch, der als Trunk-Modus fungiert, verbunden ist, wählen Sie **Netzwerkgerät**.

LAN-Assistent: Switch-Port

In diesem Bildschirm können Sie dem Switch-Port eine bestehende VLAN-Nummer zuweisen oder eine neue VLAN-Schnittstelle erstellen, die dem VLAN-Switch-Port zugewiesen werden soll.

Bestehendes VLAN

Wenn Sie den Switch-Port einem VLAN zuweisen möchten, das bereits definiert wurde, wie beispielsweise zum Standard-VLAN (VLAN 1), geben Sie die VLAN-ID-Nummer in das Feld **Netzwerk-Identifier (VLAN)** ein.

Neues VLAN

Wenn Sie eine neue VLAN-Schnittstelle erstellen möchten, der der Switch-Port zugewiesen werden soll, geben Sie die neue VLAN-ID-Nummer im Feld **Neues VLAN** ein, und geben Sie anschließend die IP-Adresse und Subnetzmaske der neuen logischen VLAN-Schnittstelle in die Felder **IP-Adresse** und **Subnetzmaske** ein.

Nehmen Sie dieses VLAN in eine IRB-Bridge auf, die eine Bridge mit Ihrem Wireless-Netzwerk bildet. (Wireless-Anwendung zur Durchführung verwenden.)

Wenn Sie dieses Kontrollkästchen aktivieren, wird der Switch-Port in eine Bridge zu Ihrem Wireless-Netzwerk eingebunden. Es muss kein anderer Teil der Bridge mit der Wireless-Anwendung konfiguriert werden. Die Felder **IP-Adresse** und **Subnetzmaske** unter **Neues VLAN** sind deaktiviert, wenn dieses Kontrollkästchen aktiviert wird.

Gehen Sie nach Erstellung dieser LAN-Konfiguration wie folgt vor, um die Wireless-Anwendung zu starten und die Bridging-Konfiguration zu vervollständigen.

Schritt 1 Wählen Sie im Cisco SDM-Menü **Extras** die Option **Wireless-Anwendung**. Die Wireless-Anwendung wird in einem separaten Browser-Fenster geöffnet.

Schritt 2 Klicken Sie in der Wireless-Anwendung auf **Wireless Express Security** und dann auf **Bridging**, um die Informationen für die Bridging-Konfiguration einzugeben.

IRB-Bridge

Wenn Sie ein VLAN als Teil einer IRB-Bridge konfigurieren, muss die Bridge zu einer Bridge-Gruppe gehören.

Um eine neue Bridge-Gruppe zu erstellen, zu der diese Schnittstelle gehören soll, klicken Sie auf **Neue Bridge-Gruppe erstellen**, und geben Sie einen Wert im Bereich von 1 bis 255 ein.

Wenn dieses VLAN zu einer bestehenden Bridge-Gruppe gehören soll, klicken Sie auf **Einer vorhandenen Bridge-Gruppe beitreten**, und wählen Sie eine Bridge-Gruppe aus.

Hinweis Wenn Sie die Bridge-Konfiguration in der Wireless-Anwendung vornehmen, müssen Sie dieselbe Bridge-Gruppennummer verwenden, die Sie auf diesem Bildschirm eingegeben haben.

BVI-Konfiguration

Weisen Sie der BVI-Schnittstelle eine IP-Adresse und eine Subnetzmaske zu. Wenn Sie auf dem vorherigen Bildschirm eine bestehende Bridge-Gruppe gewählt haben, erscheinen die IP-Adresse und die Subnetzmaske auf diesem Bildschirm. Sie können die Werte ändern oder unverändert lassen**.**

IP-Adresse

Geben Sie die IP-Adresse für die Schnittstelle im durch Punkte getrennten Dezimalformat ein. Ihr Netzwerkadministrator kann die IP-Adressen der LAN-Schnittstellen ermitteln. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Netzwerkmaske

Geben Sie die Subnetzmaske ein. Diesen Wert erhalten Sie von Ihrem Netzwerkadministrator. Die Subnetzmaske ermöglicht es dem Router, zu ermitteln, zu welchem Teil die IP-Adresse zur Definition des Netzwerks und des Hostanteils der Adresse verwendet wird.

Subnetz-Bits

Wählen Sie alternativ die Anzahl der Netzwerkbits aus. Dieser Wert wird verwendet, um die Subnetzmaske zu berechnen. Sie erhalten die Anzahl der einzugebenden Netzwerk-Bits von Ihrem Netzwerkadministrator.

DHCP-Pool für BVI

Wenn Sie den Router als DHCP-Server konfigurieren, können Sie einen Pool von IP-Adressen für die Clients im Netzwerk erstellen. Wenn der Client sich im Netz abmeldet, steht die Adresse wieder als Pool-Adresse für andere Hosts zur Verfügung.

Konfiguration des DHCP-Servers

Aktivieren Sie diese Option, wenn der Router als DHCP-Server fungieren soll. Geben Sie dann die Start- und die End-IP-Adresse des Pools ein. Geben Sie IP-Adressen desselben Subnetzes ein, zu dem die IP-Adresse gehört, die Sie der Schnittstelle zugewiesen haben. Wenn Sie der Schnittstelle beispielsweise die IP-Adresse 10.10.22.1 zugewiesen haben, verfügen Sie bei einer Subnetzmaske von 255.255.255.0 über 250 Adressen für den Pool, und Sie können z. B. die **Start-IP-Adresse** 10.10.22.2 und die **End-IP-Adresse** 10.10.22.253 angeben.

IRB für Ethernet

Wenn Ihr Router über eine Wireless-Schnittstelle verfügt, können Sie integriertes Routing und Bridging (IRB) verwenden, damit die Schnittstelle in eine Bridge zum drahtlosen LAN eingebunden wird. Zudem können Sie festlegen, dass Datenverkehr, der an das drahtlose Netzwerk gerichtet ist, über diese Schnittstelle geleitet wird. Klicken Sie auf **Ja**, wenn Sie diese Schicht-3-Schnittstelle für integriertes Routing und Bridging konfigurieren möchten.

Wenn diese Schnittstelle nicht als Teil der Bridge zur Wireless-Schnittstelle verwendet werden soll, klicken Sie auf **Nein**. Sie können sie trotzdem als reguläre Routingschnittstelle konfigurieren.

Layer 3-Ethernetkonfiguration

Cisco SDM unterstützt die Layer 3-Ethernetkonfiguration auf Routern mit installierten 3750 Switchmodulen. Sie können VLAN Konfigurationen erstellen und Router Ethernet Schnittstellen als DHCP Server bestimmen.

802.1Q-Konfiguration

Sie können ein VLAN konfigurieren, dass das 802.1Q Kapselungsprotokoll für Trunkverbindungen nicht benutzt. Definieren Sie eine VLAN ID-Nummer und überprüfen Sie das **Native VLAN**, wenn Sie nicht wollen, dass das VLAN die 802.1Q Identifizierung benutzt.

Wenn Sie die 802.1Q Identifizierung benutzen wollen, lassen Sie das VLAN Kästchen leer.

Trunk oder Routerkonfiguration

Sie können Layer 3 Ethernet Schnittstellen für 802.1Q Trunk oder für Basisrouting konfigurieren. Wenn Sie die Schnittstelle für 802.1Q Trunk konfigurieren, können Sie VLANs an der Schnittstelle und ein systemeigenes VLAN konfigurieren, das kein 802.1q Kapselungsprotokoll benutzt. Wenn Sie die Schnittstelle für das Routing konfigurieren, können Sie keine Subschnittstellen oder zusätzliche VLANs an der Schnittstelle konfigurieren.

Switchmodul konfigurieren

Wenn Sie eine Gigabit Ethernetschnittstelle für das Routing konfigurieren, können Sie dieses Fenster mit Informationen über das Switchmodul versorgen. Es ist nicht zwingend notwendig, dass Sie diese Informationen bereitstellen.

Sie können eine IP-Adresse und eine Subnetzmaske für das Switchmodul bereitstellen, ebenso erwartete Loginanmeldeinformationen, um sich in die Switchmodulschnittstelle einzuloggen.

Aktivieren Sie das Feld am Ende des Bildschirms, wenn Sie sich in das Switchmodul einloggen wollen, nachdem die Informationen in diesem Assistenten bereitgestellt wurden und die Konfiguration an den Router übergeben wurde.

Gigabit Ethernetschnittstelle konfigurieren

In diesem Fenster geben Sie eine IP-Adresse und die Informationen zur Subnetzmaske für die Gigabit Ethernetschnittstellen ein. Weitere Informationen über IP-Adressen und Subnetzmasken finden Sie LAN-Assistent: IP-Adresse und Subnetzmaske.

IP-Adresse von Physischen Schnittstellen

Geben Sie die IP-Adresse und die Subnetzmaske für die physische Gigabit Ethernetschnittstelle in diesen Feldern ein.

IP-Adresse von VLAN Subschnittstellen

Geben Sie die IP-Adresse und Subnetzmaske für die VLAN Schnittstelle ein, die Sie an der physischen Schnittstelle erstellen wollen. Diese Felder erscheinen, wenn Sie diese Schnittstelle für das Routing konfigurieren. Diese Felder erscheinen nicht, wenn Sie diese Schnittstelle für Integriertes Routing und Bridging (IRB) konfigurieren.

Übersicht

Dieses Fenster bietet eine Übersicht der Konfigurationsänderungen, die in der von Ihnen ausgewählten Schnittstelle vorgenommen wurden.

So speichern Sie diese Konfiguration in der aktiven Konfiguration des Routers und verlassen diesen Assistenten:

Klicken Sie auf **Fertig stellen**. Cisco SDM speichert die Konfigurationsänderungen in der aktiven Konfiguration des Routers. Auch wenn die Änderungen sofort wirksam werden, gehen diese verloren, wenn der Router ausgeschaltet wird.

Wenn Sie im Fenster **Benutzereinstellungen** die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktiviert haben, wird das Fenster **Senden** angezeigt. In diesem Fenster können Sie die CLI-Befehle anzeigen, die an den Router gesendet werden.

Wie gehe ich vor?

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie konfiguriere ich eine statische Route?

So konfigurieren Sie eine statische Route:

Schritt 1 Klicken Sie in der Leiste **Kategorie** auf **Routing**.

Schritt 2 Klicken Sie in der Gruppe **Statisches Routing** auf **Hinzufügen...**.

Das Dialogfeld **Statische IP-Route hinzufügen** wird angezeigt.

Schritt 3 Geben Sie im Feld **Präfix** die IP-Adresse des Zielnetzwerks der statischen Route ein.

Schritt 4 Geben Sie im Feld **Präfixmaske** die Subnetzmaske des Zielnetzwerks ein.

Schritt 5 Wenn diese statische Route als Standardroute fungieren soll, aktivieren Sie das Kontrollkästchen **Zur Standardroute machen**.

Schritt 6 Wählen Sie in der Gruppe **Weiterleitung** aus, ob eine Routerschnittstelle oder die IP-Adresse des Zielrouters als Weiterleitungsmethode für Daten identifiziert werden soll, und wählen Sie dann entweder die Weiterleitungs-Routerschnittstelle aus, oder geben Sie die IP-Adresse des Zielrouters ein.

Schritt 7 Geben Sie optional in das Feld **Distanzmetrik für diese Route** die Distanzmetrik ein, die in der Routingtabelle gespeichert werden soll.

Schritt 8 Wenn diese statische Route als permanente Route konfiguriert werden soll, d. h. dass sie nicht gelöscht wird, auch wenn die Schnittstelle deaktiviert wird oder der Router nicht mit dem nächsten Router kommunizieren kann, aktivieren Sie das Kontrollkästchen **Permanente Route**.

Schritt 9 Klicken Sie auf **OK**.

Wie zeige ich Aktivitäten in meiner LAN-Schnittstelle an?

Sie können Aktivitäten in einer LAN-Schnittstelle über den Monitor-Modus in Cisco SDM anzeigen. Der Monitor-Modus kann Statistiken über die LAN-Schnittstelle anzeigen, einschließlich der Anzahl an Paketen und Bytes, die von der Schnittstelle gesendet oder empfangen wurden, und die Anzahl an gesendeten oder empfangenen Fehlern, die aufgetreten sind. So zeigen Sie die Statistiken zu einer LAN-Schnittstelle an:

Schritt 1 Klicken Sie in der Symbolleiste auf **Monitor**.

Schritt 2 Klicken Sie im linken Bereich auf **Schnittstellenstatus**.

Schritt 3 Wählen Sie im Feld **Schnittstelle auswählen** die LAN-Schnittstelle aus, für die Sie Statistiken anzeigen möchten.

Schritt 4 Wählen Sie die Datenelemente aus, die Sie anzeigen möchten, indem Sie die dazugehörigen Kontrollkästchen aktivieren. Sie können gleichzeitig bis zu vier Statistiken anzeigen.

Schritt 5 Klicken Sie auf **Überwachung starten**, um Statistiken für alle ausgewählten Datenelemente anzuzeigen.

Daraufhin wird der Bildschirm **Details zur Schnittstelle** mit den ausgewählten Statistiken angezeigt. Der Bildschirm zeigt standardmäßig Echtzeitdaten an. Dafür wird der Router alle 10 Sekunden abgefragt. Wenn die Schnittstelle aktiv ist und Daten übertragen werden, sollten Sie jetzt sehen, dass die Anzahl der über die Schnittstelle gesendeten Pakete und Byte zunimmt.

Wie aktiviere oder deaktiviere ich eine Schnittstelle?

Sie können eine Schnittstelle deaktivieren, ohne ihre Konfiguration zu entfernen, und Sie können auch eine Schnittstelle, die Sie deaktiviert haben, wieder neu aktivieren.

Schritt 1 Klicken Sie in der Leiste **Kategorie** auf **Schnittstellen und Verbindungen**.

Schritt 2 Klicken Sie auf die Registerkarte **Schnittstelle/Verbindung bearbeiten**.

Schritt 3 Wählen Sie die Schnittstelle aus, die Sie deaktivieren oder aktivieren möchten.

Schritt 4 Wenn die Schnittstelle aktiviert ist, wird unterhalb der Schnittstellenliste die Schaltfläche **Deaktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, die Schnittstelle zu deaktivieren. Wenn die Schnittstelle derzeit deaktiviert ist, wird die Schaltfläche **Aktivieren** unter der **Schnittstellenliste** angezeigt. Klicken Sie auf diese Schaltfläche, die Schnittstelle zu deaktivieren.

Wie zeige ich die IOS-Befehle an, die ich an den Router sende?

Wenn Sie einen Assistenten zur Konfiguration einer Funktion abschließen, können Sie die Cisco IOS-Befehle anzeigen, die Sie an den Router senden, wenn Sie auf **Fertig stellen** klicken.

Schritt 1 Wählen Sie im Cisco SDM-Menü **Bearbeiten** die Option **Einstellungen** aus.

Schritt 2 Aktivieren Sie **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden**.

Schritt 3 Klicken Sie auf **OK**.

Wenn Sie das nächste Mal einen Assistenten zur Konfiguration des Routers verwenden und im Fenster **Übersicht** auf **Fertig stellen** klicken, wird das Fenster **Senden** angezeigt. In diesem Fenster können Sie die Befehle ansehen, die an die Routerkonfiguration gesendet werden. Klicken Sie auf **Senden**, wenn Sie mit dem Überprüfen der Befehle fertig sind.

Während der Bearbeitung einer Konfiguration wird das Fenster **Senden** angezeigt, wenn Sie im Dialogfeld auf **OK** klicken. In diesem Fenster können Sie die Cisco IOS-Befehle ansehen, die an den Router gesendet werden.

Wie starte ich die Wireless-Anwendung von Cisco SDM aus?

Verwenden Sie das folgende Verfahren, um die Wireless-Anwendung von Cisco SDM aus zu starten.

Schritt 1 Klicken Sie im Cisco SDM-Menü auf **Extras**, und wählen Sie die Option **Wireless-Anwendung**. Die Wireless-Anwendung wird in einem separaten Browser-Fenster gestartet.

Schritt 2 Klicken Sie im linken Rahmen auf den Titel des Konfigurationsbildschirms, mit dem Sie arbeiten möchten. Die Hilfe für den jeweiligen Bildschirm können Sie durch Anklicken des Hilfe-Symbols in der oberen rechten Ecke anzeigen. Das Symbol sieht wie ein offenes Buch mit einem Fragezeichen aus.

KAPITEL 3

802.1x-Authentifizierung

Die 802.1x-Authentifizierung erlaubt es einem Cisco IOS-Remote-Router, authentifizierte VPN-Benutzer über einen jederzeit aktiven VPN-Tunnel mit einem sicheren Netzwerk zu verbinden. Der Cisco IOS-Router authentifiziert Benutzer über einen RADIUS-Server im sicheren Netzwerk.

Die 802.1x-Authentifizierung wird auf Switch-Ports oder (geroutete) Ethernet-Ports angewandt, jedoch nicht auf beide Schnittstellentypen. Wenn die 802.1x-Authentifizierung auf einen Ethernet-Port angewandt wird, können nicht authentifizierte Benutzer außerhalb des VPN-Tunnels ins Internet geleitet werden.

Die 802.1x-Authentifizierung wird mithilfe des LAN-Assistenten auf Schnittstellen konfiguriert. Bevor Sie jedoch 802.1x auf einer Schnittstelle aktivieren können, muss AAA auf Ihrem Cisco IOS-Router aktiviert werden. Wenn Sie versuchen, den LAN-Assistenten zu verwenden, bevor AAA aktiviert ist, wird ein Fenster angezeigt, das Sie fragt, ob Sie AAA aktivieren möchten. Wenn Sie sich entscheiden, AAA zu aktivieren, dann werden die 802.1x-Konfigurationsbildschirme als Teil des LAN-Assistenten angezeigt. Wenn Sie sich entscheiden, AAA *nicht* zu aktivieren, dann werden die 802.1x-Konfigurationsbildschirme *nicht* angezeigt.

LAN-Assistent: 802.1x-Authentifizierung (Switch-Ports)

Über dieses Fenster können Sie die 802.1x-Authentifizierung auf dem Switch-Port bzw. den Switch-Ports aktivieren, die Sie im LAN-Assistenten zur Konfiguration ausgewählt haben.

802.1x-Authentifizierung aktivieren

Aktivieren Sie die Option **802.1x-Authentifizierung aktivieren**, um die 802.1x-Authentifizierung auf dem Switch-Port zu aktivieren.

Hostmodus

Wählen Sie **Einzeln** oder **Mehrere**. Der Modus **Einzeln** gewährt nur einem authentifizierten Client Zugang. Der Modus **Mehrere** gewährt einer beliebigen Anzahl von Clients Zugang, nachdem ein Client authentifiziert wurde.

Hinweis Ports auf Cisco 85x- und Cisco 87x-Routern können nur auf den Modus mit mehreren Hosts eingestellt werden. Für diese Router ist der Modus **Einzeln** deaktiviert.

Gast-VLAN

Aktivieren Sie die Option **Gast-VLAN**, um ein VLAN für Clients ohne 802.1x-Unterstützung zu aktivieren. Wenn Sie diese Option aktivieren, wählen Sie ein VLAN aus der VLAN-Dropdown-Liste aus.

Fehler bei der VLAN-Authentifizierung

Aktivieren Sie die Option **Fehler bei der VLAN-Authentifizierung**, um ein VLAN für Clients zu aktivieren, welche die 802.1x-Authorisierung nicht passieren. Wenn Sie diese Option aktivieren, wählen Sie ein VLAN aus der VLAN-Dropdown-Liste aus.

Periodische erneute Authentifizierung

Aktivieren Sie **Periodische erneute Authentifizierung**, um in regelmäßigen Abständen eine erneute Authentifizierung von 802.1x-Clients zu erzwingen. Konfigurieren Sie das Intervall lokal oder erlauben Sie dem RADIUS-Server, das Intervall festzulegen. Wenn Sie das Intervall für die erneute Authentifizierung lokal konfigurieren, geben Sie einen Wert im Bereich von 1 bis 65535 Sekunden ein. Die Standardeinstellung lautet 3600 Sekunden.

Erweiterte Optionen

Klicken Sie auf **Erweiterte Optionen**, um ein Fenster mit weiteren 802.1x-Authentifizierungsparametern zu öffnen.

Erweiterte Optionen

Über dieses Fenster können Sie die Standardwerte für eine Reihe von 802.1x-Authentifizierungsparametern ändern.

Timeout für Radius-Server

Geben Sie die Zeit in Sekunden ein, die der Cisco IOS-Router warten soll, bevor ein Timeout für die Verbindung zum RADIUS-Server erfolgt. Die Werte müssen in einem Bereich von 1 bis 65535 Sekunden liegen. Die Standardeinstellung lautet 30 Sekunden.

Timeout für Supplicant-Antwort

Geben Sie die Zeit in Sekunden ein, die der Cisco IOS-Router auf eine Antwort vom 802.1x-Client warten soll, bevor ein Timeout für die Verbindung mit dem Client erfolgt. Die Werte müssen in einem Bereich von 1 bis 65535 Sekunden liegen. Die Standardeinstellung lautet 30 Sekunden.

Timeout für erneute Versuche von Supplicant

Geben Sie die Zeit in Sekunden ein, während der der Cisco IOS-Router versuchen soll, eine Verbindung zum 802.1x-Client herzustellen, bevor ein Timeout für die Verbindung mit dem Client erfolgt. Die Werte müssen in einem Bereich von 1 bis 65535 Sekunden liegen. Die Standardeinstellung lautet 30 Sekunden.

Ruhezeitdauer

Geben Sie die Zeit in Sekunden ein, die der Cisco IOS-Router zwischen der ersten Verbindung mit einem Client und dem Senden einer Anmeldeanforderung warten soll. Die Werte müssen in einem Bereich von 1 bis 65535 Sekunden liegen. Die Standardeinstellung lautet 60 Sekunden.

Zeitdauer für Ratenlimit

Die Werte müssen in einem Bereich von 1 bis 65535 Sekunden liegen. Die Standardeinstellung lautet jedoch 0 Sekunden, wodurch **Zeitdauer für Ratenlimit** deaktiviert wird.

Maximale Versuche für erneute Authentifizierung

Geben Sie die maximale Anzahl an Versuchen für eine erneute Authentifizierung eines 802.1x-Clients durch den Cisco IOS-Router ein. Die Werte müssen in einem Bereich von 1 bis 10 liegen. Die Standardeinstellung lautet 2.

Maximale Wiederholungen

Geben Sie die maximale Anzahl an Anmeldeanforderungen ein, die an den Client gesendet werden können. Die Werte müssen in einem Bereich von 1 bis 10 liegen. Die Standardeinstellung lautet 2.

Auf Standardwerte zurücksetzen

Klicken Sie auf **Auf Standardwerte zurücksetzen**, um alle erweiterten Optionen auf die Standardwerte zurückzusetzen.

LAN-Assistent: RADIUS-Server für 802.1x-Authentifizierung

Die 802.1x-Authentifizierungsinformationen werden in einer Regeldatenbank konfiguriert und gespeichert, die auf RADIUS-Servern liegt, auf denen Cisco Secure ACS Version 3.3 läuft. Der Router muss die Anmeldeinformationen von 802.1x-Clients für gültig erklären, indem er mit dem RADIUS-Server kommuniziert. Verwenden Sie dieses Fenster, um die Informationen einzugeben, die der Router braucht, um den Kontakt mit einem oder mehreren RADIUS-Servern aufzunehmen. Auf jedem RADIUS-Server, den Sie festlegen, muss die Cisco Secure ACS Software Version 3.3 installiert und konfiguriert sein.

Hinweis Alle Ihre Cisco IOS-Routerschnittstellen mit aktivierter 802.1x-Autorisierung verwenden die in diesem Fenster eingerichteten RADIUS-Server. Wenn Sie eine neue Schnittstelle konfigurieren, wird dieser Bildschirm erneut angezeigt. Zu den RADIUS-Serverinformationen muss jedoch nichts hinzugefügt bzw. daran geändert werden.

Die RADIUS-Clientquelle auswählen

Das Konfigurieren der RADIUS-Quelle ermöglicht Ihnen, die Quellen-IP-Adresse festzulegen und in RADIUS-Paketen an den RADIUS-Server zu senden. Wenn Sie weitere Informationen über eine Schnittstelle benötigen, wählen Sie die Schnittstelle aus und klicken Sie auf die Schaltfläche **Details**.

Die Quellen-IP-Adresse in den RADIUS-Paketen, die vom Router gesendet werden, muss als die NAD-IP-Adresse in der Cisco ACS Version 3.3 oder später konfiguriert werden.

Wenn Sie **Router wählt Quelle aus** aktivieren, ist die IP-Quelladresse in den RADIUS-Paketen die Adresse der Schnittstelle, über die die RADIUS-Pakete den Router verlassen.

Wenn Sie eine Schnittstelle auswählen, ist die Quellen-IP-Adresse in den RADIUS-Paketen die Adresse der Schnittstelle, die Sie als die RADIUS-Clientquelle ausgewählt haben.

Hinweis Cisco IOS-Software gestattet die Konfiguration einer Single-RADIUS-Quellschnittstelle auf dem Router. Wenn der Router bereits eine RADIUS-Quelle konfiguriert hat und Sie eine andere Quelle auswählen, ändert sich die IP-Adresse, die in den Paketen an den RADIUS-Server steht, in die IP-Adresse der neuen Quelle und kann dann eventuell nicht mehr mit der NAD-IP-Adresse auf dem konfigurierten Cisco ACS übereinstimmen.

Details

Klicken Sie auf **Details**, um einen kurzen Einblick in die Informationen über eine Schnittstelle zu erhalten, bevor Sie diese auswählen. Auf dem Bildschirm werden die IP-Adresse und die Subnetzmaske, die der Schnittstelle zugewiesenen Zugriffsregeln und die Prüfregeln, die zugewiesenen IPSec- und QoS-Richtlinien angezeigt und angegeben, ob Easy VPN für die Schnittstelle konfiguriert wurde.

Spalten Server-IP, Timeout und Parameter

Die Spalten Server-IP, Timeout und Parameter enthalten die Informationen, die der Router für den Kontakt mit einem RADIUS-Server braucht. Wenn keine RADIUS-Server Informationen mit der ausgewählten Schnittstelle verknüpft sind, sind diese Spalten leer.

Zweck des Kontrollkästchens 802.1x

Aktivieren Sie dieses Kontrollkästchen, wenn Sie die aufgelisteten RADIUS-Server für 802.1x verwenden möchten. Der Server muss über die erforderlichen konfigurierten 802.1x-Autorisierungsinformationen verfügen, wenn 802.1x erfolgreich eingesetzt wird.

Hinzufügen, Bearbeiten und Ping

Um Informationen zu einem RADIUS-Server anzugeben, klicken Sie auf die Taste **Hinzufügen** und geben Sie die Informationen in den angezeigten Bildschirm ein. Wählen Sie eine Zeile aus und klicken Sie auf **Bearbeiten**, um die Informationen zu einem RADIUS-Server zu ändern. Wählen Sie eine Zeile aus und klicken Sie auf **Ping**, um die Verbindung zwischen Router und RADIUS-Server zu testen.

Hinweis Wenn Sie einen Ping-Test durchführen, geben Sie die IP-Adresse der RADIUS-Quellschnittstelle in das Feld **Quelle** im Dialogfeld **Ping** ein. Wenn Sie die Option **Router wählt Quelle** ausgewählt haben, müssen Sie keinen Wert in das Feld **Quelle** im Dialogfeld **Ping** eingeben.

Die Schaltflächen **Bearbeiten** und **Ping** sind deaktiviert, wenn für die ausgewählte Schnittstelle keine RADIUS-Server-Informationen zur Verfügung stehen.

802.1x-Authentifizierung (Switch-Ports) bearbeiten

In diesem Fenster können Sie 802.1x-Authentifizierungsparameter aktivieren und konfigurieren.

Wenn eine Meldung wie **802.1x kann nicht für einen im Trunk-Modus betriebenen Port konfiguriert werden** anstelle der 802.1x-Authentifizierungsparameter angezeigt wird, kann für den Switch keine 802.1x-Authentifizierung aktiviert werden.

Wenn die 802.1x-Authentifizierungsparameter angezeigt werden, aber deaktiviert sind, trifft eine der folgenden Möglichkeiten zu:

- AAA wurde nicht aktiviert.

  Um AAA zu aktivieren, rufen Sie **Konfigurieren > Zusätzliche Aufgaben > AAA** auf.

- AAA wurde aktiviert, aber es wurde keine 802.1x-Authentifizierungsrichtlinie konfiguriert.

  Um eine 802.1x-Authentifizierungsrichtlinie zu konfigurieren, rufen Sie **Konfigurieren > Zusätzliche Aufgaben > AAA > Authentifizierungsrichtlinien > 802.1x** auf.

802.1x-Authentifizierung aktivieren

Aktivieren Sie die Option **802.1x-Authentifizierung aktivieren**, um die 802.1x-Authentifizierung auf diesem Switch-Port zu aktivieren.

Hostmodus

Wählen Sie **Einzeln** oder **Mehrere**. Der Modus **Einzeln** gewährt nur einem authentifizierten Client Zugang. Der Modus **Mehrere** gewährt einer beliebigen Anzahl von Clients Zugang, nachdem ein Client authentifiziert wurde.

Hinweis Ports auf Cisco 87x-Routern können nur auf den Modus mit mehreren Hosts eingestellt werden. Für diese Router ist der Modus **Einzeln** deaktiviert.

Gast-VLAN

Aktivieren Sie die Option **Gast-VLAN**, um ein VLAN für Clients ohne 802.1x-Unterstützung zu aktivieren. Wenn Sie diese Option aktivieren, wählen Sie ein VLAN aus der VLAN-Dropdown-Liste aus.

Fehler bei der VLAN-Authentifizierung

Aktivieren Sie **Fehler bei der VLAN-Authentifizierung**, um VLAN für Clients zu aktivieren, die die 802.1x-Autorisierung nicht passieren. Wenn Sie diese Option aktivieren, wählen Sie ein VLAN aus der VLAN-Dropdown-Liste aus.

Periodische erneute Authentifizierung

Aktivieren Sie **Periodische erneute Authentifizierung**, um in regelmäßigen Abständen eine erneute Authentifizierung von 802.1x-Clients zu erzwingen. Konfigurieren Sie das Intervall lokal oder erlauben Sie dem RADIUS-Server, das Intervall festzulegen. Wenn Sie das Intervall für die erneute Authentifizierung lokal konfigurieren, geben Sie einen Wert im Bereich von 1 bis 65535 Sekunden ein. Die Standardeinstellung lautet 3600 Sekunden.

Erweiterte Optionen

Klicken Sie auf **Erweiterte Optionen**, um ein Fenster mit weiteren 802.1x-Authentifizierungsparametern zu öffnen.

LAN-Assistent: 802.1x-Authentifizierung (VLAN oder Ethernet)

Über dieses Fenster können Sie die 802.1x-Authentifizierung auf dem Ethernet-Port aktivieren, den Sie im LAN-Assistenten zur Konfiguration ausgewählt haben. Bei Cisco 87x-Routern ist dieses Fenster für die Konfiguration eines VLAN mit 802.1x-Authentifizierung verfügbar.

Hinweis Bevor Sie 802.1x auf einem VLAN konfigurieren, stellen Sie sicher, dass 802.1x *nicht* auf VLAN-Switch-Ports konfiguriert ist. Achten Sie auch darauf, dass das VLAN für DHCP konfiguriert ist.

Verwendung der 802.1x-Authentifizierung, um vertrauenswürdigen und nicht vertrauenswürdigen Verkehr auf der Schnittstelle voneinander zu trennen

Aktivieren Sie **802.1x-Authentifizierung verwenden, um vertrauenswürdigen und nicht vertrauenswürdigen Verkehr auf der Schnittstelle voneinander zu trennen**, um die 802.1x-Authentifizierung zu aktivieren.

Hinweis Der IP-Adresspool kann die IP-Adresse überschneiden, die für eine Loopback-Schnittstelle verwendet wird. Sie werden jedoch aufgefordert, eine solche Überschneidung zu bestätigen, bevor sie zugelassen wird.

Wählen Sie **Neuen Pool erstellen**, um einen neuen IP-Adresspool für die Ausgabe von IP-Adressen an nicht vertrauenswürdige Clients zu konfigurieren. Die folgenden Felder können bereits mit zuvor eingegebenen Informationen gefüllt sein, Sie können sie jedoch ändern oder ausfüllen:

Netzwerk	Geben Sie die IP-Netzwerkadresse ein, aus welcher der Pool von IP-Adressen abgeleitet wird.
Subnetzmaske	Geben Sie die Subnetzmaske ein, um das Netzwerk und die Host-Teile der IP-Adresse zu definieren, die in das Feld **Netzwerk** eingegeben wurde.

DNS-Server 1	Der DNS-Server ist ein Server, der eine Zuordnung eines bekannten Gerätenamens mit dessen IP-Adresse vornimmt. Wenn ein DNS-Server für Ihr Netzwerk konfiguriert ist, geben Sie die IP-Adresse für diesen Server ein.
DNS-Server 2	Wenn sich ein zusätzlicher DNS-Server im Netzwerk befindet, geben Sie die IP-Adresse für diesen Server ein.
WINS-Server 1	Einige Clients erfordern eventuell den Windows-Internet-Namensserver (Windows Internet Naming Service, WINS) für eine Verbindung mit Geräten im Internet. Wenn ein WINS-Server im Netzwerk konfiguriert ist, geben Sie die IP-Adresse für diesen Server ein.
WINS-Server 2	Wenn sich ein zusätzlicher WINS-Server im Netzwerk befindet, geben Sie die IP-Adresse für diesen Server ein.

Wenn Sie einen vorhandenen IP-Adresspool für die Ausgabe von IP-Adressen an nicht vertrauenswürdige Clients verwenden möchten, wählen Sie **Select an existing pool** (Vorhandenen Pool auswählen). Wählen Sie den vorhandenen Pool aus dem Dropdown-Menü. Um weitere Informationen zu einem vorhandenen Pool anzuzeigen, klicken Sie auf **Details**.

Ausnahmelisten

Klicken Sie auf **Ausnahmelisten**, um eine Ausnahmeliste zu erstellen oder zu bearbeiten. Eine Ausnahmeliste schließt bestimmte Clients von der 802.1x-Authentifizierung aus, damit sie den VPN-Tunnel verwenden können.

Cisco IP-Telefone von der 802.1x-Authentifizierung ausschließen

Aktivieren Sie die Option **Exempt Cisco IP phones from 802.1x authentication** (Cisco IP-Telefone von der 802.1x-Authentifizierung ausschließen)**,** um Cisco IP-Telefone von der 802.1x-Authentifizierung auszuschließen, sodass sie den VPN-Tunnel verwenden können.

802.1x-Ausnahmeliste

Eine Ausnahmeliste schließt bestimmte Clients von der 802.1x-Authentifizierung aus, damit sie den VPN-Tunnel verwenden können. Ausgeschlossene Clients werden über ihre MAC-Adresse identifiziert.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um ein Fenster zu öffnen, in dem Sie die MAC-Adresse eines Clients hinzufügen können. Die MAC-Adresse muss dem Format eines der folgenden Beispiele entsprechen:

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4

Cisco SDM weist falsch formatierte MAC-Adressen zurück, es sei denn, die MAC-Adressen sind kürzer als das angegebene Beispiel. Kürzere MAC-Adressen werden durch Nullen („0“) für fehlende Stellen aufgefüllt.

Hinweis Die 802.1x-Funktion von Cisco SDM unterstützt nicht die CLI-Option, die Richtlinien mit MAC-Adressen verknüpft, und nimmt in der Ausnahmeliste keine MAC-Adressen auf, denen eine Richtlinie zugeordnet ist.

Löschen

Klicken Sie auf **Löschen**, um einen ausgewählten Client aus der Ausnahmeliste zu entfernen.

802.1x-Authentifizierung auf Layer-3-Schnittstellen

In diesem Fenster können Sie die 802.1x-Authentifizierung auf einer Layer 3-Schnittstelle konfigurieren. Es führt Ethernet-Ports und VLAN-Schnittstellen auf, die über 802.1x-Authentifizierung verfügen oder für die eine solche konfiguriert werden kann, und erlaubt Ihnen, eine virtuelle Vorlagenschnittstelle für nicht vertrauenswürdige Clients auszuwählen und eine Ausnahmeliste für Clients zu erstellen, um die 802.1x-Authentifizierung zu umgehen.

Hinweis Wenn mit der CLI Richtlinien festgelegt wurden, werden sie in diesem Fenster als schreibgeschützte Information angezeigt. In diesem Fall können Sie 802.1x in diesem Fenster lediglich aktivieren oder deaktivieren.

Erforderliche Aufgaben

Wenn in diesem Fenster eine erforderliche Aufgabe angezeigt wird, muss sie abgeschlossen werden, bevor die 802.1x-Authentifizierung konfiguriert werden kann. Es wird eine Meldung angezeigt, welche die erforderliche Aufgabe erklärt, zusammen mit einem Link zu dem Fenster, in dem die Aufgabe erledigt werden kann.

802.1x-Authentifizierung global aktivieren

Aktivieren Sie die Option **802.1x-Authentifizierung global aktivieren**, um die 802.1x-Authentifizierung auf allen Ethernet-Ports zu aktivieren.

Schnittstellentabelle

Die Tabelle **Schnittstellen** enthält folgende Spalten:

Schnittstelle – Zeigt den Namen der Ethernet- oder VLAN-Schnittstelle an.

802.1x-Authentifizierung – Gibt an, ob die 802.1x-Authentifizierung für den Ethernet-Port aktiviert ist.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um ein Fenster mit editierbaren 802.1x-Authentifizierungsparametern zu öffnen. Die Parameter sind die 802.1x-Authentifizierungseinstellungen für die in der Schnittstellentabelle gewählte Schnittstelle.

Richtlinie für nicht vertrauenswürdige Benutzer

Wählen Sie aus der Dropdown-Liste eine virtuelle Vorlagenschnittstelle. Die gewählte virtuelle Vorlagenschnittstelle repräsentiert die Richtlinie, die auf Clients angewandt wird, welche die 802.1x-Authentifizierung nicht passieren.

Klicken Sie auf die Schaltfläche **Details**, um weitere Informationen zur gewählten virtuellen Vorlagenschnittstelle anzuzeigen.

Ausnahmeliste

Weitere Informationen über die Ausnahmeliste finden Sie unter 802.1x-Ausnahmeliste.

Cisco IP-Telefone von der 802.1x-Authentifizierung ausschließen

Aktivieren Sie die Option **Exempt CiscoIP phones from 802.1x authentication** (Cisco IP-Telefone von der 802.1x-Authentifizierung ausschließen), um Cisco IP-Telefone von der 802.1x-Authentifizierung auszuschließen, sodass sie den VPN-Tunnel verwenden können.

Änderungen übernehmen

Klicken Sie auf **Änderungen übernehmen**, damit die vorgenommenen Änderungen wirksam werden.

Änderungen verwerfen

Klicken Sie auf **Änderungen verwerfen,** um die vorgenommenen Änderungen zu verwerfen.

802.1x-Authentifizierung bearbeiten

Über dieses Fenster können Sie die Standardwerte für eine Reihe von 802.1x-Authentifizierungsparametern aktivieren und ändern.

802.1x-Authentifizierung aktivieren

Aktivieren Sie die Option **802.1x-Authentifizierung aktivieren**, um die 802.1x-Authentifizierung auf dem Ethernet-Port zu aktivieren.

Periodische erneute Authentifizierung

Aktivieren Sie **Periodische erneute Authentifizierung**, um in regelmäßigen Abständen eine erneute Authentifizierung von 802.1x-Clients zu erzwingen. Konfigurieren Sie das Intervall lokal oder erlauben Sie dem RADIUS-Server, das Intervall festzulegen. Wenn Sie das Intervall für die erneute Authentifizierung lokal konfigurieren, geben Sie einen Wert im Bereich von 1 bis 65535 Sekunden ein. Die Standardeinstellung lautet 3600 Sekunden.

Erweiterte Optionen

Klicken Sie auf Erweiterte Optionen, um eine Beschreibung der Felder im Feld **Erweiterte Optionen** zu erhalten.

Wie gehe ich vor?

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie lässt sich die 802.1x-Authentifizierung auf mehreren Ethernet-Ports konfigurieren?

Nachdem Sie die 802.1x-Authentifizierung auf einer Schnittstelle konfiguriert haben, zeigt der LAN-Assistent keine 802.1x-Optionen für Ethernet-Ports mehr an, da Cisco SDM die 802.1x-Konfiguration global verwendet.

Hinweis Für die Konfiguration von Switches zeigt der LAN-Assistent weiterhin die 802.1x-Optionen an.

Wenn Sie die 802.1x-Authentifizierungsinformationen auf einem Ethernet-Port bearbeiten möchten, wählen Sie **Konfigurieren > Zusätzliche Aufgaben > 802.1x**.

KAPITEL 4

Verbindungserstellungsassistenten

Mit den Verbindungserstellungsassistenten können Sie LAN- und WAN-Verbindungen für alle Cisco SDM-unterstützten Schnittstellen konfigurieren.

Verbindung erstellen

In diesem Fenster können Sie neue LAN- und WAN-Verbindungen erstellen.

Hinweis Sie können Cisco SDM nicht zur Erstellung von WAN-Verbindungen für Router der Cisco 7000 Serie verwenden.

Erstellen einer neuen WAN-Verbindung

Wählen Sie einen Verbindungstyp aus, um sie an den physischen Schnittstellen, die auf Ihrem Router zur Verfügung stehen, zu konfigurieren. Nur nicht konfigurierte Schnittstellen stehen zur Verfügung. Wenn Sie auf die Taste wegen eines Verbindungstyps klicken, erscheint ein Beispieldiagramm, das diesen Verbindungstyp illustriert. Wenn alle Schnittstellen konfiguriert wurden, wird dieses Fenster nicht angezeigt.

Wenn der Router über Asynchronous Transfer Mode (ATM)- oder serielle Schnittstellen verfügt, können mehrere Verbindungen von einer einzelnen Schnittstelle konfiguriert werden, da Cisco Router and Security Device Manager II (Cisco SDM) für jede Schnittstelle dieses Typs Unterschnittstellen konfiguriert.

Das Optionsfeld **Andere (von Cisco SDM nicht unterstützt)** wird angezeigt, wenn eine nicht unterstützte logische oder physikalische Schnittstelle vorhanden ist, oder eine unterstützte Schnittstelle vorhanden ist, deren Konfiguration nicht unterstützt wird. Wenn Sie auf das Optionsfeld **Andere (Nicht von Cisco SDM unterstützt)** klicken, wird die Option **Neue Verbindung erstellen** deaktiviert.

Wenn der Router über Wireless-Schnittstellen verfügt, jedoch kein Optionsfeld **Wireless** angezeigt wird, sind Sie nicht als Cisco SDM-Administrator angemeldet. Wenn Sie die Wireless-Anwendung verwenden müssen, wählen Sie im Cisco SDM-Menü **Extras** die Option **Wireless-Anwendung**.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Lernen, wie Konfigurationen durchgeführt werden, bei denen dieser Assistent keine Unterstützung bietet.	Lesen Sie eine der folgenden Vorgehensweisen: • Wie zeige ich die IOS-Befehle an, die ich an den Router sende? • Wie konfiguriere ich eine nicht unterstützte WAN-Schnittstelle? • Wie aktiviere oder deaktiviere ich eine Schnittstelle? • Wie zeige ich Aktivitäten auf meiner WAN-Schnittstelle an? • Wie konfiguriere ich NAT auf einer WAN-Schnittstelle? • Wie konfiguriere ich eine statische Route? • Wie konfiguriere ich ein Protokoll für dynamisches Routing? • Wie konfiguriere ich Dial-on-Demand Routing für meine ISDN- oder asynchrone Schnittstelle?
Konfigurieren einer Schnittstelle, die nicht von Cisco SDM unterstützt wird.	Schauen Sie im Softwarekonfigurationshandbuch für den Router nach, um Informationen zur Verwendung der CLI für die Konfiguration der Schnittstelle zu bekommen.

Willkommensfenster für den WAN-Schnittstellenassistenten

In diesem Fenster werden die Verbindungstypen aufgeführt, die Sie mit Cisco SDM für diese Schnittstelle konfigurieren können. Wenn Sie für diese Schnittstelle einen anderen Verbindungstyp konfigurieren müssen, können Sie dazu die CLI verwenden.

Willkommensfenster für den ISDN-Assistenten

PPP ist der einzige Codierungstyp, der von Cisco SDM über ein ISDN BRI unterstützt wird.

Willkommensfenster für den Analogmodem-Assistenten

PPP ist der einzige Codierungstyp, der von Cisco SDM über eine analoge Modemverbindung unterstützt wird.

Willkommensfenster für den Assistenten für die zusätzliche Sicherung

Die Option zur Konfiguration des zusätzlichen Ports als Wählverbindung erscheint nur für die Cisco 831- und 837-Router.

Das Optionsfeld für zusätzliche Dial-Backup-Verbindungen wird deaktiviert, wenn eine der folgenden Bedingungen existiert:

- Es existiert mehr als eine Standardroute.
- Eine Standardroute existiert und ist mit einer anderen als der primären WAN Schnittstelle konfiguriert.

Die Option für zusätzliche Dial-Backup-Verbindungen wird nicht angezeigt, wenn eine der folgenden Bedingungen existiert:

- Der Router verwendet kein Cisco IOS-Abbild, das die Funktion für zusätzliche Dial-Backups unterstützt.
- Eine primäre WAN-Schnittstelle ist nicht konfiguriert.
- Die asynchrone Schnittstelle ist bereits konfiguriert.
- Die asynchrone Schnittstelle von Cisco SDM ist nicht konfiguriert, da sich in der vorhandenen Konfiguration nicht unterstützte Cisco IOS-Befehle befinden.

Schnittstelle auswählen

Dieses Fenster wird angezeigt, wenn mehrere Schnittstellen des im Fenster **Verbindung erstellen** ausgewählten Typs vorhanden sind. Wählen Sie die Schnittstelle aus, die Sie für diese Verbindung verwenden möchten.

Wenn Sie eine Ethernet-Schnittstelle konfigurieren, fügt Cisco SDM den Beschreibungstext $ETH-WAN$ in die Konfigurationsdatei ein, um die Schnittstelle zukünftig als WAN-Schnittstelle zu erkennen.

Kapselung: PPPoE

In diesem Fenster können Sie die PPPoE (Point-to-Point-Protocol over Ethernet)-Kapselung aktivieren. Dies ist erforderlich, wenn Ihr Service-Provider oder Netzwerkadministrator die Kommunikation von Remote-Routern nur über PPPoE zulässt.

PPPoE ist ein Protokoll, das von vielen ADSL (Asymmetric Digital Subscriber Line)-Service-Providern verwendet wird. Fragen Sie Ihren Service-Provider, ob PPPoE über Ihre Verbindung verwendet wird.

Wenn Sie die PPPoE-Kapselung wählen, fügt Cisco SDM automatisch eine Dialer-Schnittstelle zur Konfiguration hinzu. Dies wird im Übersichtsfenster angezeigt.

Aktivieren der PPPoE-Kapselung

Wenn es bei Ihrem Service-Provider erforderlich ist, dass der Router PPPoE verwendet, aktivieren Sie dieses Kontrollkästchen, um die PPPoE-Kapselung zu aktivieren. Deaktivieren Sie dieses Kontrollkästchen, wenn Ihr Service-Provider PPPoE nicht verwendet. Dieses Kontrollkästchen ist nicht verfügbar, wenn auf Ihrem Router eine Cisco IOS-Version ausgeführt wird, die die PPPoE-Kapselung nicht unterstützt.

IP-Adresse: ATM oder Ethernet mit PPPoE/PPPoA

Wählen Sie die Methode aus, die von der WAN-Schnittstelle zur Ermittlung einer IP-Adresse verwendet werden soll.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein.

Dynamisch (DHCP-Client)

Wenn Sie **Dynamisch** wählen, fordert der Router bei einem Remote-DHCP-Server eine IP-Adresse an. Geben Sie den Namen des DHCP-Servers ein, der die Adressen zuweisen soll.

Keine IP-Nummerierung

Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie anschließend die Schnittstelle aus, welche die IP-Adresse verwenden soll, die Sie gerade konfigurieren.

Easy IP (IP ausgehandelt)

Wählen Sie die Option **Easy IP (IP ausgehandelt)**, wenn der Router über die PPP/IPCP-Adressenaushandlung eine IP-Adresse erhält.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

IP-Adresse: ATM mit RFC 1483-Routing

Wählen Sie die Methode aus, die von der WAN-Schnittstelle zur Ermittlung einer IP-Adresse verwendet werden soll.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamisch (DHCP-Client)

Wenn Sie die Option **Dynamisch** wählen, least der Router eine IP-Adresse von einem Remote-DHCP-Server. Geben Sie den Namen des DHCP-Servers ein, der die Adressen zuweisen soll.

Keine IP-Nummerierung

Klicken Sie auf **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie anschließend die Schnittstelle aus, welche die IP-Adresse verwenden soll, die Sie gerade konfigurieren.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

IP-Adresse: Ethernet ohne PPPoE

Wählen Sie die Methode aus, die von der WAN-Schnittstelle zur Ermittlung einer IP-Adresse verwendet werden soll.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamisch (DHCP-Client)

Wenn Sie die Option **Dynamisch** wählen, least der Router eine IP-Adresse von einem Remote-DHCP-Server. Geben Sie den Namen des DHCP-Servers ein, der die Adressen zuweisen soll.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

IP-Adresse: Seriell mit Point-to-Point-Protokoll

Wählen Sie die Methode aus, die das Point-to-Point-Protokoll zur Ermittlung einer IP-Adresse verwenden soll.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Keine IP-Nummerierung

Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie anschließend die Schnittstelle aus, welche die IP-Adresse verwenden soll, die Sie gerade konfigurieren.

Easy IP (IP ausgehandelt)

Wählen Sie die Option **Easy IP (IP ausgehandelt)**, wenn der Router über die PPP/IPCP-Adressenaushandlung eine IP-Adresse erhält.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

IP-Adresse: Seriell mit HDLC oder Frame Relay

Wählen Sie die Methode aus, die von der WAN-Schnittstelle zur Ermittlung einer IP-Adresse verwendet werden soll. Wenn die Frame Relay-Kapselung verwendet wird, erstellt Cisco SDM eine Unterschnittstelle, und die IP-Adresse wird dieser Unterschnittstelle zugewiesen, die Cisco SDM erstellt.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Keine IP-Nummerierung

Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie anschließend die Schnittstelle aus, welche die IP-Adresse verwenden soll, die Sie gerade konfigurieren.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

IP-Adresse: ISDN BRI oder Analogmodem

Wählen Sie die Methode aus, welche die ISDN BRI- oder Analogmodem-Schnittstelle zur Ermittlung einer IP-Adresse verwenden soll.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Keine IP-Nummerierung

Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie anschließend die Schnittstelle mit der IP-Adresse aus, welche die Schnittstelle, die Sie gerade konfigurieren, verwenden soll.

Easy IP (IP ausgehandelt)

Wählen Sie die Option **IP ausgehandelt**, wenn die Schnittstelle bei jeder Verbindungsherstellung eine IP-Adresse über PPP/IPCP-Adressenaushandlung von Ihrem Internet-Service-Provider erhält.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren möchten, sobald sich die WAN Schnittstellen-IP-Adressen ändern. Klicken Sie auf die Schaltfläche **Dynamisches DNS**, um das dynamische DNS zu konfigurieren.

Authentifizierung

Diese Seite wird angezeigt, wenn Sie folgendes aktivieren oder konfigurieren:

- PPP für eine serielle Verbindung
- PPPoE- oder PPPoA-Kapselung für eine ATM Verbindung
- PPPoE- oder PPPoA-Kapselung für eine Ethernet Verbindung
- Eine ISDN BRI oder eine analoge Modemverbindung

Ihr Service-Provider oder Netzwerkadministrator kann ein CHAP-Kennwort (CHAP = Challenge Handshake Authentication Protocol) oder ein PAP-Kennwort (PAP = Password Authentication Protocol) verwenden, um die Verbindung zwischen den Geräten zu sichern. Dieses Kennwort sichert sowohl den eingehenden als auch den ausgehenden Zugriff.

Authentifizierungstyp

Aktivieren Sie das Kontrollkästchen für den Authentifizierungstypen, den Ihr Service-Provider verwendet. Wenn Sie nicht wissen, welchen Typ Ihr Service-Provider verwendet, können Sie beide Kästchen aktivieren: der Router probiert dann beide Authentifizierungstypen aus und hat bei einem Versuch Erfolg.

Die CHAP-Authentifizierung ist sicherer als die PAP-Authentifizierung.

Benutzername

Dieser Benutzername wird für die CHAP- oder PAP-Authentifizierung verwendet.

Kennwort

Geben Sie das Kennwort auf exakt die gleiche Weise ein, wie Sie es von Ihrem Service-Provider erhalten haben. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. So ist das Kennwort „cisco“ zum Beispiel nicht identisch mit dem Kennwort „Cisco“.

Kennwort bestätigen

Geben Sie hier dasselbe Kennwort wie in das vorhergehende Feld ein.

Switch-Typ und SPIDs

Für ISDN BRI-Verbindungen ist die Identifizierung des ISDN-Switch-Typs und in einigen Fällen die Identifizierung der B-Kanäle mittels Serviceprofil ID (SPID)-Nummern erforderlich. Die entsprechenden Informationen erhalten Sie von Ihrem Service-Provider.

ISDN-Switch-Typ

Wählen Sie den ISDN-Switch-Typ. Wenden Sie sich an Ihren ISDN-Service-Provider, um den Switch-Typ für Ihre Verbindung zu erfahren.

Cisco SDM unterstützt die folgenden BRI-Switch-Typen:

- Für Nordamerika:
  - basic-5ess – Lucent (AT&T) Basic Rate 5ESS-Switch
  - basic-dms100 – Northern Telecom DMS-100 Basic Rate-Switch
  - basic-ni – Nationale ISDN-Switches
- Für Australien, Europa und Großbritannien:
  - basic-1tr6 – Deutscher 1TR6 ISDN-Switch
  - basic-net3 – NET3 ISDN BRI für die Switch Typen Norwegen NET3, Australien NET3 und Neuseeland NET3; ETSI-entsprechende Switch-Typen für Euro-ISDN E-DSS1-Signalsysteme
  - vn3 – Französische ISDN BRI-Switches
- Für Japan:
  - ntt – Japanische NTT ISDN-Switches
- Für Voice oder PBX-Systeme:
  - basic-qsig – PINX (PBX)-Switches mit QSIG-Signalen mittels Q.931

Ich verfüge über SPIDs

Aktivieren Sie dieses Kontrollkästchen, wenn Ihr Service-Provider SPIDs benötigt.

Einige Service-Provider verwenden SPIDs, um die Dienste, die Sie abonniert haben, mit einem ISDN-Gerät zu definieren, das auf den ISDN-Service-Provider zugreift. Der Service-Provider weist beim erstmaligen Abonnieren des Dienstes das ISDN-Gerät einem oder mehreren SPIDs zu. Wenn Sie einen Service-Provider verwenden, der SPIDs benötigt, kann Ihr ISDN-Gerät erst dann Anrufe tätigen oder empfangen, wenn es beim Zugriff des Geräts auf den Switch eine gültige, zugewiesene SPID an den Service-Provider übermittelt, um die Verbindung zu initialisieren.

Momenten sind SPIDs nur für Switch-Typen DMS-100 und NI erforderlich. Der Switch-Typ AT&T 5ESS kann eine SPID unterstützen, es wird jedoch empfohlen, den ISDN-Dienst ohne SPIDs einzurichten. SPIDs sind außerdem nur bei der ISDN-Schnittstelle für den lokalen Zugriff von Bedeutung. Remote-Router empfangen die SPID niemals.

Eine SPID ist meist eine 7-stellige Telefonnummer mit einigen optionalen Nummern. Service-Provider verwenden jedoch möglicherweise unterschiedliche Nummerierungschemata. Dem Switch-Typ DMS-100 sind zwei SPIDs zugeordnet, eine für jeden B-Kanal.

SPID1

Geben Sie die SPID für den ersten BRI B-Kanal ein, die Sie von Ihrem Internet-Service-Provider erhalten haben.

SPID2

Geben Sie die SPID für den zweiten BRI B-Kanal ein, die Sie von Ihrem Internet-Service-Provider erhalten haben.

Wähl-Zeichenfolge

Geben Sie die Telefonnummer des Remote-Endpunkts der ISDN BRI- oder Analogmodem-Verbindung ein. Hierbei handelt es sich um die Telefonnummer, die eine ISDN BRI- oder Analogmodem-Verbindung wählt, wenn eine Verbindung hergestellt werden soll. Sie erhalten die Wähl-Zeichenfolge von Ihrem Service-Provider.

Sicherungskonfiguration

ISDN BRI- und Analogmodem-Schnittstellen können so konfiguriert werden, dass sie als Sicherungsschnittstellen für andere, primäre Schnittstellen fungieren. In diesem Fall wird eine ISDN- oder Analogmodem-Verbindung nur dann hergestellt, wenn die primäre Schnittstelle ausfällt. Wenn die primäre Schnittstelle und Verbindung ausfällt, startet die ISDN- oder Analogmodem-Schnittstelle sofort einen Wählvorgang und versucht, eine Verbindung herzustellen, damit die Netzwerkdienste nicht verloren gehen.

Wählen Sie aus, ob diese ISDN BRI- oder Analogmodem-Verbindung als Sicherungsverbindung eingesetzt werden soll.

Beachten Sie, dass folgende Voraussetzungen erfüllt sein müssen:

- Die primäre Schnittstelle muss für site-to-site-VPN konfiguriert sein.
- Das Cisco IOS-Image auf Ihrem Router muss die Funktion SAA ICMP Echo Enhancement unterstützen.

Sicherungskonfiguration: Primäre Schnittstelle und Primäre Next Hop-IP-Adresse

Damit die ISDN BRI- oder Analogmodem-Verbindung als Sicherungsverbindung fungieren kann, muss diese Verbindung mit einer anderen Schnittstelle auf dem Router verknüpft sein, der die primäre Verbindung herstellt. Die ISDN BRI- oder Analogmodem-Verbindung wird nur dann hergestellt, wenn die Verbindung auf der primären Schnittstelle ausfällt.

Primäre Schnittstelle

Wählen Sie die Router-Schnittstelle, welche die primäre Verbindung halten soll.

Primäre Next Hop-IP-Adresse

Dieses Feld ist optional. Geben Sie die IP-Adresse ein, zu der die primäre Schnittstelle eine Verbindung herstellt, wenn sie aktiv ist. Diese IP-Adresse wird *Next Hop IP-Adresse* genannt.

Next Hop-Sicherungs-IP-Adresse

Dieses Feld ist optional. Geben Sie die IP-Adresse ein, zu der die Sicherungsschnittstelle eine Verbindung herstellt, wenn sie aktiv ist. Diese IP-Adresse wird *Next Hop IP-Adresse* genannt.

Sicherungskonfiguration: Hostname oder IP-Adresse, der bzw. die verfolgt werden soll

Auf diesem Bildschirm können Sie einen bestimmten Host identifizieren, zu dem eine Verbindung aufrechterhalten werden muss. Der Router verfolgt die Konnektivität zu diesem Host und startet eine Sicherungsverbindung über die ISDN BRI- oder Analogmodem-Schnittstelle, wenn er feststellt, dass die Konnektivität über die primäre Schnittstelle verloren gegangen ist.

IP-Adresse, die verfolgt werden soll

Geben Sie die IP-Adresse oder den Hostnamen des Zielhosts ein, deren/dessen Verbindung verfolgt werden soll. Geben Sie als zu verfolgenden Standort ein Ziel ein, das nicht so häufig kontaktiert wird.

Erweiterte Optionen

Basierend auf der Konfiguration des Routers stehen zwei erweiterte Optionen zur Verfügung: Statische Standardroute und Port Address Translation (PAT). Wenn die Option **Statische Standardroute** nicht im Fenster angezeigt wird, wurde auf dem Router bereits eine statische Route konfiguriert. Wenn die Option **PAT** nicht im Fenster angezeigt wird, wurde PAT auf dem Router bereits konfiguriert.

Statische Standardroute

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine statische Route zu der äußeren Schnittstelle konfigurieren möchten, an die der ausgehende Datenverkehr geleitet wird. Wenn auf dem Router bereits eine statische Route konfiguriert wurde, erscheint dieses Kontrollkästchen nicht.

Next Hop-Adresse

Wenn Ihr Service-Provider Ihnen eine Next Hop-IP-Adresse zur Verwendung gegeben hat, geben Sie die IP-Adresse in dieses Feld ein. Wenn Sie dieses Feld leer lassen, verwendet Cisco SDM die WAN-Schnittstelle, die Sie konfigurieren, als Next-Hop-Schnittstelle.

Port Address Translation

Wenn Geräte im LAN über private Adressen verfügen, können Sie zulassen, dass sie eine einzelne öffentliche IP-Adresse gemeinsam nutzen. Durch die Verwendung von PAT können Sie sicherstellen, dass der Datenverkehr an das richtige Ziel gelangt. PAT repräsentiert Hosts mit einer einzelnen IP-Adresse in einem LAN und verwendet unterschiedliche Portnummern, um die Hosts voneinander zu unterscheiden. Wenn PAT bereits auf einer Schnittstelle konfiguriert wurde, wird die Option **PAT** nicht angezeigt.

Zu übersetzende innere Schnittstelle

Wählen Sie die innere Schnittstelle aus, die mit dem Netzwerk verbunden ist, dessen Host-IP-Adressen übersetzt werden sollen.

Kapselung

Wählen Sie in diesem Fenster den Kapselungstyp aus, den der WAN-Link verwenden soll. Fragen Sie Ihren Service-Provider oder Netzwerkadministrator, welcher Kapselungstyp für diesen Link verwendet wird. Die verfügbaren Kapselungstypen werden durch den Schnittstellentyp festgelegt.

Automatische Erkennung

Klicken Sie auf **Automatische Erkennung**, wenn Cisco SDM den Kapselungstyp ermitteln soll. Wenn Cisco SDM Erfolg hat, werden der Kapselungstyp und weitere erkannte Konfigurationsparameter automatisch bereitgestellt.

Hinweis Cisco SDM unterstützt die automatische Erkennung auf SB106-, SB107-, Cisco 836- und Cisco 837-Routern. Wenn Sie jedoch einen Cisco 837-Router konfigurieren und auf diesem Router eine Cisco IOS-Version 12.3(8)T oder 12.3(8.3)T ausgeführt wird, wird die automatische Erkennung nicht unterstützt.

Verfügbare Kapselungen

In der nachfolgenden Tabelle werden die Kapselungen aufgeführt, die verfügbar sind, wenn Sie über eine ADSL-, G.SHDSL- oder ADSL über ISDN-Schnittstelle verfügen.

Kapselung	Beschreibung
PPPoE	Bietet die Point-to-Point-Protocol over Ethernet (PPPoE)-Kapselung. Diese Option ist verfügbar, wenn Sie eine Ethernet-Schnittstelle oder eine ATM-Schnittstelle ausgewählt haben. Wenn Sie PPPoE über eine ATM-Schnittstelle konfigurieren, werden eine ATM-Unterschnittstelle und eine Dialer-Schnittstelle erstellt. Das Optionsfeld **PPPoE** wird deaktiviert, wenn auf Ihrem Router eine Cisco IOS-Version ausgeführt wird, welche die PPPoE-Kapselung nicht unterstützt.

Kapselung	Beschreibung
PPPoA	Point-to-Point Protocol over ATM. Diese Option ist verfügbar, wenn Sie eine ATM-Schnittstelle ausgewählt haben. Wenn Sie PPPoA über eine ATM-Schnittstelle konfigurieren, werden eine ATM-Unterschnittstelle und eine Dialer-Schnittstelle erstellt. Das Optionsfeld PPPoA wird deaktiviert, wenn auf Ihrem Router eine Cisco IOS-Version ausgeführt wird, welche die PPPoA-Kapselung nicht unterstützt.
RFC 1483-Routing mit AAL5-SNAP	Diese Option ist verfügbar, wenn Sie eine ATM-Schnittstelle ausgewählt haben. Wenn Sie eine RFC 1483-Verbindung konfigurieren, wird eine ATM-Subschnittstelle erstellt. Diese Unterschnittstelle wird im Übersichtsfenster angezeigt.
RFC1483-Routing mit AAL5-MUX	Diese Option ist verfügbar, wenn Sie eine ATM-Schnittstelle ausgewählt haben. Wenn Sie eine RFC 1483-Verbindung konfigurieren, wird eine ATM-Subschnittstelle erstellt. Diese Unterschnittstelle wird im Übersichtsfenster angezeigt.

In der nachfolgenden Tabelle werden die Kapselungen aufgeführt, die verfügbar sind, wenn Sie über eine serielle Schnittstelle verfügen.

Kapselung	Beschreibung
Frame Relay	Bietet Frame Relay-Kapselung. Diese Option ist verfügbar, wenn Sie eine serielle Schnittstelle ausgewählt haben. Wenn Sie eine Frame Relay-Verbindung konfigurieren, wird eine serielle Subschnittstelle erstellt. Diese Unterschnittstelle wird im Übersichtsfenster angezeigt. **Hinweis** Wenn eine serielle Frame Relay-Verbindung zu einer Schnittstelle hinzugefügt wurde, wird in diesem Fenster nur die Frame Relay-Kapselung aktiviert, wenn zu einem späteren Zeitpunkt weitere serielle Verbindungen auf derselben Schnittstelle konfiguriert werden.
Point-to-Point-Protokoll	Bietet PPP-Kapselung. Diese Option ist verfügbar, wenn Sie eine serielle Schnittstelle ausgewählt haben.
High-Level Data Link Control	Bietet HDLC-Kapselung. Diese Option ist verfügbar, wenn Sie eine serielle Schnittstelle ausgewählt haben.

PVC

ATM-Routing verwendet ein zweischichtiges hierarchisches Schema, virtuelle Pfade und virtuelle Kanäle, bezeichnet durch den Virtual Path Identifier (VPI) bzw. den Virtual Channel Identifier (VCI). Ein bestimmter virtueller Pfad kann verschiedene virtuelle Kanäle enthalten, die den einzelnen Verbindungen entsprechen. Wenn auf Grundlage der VPI ein Switching durchgeführt wird, werden alle Zellen in diesem bestimmten virtuellen Pfad unabhängig von der VCI umgeschaltet. Ein ATM-Switch kann entsprechend VCI, VPI, oder sowohl VCI als auch VPI leiten.

VPI

Geben Sie den VPI-Wert ein, den Sie von Ihrem Service-Provider oder Systemadministrator erhalten haben. Der Virtual Path Identifier (VPI) wird beim ATM-Switching und -Routing zur Identifizierung des Pfads verwendet, der für verschiedene Verbindungen verwendet wird. Geben Sie den VPI-Wert ein, den Sie von Ihrem Service-Provider erhalten haben.

VCI

Geben Sie den VCI-Wert ein, den Sie von Ihrem Service-Provider oder Systemadministrator erhalten haben. Der Virtual Circuit Identifier (VCI) wird beim ATM-Switching und -Routing zur Identifizierung einer bestimmten Verbindung innerhalb eines Pfads verwendet, der gemeinsam mit anderen Verbindungen verwendet werden kann. Geben Sie den VCI-Wert ein, den Sie von Ihrem Service-Provider erhalten haben.

Cisco IOS-Standardwerte

Bei den in der folgenden Tabelle angezeigten Werten handelt es sich um Cisco IOS-Standards. Cisco SDM überschreibt diese Werte nicht, wenn sie sich während einer früheren Konfiguration geändert haben. Wenn Ihr Router jedoch zuvor nicht konfiguriert wurde, werden diese Werte verwendet:

Verbindungstyp	Parameter	Wert
ADSL	• Betriebsmodus	• Auto
G.SHDSL	• Betriebsmodus • Übertragungsrate der Leitung • Gerätetyp	• Annex A (Annex A (Vereinigte Staaten) • Auto • CPE
ADSL over ISDN	• Betriebsmodus	• Auto

Konfigurieren von LMI und DLCI

Wenn Sie eine Verbindung mit Frame Relay-Kapselung konfigurieren, müssen Sie das Protokoll angeben, das zur Überwachung der Verbindung verwendet wurde, Local Management Identifier (LMI) genannt, und eine eindeutige Kennung für diese bestimmte Verbindung angeben, Data Link Connection Identifier (DLCI) genannt.

LMI-Typ

Fragen Sie Ihren Service-Provider, welchen der folgenden LMI-Typen Sie verwenden sollten.

LMI-Typ	Beschreibung
ANSI	Annex D, definiert vom American National Standards Institute (ANSI) Standard T1.617.
Cisco	LMI Typ, der von Cisco Systems zusammen mit drei anderen Unternehmen definiert wurde.
ITU-T Q.933	ITU-T Q.933 Annex A.
Autosense	Die Standardeinstellung. Mit dieser Einstellung kann der Router ermitteln, welcher LMI-Typ verwendet wird, indem er mit dem Switch kommuniziert und diesen Typ dann verwendet. Wenn die Funktion **autosense** fehlschlägt, verwendet der Router den Cisco LMI-Typ.

DLCI

Geben Sie den DCLI in dieses Feld ein. Diese Nummer muss bei allen DLCIs, die auf dieser Schnittstelle verwendet werden, eindeutig sein.

IETF Frame Relay-Kapselung verwenden

Internet Engineering Task Force (IETF)-Kapselung. Diese Option wird bei der Verbindung zu Routern von Drittherstellern verwendet. Aktivieren Sie dieses Kontrollkästchen, wenn Sie auf dieser Schnittstelle eine Verbindung zu dem Router eines Drittanbieters herstellen.

Takteinstellungen konfigurieren

Das Fenster **Takteinstellungen** ist verfügbar, wenn Sie einen T1- oder E1-Link konfigurieren. Auf dieser Seite werden die Standard-Takteinstellungen für Frame Relay angezeigt. Diese Einstellungen sollten Sie nur dann ändern, wenn Sie andere Anforderungen haben.

Taktquelle

Die Option **internal** gibt an, dass der Takt intern generiert wird. Die Option **line** gibt an, dass die Taktquelle vom Netzwerk abgerufen wird. Der Takt synchronisiert die Datenübertragung. Die Standardeinstellung ist **line**.

T1-Framing

In diesem Feld wird der T1- oder E1-Link für den Betrieb mit D4 Super Frame (sf) oder Extended Superframe (esf) konfiguriert. Die Standardeinstellung ist **esf**.

Leitungscode

In diesem Feld wird der Router für den Betrieb mit Binary 8-Zeros Substitution (B8ZS)- oder Alternate Mark Inversion (AMI) T1-Leitungen konfiguriert. Mit der Einstellung B8ZS wird die Dichte in einer T1 oder E1-Leitung durch Ersetzen von beabsichtigten Bipolar Violations an den Bitpositionen 4 und 7 über eine Sequenz von acht Null-Bits sichergestellt. Wenn der Router mit der AMI-Einstellung konfiguriert ist, müssen Sie die Dichte in T1-Leitung mit der invertierten Datencodierungseinstellung sicherstellen. Die Standardeinstellung ist **b8zs**.

Datencodierung

Klicken Sie auf **inverted**, wenn Sie wissen, dass die Benutzerdaten auf diesem Link invertiert werden, oder wenn das Feld Leitungscode auf AMI eingestellt ist. Lassen Sie diese Option andernfalls auf den Standardwert **normal** eingestellt. Die Dateninvertierung wird mit bitorientierten Protokollen wie HDLC, PPP und Link Access Procedure, Balanced (LAPB) verwendet, um auf einer T1-Leitung mit AMI-Codierung die Dichte sicherzustellen. Diese bitorientierten Protokolle fügen nach je fünf *Einer*-Bits im Datenstrom eine *Null* ein. Auf diese Weise wird sichergestellt, dass mindestens alle acht Bit eine Null vorhanden ist. Wenn der Datenstrom invertiert wird, wird sichergestellt, dass mindestens eines von acht Bit eine Eins ist.

Cisco SDM stellt die Datencodierung auf **inverted** ein, wenn der Leitungscode AMI ist und keine Zeitrahmen für 56 KBit/s konfiguriert sind. Wenn Sie keine invertierte Datencodierung mit dem AMI-Leitungscode nutzen möchten, müssen Sie mit der CLI alle Zeitrahmen auf 56 kbps einstellen.

Facilities Data Link (FDL)

In diesem Feld wird das Verhalten des Routers auf dem Facilities Data Link (FDL) des Extended Superframe konfiguriert. Wenn der Router mit **att** konfiguriert ist, wird AT&T TR 54016 implementiert. Wenn der Router mit **ansi** konfiguriert ist, wird ANSI T1.403 implementiert. Wenn Sie beides auswählen, implementiert der Router sowohl **att** als auch **ansi**. Wenn Sie keine Option auswählen, ignoriert der Router die FDL. Die Standardeinstellung ist **keine**. Wenn das T1- oder E1-Framing auf **sf** gesetzt ist, stellt Cisco SDM für FDL die Option **keine** ein und aktiviert den Schreibschutz für das Feld.

Line Build Out (LBO)

Dieses Feld wird zum Konfigurieren des Line Build Out (LBO) für den T1 Link verwendet. Das LBO verringert die Übertragungsstärke des Signals um -7,5 oder -15 Dezibel. Es wird vermutlich auf aktuellen T1 oder E1-Leitungen nicht benötigt. Die Standardeinstellung ist **keine**.

Remote-Loopback-Anforderungen

In diesem Feld wird festgelegt, ob der Router in den Modus Loopback eintritt, wenn ein Loopback-Code in der Leitung empfangen wird. Wenn Sie die Option **full** wählen, verarbeitet der Router vollständige Loopbacks. Wenn Sie dagegen die Option **payload-v54** wählen, wählt der Router Payload-Loopbacks.

Generierung/Ermittlung von Remote-Alarmen aktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass der T1-Link des Routers Remote-Alarme (gelbe Alarme) generiert und Remote-Alarme erkennt, die von dem Peer am anderen Ende des Link gesendet wurden.

Der Remote-Alarm wird von einem Router übermittelt, wenn er einen Alarmzustand entdeckt: entweder einen roten Alarm (Signalverlust) oder einen blauen Alarm (Unframed 1). Die CSU/DSU (Receiving Channel Service Unit/Data Service Unit) erkennt dann, dass in der Leitung ein Fehler aufgetreten ist.

Diese Einstellung sollte nur verwendet werden, wenn T1-Framing auf **esf** gesetzt ist.

Verbindung löschen

Sie können eine im Fenster **Schnittstelle/Verbindung bearbeiten** angezeigte WAN-Verbindung löschen. Dieses Fenster wird angezeigt, wenn Sie eine Schnittstellenkonfiguration löschen und die Verbindung, die Sie löschen möchten, Verknüpfungen wie Zugriffsregeln enthält, die auf diese Schnittstelle angewendet wurden. In diesem Fenster können Sie Verknüpfungen speichern, um sie mit einer anderen Verbindung zu verwenden.

Wenn Sie eine Verbindung löschen und durch den Löschvorgang ein Verbindungstyp verfügbar wird, der zuvor nicht verfügbar war, wird die Liste **Neue Verbindung erstellen** aktualisiert.

Sie können alle Verknüpfungen dieser Verbindung automatisch löschen oder die Verknüpfungen zu einem späteren Zeitpunkt löschen.

So zeigen Sie die Verknüpfungen einer Verbindung an:

Klicken Sie auf **Details anzeigen**.

So löschen Sie die Verbindung mit allen Verknüpfungen:

Klicken Sie auf **Alle Verknüpfungen automatisch löschen**, und klicken Sie dann auf **OK**. Cisco SDM löscht jetzt die Verbindung mit allen Verknüpfungen.

So löschen Sie die Verknüpfungen manuell:

Wenn Sie die Verknüpfungen manuell löschen möchten, klicken Sie auf **Details anzeigen**, um eine Liste der Verknüpfungen dieser Verbindung anzuzeigen. Notieren Sie sich die Verknüpfungen, und wählen Sie die Option **Ich lösche die Verknüpfungen später**. Klicken Sie dann auf **OK**. Sie können alle Verknüpfungen dieser Verbindung löschen. Folgen Sie dazu den Anweisungen in der folgenden Liste.

Es gibt die folgenden Verknüpfungen mit den folgenden Anweisungen zum Löschen:

- Statische Standardroute – Die Schnittstelle wird als Forwarding-Schnittstelle für die statische Standardroute konfiguriert. Wenn Sie die statische Route, mit der diese Schnittstelle verknüpft ist, löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Routing**. Klicken Sie in der Tabelle **Statisches Routing** auf die statische Route, und klicken Sie dann auf **Löschen**.
- Port Address Translation – PAT wird mit der Schnittstelle konfiguriert, auf der diese Verbindung erstellt wurde. Wenn Sie die PAT-Verknüpfung löschen möchten, klicken Sie auf **Konfigurieren**, und klicken Sie dann auf **NAT**. Klicken Sie auf die Regel, die mit dieser Verbindung verknüpft ist, und klicken Sie dann auf **Löschen**.
- NAT – Die Schnittstelle wird entweder als eine innere oder eine äußere NAT-Schnittstelle konfiguriert. Wenn Sie die NAT-Verknüpfung löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Verbindung, und anschließend auf **Bearbeiten**. Klicken Sie auf die Registerkarte **NAT**, wählen Sie im daraufhin angezeigten Dropdown-Menü die Option **Keine**.
- ACL – Eine ACL (Access Control List, Zugriffssteuerungsliste) wird auf die Schnittstelle angewendet, auf der die Verbindung erstellt wurde. Wenn Sie die ACL löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Verbindung, und klicken Sie dann auf **Bearbeiten**. Klicken Sie auf die Registerkarte **Verknüpfung**, klicken Sie dann im Gruppenfeld **Zugriffsregel** auf die Schaltfläche **...** neben den Feldern **Eingehend** und **Ausgehend**.

Klicken Sie anschließend auf **Keine**.

- Prüfregel – Eine Prüfregel wird auf die Schnittstelle angewendet, auf der die Verbindung erstellt wurde. Wenn Sie die Prüfregel löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Verbindung, und klicken Sie dann auf **Bearbeiten**. Klicken Sie auf die Registerkarte **Verknüpfung**, und wählen Sie dann im Bereich der Prüfregeln sowohl im Feld **Eingehend** als auch im Feld **Ausgehend** die Option **Keine**.
- Kryptografie – Eine Crypto Map wird auf die Schnittstelle angewendet, auf der die Verbindung erstellt wurde. Wenn Sie die Crypto Map löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Verbindung, und anschließend auf **Bearbeiten**. Klicken Sie auf die Registerkarte **Verknüpfung**. Klicken Sie dann im VPN-Bereich im Feld **IPSec-Richtlinie** auf die Schaltfläche **Keine**.
- EZVPN – Eine Easy VPN wird auf die Schnittstelle angewendet, auf der die Verbindung erstellt wurde. Wenn Sie Easy VPN löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Verbindung, und anschließend auf **Bearbeiten**. Klicken Sie auf die Registerkarte **Verknüpfung**. Klicken Sie dann im VPN-Bereich im Feld **Easy VPN** auf die Schaltfläche **Keine**.
- VPDN – VPDN-Befehle, die für eine PPPoE-Konfiguration erforderlich sind, sind in der Routerkonfiguration vorhanden. Wenn weitere PPPoE-Verbindungen auf dem Router konfiguriert sind, sollten Sie die VPDN-Befehle nicht löschen.
- ip tcp adjust mss – Dieser Befehl wird auf eine LAN-Schnittstelle angewendet, um die maximale TCP-Größe einzustellen. Wenn weitere PPPoE-Verbindungen auf dem Router konfiguriert sind, sollten Sie diesen Befehl nicht löschen.
- Sicherungsverbindung – Wenn für den primären Server eine Sicherungsverbindung konfiguriert ist. Um die Verknüpfung zu löschen, klicken Sie auf **Konfigurieren**, und klicken Sie dann auf **Schnittstellen und Verbindungen**. Klicken Sie in der Schnittstellenliste auf die Sicherungsschnittstelle, und klicken Sie dann auf **Bearbeiten**. Klicken Sie auf die Registerkarte **Sicherung**, und deaktivieren Sie das Kontrollkästchen **Sicherung aktivieren**.

- PAT in Sicherungsverbindung – Auf der Sicherungsschnittstelle ist PAT konfiguriert. Wenn Sie die PAT-Verknüpfung löschen möchten, klicken Sie auf **Konfigurieren**, und klicken Sie dann auf **NAT**. Klicken Sie auf die Regel, die mit dieser Verbindung verknüpft ist, und klicken Sie dann auf **Löschen**.
- Floating-Standardroute in Sicherungsverbindung – Die Sicherungsschnittstelle ist mit einer statischen Floating-Standardroute konfiguriert. Wenn Sie die statische Floating-Standardroute löschen möchten, klicken Sie auf **Konfigurieren** und anschließend auf **Routing**. Klicken Sie in der Tabelle **Statisches Routing** auf die statische Floating-Route, und klicken Sie dann auf **Löschen**.

Übersicht

Auf diesem Bildschirm wird eine Übersicht über den WAN-Link angezeigt, den Sie konfiguriert haben. Sie können diese Informationen überprüfen, und wenn Sie Änderungen vornehmen müssen, können Sie auf die Schaltfläche **Zurück** klicken, um zu dem betreffenden Bildschirm zurückzukehren, auf dem Sie Änderungen vornehmen müssen.

Konnektivität nach der Konfiguration testen

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Cisco SDM die Verbindung testet, die Sie konfiguriert haben, nachdem die Befehle an den Router gesendet wurden. Cisco SDM testet die Verbindung und meldet die Ergebnisse in einem separaten Fenster.

So speichern Sie diese Konfiguration in der aktiven Konfiguration des Routers und verlassen diesen Assistenten:

Klicken Sie auf **Fertig stellen**. Cisco SDM speichert die Konfigurationsänderungen in der aktiven Konfiguration des Routers. Die Änderungen werden sofort wirksam; beim Abschalten des Routers gehen sie jedoch verloren.

Wenn Sie im Cisco SDM-Fenster **Einstellungen** die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktiviert haben, wird das Fenster **Senden** angezeigt. In diesem Fenster können Sie die CLI-Befehle anzeigen, die an den Router gesendet werden.

Konnektivitätstest und Fehlerbehebung

In diesem Fenster können Sie eine konfigurierte Verbindung testen, indem Sie einen Ping-Befehl an einen Remote-Host senden. Wenn der Ping-Befehl fehlschlägt, meldet Cisco SDM die mögliche Ursache und schlägt Maßnahmen vor, anhand derer Sie das Problem beheben können.

Welche Verbindungstypen können getestet werden?

Cisco SDM kann Fehler in ADSL-, G.SHDSL V1- und G.SHDSL V2-Verbindungen beheben. Dazu verwendet es PPPoE-, AAL5SNAP- oder AAL5MUX-Kapselung.

Cisco SDM kann Fehler in Ethernet-Verbindungen mit PPPoE-Kapselung beheben.

In Ethernet-Verbindungen ohne Kapselung, seriellen und T1 oder E1-Verbindungen, Analogverbindungen und ISDN-Verbindungen kann Cisco SDM keine Fehler beheben. Für diese Verbindungstypen bietet Cisco SDM grundlegende Ping-Tests (Basic Ping Testing).

Was ist Basic Ping Testing?

Beim Basic Ping Testing geht Cisco SDM folgendermaßen vor:

1. Es prüft den Status der Schnittstelle, um festzustellen, ob sie aktiv oder inaktiv ist.
2. Es prüft DNS-Einstellungen, um festzustellen, ob es sich um Cisco SDM-Standardoptionen oder benutzerdefinierte Hostnamen handelt.
3. Es sucht auf der Schnittstelle nach DHCP- und IPCP-Konfigurationen.
4. Es beendet den Schnittstellentest.
5. Es führt ein Ping für das Ziel durch.

Cisco SDM meldet die Ergebnisse dieser einzelnen Prüfungen in den Spalten **Aktivität/Status**. Wenn der Ping-Vorgang erfolgreich war, wird die Verbindung als erfolgreich gemeldet. Anderenfalls wird die Verbindung als inaktiv gemeldet und der fehlgeschlagene Test wird vermerkt.

Wie führt Cisco SDM die Fehlerbehebung durch?

Wenn Cisco SDM bei einer Verbindung eine Fehlerbehebung durchführt, erfolgt eine ausführlichere Prüfung als beim grundlegenden Ping-Test. Wenn der Router einen Test nicht besteht, führt Cisco SDM weitere Prüfungen durch, um Sie über die möglichen Gründe für den Ausfall zu informieren. Bei einem inaktiven Status von Layer 2 versucht Cisco SDM beispielsweise, die Gründe zu ermitteln, meldet diese und empfiehlt dann Maßnahmen, die Sie ergreifen können, um das Problem zu beheben. Cisco SDM führt die folgenden Aufgaben durch:

1. Der Schnittstellenstatus wird überprüft. Wenn das Protokoll von Layer 2 aktiv ist, fährt Cisco SDM mit Schritt 2 fort.

   Bei einem inaktiven Protokollstatus von Layer 2 prüft Cisco SDM den ATM PVC-Status für XDSL-Verbindungen oder den PPPoE-Status für gekapselte Ethernet-Verbindungen.

   - Wenn der ATM PVC-Test fehlschlägt, zeigt Cisco SDM mögliche Gründe für den Fehler an und schlägt Maßnahmen vor, anhand derer Sie das Problem beheben können.
   - Wenn die PPPoE-Verbindung inaktiv ist, liegt ein Problem in der Verkabelung vor, und Cisco SDM zeigt entsprechende Gründe und Maßnahmen an.

   Nachdem diese Prüfungen durchgeführt wurden, wird der Test beendet, und Cisco SDM meldet die Ergebnisse und schlägt Maßnahmen vor.

2. Es prüft DNS-Einstellungen, um festzustellen, ob es sich um Cisco SDM-Standardoptionen oder benutzerdefinierte Hostnamen handelt.

3. Es prüft die Konfiguration und den Status von DHCP- und IPCP. Wenn der Router eine IP-Adresse über DHCP oder IPCP aufweist, fährt Cisco SDM mit Schritt 4 fort.

   Wenn der Router für DHCP oder IPCP konfiguriert ist, jedoch durch keine dieser beiden Methoden eine IP-Adresse erhalten hat, führt Cisco SDM die Tests aus Schritt 1. durch. Der Test wird beendet, und Cisco SDM berichtet die Ergebnisse und schlägt Maßnahmen vor.

4. Es führt ein Ping für das Ziel durch. Wenn der Ping-Vorgang erfolgreich ist, meldet Cisco SDM den Erfolg.

Wenn der Ping-Befehl auf einer xDSL-Verbindung mit PPPoE-Kapselung fehlschlägt, prüft Cisco SDM Folgendes:

- den ATM PVC-Status
- den PPPoE-Tunnelstatus
- den PPP-Authentifizierungsstatus

Nachdem diese Prüfungen durchgeführt wurden, meldet Cisco SDM den Grund, warum der Ping-Befehl fehlgeschlagen ist.

Wenn der Ping-Befehl auf einer Ethernet-Verbindung mit PPPoE-Kapselung fehlschlägt, prüft Cisco SDM Folgendes:

- den PPPoE-Tunnelstatus
- den PPP-Authentifizierungsstatus

Nachdem diese Prüfungen durchgeführt wurden, meldet Cisco SDM den Grund, warum der Ping-Befehl fehlgeschlagen ist.

Wenn der Ping-Befehl auf einer xDSL-Verbindung mit AAL5SNAP- oder AAL5MUX-Kapselung fehlschlägt, prüft Cisco SDM den ATM PVC-Status und meldet den Grund, warum der Ping-Befehl fehlgeschlagen ist.

IP-Adresse/Hostname

Geben Sie den Servernamen für den Ping-Befehl zum Testen der WAN-Schnittstelle ein.

Automatisch von SDM festgelegt

Cisco SDM führt einen Ping-Befehl am Standardhost durch, um die WAN-Schnittstelle zu testen. Cisco SDM erkennt die statisch konfigurierten DNS-Server und dynamisch importierten DNS-Server des Routers. Cisco SDM sendet einen Ping-Befehl an diese Server. Cisco SDM meldet einen Erfolg, wenn während des Tests erfolgreiche Ping-Befehle durch die Schnittstelle geleitet werden. Wenn keiner der Ping-Befehle erfolgreich ist oder während des Tests keine erfolgreichen Ping-Befehle durch die Schnittstelle geleitet wurden, meldet Cisco SDM einen Fehler.

Benutzerdefiniert

Geben Sie die IP-Adresse des gewünschten Hostnamens zum Testen der WAN-Schnittstelle ein.

Übersicht

Klicken Sie auf diese Schaltfläche, wenn Sie eine Übersicht über die Fehlerbehebungsinformationen anzeigen möchten.

Details

Klicken Sie auf diese Schaltfläche, wenn Sie ausführliche Fehlerbehebungsinformationen anzeigen möchten.

Aktivität

In dieser Spalte werden die Aktivitäten zur Fehlerbehebung aufgeführt.

Status

Zeigt den Status der einzelnen Fehlerbehebungsaktivitäten durch die folgenden Symbole und Warntexte an:

 Die Verbindung ist aktiv.

 Die Verbindung ist nicht aktiv.

 Test erfolgreich.

 Test fehlgeschlagen.

Grund

In diesem Feld werden die möglichen Ursachen für den Verbindungsausfall an der WAN-Schnittstelle angezeigt.

Empfohlene Aktion(en)

In diesem Feld finden Sie eine mögliche Maßnahme/Lösung, um das Problem zu beheben.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Fehler in der WAN-Schnittstellenverbindung beheben.	Klicken Sie auf die Schaltfläche **Start**. Während der Ausführung des Tests wechselt die Bezeichnung der Schaltfläche **Start** zu **Stopp**. Sie können die Fehlerbehebung während der Durchführung des Tests abbrechen.
Den Testbericht speichern.	Klicken Sie auf die Schaltfläche **Bericht speichern**, um den Testbericht in HTML-Format zu speichern. Diese Schaltfläche ist nur während der Durchführung eines Tests oder nach Abschließen des Tests verfügbar.

Wie gehe ich vor?

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie zeige ich die IOS-Befehle an, die ich an den Router sende?

Siehe Wie zeige ich die IOS-Befehle an, die ich an den Router sende?.

Wie konfiguriere ich eine nicht unterstützte WAN-Schnittstelle?

Cisco SDM unterstützt nicht die Konfiguration aller WAN-Schnittstellen, die Ihr Router möglicherweise unterstützt. Wenn Cisco SDM eine Schnittstelle in Ihrem Router ermittelt, die es nicht unterstützt, oder eine unterstützte Schnittstelle mit einer nicht unterstützten Konfiguration, zeigt Cisco SDM das Optionsfeld **Andere (Nicht von Cisco SDM unterstützt)** an. Die nicht unterstützte Schnittstelle wird im Fenster **Schnittstellen und Verbindungen** angezeigt, kann jedoch mit Cisco SDM nicht konfiguriert werden.

Wenn Sie eine nicht unterstützte Schnittstelle konfigurieren möchten, müssen Sie die Befehlszeilenschnittstelle (Command-Line Interface, CLI) des Routers verwenden.

Wie aktiviere oder deaktiviere ich eine Schnittstelle?

Sie können eine Schnittstelle deaktivieren, ohne ihre Konfiguration zu entfernen, und Sie können auch eine Schnittstelle, die Sie deaktiviert haben, wieder neu aktivieren.

Schritt 1 Klicken Sie in der Cisco SDM-Symbolleiste auf **Konfigurieren**.

Schritt 2 Klicken Sie im linken Bereich auf **Schnittstellen und Verbindungen**.

Schritt 3 Klicken Sie auf die Schnittstelle, die Sie deaktivieren oder erneut aktivieren möchten.

Schritt 4 Wenn die Schnittstelle aktiviert ist, wird unterhalb der Schnittstellenliste die Schaltfläche **Deaktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, um die Schnittstelle zu deaktivieren. Wenn die Schnittstelle momentan deaktiviert ist, wird unterhalb an dieser Stelle die Schaltfläche **Aktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, die Schnittstelle zu deaktivieren.

Wie zeige ich Aktivitäten auf meiner WAN-Schnittstelle an?

Mit der Monitor-Funktion von Cisco SDM können Sie die Aktivitäten auf WAN-Schnittstellen anzeigen. Die Monitor-Bildschirme können Statistiken über die WAN-Schnittstelle anzeigen, einschließlich der Anzahl von Paketen und Bytes, die von der Schnittstelle gesendet oder empfangen wurden, und der Anzahl der Sende- oder Empfangsfehler, die aufgetreten sind. So zeigen Sie Statistiken zu einer WAN-Schnittstelle an:

Schritt 1 Klicken Sie in der Symbolleiste auf **Monitor**.

Schritt 2 Klicken Sie im linken Bereich auf **Schnittstellenstatus**.

Schritt 3 Wählen Sie im Feld **Schnittstelle auswählen** die WAN-Schnittstelle, für die Sie Statistiken anzeigen möchten.

Schritt 4 Wählen Sie die Datenelemente, die Sie anzeigen möchten, indem Sie die dazugehörigen Kontrollkästchen aktivieren. Sie können gleichzeitig bis zu vier Statistiken anzeigen.

Schritt 5 Klicken Sie auf **Details anzeigen**, um Statistiken für alle ausgewählten Datenelemente anzuzeigen.

Daraufhin wird der Bildschirm **Details zur Schnittstelle** mit den ausgewählten Statistiken angezeigt. Der Bildschirm zeigt standardmäßig Echtzeitdaten an. Dafür wird der Router alle 10 Sekunden abgefragt. Wenn die Schnittstelle aktiv ist und Daten übertragen werden, sollten Sie jetzt sehen, dass die Anzahl der über die Schnittstelle gesendeten Pakete und Byte zunimmt.

Wie konfiguriere ich NAT auf einer WAN-Schnittstelle?

Schritt 1 Klicken Sie in der Cisco SDM-Symbolleiste auf **Konfigurieren**.

Schritt 2 Wählen Sie im linken Bereich **NAT** aus.

Schritt 3 Klicken Sie im NAT-Fenster auf **NAT-Schnittstellen bestimmen**.

Schritt 4 Suchen Sie nach der Schnittstelle, für die Sie NAT konfigurieren möchten.

Schritt 5 Aktivieren Sie das Kontrollkästchen **Innere (vertrauenswürdig)** neben der Schnittstelle, um diese Schnittstelle als eine innere, oder vertrauenswürdige, Schnittstelle zu kennzeichnen. Eine Schnittstelle wird meist dann als innere Schnittstelle gekennzeichnet, wenn sie in einem LAN eingesetzt wird, dessen Ressourcen geschützt werden müssen. Aktivieren Sie das Kontrollkästchen **Äußere (nicht vertrauenswürdig)**, um die Schnittstelle als äußere Schnittstelle zu kennzeichnen. Äußere Schnittstellen sind meist mit einem nicht vertrauenswürdigen Netzwerk verbunden. Klicken Sie auf **OK**.

Die Schnittstelle wird zu dem Pool der Schnittstellen hinzugefügt, die NAT verwenden.

Schritt 6 Überprüfen Sie die Regeln der Network Address Translation im NAT-Fenster. Wenn Sie eine Regel hinzufügen, löschen oder modifizieren müssen, klicken Sie auf die entsprechende Schaltfläche im NAT-Fenster, um die gewünschte Konfiguration durchzuführen.

Weitere Informationen finden Sie unter den folgenden Links:

- Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen
- Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen
- Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen
- Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen

Wie konfiguriere ich NAT auf einer nicht unterstützten Schnittstelle?

Cisco SDM kann die Network Address Translation (NAT) auf einem Schnittstellentyp konfigurieren, der von Cisco SDM nicht unterstützt wird. Bevor Sie die Firewall konfigurieren können, müssen Sie die Schnittstelle zunächst mit der CLI des Routers konfigurieren. Die Schnittstelle muss mindestens eine konfigurierte IP-Adresse haben und in Betrieb sein. Um zu überprüfen, ob die Verbindung funktioniert, stellen Sie fest, ob als Schnittstellenstatus **Aktiv** angegeben ist.

Nachdem Sie die nicht unterstützte Schnittstelle mit der CLI konfiguriert haben, können Sie NAT mit Cisco SDM konfigurieren. Die nicht unterstützte Schnittstelle wird in der Liste der Routerschnittstellen als „Andere“ angezeigt.

Wie konfiguriere ich ein Protokoll für dynamisches Routing?

So konfigurieren Sie ein Dynamisches Routing-Protokoll:

Schritt 1 Klicken Sie in der Symbolleiste auf **Konfigurieren**.

Schritt 2 Klicken Sie im linken Bereich auf **Routing**.

Schritt 3 Klicken Sie im Bereich **Dynamisches Routing** auf das Protokoll für dynamisches Routing, das Sie konfigurieren möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Daraufhin wird das Dialogfeld **Dynamisches Routing** mit einer Registerkarte für das ausgewählte Protokoll für dynamisches Routing angezeigt.

Schritt 5 Verwenden Sie die Felder im Dialogfeld **Dynamic Routing**, um das Protokoll für dynamisches Routing zu konfigurieren. Wenn Sie für eines der Felder im Dialogfeld eine Erläuterung benötigen, klicken Sie auf **Hilfe**.

Schritt 6 Wenn Sie die Konfiguration des Protokolls für dynamisches Routing abgeschlossen haben, klicken Sie auf **OK**.

Wie konfiguriere ich Dial-on-Demand Routing für meine ISDN- oder asynchrone Schnittstelle?

ISDN BRI- und asynchrone Verbindungen sind Wählverbindungen. Das bedeutet, dass der Router eine vorkonfigurierte Telefonnummer wählen muss, um eine Verbindung herzustellen. Da die Kosten für diesen Verbindungstyp meist durch die Zeitspanne festgelegt werden, die eine solche Verbindung aufrechterhalten wurde, und eine Telefonleitung im Falle einer asynchronen Verbindung belegt wird, ist es oftmals eine gute Lösung, Dial-on-Demand Routing (DDR) für diese Verbindungstypen zu konfigurieren.

Cisco SDM kann Sie folgendermaßen bei der Konfiguration von DDR unterstützen:

- Sie können eine Regel (oder ACL) mit der Verbindung verknüpfen, sodass der Router die Verbindung nur dann herstellt, wenn er Netzwerk-Datenverkehr erkennt, den Sie mit der verknüpften Regel als interessant gekennzeichnet haben.
- Sie können Timeouts für den Ruhezustand festlegen, sodass der Router eine Verbindung nach einer bestimmten Zeitspanne ohne Aktivität in der Verbindung beendet.
- Sie können Multilink PPP aktivieren, sodass eine ISDN BRI-Verbindung nur einen der beiden B-Kanäle verwendet, ausgenommen, es wird ein festgelegter Prozentsatz der Bandbreite auf dem ersten B-Kanal überschritten. Dies hat den Vorteil, dass Kosten gespart werden können, wenn der Datenverkehr im Netzwerk gering ist und der zweite B-Kanal nicht benötigt wird. Sie können jedoch bei Bedarf trotzdem die volle Bandbreite Ihrer ISDN BRI-Verbindung nutzen.

So konfigurieren Sie DDR auf einer vorhandenen ISDN BRI oder als asynchrone Verbindung:

Schritt 1 Klicken Sie in der Cisco SDM-Symbolleiste auf **Konfigurieren**.

Schritt 2 Klicken Sie im linken Bereich auf **Schnittstellen und Verbindungen**.

Schritt 3 Klicken Sie auf die ISDN- oder asynchrone Schnittstelle, auf der Sie DDR konfigurieren möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Es erscheint die Registerkarte **Verbindung**.

Schritt 5 Klicken Sie auf **Optionen**.

Das Dialogfeld **Dialer Option bearbeiten** wird angezeigt.

Schritt 6 Wenn Sie möchten, dass der Router die Verbindung nur dann herstellt, wenn er bestimmten IP-Datenverkehr erkennt, klicken Sie auf das Optionsfeld **Datenverkehr auf der Basis der ausgewählten ACL filtern**, und geben Sie entweder eine Regel-Nummer (ACL-Nummer) ein, die kennzeichnet, bei welchem IP-Datenverkehr der Router herauswählen soll, oder klicken Sie auf die Schaltfläche **...**, um die Liste mit den Regeln zu durchsuchen und die Regel in der Liste zu wählen, mit der Sie den IP-Datenverkehr identifizieren möchten.

Schritt 7 Wenn Sie den Router so konfigurieren möchten, dass die Verbindung beendet wird, wenn sie sich für eine bestimmte Zeitspanne im Ruhezustand befindet, d. h., kein Datenverkehr durch die Verbindung geleitet wird, geben Sie in das Feld **Leerlauf-Timeout** die Anzahl von Sekunden ein, die eine Verbindung im Ruhezustand verbleiben kann, bis der Router die Verbindung trennt.

Schritt 8 Wenn Sie eine ISDN-Verbindung bearbeiten und den zweiten B-Kanal nur dann verwenden möchten, wenn der Datenverkehr im ersten B-Kanal einen bestimmten Schwellenwert überschreitet, aktivieren Sie das Kontrollkästchen **Multilink-PPP aktivieren**, und geben Sie in das Feld **Auslastungsschwellenwert** eine Zahl zwischen 1 und 255 ein, um den Schwellenwert auf dem ersten B-Kanal festzulegen. Dabei entspricht 255 einer Bandbreite von 100 %. Wenn der Datenverkehr auf diesem Kanal den Schwellenwert überschreitet, stellt der Router eine Verbindung zum zweiten B-Kanal her. Zusätzlich können Sie im Feld **Datenrichtung** festlegen, ob dieser Schwellenwert für ausgehenden oder eingehenden Datenverkehr gelten soll.

Schritt 9 Klicken Sie auf **OK**.

Wie kann ich die Konfiguration einer Wireless-Schnittstelle bearbeiten?

Sie müssen die Wireless-Anwendung zur Bearbeitung einer bestehenden Wireless-Schnittstellenkonfiguration verwenden.

Schritt 1 Klicken Sie in der Cisco SDM-Symbolleiste auf **Konfigurieren**.

Schritt 2 Klicken Sie im linken Rahmen auf **Schnittstellen und Verbindungen**, und klicken Sie dann auf die Registerkarte **Schnittstelle/Verbindung bearbeiten**.

Schritt 3 Wählen Sie die Wireless-Schnittstelle, und klicken Sie auf **Bearbeiten**. Auf der Registerkarte **Verbindungen** können Sie die IP-Adresse oder die Bridging-Informationen ändern. Wenn Sie weitere Wireless-Parameter ändern möchten, klicken Sie auf **Wireless-Anwendung starten**.

KAPITEL 5

Schnittstelle/Verbindung bearbeiten

Dieses Fenster zeigt die Schnittstellen und Verbindungen des Routers an. In diesem Fenster können Sie darüber hinaus Verbindungen hinzufügen, bearbeiten und löschen sowie Verbindungen aktivieren oder deaktivieren.

Hinzufügen

Wenn Sie eine nicht konfigurierte physische Schnittstelle wählen und auf **Hinzufügen** klicken, enthält das Menü Auswahloptionen zum Hinzufügen einer Verbindung zu dieser Schnittstelle. Klicken Sie auf **Hinzufügen**, um ein neues Loopback oder eine Tunnelschnittstelle zu erstellen. Wenn das Cisco IOS-Abbild auf dem Router virtuelle Vorlagenschnittstellen (VTI) unterstützt, enthält das Kontextmenü eine Option, um eine VTI hinzuzufügen. Wenn auf dem Router Switch-Ports vorhanden sind, können Sie ein neues VLAN hinzufügen.

Wenn Sie eine Schnittstelle erneut konfigurieren möchten und nach dem Klicken auf **Hinzufügen** keinerlei Auswahloptionen mit Ausnahme von **Loopback** und **Tunnel** angezeigt werden, wählen Sie die Schnittstelle aus, und klicken Sie auf **Löschen**. Sämtliche Verbindungstypen, die für diese Art der Schnittstelle verfügbar sind, werden im Menü **Hinzufügen** aufgeführt. Klicken Sie auf **Verfügbare Schnittstellenkonfigurationen**, um anzuzeigen, welche Konfigurationen für eine Schnittstelle verfügbar sind.

Bearbeiten

Wenn Sie eine Schnittstelle auswählen und auf **Bearbeiten** klicken, wird ein Dialogfeld geöffnet. Wenn es sich bei der Schnittstelle um eine unterstützte und konfigurierte Schnittstelle und nicht um einen Switch-Port handelt, enthält das Dialogfeld folgende Registerkarten:

- Verbindung
- Registerkarte Verknüpfung
- Registerkarte NAT
- Anwendungsdienst
- Registerkarte Allgemein

Wenn die Schnittstelle nicht unterstützt wird, enthält das Dialogfeld die Registerkarte **Verbindung** *nicht*. Wenn Sie einen Switch-Port auswählen, wird das Dialogfeld **Switch-Portmodus bearbeiten** angezeigt. Die Schaltfläche **Bearbeiten** ist deaktiviert, wenn die Schnittstelle unterstützt wird und nicht konfiguriert ist.

Löschen

Wenn Sie eine Verbindung auswählen und auf **Löschen** klicken, wird ein Dialogfeld mit Informationen zu den Verknüpfungen, über die diese Schnittstelle verfügt, angezeigt, und Sie werden gefragt, ob Sie die Verknüpfungen zusammen mit der Verbindung entfernen möchten. Sie können nur die Verbindung oder die Verbindung mit sämtlichen zugehörigen Verknüpfungen löschen.

Übersicht

Durch Klicken auf die Schaltfläche **Übersicht**, werden Details zur Verbindung ausgeblendet, sodass nur noch Informationen zur IP-Adresse, zum Typ, zum Slot und zum Status sowie die Beschreibung angezeigt werden.

Details

Durch Klicken auf **Details** wird der nachfolgend erläuterte Bereich **Details zur Schnittstelle** angezeigt. Standardmäßig werden diese Schnittstellendetails angezeigt.

Aktivieren oder Deaktivieren

Wenn die gewählte Schnittstelle oder Verbindung unterbrochen ist, erscheint dies als die Schaltfläche **Aktivieren**. Klicken Sie auf die Schaltfläche **Aktivieren**, um die gewählte Schnittstelle oder Verbindung wiederherzustellen. Wenn die gewählte Schnittstelle oder Verbindung steht, erscheint dies als die Schaltfläche **Deaktivieren**. Klicken Sie auf die Schaltfläche **Deaktivieren**, um die Schnittstelle oder Verbindung zu unterbrechen. Diese Schaltfläche kann nicht bei einer Schnittstelle benutzt werden, deren Konfiguration nicht an den Router übermittelt wurde.

Verbindung testen

Klicken Sie auf diese Schaltfläche, um die ausgewählte Verbindung zu testen. Daraufhin wird ein Dialogfeld angezeigt, in dem Sie einen Remote-Host festlegen können, der während dieser Verbindung Ping-Befehle aussendet. Das Dialogfeld meldet dann den Erfolg oder das Scheitern des Tests. Wenn der Test fehlschlägt, werden Informationen zu der Ursache des Fehlschlagens sowie Informationen angegeben, welche Schritte Sie unternehmen müssen, um das Problem zu beheben.

Schnittstellenliste

Die Schnittstellenliste zeigt die physikalischen Schnittstellen und logischen Verbindungen an, für die sie konfiguriert sind.

Schnittstellen

In dieser Spalte werden die physischen und logischen Schnittstellen namentlich aufgeführt. Wenn eine logische Schnittstelle für eine physikalische Schnittstelle konfiguriert ist, wird die logische Schnittstelle unter der physischen Schnittstelle angezeigt.

Wenn Cisco SDM auf einem Router der Cisco 7000-Familie ausgeführt wird, ist das Herstellen einer Verbindung nur über Ethernet- und Fast Ethernet-Schnittstellen möglich.

IP-Adresse

Diese Spalte kann die folgenden IP-Adressentypen enthalten:

- Die konfigurierte IP-Adresse der Schnittstelle.
- **DHCP-Client** – Die Schnittstelle empfängt eine IP-Adresse von einem DHCP-Server (DHCP = Dynamic Host Configuration Protocol).

- **IP ausgehandelt** – Nach Aushandlung der Parameter mit dem Remote-Gerät erhält die Schnittstelle eine IP-Adresse.
- **Keine IP-Nummerierung** – Der Router verwendet eine IP-Adresse aus einem Pool, den Sie von Ihrem Service-Provider für Ihren Router und für die Geräte im LAN erhalten haben.
- Nicht zutreffend – Dem Schnittstellentyp kann keine IP-Adresse zugewiesen werden.

Typ

Die Spalte **Typ** zeigt den Schnittstellentyp an, wie beispielsweise Ethernet, Seriell oder ATM.

Slot

Die Nummer des physischen Steckplatzes im Router, in dem die Schnittstelle installiert ist. Wenn Cisco SDM auf einem Cisco 1710-Router ausgeführt wird, ist das Feld **Slot** leer.

Status

Diese Spalte zeigt an, ob diese Schnittstelle aktiv oder inaktiv ist. Das grüne Symbol mit der nach oben gerichteten Pfeilspitze gibt an, dass die Schnittstelle aktiv ist. Das rote Symbol mit der nach unten gerichteten Pfeilspitze gibt an, dass die Schnittstelle inaktiv ist.

Beschreibung

Diese Spalte enthält alle Beschreibungen, die für diese Verbindung bereitgestellt wurden.

Details zur Schnittstelle

Dieser Bereich des Fensters zeigt Verknüpfungs- und, sofern zutreffend, Verbindungsdetails zu der in der **Schnittstellenliste** ausgewählten Schnittstelle an. Zu den Verknüpfungsdetails gehören Informationen wie Network Address Translation (NAT), Zugriffsinformationen und Prüfregeln, IPSec-Richtlinien und Easy VPN-Konfigurationen. Verbindungsdetails umfassen die IP-Adresse, den Kapselungstyp und DHCP-Optionen.

Elementname

Der Name des Konfigurationselements, wie die IP-Adresse/Subnetzmaske oder IPSec-Richtlinie. Die tatsächlich aufgeführten Elemente in dieser Spalte richten sich nach dem Typ der ausgewählten Schnittstelle.

Elementwert

Wenn das betreffende Element über einen konfigurierten Wert verfügt, wird dieser in dieser Spalte angezeigt.

Was möchten Sie tun?

Aufgabe:	Vorgehensweise:
Hinzufügen einer neuen Verbindung	Klicken Sie auf **Hinzufügen**, und wählen Sie eine Verbindung aus dem Kontextmenü aus.
Hinzufügen einer neuen logischen Schnittstelle	Klicken Sie auf **Hinzufügen**, und wählen Sie eine logische Schnittstelle aus dem Kontextmenü aus.
Hinzufügen einer VLAN-Schnittstelle	Klicken Sie auf **Hinzufügen**, wählen Sie **Neue logische Schnittstelle** aus dem Kontextmenü aus, und wählen Sie anschließend **VLAN** aus dem Untermenü aus.
Bearbeiten einer vorhandenen Schnittstelle	Markieren Sie die Schnittstelle, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**. **Hinweis** Bei der Bearbeitung eines GRE-Tunnels wird die Registerkarte **Verbindung** nicht angezeigt, wenn der GRE-Tunnel nicht auf die Nutzung des Modus **gre ip** eingestellt ist.
Zurücksetzen einer physikalischen Schnittstelle in einen nicht konfigurierten Status	Wählen Sie die physikalische Schnittstelle aus, und klicken Sie auf **Zurücksetzen**.

Aufgabe:	Vorgehensweise:
Löschen einer logischen Schnittstelle	Wählen Sie die Schnittstelle aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
Informationen zum Ausführen verwandter Konfigurationsaufgaben	Lesen Sie eine der folgenden Vorgehensweisen: • Wie konfiguriere ich eine statische Route? • Wie zeige ich Aktivitäten in meiner LAN-Schnittstelle an? • Wie aktiviere oder deaktiviere ich eine Schnittstelle? • Wie zeige ich die IOS-Befehle an, die ich an den Router sende? • Wie konfiguriere ich eine nicht unterstützte WAN-Schnittstelle? • Wie zeige ich Aktivitäten auf meiner WAN-Schnittstelle an? • Wie konfiguriere ich NAT auf einer WAN-Schnittstelle? • Wie konfiguriere ich eine statische Route? • Wie konfiguriere ich ein Protokoll für dynamisches Routing?

Warum sind einige Schnittstellen oder Verbindungen schreibgeschützt?

Wenn keine Änderungen an einer zuvor konfigurierten Schnittstelle oder Unterschnittstelle mit Cisco SDM vorgenommen werden können, kann dies zahlreiche Ursachen haben.

- Mögliche Ursachen dazu, warum in der **Schnittstellenliste** eine vorher konfigurierte serielle Schnittstelle oder Unterschnittstelle als schreibgeschützt aufgeführt wird, finden Sie im Hilfethema Ursachen, warum eine serielle Schnittstellen- oder Unterschnittstellenkonfiguration schreibgeschützt sein kann.
- Mögliche Ursachen dafür, warum eine vorher konfigurierte ATM-Schnittstelle oder -Unterschnittstelle in der **Schnittstellenliste** als schreibgeschützt aufgeführt wird, finden Sie im Hilfethema Ursachen, warum eine ATM-Schnittstellen- oder Unterschnittstellenkonfiguration schreibgeschützt sein kann.

- Mögliche Ursachen dafür, warum eine vorher konfigurierte Ethernet-LAN- oder WAN-Schnittstelle in der **Schnittstellenliste** als schreibgeschützt aufgeführt wird, finden Sie im Hilfethema Ursachen, warum eine Ethernet-Schnittstellenkonfiguration schreibgeschützt sein kann.
- Mögliche Ursachen dafür, warum eine vorher konfigurierte ISDN BRI-Schnittstelle in der **Schnittstellenliste** als schreibgeschützt aufgeführt wird, finden Sie im Hilfethema Ursachen, warum eine ISDN BRI-Schnittstellenkonfiguration schreibgeschützt sein kann.

Verbindung: Ethernet für IRB

Dieses Dialogfeld enthält folgende Felder, wenn Sie in der Liste **Konfigurieren** den Eintrag **Ethernet für IRB** gewählt haben.

Aktuelle Bridge-Gruppe/Verknüpfte BVI

Diese schreibgeschützten Felder geben den aktuellen Bridge-Gruppenwert und den aktuellen Namen der virtuellen Schnittstelle der Bridge-Gruppe (BVI) an.

Eine neue Bridge-Gruppe erstellen/Einer vorhandenen Bridge-Gruppe beitreten

Legen Sie fest, ob diese Schnittstelle zu einer neuen oder einer bestehenden Bridge-Gruppe gehören soll. Wenn Sie eine neue Bridge-Gruppe erstellen wollen, geben Sie eine Zahl im Bereich von 1 bis 255 ein. Wenn die Schnittstelle hingegen zu einer bestehenden Bridge-Gruppe hinzugefügt werden soll, wählen Sie die BVI-Schnittstelle, die bereits zu dieser Gruppe gehört.

IP-Adresse

Geben Sie die IP-Adresse und Subnetzmaske in die jeweiligen Textfelder ein.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Ethernet für Routing

Dieses Dialogfeld enthält folgende Felder, wenn Sie in der Liste **Konfigurieren** den Eintrag **Ethernet für Routing** gewählt haben.

IP-Adresse

Geben Sie eine IP-Adresse und eine Subnetzmaske in die IP-Adressfelder ein. Diese Adresse ist die Absender-IP-Adresse für den Datenverkehr, der von dieser Schnittstelle ausgeht, und die Ziel-IP-Adresse für Datenverkehr, der an die Hosts dieser Schnittstelle geleitet werden soll.

DHCP-Relay

Klicken Sie darauf, damit der Router als DHCP-Relay fungiert. Ein Gerät, das als DHCP-Relay fungiert, leitet DHCP-Anforderungen an einen DHCP-Server weiter. Wenn einem Gerät eine IP-Adresse dynamisch zugeordnet werden muss, wird eine Broadcast-Übertragung einer DHCP-Anforderung durchgeführt. Ein DHCP-Server antwortet auf diese Anforderung mit einer IP-Adresse. In einem Subnetzwerk kann maximal ein DHCP-Relay oder ein DHCP-Server vorhanden sein.

Hinweis Wenn der Router als DHCP-Relay-Server konfiguriert war und so konfiguriert ist, dass er über mehr als eine Remote-DHCP-Server-IP-Adresse verfügt, sind diese Felder deaktiviert.

IP-Adresse des Remote-DHCP-Servers

Geben Sie die IP-Adresse des DHCP-Servers ein, der Geräten im LAN Adressen zuweist.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Existierende Dynamische DNS Methoden

In diesem Fenster können Sie eine dynamische DNS Methode auswählen, um sie mit einer WAN-Schnittstelle zu verknüpfen.

Aus der Liste der existierenden dynamischen DNS-Methoden gehen die einzelnen Methodennamen und die verknüpften Parameter hervor. Wählen Sie aus der Liste eine Methode aus, und klicken Sie anschließend auf **OK**, um sie mit der WAN Schnittstelle zu verknüpfen.

Um dynamische DNS-Methoden hinzuzufügen, zu bearbeiten oder zu löschen, klicken Sie auf **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methoden**.

Eine Dynamische DNS Methode hinzufügen

In diesem Fenster können Sie eine dynamische DNS Methode hinzufügen. Wählen Sie den Methodentyp, HTTP oder IETF aus und konfigurieren Sie die Methode.

HTTP

HTTP ist eine dynamische DNS Methode, der einen DNS Service-Provider, mit Änderungen an der verknüpften Schnittstellen IP-Adresse, aktualisiert.

Server

Wenn Sie HTTP verwenden, wählen Sie die Domänenadresse des DNS-Dienstanbieters aus dem Dropdown-Menü.

Benutzername

Wenn Sie HTTP verwenden, geben Sie einen Benutzernamen ein, um auf den DNS-Dienstanbieter zuzugreifen.

Kennwort

Wenn Sie HTTP verwenden, geben Sie einen Benutzernamen ein, um auf den DNS-Dienstanbieter zuzugreifen.

IETF

IETF ist eine dynamische DNS Methode, der einen DNS Service-Provider, mit Änderungen an der verknüpften Schnittstellen IP-Adresse, aktualisiert.

DNS Server

Wenn Sie IETF benutzen und kein DNS Server für den Router unter **Konfigurieren > Zusätzliche Aufgaben > DNS** konfiguriert wurde, geben Sie die IP-Adresse Ihres DNS Servers ein:

Hostname

Geben Sie einen Hostnamen ein, wenn unter **Konfigurieren > Zusätzliche Aufgaben > Router-Eigenschaften > Bearbeiten > Host** keiner konfiguriert wurde oder wenn Sie den konfigurierten Hostnamen überschreiben wollen. Wenn die Schnittstellen IP-Adresse aktualisiert wird, übergibt die dynamische DNS Methode den Hostnamen zusammen mit der neuen IP-Adresse der Schnittstelle.

Domainname

Geben Sie einen Domainnamen ein, wenn unter **Konfigurieren > Zusätzliche Aufgaben > Router-Eigenschaften > Bearbeiten > Domain** keiner konfiguriert ist oder wenn Sie den konfigurierten Domainnamen überschreiben wollen. Wenn die Schnittstellen IP-Adresse aktualisiert wird, übergibt die dynamische DNS-Methode den Domainnamen zusammen mit der neuen IP-Adresse der Schnittstelle.

Wireless

Verfügt der Router über eine drahtlose Schnittstelle, können Sie von dieser Registerkarte aus die Wireless-Anwendung starten. Über die Menübefehle **Extras > Wireless-Anwendung** können Sie die Wireless-Anwendung ebenfalls aufrufen.

Verknüpfung

Verwenden Sie dieses Fenster, um Verknüpfungen zwischen Schnittstellen und Regeln oder VPN-Verbindungen anzuzeigen, zu erstellen, zu bearbeiten oder zu löschen.

Schnittstelle

Der Name der Schnittstelle, die Sie im Fenster **Schnittstellen und Verbindungen** ausgewählt haben.

Zone

Wenn diese Schnittstelle einer Sicherheitszone angehört, wird der Name der Zone in diesem Feld angezeigt. Wenn Sie diese Schnittstelle in eine Sicherheitszone aufnehmen möchten, klicken Sie auf die Schaltfläche rechts neben dem Feld, wählen **Zone auswählen** und geben die Zone im angezeigten Dialogfeld an. Wenn Sie eine neue Zone erstellen müssen, wählen Sie **Zone erstellen**, geben einen Namen für die Zone im angezeigten Dialogfeld ein und klicken auf **OK**. Der Name der erstellten Zone wird im Zonenfeld angezeigt.

Zugriffsregel

Die Namen oder Nummern aller Zugriffsregeln, die mit dieser Schnittstelle verknüpft sind. Zugriffsregeln steuern das Zulassen oder Verweigern von Datenverkehr, der mit den in der Regel angegebenen IP-Adressen und Dienstkriterien übereinstimmt.

Eingehend

Der Name oder die Nummer einer Zugriffsregel, die auf eingehenden Datenverkehr in dieser Schnittstelle angewendet wird. Wenn Sie eine Regel anwenden möchten, klicken Sie auf die Schaltfläche **...**, und wählen Sie entweder eine bestehende Regel aus oder erstellen eine Regel und wählen diese aus.

Wenn eine Regel auf eingehenden Datenverkehr in einer Schnittstelle angewendet wird, filtert die Regel Datenverkehr, bevor dieser in den Router eintritt. Alle Pakete, die nicht von der Regel zugelassen werden, werden entfernt, und es erfolgt kein Routing an eine andere Schnittstelle. Wenn Sie eine Regel in eingehender Richtung auf eine Schnittstelle anwenden, verhindern Sie nicht nur, dass die Daten in ein vertrauenswürdiges Netzwerk gelangen, das mit dem Router verbunden ist, sondern auch, dass sie vom lokalen Router woanders hin weitergeleitet werden.

Ausgehend

Der Name oder die Nummer einer Zugriffsregel, die auf ausgehenden Datenverkehr in dieser Schnittstelle angewendet wird. Wenn Sie eine Regel anwenden möchten, klicken Sie auf die Schaltfläche **...**, und wählen Sie entweder eine bestehende Regel aus oder erstellen eine Regel und wählen diese aus.

Wenn der ausgehende Datenverkehr auf einer Schnittstelle mit einer Regel versehen wird, filtert die Regel den Datenverkehr im Router nach dem Datenempfang und vor dem Verlassen der Schnittstelle. Alle Pakete, die nicht von der Regel zugelassen werden, werden entfernt, bevor sie die Schnittstelle verlassen.

Prüfregel

Die Namen der Prüfregeln, die mit dieser Schnittstelle verknüpft sind. Prüfregeln erstellen einen temporären Durchlass in Firewalls, sodass die Hosts innerhalb der Firewall, die Sitzungen eines bestimmten Typs gestartet haben, zurücklaufenden Datenverkehr desselben Typs empfangen können.

Eingang

Der Name oder die Nummer einer Prüfregel, die auf eingehenden Datenverkehr in dieser Schnittstelle angewendet wird. Wenn Sie eine Eingangsregel anwenden möchten, klicken Sie auf das Dropdown-Menü **Eingang** und wählen eine Regel aus.

Ausgang

Der Name oder die Nummer einer Prüfregel, die auf ausgehenden Datenverkehr in dieser Schnittstelle angewendet wird. Wenn Sie eine Ausgangsregel anwenden möchten, klicken Sie auf das Dropdown-Menü **Ausgang** und wählen eine Regel aus.

VPN

VPNs schützen Datenverkehr, der eventuell über Leitungen gesendet wird, die Ihre Organisation nicht kontrollieren kann. Sie können die gewählte Schnittstelle in einem VPN verwenden, indem Sie diese mit einer IPSec-Richtlinie verknüpfen.

IPSec-Richtlinie

Die konfigurierte IPSec-Richtlinie, die mit dieser Schnittstelle verknüpft ist. Um die Schnittstelle mit einer IPSec-Richtlinie zu verknüpfen, wählen Sie die Richtlinie aus dieser Liste aus.

Hinweis Eine Schnittstelle kann nur mit einer IPSec-Richtlinie verknüpft werden.

Hinweis Um einen GRE over IPSec-Tunnel zu erstellen, müssen Sie zunächst die Richtlinie mit der Tunnelschnittstelle verknüpfen und dann eine Verknüpfung mit der Quellschnittstelle für den Tunnel herstellen. Wenn Sie beispielsweise eine Richtlinie mit **Tunnel3** verknüpfen möchten, dessen Schnittstelle **Seriell0/0** ist, müssen Sie zuerst **Tunnel3** im Fenster **Schnittstellen und Verbindungen** auswählen, auf **Bearbeiten** klicken, eine Verknüpfung mit der Richtlinie herstellen und anschließend auf **OK** klicken. Dann müssen Sie die Schnittstelle **Seriell0/0** auswählen und eine Verknüpfung mit derselben Richtlinie herstellen.

EzVPN

Wenn die Schnittstelle in einer Easy VPN-Verbindung verwendet wird, wird der Name der Verbindung hier angezeigt.

Hinweis Eine Schnittstelle kann nicht in einer Virtual Private Network-(VPN-)Verbindung und zugleich in einer Easy VPN-Verbindung verwendet werden.

Vornehmen von Änderungen an Verknüpfungen

Wenn Sie die Verknüpfungseigenschaften einer Schnittstelle ändern, werden die Änderungen im unteren Bereich des Fensters Schnittstellen und Verknüpfungen Bearbeiten angezeigt. Wenn Sie beispielsweise eine IPSec-Richtlinie mit der Schnittstelle verknüpfen, wird der Name der IPSec-Richtlinie im unteren Bereich des Fensters angezeigt. Wenn Sie eine Verknüpfung löschen, ändert sich der Wert in der Spalte **Elementwert** in **<Keine>**.

NAT

Wenn Sie diese Schnittstelle in einer NAT-Konfiguration verwenden möchten, müssen Sie diese entweder als innere oder als äußere Schnittstelle einrichten. Wählen Sie die Datenverkehrsrichtung aus, auf die NAT angewendet werden soll. Wenn die Schnittstelle mit einem LAN verbunden ist, das vom Router bedient wird, wählen Sie **Innen**. Wenn sie mit dem Internet oder mit dem WAN Ihrer Organisation verbunden ist, wählen Sie **Außen**. Wenn Sie eine Schnittstelle ausgewählt haben, die nicht in einer NAT-Konfiguration wie beispielsweise einer logischen Schnittstelle verwendet werden kann, ist dieses Feld deaktiviert und enthält den Wert **Nicht unterstützt**.

Switch-Portmodus bearbeiten

In diesem Fenster können Sie VLAN-Informationen für Ethernet-Switch-Ports bearbeiten.

Modusgruppe

Wählen Sie den VLAN-Informationstyp aus, der über diesen Ethernet-Switch-Port übertragen werden soll. Wenn Sie **Zugriff** wählen, leitet der Switch-Port nur Daten weiter, die für die jeweilige VLAN-Nummer vorgesehen sind. Wenn Sie **Trunk** wählen, leitet der Switch-Port Daten an alle VLANs weiter, einschließlich der VLAN-Daten selbst. Wählen Sie **Trunk** nur dann, wenn es sich um VLAN-Ports im Vermittlungsbetrieb (Trunking) handelt, die mit anderen Vernetzungsgeräten wie etwa einem weiteren Switch verbunden sind, und wenn an diesen Switch Geräte aus mehreren VLANs angeschlossen sind.

VLAN

Um den Switch-Port mit einem VLAN zu verknüpfen, geben Sie die VLAN-Nummer ein, zu dem der Switch-Port gehören soll. Wenn der Switch-Port nicht bereits mit einem VLAN verknüpft ist, zeigt dieses Feld den Standardwert **VLAN 1** an. Um eine neue VLAN-Schnittstelle mit entsprechender VLAN-ID zu erstellen, geben Sie die VLAN-ID hier ein, und aktivieren Sie das Kontrollkästchen **VLAN in Schnittstellenliste anzeigen**.

Kontrollkästchen VLAN in Schnittstellenliste anzeigen

Aktivieren Sie diese Option, wenn Sie ein neues VLAN mit der im Feld **VLAN** angegebenen VLAN-ID erstellen möchten.

Stapel-Partner

Wählen Sie ein Switch-Modul aus, das als Stapel-Partner verwendet werden soll. Wenn ein Gerät mehrere Switch-Module enthält, müssen diese vor anderen Stapel-Partnern gestapelt werden.

Bridge-Gruppennummer

Wenn dieser Switch-Port Teil einer Bridge zu einem drahtlosen Netzwerk sein soll, geben Sie die Nummer einer bestehenden Bridge-Gruppe ein.

Geschwindigkeit

Wählen Sie die passende Geschwindigkeit für das Netzwerk, das mit dem Switch-Port verbunden wird. Alternativ können Sie auch **auto** (autom.) wählen, um die Geschwindigkeit automatisch auf den optimalen Wert einstellen zu lassen.

Duplex

Wählen Sie **full** (voll), **half** (halb) oder **auto** (automatisch), damit das Gerät automatisch den richtigen Duplexmodus für die Kommunikation mit dem Netzwerk einstellt, das über den Switch-Port angesprochen wird.

Wenn unter **Geschwindigkeit** die Option **auto** (automatisch) eingestellt wurde, ist **Duplex** deaktiviert.

Leistungseingang

Die Dropdown-Liste **Leistungseingang** wird angezeigt, wenn der Switch-Port eine Spannungsversorgung für angeschlossene Geräte bietet. Wählen Sie einen der folgenden Werte aus:

- **auto** - Aktiviert die automatische Erkennung und Energieversorgung integrierter Geräte.
- **nie** - Integrierte Energieversorgung niemals aktivieren.

Anwendungsdienst

In diesem Fenster können Sie QoS-Richtlinien sowie Anwendungs- und Protokollüberwachungen an die gewählte Schnittstelle anbinden.

QoS

Um eine QoS-Richtlinie auf die Schnittstelle in eingehender Richtung anzusetzen, wählen Sie in der Dropdownliste **Eingehend** eine QoS-Richtlinie aus.

Um eine QoS-Richtlinie auf die Schnittstelle in ausgehender Richtung anzusetzen, wählen Sie in der Dropdownliste **Ausgehend** eine QoS-Richtlinie aus.

Zum Überwachen von QoS-Statistiken zu der Schnittstelle klicken Sie auf **Monitor > Datenverkehrsstatus > QoS**.

Netflow

Um eine Netflow-Statistiküberwachung auf die Schnittstelle in eingehender Richtung anzusetzen, aktivieren Sie das Kontrollkästchen **Eingehend**.

Um eine Netflow-Statistiküberwachung auf die Schnittstelle in ausgehender Richtung anzusetzen, aktivieren Sie das Kontrollkästchen **Ausgehend**.

Zum Überwachen von Netflow-Statistiken auf der Schnittstelle klicken Sie auf **Monitor > Schnittstellenstatus**. Zum Überwachen der Datenquellen und Protokolle mit dem stärksten Kommunikationsaufkommen klicken Sie auf **Monitor > Datenverkehrsstatus > Wichtigste N Datenverkehrsflüsse**.

NBAR

Für den Einsatz von NBAR (Network-based application recognition) auf der Schnittstelle aktivieren Sie das Kontrollkästchen **NBAR-Protokoll**.

Zum Überwachen von NBAR-Statistiken zu der Schnittstelle klicken Sie auf **Monitor > Datenverkehrsstatus > Anwendung/Datenverkehrsprotokoll (NBAR)**.

Allgemein

Dieses Fenster zeigt allgemeine Sicherheitseinstellungen an und ermöglicht Ihnen das Aktivieren oder Deaktivieren dieser Einstellungen über das Kontrollkästchen neben dem Namen und der Beschreibung. Wenn Sie für die Funktion **Sicherheitsprüfung** das Deaktivieren bestimmter Eigenschaften zugelassen haben und Sie diese wieder aktivieren möchten, können Sie sie in diesem Fenster erneut aktivieren. Es folgen die Eigenschaften, die in diesem Fenster enthalten sind.

Beschreibung

In diesem Feld können Sie eine kurze Beschreibung der Schnittstellenkonfiguration eingeben. Diese Beschreibung wird im Fenster Schnittstelle und Verbindungen bearbeiten angezeigt. Eine Beschreibung wie „Kontozuordnung“ oder „Test Netz 5“ hilft anderen Cisco SDM-Benutzern, den Zweck der Konfiguration zu verstehen.

IP Directed Broadcasts

Ein IP Directed Broadcast ist ein Datagramm, das an die Broadcast-Adresse eines Subnetzes gesendet wird, an welches das Absendergerät nicht direkt angeschlossen ist. Das Directed Broadcast wird als Unicast-Paket durch das Netzwerk geleitet, bis es am Ziel-Subnetz eintrifft. Dort wird es in ein Link-Layer Broadcast konvertiert. Aufgrund der Eigenschaften der IP-Adressierungsarchitektur kann nur der letzte Router in der Kette, derjenige, der direkt an das Ziel-Subnetz angeschlossen ist, ein Directed Broadcast endgültig identifizieren. Directed Broadcasts werden ab und zu für legale Zwecke verwendet; diese Verwendung ist außerhalb der Finanzdienstleistungsbranche jedoch nicht üblich.

IP Directed Broadcasts werden im extrem häufigen und beliebten Denial-of-Service-Angriff „Smurf“ verwendet und können auch für ähnliche Angriffe eingesetzt werden. Bei einem Smurf-Angriff sendet der Hacker eine ICMP-Echoanforderung von einer gefälschten Quelladresse an eine Directed Broadcast-Adresse. Daraufhin senden alle Hosts im Ziel-Subnetz Antworten an die gefälschte Quelle. Durch das Senden eines fortlaufenden Stroms solcher Anforderungen ist der Hacker in der Lage, einen viel größeren Antwortstrom zu erzeugen, der den Host, dessen Adresse gefälscht wird, vollständig überschwemmen kann.

Wenn IP Directed Broadcasts deaktiviert werden, werden Directed Broadcasts, die anderenfalls an dieser Schnittstelle explosionsartig in Link-Layer Broadcasts konvertiert würden, stattdessen geschlossen.

IP Proxy Arp

ARP wird vom Netzwerk verwendet, um IP-Adressen in MAC-Adressen zu konvertieren. Normalerweise ist ARP auf ein einzelnes LAN beschränkt, ein Router kann jedoch als Proxy für ARP-Anfragen dienen, sodass ARP-Anfragen über mehrere LAN-Segmente hinweg verfügbar sind. Da Proxy ARP die LAN-Sicherheitsbarriere durchbricht, sollte es nur zwischen zwei LANs mit gleicher Sicherheitsstufe und nur wenn nötig verwendet werden.

IP route-cache flow

Diese Option aktiviert die Cisco IOS Netflow-Funktion. Mit Netflow können Sie die Paketverteilung, die Protokollverteilung und aktuelle Datenströme im Router bestimmen. Diese Informationen sind für bestimmte Aufgaben sehr wertvoll, wie zum Beispiel bei der Suche nach der Quelle von IP-Adressen-Spoofing-Attacken.

Hinweis Mit der Option IP Route Cache-Flow wird Netflow sowohl für den eingehenden als auch für den ausgehenden Datenverkehr aktiviert. Zum Aktivieren von Netflow auf dem eingehenden *oder* ausgehenden Datenverkehr stellen Sie die Netflow-Optionen entsprechend ein, die auf der Registerkarte **Anwendungsdienst** zu finden sind.

IP Redirects

ICMP-Weiterleitungsmeldungen weisen einen Endknoten an, einen speziellen Router als Teil seines Pfads zu einem bestimmten Ziel zu verwenden. In einem ordnungsgemäß funktionierenden IP-Netzwerk sendet ein Router Weiterleitungen nur an Hosts innerhalb seiner eigenen lokalen Subnetze, kein Endknoten sendet jemals eine Weiterleitung und keine Weiterleitung wird jemals um mehr als einen Netzwerk-Hop geleitet. Ein Hacker könnte diese Regeln jedoch verletzen; einige Angriffe basieren auf diesem Prinzip. Das Deaktivieren von ICMP-Weiterleitungen hat keine Auswirkungen auf den Netzwerkbetrieb, kann jedoch Weiterleitungsattacken verhindern.

IP Mask Reply

ICMP-Maskenanforderungsmeldungen werden gesendet, wenn ein Netzwerkgerät die Subnetzmaske für ein bestimmtes Subnetzwerk im Verbundnetzwerk kennen muss. ICMP-Maskenanforderungsmeldungen werden von den Geräten, die über die gewünschten Informationen verfügen, an das Gerät gesendet, das die Informationen anfordert. Diese Meldungen können von einem Hacker verwendet werden, um in den Besitz von Netzwerkzuordnungsinformationen zu gelangen.

IP Unreachables

„Host unerreichbar“-Meldungen von ICMP werden ausgegeben, wenn ein Router ein Nonbroadcast-Paket erhält, das ein unbekanntes Protokoll verwendet, oder wenn der Router ein Paket empfängt, das er nicht an das Endziel ausliefern kann, da ihm keine Route zur Zieladresse bekannt ist. Diese Meldungen können von einem Hacker verwendet werden, um in den Besitz von Netzwerkzuordnungsinformationen zu gelangen.

Ethernet-Konfigurationstyp auswählen

Dieses Fenster wird angezeigt, wenn Sie auf eine Schnittstelle im Fenster **Schnittstellen und Verbindungen** klicken und Cisco SDM nicht ermitteln kann, ob die Schnittstelle als LAN-Schnittstelle oder als WAN-Schnittstelle konfiguriert ist. Wenn Sie eine Schnittstelle unter Verwendung von Cisco SDM konfigurieren, können Sie diese als innere oder äußere Schnittstelle angeben, und Cisco SDM fügt entsprechend Ihrer Angabe einen beschreibenden Kommentar zur Konfigurationsdatei hinzu. Wenn Sie eine Schnittstelle mit der Befehlszeilenschnittstelle (Command Line Interface, CLI) konfigurieren, enthält die Konfiguration nicht diesen beschreibenden Kommentar, und Cisco SDM verfügt nicht über diese Informationen.

So geben Sie an, dass es sich bei der Schnittstelle um eine LAN-Schnittstelle handelt:

Klicken Sie auf **LAN** und anschließend auf **OK**. Cisco SDM fügt die Befehlszeile $ETH-LAN$ zur Konfiguration der Schnittstelle hinzu. Die Schnittstelle erscheint im Fenster des LAN-Assistenten und wird mit der Angabe **Innen** im Fenster **Schnittstellen und Verbindungen** angezeigt.

So geben Sie an, dass es sich bei der Schnittstelle um eine WAN-Schnittstelle handelt:

Klicken Sie auf **WAN** und anschließend auf **OK**. Cisco SDM fügt die Befehlszeile $ETH-WAN$ zur Konfiguration der Schnittstelle hinzu. Die Schnittstelle erscheint im Fenster des WAN-Assistenten und wird mit der Angabe **Außen** im Fenster **Schnittstellen und Verbindungen** angezeigt.

Verbindung: VLAN

In diesem Fenster können Sie eine neue VLAN-Schnittstelle konfigurieren.

VLAN ID

Geben Sie die ID-Nummer der neuen VLAN-Schnittstelle ein. Während Sie eine VLAN-Schnittstelle bearbeiten, können Sie die VLAN-ID nicht ändern.

Kontrollkästchen Natives VLAN

Überprüfen Sie, ob dieses VLAN kein Kabelkanal VLAN ist.

IP-Adressfelder

IP-Adressentyp

Legen Sie fest, ob die VLAN-Schnittstelle über eine statische IP-Adresse oder über keine IP-Adresse verfügen soll. Dieses Feld ist sichtbar, wenn im Feld **Konfigurieren als** die Option **Nur VLAN** ausgewählt ist.

IP-Adresse

Geben Sie die IP-Adresse der VLAN-Schnittstelle ein.

Subnetzmaske

Geben Sie die Subnetzmaske der VLAN-Schnittstelle ein, oder geben Sie die Anzahl der Subnet-Bits über das Scroll-Feld an.

DHCP Relay

Weitere Informationen erhalten Sie, wenn Sie auf DHCP-Relay klicken.

Subschnittstellenliste

In diesem Fenster werden die von Ihnen ausgewählten Subschnittstellen angezeigt, die für die Schnittstelle konfiguriert wurden. Für jede konfigurierte Subschnittstelle werden im Fenster die Subschnittstellen-ID, die VLAN-ID, die IP-Adresse und –Maske und eine Beschreibung über eingetragene Subschnittstellen angezeigt. Besitzt der Router zum Beispiel die Schnittstelle FastEthernet 1 und die Subschnittstellen FastEthernet1.3 und FastEthernet1.5 sind konfiguriert, kann Folgendes in diesem Fenster angezeigt werden:

```
5       56      56.8.1.1/255.255.255.0
3       67      Brücke Nr. 77
```

In diesem Beispiel ist FastEthernet1.5 für das Routing konfiguriert und FastEthernet1.3 für IRB.

Hinweis Sie müssen eine physische Schnittstelle auswählen, bei der die Subschnittstellen konfiguriert werden, um das Fenster anzuzeigen. Im beschriebenen Beispiel müssten Sie dazu ein FastEthernet 1 auswählen, um das Fenster anzuzeigen. Wenn Sie FastEthernet1.3 oder FastEthernet1.5 auswählen und auf Bearbeiten klicken, zeigen Sie den Bearbeitungsdialog mit den Informationen über diese Schnittstelle an.

Tasten Hinzufügen, Bearbeiten und Löschen

Benutzen Sie diese Tasten, um Subschnittstellen von der ausgewählten physischen Schnittstelle zu erstellen, zu bearbeiten und zu löschen.

Add or Edit BVI Interface (BVI-Schnittstelle hinzufügen oder bearbeiten)

In diesem Fenster können Sie eine virtuelle Schnittstelle der Bridge-Gruppe (BVI) hinzufügen oder bearbeiten. Wenn Ihr Router über eine Dot11Radio-Schnittstelle verfügt, wird automatisch eine BVI-Schnittstelle erstellt, wenn Sie eine neue Bridge-Gruppe konfigurieren. Das geschieht, damit IRB-Bridging unterstützt wird. In diesem Fenster können Sie die IP-Adresse und die Subnetzmaske ändern.

IP-Adresse/Subnetzmaske

Geben Sie die IP-Adresse und die Subnetzmaske ein, die Sie der BVI zuweisen möchten.

Loopback-Schnittstelle hinzufügen oder bearbeiten

In diesem Fenster können Sie eine Loopback-Schnittstelle zur ausgewählten Schnittstelle hinzufügen.

IP-Adresse

Legen Sie fest, ob die Loopback-Schnittstelle über keine IP-Adresse oder über eine statische IP-Adresse verfügen soll.

Statische IP-Adresse

Wenn Sie **Statische IP-Adresse** auswählen, geben Sie die IP-Adresse in dieses Feld ein.

Subnetzmaske

Geben Sie die Subnetzmaske in dieses Feld ein, oder wählen Sie die Anzahl der Subnet-Bits aus dem Feld auf der rechten Seite aus. Die Subnetzmaske zeigt dem Router, welche Bits der IP-Adresse für die Netzwerkadresse und welche Bits für die Hostadresse bestimmt sind.

Verbindung: Virtuelle Vorlagenschnittstelle

Sie können eine VTI als Teile einer 802.1x- oder VPN-Konfiguration hinzufügen oder bearbeiten. Wenn Sie eine VTI bearbeiten, werden die Felder, die Sie bearbeiten können, auf der Registerkarte **Verbindung** angezeigt.

Schnittstellentyp

Wählen Sie entweder **Standard** oder **Tunnel**. Wenn Sie Tunnel wählen, müssen Sie auch einen Tunnelmodus auswählen.

IP-Adresse

Wählen Sie **Keine Nummerierung**. Die VTI verwendet die IP-Adresse der physischen Schnittstelle, die im Feld **Keine Nummerierung für** ausgewählt ist.

Keine Nummerierung für

Dieses Feld wird angezeigt, wenn Sie **Keine Nummerierung für** im Feld **IP-Adresse** ausgewählt haben. Wählen Sie die Schnittstelle aus, deren IP-Adresse diese VTI verwenden soll.

Tunnelmodus

Wählen Sie **IPSec-IPv4**.

Verbindung: Ethernet LAN

Verwenden Sie dieses Fenster, um die Eigenschaften der IP-Adresse und von DHCP einer Ethernet-Schnittstelle zu konfigurieren, die Sie als LAN-Schnittstelle verwenden möchten.

IP-Adresse

Geben Sie die IP-Adresse für diese Schnittstelle ein. Den IP-Adressenwert erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Diesen Wert erhalten Sie von Ihrem Netzwerkadministrator. Mit der Subnetzmaske kann der Router ermitteln, welcher Anteil der IP-Adresse zur Definition des Netzwerks und welcher Anteil für das Subnetz verwendet wird.

DHCP-Relay

Klicken Sie darauf, damit der Router als DHCP-Relay fungiert. Ein Gerät, das als DHCP-Relay fungiert, leitet DHCP-Anforderungen an einen DHCP-Server weiter. Wenn einem Gerät eine IP-Adresse dynamisch zugeordnet werden muss, wird eine Broadcast-Übertragung einer DHCP-Anforderung durchgeführt. Ein DHCP-Server antwortet auf diese Anforderung mit einer IP-Adresse. In einem Subnetzwerk darf nicht mehr als 1 DHCP-Relay oder 1 DHCP-Server vorhanden sein.

Hinweis Wenn der Router als DHCP-Relay-Server mit mehr als einer Remote-DHCP-Server-IP-Adresse konfiguriert ist, ist diese Schaltfläche deaktiviert.

IP-Adresse des Remote-DHCP-Servers

Geben Sie nach dem Klicken auf **DHCP-Relay** die IP-Adresse des DHCP-Servers ein, von dem die Geräte im LAN ihre Adressen beziehen.

Verbindung: Ethernet WAN

In diesem Fenster können Sie eine Ethernet-WAN-Verbindung hinzufügen.

Aktivieren der PPPoE-Kapselung

Klicken Sie auf diese Option, wenn die Verbindung eine Point-to-Point Protocol over Ethernet (PPPoE)-Kapselung verwenden muss. Ihr Service-Provider informiert Sie darüber, ob die Verbindung PPPoE verwendet. Wenn Sie eine PPPoE-Verbindung konfigurieren, wird automatisch eine Dialer-Schnittstelle erstellt.

IP-Adresse

Wählen Sie einen der folgenden IP-Adressentypen aus, und geben Sie die Informationen in die angezeigten Felder ein. Wenn die Ethernet-Verbindung nicht PPPoE verwendet, werden nur die Optionen **Statische IP-Adresse** und **Dynamisch** angezeigt.

Statische IP-Adresse

Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamisch (DHCP-Client)

Wenn Sie **Dynamisch** wählen, fordert der Router bei einem Remote-DHCP-Server eine IP-Adresse an. Geben Sie den Namen des DHCP-Servers ein, von dem Adressen geleast werden können.

Keine IP-Nummerierung

Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie dann die Schnittstelle aus, für deren IP-Adresse Sie die Schnittstelle teilen müssen.

Easy IP (IP ausgehandelt)

Wählen Sie **Easy IP (IP ausgehandelt)**, wenn der Router über die Adressenaushandlung Point-to-Point-Protocol/IP Control-Protocol (PPP/IPCP) eine IP-Adresse anfordern soll.

Authentifizierung

Klicken Sie hier, um die Kennwortangaben für die CHAP/PAP-Authentifizierung einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Ethernet-Eigenschaften)

Über dieses Fenster können Sie Eigenschaften für einen Ethernet-WAN-Link konfigurieren.

Aktivieren der PPPoE-Kapselung

Klicken Sie auf **PPPoE-Kapselung aktivieren**, wenn Ihr Service-Provider Sie dazu auffordert. PPPoE gibt die Point-to-Point-Protocol over Ethernet-Kapselung an.

IP-Adresse

Statische IP-Adresse

Verfügbar für PPPoE-Kapselung und ohne Kapselung. Wenn Sie **statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse und Subnetzmaske oder die Netzwerkbits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamisch (DHCP-Client)

Verfügbar für PPPoE-Kapselung und ohne Kapselung. Wenn Sie **Dynamisch** wählen, fordert der Router bei einem Remote-DHCP-Server eine IP-Adresse an. Geben Sie den Namen des DHCP-Servers ein, der die Adressen zuweisen soll.

Keine IP-Nummerierung

Verfügbar für PPPoE-Kapselung. Wählen Sie **Keine IP-Nummerierung**, wenn Sie möchten, dass die Schnittstelle eine IP-Adresse, die bereits einer anderen Schnittstelle zugewiesen ist, mit dieser Schnittstelle gemeinsam nutzt. Wählen Sie dann die Schnittstelle aus, für deren IP-Adresse Sie die Schnittstelle teilen müssen.

Easy IP (IP ausgehandelt)

Verfügbar für PPPoE-Kapselung. Wählen Sie die Option **Easy IP (IP ausgehandelt)**, wenn der Router nach der PPP/IPCP-Adressenaushandlung eine IP-Adresse erhält.

Authentifizierung

Klicken Sie hier, um die Kennwortangaben für die CHAP/PAP-Authentifizierung einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Ethernet with No Encapsulation (Ethernet ohne Kapselung)

Verwenden Sie dieses Fenster, um eine Ethernet-Verbindung ohne Kapselung zu konfigurieren.

IP-Adresse

Legen Sie fest, wie der Router eine IP-Adresse für diesen Link erhalten soll.

- **Statische IP-Adresse** – Wenn Sie **Statische IP-Adresse** wählen, geben Sie die IP-Adresse und die Subnetzmaske oder die Netzwerk-Bits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.
- **Dynamische IP-Adresse** – Wenn Sie **Dynamisch** wählen, weist der Remote-DHCP-Server dem Router eine vorübergehende IP-Adresse zu. Geben Sie anschließend den Namen oder die IP-Adresse des DHCP-Servers ein.

Hostname

Wenn Ihr Service-Provider einen Hostnamen für den Router in die DHCP-Antwort einfügt, die eine dynamische IP-Adresse enthält, können Sie diesen Namen zu Informationszwecken in dieses Feld eingeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: ADSL

In diesem Fenster können Sie Eigenschaften eines PPPoE-Links, der von einer ADSL-Verbindung unterstützt wird, angeben oder bearbeiten.

Kapselung

Wählen Sie den Kapselungstyp aus, der für diesen Link verwendet wird.

- PPPoE gibt die Point-to-Point Protocol over Ethernet-Kapselung an.
- PPPoA gibt die Point-to-Point Protocol over ATM-Kapselung an.
- RFC 1483-Routing (**AAL5 SNAP**) gibt an, dass jede PVC-Verbindung mehrere Protokolle transportieren kann.
- RFC 1483-Routing (**AAL5 MUX**) gibt an, dass jede PVC-Verbindung nur einen Protokolltyp transportieren kann.

Wenn Sie eine Verbindung bearbeiten, wird die Kapselung angezeigt; diese kann jedoch nicht bearbeitet werden. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Weitere Informationen über diese Kapselungstypen finden Sie unter Kapselung.

Virtual Path Identifier

Der Virtual Path Identifier (VPI) wird beim ATM-Switching und -Routing zur Identifizierung des Pfads verwendet, der für verschiedene Verbindungen verwendet wird. Geben Sie den VPI-Wert ein, den Sie von Ihrem Service-Provider erhalten haben.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

Virtual Circuit Identifier

Der Virtual Circuit Identifier (VCI) wird beim ATM-Switching und -Routing zur Identifizierung einer bestimmten Verbindung innerhalb eines Pfads verwendet, der gemeinsam mit ihrer Verbindung mit anderen Verbindungen verwendet werden kann. Geben Sie den VCI-Wert ein, den Sie von Ihrem Service-Provider erhalten haben.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

IP-Adresse

Legen Sie fest, wie der Router eine IP-Adresse für diesen Link erhalten soll.

- **Statische IP-Adresse** – Wenn Sie **Statische IP-Adresse** wählen, geben Sie die IP-Adresse und die Subnetzmaske oder die Netzwerk-Bits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.
- **Dynamische IP-Adresse** – Wenn Sie **Dynamisch** wählen, weist der Remote-DHCP-Server dem Router eine vorübergehende IP-Adresse zu. Geben Sie anschließend den Namen oder die IP-Adresse des DHCP-Servers ein.
- **Keine IP-Nummerierung** – Wählen Sie diese Option, wenn eine IP-Adresse, die bereits von einer anderen Schnittstelle genutzt wird, auch für dies Schnittstelle verwendet werden soll. Wählen Sie dann die Schnittstelle aus, für deren IP-Adresse Sie die Schnittstelle teilen müssen.
- IP ausgehandelt – Diese Schnittstelle bezieht eine IP-Adresse über die Adressenaushandlung PPP/IP Control Protocol (IPCP).

Hostname

Wenn Ihr Service-Provider einen Hostnamen für DHCP-Option 12 bereitgestellt hat, geben Sie diesen hier ein.

Betriebsmodus

Wählen Sie einen der folgenden Werte aus:

- **auto** – Nach der automatischen Aushandlung der Kommunikationsparameter mit dem DSLAM (Digital Subscriber Access Line Multiplexer) in der Vermittlungsstelle wird die ADSL-Leitung (Asymmetric Digital Subscriber Line) entsprechend konfiguriert.
- **ansi-dmt** – Konfigurieren Sie die ADSL-Leitung für den Trainingsvorgang (Synchronisierung) des ANSI T1.413 Issue 2-Modus.
- **itu-dmt** – Die ADSL-Leitungsparameter werden gemäß ITU-Protokoll G992.1 konfiguriert.
- **adls2** – Zur Konfiguration der ADSL-Leitungsparameter wird das ITU-Protokoll G.992.3 herangezogen. Dieser Modus steht für HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, und HWIC-1ADSLI ADSL Netzwerkmodule zur Verfügung.
- **adsl2+** – Zur Konfiguration der ADSL-Leitung wird das ITU-Protokoll G.992.4 eingesetzt. Dieser Modus steht für HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, und HWIC-1ADSLI ADSL Netzwerkmodule zur Verfügung.
- **splitterless** – Konfigurieren Sie die ADSL-Leitung für den Trainingsvorgang (Synchronisierung) des G.Lite-Modus. Dieser Modus steht für ältere ADSL Netzwerkmodule wie zum Beispiel WIC-1ADSL zur Verfügung.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Multilink-PPP aktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn auf dieser Schnittstelle das Multilink-PPP-Protokoll (Multilink Point-to-Point) nutzen möchten. Mit MLP kann die Leistung eines Netzwerks mit mehreren WAN-Verbindungen durch Lastausgleichsfunktionen, Paketfragmentierung, bedarfsabhängige Bandbreitenreservierung und andere Funktionen verbessert werden.

Verbindung: ADSL over ISDN

Fügen Sie eine ADSL over ISDN-Verbindung über dieses Fenster hinzu bzw. bearbeiten Sie diese in diesem Fenster.

Kapselung

Wählen Sie den Kapselungstyp für diesen Link aus.

- **PPPoE** gibt die Point-to-Point Protocol over Ethernet-Kapselung an.
- **RFC 1483-Routing** (**AAL5 SNAP**) gibt an, dass jede PVC-Verbindung mehrere Protokolle übertragen kann.
- **RFC 1483-Routing** (**AAL5 MUX**) gibt an, dass jede PVC-Verbindung nur einen Protokolltyp transportieren kann.

Wenn Sie eine Verbindung bearbeiten, wird die Kapselung angezeigt; diese kann jedoch nicht bearbeitet werden. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Virtual Path Identifier

Der Virtual Path Identifier (VPI) wird beim ATM-Switching und -Routing zur Identifizierung des Pfads verwendet, der für verschiedene Verbindungen verwendet wird. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

Virtual Circuit Identifier

Der Virtual Circuit Identifier (VCI) wird beim ATM-Switching und -Routing zur Identifizierung einer bestimmten Verbindung innerhalb eines Pfads verwendet, der gemeinsam mit ihrer Verbindung mit anderen Verbindungen verwendet werden kann. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

IP-Adresse

Legen Sie fest, wie der Router eine IP-Adresse für diesen Link erhalten soll.

- **Statische IP-Adresse** – Wenn Sie **Statische IP-Adresse** wählen, geben Sie die IP-Adresse und die Subnetzmaske oder die Netzwerk-Bits in die entsprechenden Felder ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.
- **Dynamische IP-Adresse** – Wenn Sie **Dynamisch** wählen, weist der Remote-DHCP-Server dem Router eine vorübergehende IP-Adresse zu. Geben Sie anschließend den Namen oder die IP-Adresse des DHCP-Servers ein.
- **Keine IP-Nummerierung** – Wählen Sie diese Option, wenn eine IP-Adresse, die bereits von einer anderen Schnittstelle genutzt wird, auch für dies Schnittstelle verwendet werden soll. Wählen Sie dann die Schnittstelle aus, für deren IP-Adresse Sie die Schnittstelle teilen müssen.
- IP ausgehandelt – Diese Schnittstelle bezieht eine IP-Adresse über die Adressenaushandlung PPP/IP Control Protocol (IPCP).

Betriebsmodus

Bestimmen Sie, in welchem Modus die ADSL-Leitung beim Training arbeiten soll.

Hinweis Wenn die Cisco IOS-Version, die auf dem Router ausgeführt wird, nicht alle fünf Betriebsmodi unterstützt, werden nur die von Ihrer Cisco IOS-Version unterstützten Betriebsmodi angezeigt.

- **annexb** – Standard-Annex-B-Modus von ITU-T G.992.1
- **annexb-ur2** – ITU-T G.992.1 Annex-B-Modus
- **auto** – Nach der automatischen Aushandlung der Kommunikationsparameter mit dem DSLAM (Digital Subscriber Access Line Multiplexer) in der Vermittlungsstelle wird die ADSL-Leitung (Asymmetric Digital Subscriber Line) entsprechend konfiguriert.
- **etsi** – Modus des European Telecommunications Standards Institute
- **multimode** – Ein Modus, den die Firmware zur Schaffung optimaler Betriebsbedingungen auf der DSL-Leitung (Digital Subscriber Line) einstellt. Je nach aktueller DSLAM-Einstellung kann es sich bei dem endgültigen Modus entweder um ETSI oder um den Annex-B-Standard handeln.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.
- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.
- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Multilink-PPP aktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn auf dieser Schnittstelle das Multilink-PPP-Protokoll (Multilink Point-to-Point) nutzen möchten. Mit MLP kann die Leistung eines Netzwerks mit mehreren WAN-Verbindungen durch Lastausgleichsfunktionen, Paketfragmentierung, bedarfsabhängige Bandbreitenreservierung und andere Funktionen verbessert werden.

Verbindung: G.SHDSL

In diesem Fenster können Sie eine G.SHDSL-Verbindung erstellen oder bearbeiten.

Hinweis Wenn die Verbindung, die Sie konfigurieren wollen, mit einer DSL Steuerung arbeitet, erscheinen die Felder Ausrüstungstyp und Betriebsmodus nicht im Dialog.

Kapselung

Wählen Sie den Kapselungstyp aus, der für diesen Link verwendet wird.

- **PPPoE** gibt die Point-to-Point Protocol over Ethernet-Kapselung an.
- **PPPoA** gibt die Point-to-Point Protocol over ATM-Kapselung an.
- **RFC 1483-Routing** (**AAL5 SNAP**) gibt an, dass jede PVC-Verbindung mehrere Protokolle übertragen kann.
- **RFC 1483-Routing** (**AAL5 MUX**) gibt an, dass jede PVC-Verbindung nur einen Protokolltyp transportieren kann.

Wenn Sie eine Verbindung bearbeiten, wird die Kapselung angezeigt; diese kann jedoch nicht bearbeitet werden. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Weitere Informationen über diese Kapselungstypen finden Sie unter Kapselung.

Virtual Path Identifier

Der Virtual Path Identifier (VPI) wird beim ATM-Switching und -Routing zur Identifizierung des Pfads verwendet, der für verschiedene Verbindungen verwendet wird. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

Virtual Circuit Identifier

Der Virtual Circuit Identifier (VCI) wird beim ATM-Switching und -Routing zur Identifizierung einer bestimmten Verbindung innerhalb eines Pfads verwendet, der gemeinsam mit ihrer Verbindung mit anderen Verbindungen verwendet werden kann. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

IP-Adresse

Legen Sie fest, wie der Router eine IP-Adresse für diesen Link beziehen soll. Diese Felder, die in diesem Bereich angezeigt werden, ändern sich je nach dem ausgewählten Kapselungstyp. Fragen Sie Ihren Service-Provider oder Netzwerkadministrator nach der Methode, die der Router für den Erhalt einer IP-Adresse verwenden soll.

Statische IP-Adresse

Wenn Sie **Statische IP-Adresse** wählen, geben Sie die für die Schnittstelle bestimmte IP-Adresse und die Subnetzmaske oder die Netzwerk-Bits ein. Die entsprechenden Informationen erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamische IP-Adresse

Wenn Sie eine Dynamische IP-Adresse wählen, erhält die Schnittstelle eine IP-Adresse von einem DHCP-Server im Netzwerk. Wenn der DHCP-Server die DHCP-Option 12 verwendet, übergibt er zusammen mit der vorgesehenen IP-Adresse einen Hostnamen an den Router. Wenden Sie sich an Ihren Service-Provider oder Netzwerkadministrator, um zu ermitteln, welcher Hostname übermittelt wird.

Keine IP-Nummerierung

Wählen Sie diese Option aus, wenn die Schnittstelle eine IP-Adresse gemeinsam mit einer Ethernet-Schnittstelle im Router verwenden soll. Wenn Sie diese Option auswählen, müssen Sie aus der Dropdown-Liste die Ethernet-Schnittstelle auswählen, deren Adresse Sie verwenden möchten.

IP-Adresse für Remote-Verbindung in Hauptbüro

Geben Sie die IP-Adresse des Gateway-Systems an, zu dem eine Verbindung für diesen Link hergestellt werden soll. Diese IP-Adresse erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator. Das Gateway ist das System, zu dem der Router eine Verbindung herstellen muss, um Zugriff auf das Internet oder auf das WAN Ihrer Organisation zu erhalten.

Gerätetyp

Wählen Sie einen der folgenden Werte aus:

CPE

Customer Premises Equipment – Teilnehmer-Endgerät. Wenn es sich beim Kapselungstyp um PPPoE handelt, wird CPE automatisch ausgewählt, und das Feld ist deaktiviert.

CO

Central Office – Hauptbüro.

Betriebsmodus

Wählen Sie einen der folgenden Werte aus:

Annex A (US-Signalisierung)

Konfiguriert die regionalen Betriebsparameter für Nordamerika.

Annex B (europäische Signalisierung)

Konfiguriert die regionalen Betriebsparameter für Europa.

Multilink-PPP aktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn auf dieser Schnittstelle das Multilink-PPP-Protokoll (Multilink Point-to-Point) nutzen möchten. Mit MLP kann die Leistung eines Netzwerks mit mehreren WAN-Verbindungen durch Lastausgleichsfunktionen, Paketfragmentierung, bedarfsabhängige Bandbreitenreservierung und andere Funktionen verbessert werden.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

DSL-Controller konfigurieren

Cisco SDM unterstützt die Konfiguration der Cisco WIC-1SHDSL-V2. Diese WAN-Schnittstellenkarte (WAN Interface Card, WIC) unterstützt TI, E1 oder eine G.SHDSL-Verbindung über eine ATM-Schnittstelle. Cisco SDM unterstützt nur eine G.SHDSL-Verbindung, welche die ATM-Schnittstelle verwendet. In diesem Fenster können Sie den Controller-Modus in der WIC auf ATM einstellen und so eine G.SHDSL-Verbindung aktivieren. Darüber hinaus können Sie Informationen zum DSL-Controller für die G.SHDSL-Verbindung erstellen oder bearbeiten.

Controller-Modus

Cisco SDM unterstützt in diesem Controller nur den ATM-Modus, der eine G.SHDSL-Verbindung bereitstellt. Dieses Feld wird automatisch auf den ATM-Modus eingestellt, wenn Sie auf die Schaltfläche **OK** klicken.

Gerätetyp

Bestimmten Sie, ob Ihre Verbindung direkt bei der Vermittlungsstelle oder bei der Anlage am Kundenstandort endet.

Betriebsmodus

Wählen Sie aus, ob die DSL-Verbindung die Annex A-Signalisierung (für DSL-Verbindungen in die Vereinigten Staaten) oder Annex B-Signalisierung (für DSL-Verbindungen in Europa) verwenden soll.

Leitungsmodus

Legen Sie fest, ob es sich um eine 2-Draht- oder 4-Draht-G.SHDSL-Verbindung handelt.

Leitungsnummer

Wählen Sie die Nummer der Schnittstelle für die Verbindung aus.

Übertragungsrate der Leitung

Legen Sie die DSL-Leitungsgeschwindigkeit für den G.SHDSL-Port fest. Wenn Sie eine 2-Draht-Verbindung ausgewählt haben, können Sie entweder **auto** wählen, wodurch die Schnittstelle so konfiguriert wird, dass die Übertragungsgeschwindigkeit zwischen dem G.SHDSL-Port und dem DSLAM automatisch ausgehandelt wird, oder Sie stellen die tatsächliche DSL-Leitungsgeschwindigkeit ein. Die unterstützten Übertragungsraten sind 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056 und 2312.

Wenn Sie eine 4-Draht-Verbindung ausgewählt haben, müssen Sie eine feste Leitungsgeschwindigkeit einstellen. Die unterstützten Leitungsraten für eine 4-Draht-Verbindung sind 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480 und 4608

Hinweis Wenn an gegenüberliegenden Enden des DSL-Uplinks verschiedene Übertragungsraten der DSL-Leitungen konfiguriert sind, entspricht die tatsächliche Übertragungsrate immer der niedrigeren Rate.

Ton-Rauschen-Verhältnis aktivieren

Der Wert für das Ton-Rauschen-Verhältnis bietet dem Modem einen Schwellenwert, das so ermitteln kann, ob es seine Leistung entsprechend dem in der Verbindung auftretenden Rauschen erhöhen oder reduzieren soll. Wenn Sie die Übertragungsrate der Leitung auf *auto* eingestellt haben, können Sie diese Funktion aktivieren, um die größtmögliche Qualität für die DSL-Verbindung zu erreichen. Beachten Sie, dass Sie diese Funktion nicht verwenden können, wenn die Übertragungsrate nicht flexibel ist. Um die Option Ton-Rauschen-Verhältnis aktivieren zu aktivieren, markieren Sie dieses Kontrollkästchen und wählen die Verhältnisgrenzen in den Feldern Aktuell und Snext aus. Um diese Funktion zu deaktivieren, nehmen Sie den Eintrag aus dem Prüffeld.

Aktuell

Geben Sie für die aktuelle Verbindung den Rauschabstand in Dezibel (dB) an. Je niedriger Sie hier das Verhältnis festlegen, desto mehr Rauschen wird in der Verbindung toleriert. Je niedriger der dB-Wert ist, desto mehr Störsignale lässt das DSL-Modem auf der Leitung zu, was möglicherweise zu einer schlechteren Verbindungsqualität, aber zu einem höheren Durchsatz führen kann. Bei einem höheren dB-Wert unterdrückt das Modem stärker die Störsignale, was möglicherweise zu einer höheren Verbindungsqualität, jedoch zu einem geringeren Durchsatz führen kann.

Snext

Legen Sie das Self Near End Cross Talk-(Snext-)Ton-Rauschen-Verhältnis in Dezibel fest.

DSL-Verbindungen

Dieses Feld zeigt alle G.SHDSL-Verbindungen an, die derzeit in diesem Controller konfiguriert sind. Um eine neue G.SHDSL-Verbindung zu konfigurieren, klicken Sie auf **Hinzufügen**. Dadurch wird die Seite G.SHDSL-Verbindung hinzufügen angezeigt, über die Sie die neue Verbindung konfigurieren können. Um eine bestehende G.SHDSL-Verbindung zu konfigurieren, wählen Sie die Verbindung in diesem Feld aus, und klicken Sie auf **Bearbeiten**. Dadurch wird ebenfalls die Seite G.SHDSL-Verbindung hinzufügen angezeigt, über die Sie die Verbindungskonfiguration bearbeiten können. Um eine Verbindung zu löschen, wählen Sie die Verbindung in diesem Feld aus, und klicken Sie auf **Löschen**.

G.SHDSL-Verbindung hinzufügen

In diesem Fenster können Sie eine G.SHDSL-Verbindung erstellen oder bearbeiten.

Kapselung

Wählen Sie den Kapselungstyp aus, der für diesen Link verwendet wird.

- **PPPoE** gibt die Point-to-Point Protocol over Ethernet-Kapselung an.
- **PPPoA** gibt die Point-to-Point Protocol over ATM-Kapselung an.
- **RFC 1483-Routing** (**AAL5 SNAP**) gibt an, dass jede PVC-Verbindung mehrere Protokolle übertragen kann.
- **RFC 1483-Routing** (**AAL5 MUX**) gibt an, dass jede PVC-Verbindung nur einen Protokolltyp übertragen kann.

Wenn Sie eine Verbindung bearbeiten, wird die Kapselung angezeigt; diese kann jedoch nicht bearbeitet werden. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Virtual Path Identifier

Der Virtual Path Identifier (VPI) wird beim ATM-Switching und -Routing zur Identifizierung des Pfads verwendet, der für verschiedene Verbindungen verwendet wird. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Werts wieder her.

Virtual Circuit Identifier

Der Virtual Circuit Identifier (VCI) wird beim ATM-Switching und -Routing zur Identifizierung einer bestimmten Verbindung innerhalb eines Pfads verwendet, der gemeinsam mit anderen Verbindungen verwendet werden kann. Diesen Wert erhalten Sie von Ihrem Service-Provider.

Wenn Sie eine bestehende Verbindung bearbeiten, ist dieses Feld deaktiviert. Wenn Sie diesen Wert ändern müssen, löschen Sie die Verbindung, und stellen Sie sie wieder unter Verwendung des erforderlichen Werts her.

IP-Adresse

Wählen Sie aus, wie der Router eine IP-Adresse für diesen Link erhalten soll. Diese Felder, die in diesem Bereich angezeigt werden, ändern sich je nach dem ausgewählten Kapselungstyp. Fragen Sie Ihren Service-Provider oder Netzwerkadministrator nach der Methode, die der Router für den Erhalt einer IP-Adresse verwenden soll.

Statische IP-Adresse

Wenn Sie **Statische IP-Adresse** wählen, geben Sie die IP-Adresse, die die Schnittstelle verwenden soll, sowie die Subnetzmaske oder die Netzwerk-Bits ein. Die entsprechenden Informationen erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Dynamische IP-Adresse

Wenn Sie eine **Dynamische IP-Adresse** wählen, erhält die Schnittstelle eine IP-Adresse von einem DHCP-Server im Netzwerk. Wenn der DHCP-Server DHCP-Option 12 verwendet, sendet er einen Hostnamen zusammen mit der zu verwendenden IP-Adresse an den Router. Wenden Sie sich an Ihren Service-Provider oder Netzwerkadministrator, um den gesendeten Hostnamen zu ermitteln.

Keine IP-Nummerierung

Wählen Sie diese Option aus, wenn die Schnittstelle eine IP-Adresse gemeinsam mit einer Ethernet-Schnittstelle im Router verwenden soll. Wenn Sie diese Option auswählen, müssen Sie die Ethernet-Schnittstelle in der Dropdown-Liste angeben, deren Adresse Sie verwenden möchten.

Beschreibung

Geben Sie für die Verbindung eine Beschreibung ein, um sie leichter erkennen und betreuen zu können.

Multilink-PPP aktivieren

Aktivieren Sie dieses Kontrollkästchen, wenn auf dieser Schnittstelle das Multilink-PPP-Protokoll (Multilink Point-to-Point) nutzen möchten. Mit MLP kann die Leistung eines Netzwerks mit mehreren WAN-Verbindungen durch Lastausgleichsfunktionen, Paketfragmentierung, bedarfsabhängige Bandbreitenreservierung und andere Funktionen verbessert werden.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Aktivieren Sie die dynamische DNS-Option, damit Ihre DNS-Server automatisch aktualisiert werden, sobald sich die IP-Adresse auf der WAN-Schnittstelle ändert.

Hinweis Diese Funktion erscheint nur, wenn sie vom IOS Ihres Cisco-Servers unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld **Dynamische DNS Methode** genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und aktivieren Sie die Verwendung einer vorhandenen Methode. Ein Fenster mit einer Liste aller vorhandenen dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Serial Interface, Frame Relay Encapsulation (Serielle Schnittstelle, Frame Relay-Kapselung)

Füllen Sie diese Felder aus, wenn Sie eine serielle Unterschnittstelle für Frame Relay-Kapselung konfigurieren. Wenn Sie eine Verbindung bearbeiten oder eine Schnittstelle im Fenster **Schnittstelle/Verbindung bearbeiten** erstellen, wird die Kapselung zwar angezeigt, sie lässt sich jedoch nicht bearbeiten. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Kapselung

Frame Relay ausgewählt.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse** oder **Keine IP-Nummerierung**.

IP-Adresse

Wenn Sie **Statische IP-Adresse** gewählt haben, geben Sie die IP-Adresse für diese Schnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Wenn Sie **Statische IP-Adresse** gewählt haben, geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Subnetz-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Geben Sie alternativ die Netzwerkbits ein, um anzugeben, zu welchem Teil die IP-Adresse die Netzwerkadresse bereitstellt.

Keine IP-Nummerierung

Wenn Sie Keine IP-Nummerierung ausgewählt haben, verwendet die Schnittstelle eine IP-Adresse gemeinsam mit einer anderen Schnittstelle, der diese IP-Adresse bereits zugewiesen wurde. Wählen Sie die Schnittstelle aus, für deren IP-Adresse die Schnittstelle geteilt werden soll.

DLCI

Geben Sie einen Data Link Connection Identifier (DLCI) in dieses Feld ein. Diese Nummer muss bei allen DLCIs, die auf dieser Schnittstelle verwendet werden, eindeutig sein. Der DLCI enthält einen eindeutigen Frame Relay-Identifier für diese Verbindung.

Wenn Sie eine bestehende Verbindung bearbeiten, wird das Feld **DLCI** deaktiviert. Wenn Sie den DLCI ändern müssen, löschen Sie die Verbindung, und stellen Sie sie wieder her.

LMI-Typ

Erkundigen Sie sich bei Ihren Service-Provider, welche der folgenden lokalen Verwaltungsschnittstellentypen (Local Management Interface, LMI) Sie verwenden sollten. Der LMI-Typ gibt das Protokoll an, dass zur Überwachung der Verbindung verwendet wird:

ANSI

Annex D, definiert vom American National Standards Institute (ANSI) Standard T1.617.

Cisco

LMI-Typ, der von Cisco zusammen mit drei anderen Unternehmen definiert wurde.

ITU-T Q.933

ITU-T Q.933 Annex A.

Autosense

Standard. Mit dieser Einstellung kann der Router ermitteln, welcher LMI-Typ durch den Switch verwendet wird und diesen Typ dann verwenden. Wenn Autosense fehlschlägt, verwendet der Router den Cisco LMI-Typ.

IETF Frame Relay-Kapselung verwenden

Aktivieren Sie dieses Kontrollkästchen, um die Internet Engineering Task Force-Kapselung (IETF) zu verwenden. Diese Option wird bei der Verbindung zu Routern von Drittherstellern verwendet. Aktivieren Sie dieses Kontrollkästchen, wenn Sie diese Schnittstelle für Verbindungen mit dem Router eines Drittanbieters verwenden.

Takteinstellungen

In den meisten Fällen sollten die Standardwerte der Takteinstellungen nicht geändert werden. Wenn Sie wissen, dass Ihre Anforderungen nicht den Standardwerten entsprechen, klicken Sie auf diese Schaltfläche, und passen Sie die neuen Takteinstellungen im angezeigten Fenster an.

Die Schaltfläche Takteinstellungen wird nur dann angezeigt, wenn Sie eine serielle T1 oder E1-Verbindung konfigurieren.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Serial Interface, PPP Encapsulation (Serielle Schnittstelle, PPP-Kapselung)

Füllen Sie diese Felder aus, wenn Sie eine serielle Schnittstelle für Point-to-Point-Protocol-Kapselung konfigurieren. Wenn Sie eine Verbindung bearbeiten oder eine Schnittstelle im Fenster **Schnittstelle/Verbindung bearbeiten** erstellen, wird die Kapselung zwar angezeigt, sie lässt sich jedoch nicht bearbeiten. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Kapselung

PPP ausgewählt.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse**, **Keine IP-Nummerierung** oder **ausgehandelt**: Wenn Sie **Keine IP-Nummerierung** auswählen, bestimmen Sie die Schnittstelle, deren IP-Adresse auch für diese Schnittstelle übernommen werden soll. Wenn Sie **IP ausgehandelt** auswählen, erhält der Router eine IP-Adresse vom Service-Provider dieser Schnittstelle. Wenn Sie **Geben Sie eine IP-Adresse an** wählen, füllen Sie die folgenden Felder aus.

IP-Adresse

Geben Sie die IP-Adresse für diese Point-to-Point-Unterschnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Netzwerk-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Geben Sie alternativ die Netzwerkbits ein, um anzugeben, wie viele Bits der IP-Adresse die Netzwerkadresse bereitstellen.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Takteinstellungen

In den meisten Fällen sollten die Standardwerte der Takteinstellungen nicht geändert werden. Wenn Sie wissen, dass Ihre Anforderungen nicht den Standardwerten entsprechen, klicken Sie auf diese Schaltfläche, und passen Sie die neuen Takteinstellungen im angezeigten Fenster an.

Die Schaltfläche Takteinstellungen wird nur dann angezeigt, wenn Sie eine serielle T1 oder E1-Verbindung konfigurieren.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Serial Interface, HDLC Encapsulation (Serielle Schnittstelle, HDLC-Kapselung)

Füllen Sie diese Felder aus, wenn Sie eine serielle Schnittstelle für die HDLC-Kapselung konfigurieren möchten. Wenn Sie eine Verbindung bearbeiten oder eine Schnittstelle im Fenster **Schnittstelle/Verbindung bearbeiten** erstellen, wird die Kapselung zwar angezeigt, sie lässt sich jedoch nicht bearbeiten. Wenn Sie den Kapselungstyp ändern müssen, löschen Sie die Verbindung, und stellen Sie sie unter Verwendung des erforderlichen Kapselungstyps wieder her.

Kapselung

HDLC ausgewählt.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse** oder **Keine IP-Nummerierung**. Wenn Sie **keine IP-Nummerierung** auswählen, bestimmen Sie die Schnittstelle, deren IP-Adresse auch für diese Schnittstelle übernommen werden soll. Wenn Sie **Statische IP-Adresse** wählen, füllen Sie die folgenden Felder aus.

IP-Adresse

Geben Sie die IP-Adresse für diese Schnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Netzwerk-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Bestimmen Sie alternativ die Anzahl an Bits, aus denen hervorgeht, aus welchem Bereich der IP-Adresse die Netzwerkadresse gewonnen wird.

Takteinstellungen

In den meisten Fällen sollten die Standardwerte der Takteinstellungen nicht geändert werden. Wenn Sie wissen, dass Ihre Anforderungen nicht den Standardwerten entsprechen, klicken Sie auf diese Schaltfläche, und passen Sie die neuen Takteinstellungen im angezeigten Fenster an.

Die Schaltfläche Takteinstellungen wird nur dann angezeigt, wenn Sie eine serielle T1 oder E1-Verbindung konfigurieren.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

GRE-Tunnelschnittstelle hinzufügen/bearbeiten

Sie können einen GRE-Tunnel zu einer Schnittstelle hinzufügen oder eine bestehende Schnittstelle über dieses Fenster bearbeiten. Dieses Fenster wird nicht angezeigt, wenn der GRE-Tunnel nicht unter Verwendung des Modus **gre ip** konfiguriert wurde.

Tunnelnummer

Geben Sie eine Nummer für diesen Tunnel ein.

Tunnelquelle

Wählen Sie die Schnittstelle aus, die der Tunnel verwenden soll. Diese Schnittstelle muss vom anderen Ende des Tunnels erreichbar sein, daher muss sie über eine öffentliche, Routing-fähige IP-Adresse verfügen.

Tunnelziel

Das Tunnelziel ist die Schnittstelle im Router am anderen Tunnelende. Bestimmen Sie, ob Sie eine IP-Adresse oder einen Hostnamen angeben möchten, und geben Sie dann die entsprechenden Informationen ein. Wenn Sie **IP-Adresse** ausgewählt haben, geben Sie die IP-Adresse und die Subnetzmaske im durch Punkte getrennten Dezimalformat ein, wie beispielsweise 192.168.20.1 und 255.255.255.0.

Stellen Sie sicher, dass die Adresse oder der Hostname über den **ping**-Befehl erreichbar ist, anderenfalls kann der Tunnel nicht ordnungsgemäß erstellt werden.

Tunnel-IP-Adresse

Geben Sie die IP-Adresse des Tunnels im durch Punkte getrennten Dezimalformat ein, beispielsweise 192.168.20.1. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Kontrollkästchen GRE Keepalive

Aktivieren Sie die Option, wenn der Router GRE Keepalives senden soll. Geben Sie das Intervall in Sekunden an, in dem Keepalives gesendet werden, sowie die Wartezeit in Sekunden für die Zeitdauer zwischen erneuten Versuchen.

Maximum Transmission Unit

Geben Sie die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) ein. Wenn Sie die Größe an einen niedrigeren Wert anpassen möchten, wenn durch eine solche Anpassung eine Paketfragementierung vermieden werden kann, klicken Sie auf **Adjust MTU to avoid fragmentation**.

Bandbreite

Klicken Sie darauf, um die Bandbreite für diesen Tunnel anzugeben.

Verbindung: ISDN BRI

Füllen Sie diese Felder aus, wenn Sie eine ISDN BRI-Verbindung konfigurieren. Da Cisco SDM nur PPP-Kapselung über eine ISDN BRI-Verbindung unterstützt, kann die angezeigte Kapselung nicht bearbeitet werden.

Kapselung

PPP ausgewählt.

ISDN-Switch-Typ

Wählen Sie den ISDN-Switch-Typ. Wenden Sie sich an Ihren ISDN-Service-Provider, um den Switch-Typ für Ihre Verbindung zu erfahren.

Cisco SDM unterstützt die folgenden BRI-Switch-Typen:

- Für Nordamerika:
  - basic-5ess – Lucent (AT&T) Basic Rate 5ESS-Switch
  - basic-dms100 – Northern Telecom DMS-100 Basic Rate-Switch
  - basic-ni – Nationale ISDN-Switches
- Für Australien, Europa und Großbritannien:
  - basic-1tr6 – Deutscher 1TR6 ISDN-Switch
  - basic-net3 – NET3 ISDN BRI für die Switch Typen Norwegen NET3, Australien NET3 und Neuseeland NET3; ETSI-entsprechende Switch-Typen für Euro-ISDN E-DSS1-Signalsysteme
  - vn3 – Französische ISDN BRI-Switches

- Für Japan:
  - ntt – Japanische NTT ISDN-Switches
- Voice-/PBX-Systeme:
  - basic-qsig – PINX (PBX)-Switches mit QSIG-Signalisierung über Q.931 ()

SPIDs

Klicken Sie auf diese Option, um die SPID-Informationen (Service Profile ID) einzugeben.

Einige Service-Provider verwenden SPIDs, um die Dienste zu definieren, die vom ISDN-Gerät abonniert wurden, das auf den ISDN-Service-Provider zugreift. Der Service-Provider weist beim erstmaligen Abonnieren des Dienstes das ISDN-Gerät einem oder mehreren SPIDs zu. Wenn Sie einen Service-Provider nutzen, für den SPIDs erforderlich sind, kann Ihr ISDN-Gerät keine Anrufe tätigen oder empfangen, bevor eine gültige, zugewiesene SPID an den Service-Provider gesendet wurde, wenn auf den Switch für die Initialisierung der Verbindung zugegriffen wird.

SPIDs ist nur für die Switch-Typen DMS-100 und NI erforderlich. Der 5ESS-Switch-Typ von Lucent (AT&T) bietet wahrscheinlich eine SPID-Unterstützung, wir empfehlen jedoch die Einrichtung des ISDN-Dienstes ohne SPIDs. Darüber hinaus sind SPIDs nur in der lokalen Schnittstelle für den ISDN-Zugriff von Bedeutung. Remote-Router empfangen die SPID niemals.

Eine SPID ist normalerweise eine siebenstellige Telefonnummer mit einigen optionalen Nummern. Service-Provider verwenden jedoch möglicherweise unterschiedliche Nummerierungschemata. Dem Switch-Typ DMS-100 sind zwei SPIDs zugeordnet, eine für jeden B-Kanal.

Remote-Telefonnummer

Geben Sie die Telefonnummer für das Ziel der ISDN-Verbindung ein.

Optionen

Klicken Sie auf diese Option, um ACLs zu einer Dialer-Liste zuzuweisen, interessanten Datenverkehr zu identifizieren, Timer-Einstellungen festzulegen oder Multilink-PPP zu aktivieren oder zu deaktivieren.

Beim Identifizieren von interessantem Datenverkehr wird die DFÜ-Verbindung des Routers beendet, und der Router erstellt nur dann eine aktive Verbindung, wenn dieser interessanten Datenverkehr ermittelt.

Einstellungen für Zeitwerte veranlassen den Router dazu, einen Anruf automatisch zu unterbrechen, wenn sich die Leitung für die angegebene Zeitdauer im Ruhezustand befindet.

Multilink-PPP kann konfiguriert werden, um einen Lastausgleich zwischen ISDN B-Kanälen zu ermöglichen.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse**, **Keine IP-Nummerierung** oder **ausgehandelt**. Wenn Sie **Geben Sie eine IP-Adresse an** wählen, füllen Sie die folgenden Felder aus.

IP-Adresse

Geben Sie die IP-Adresse für diese Point-to-Point-Unterschnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Netzwerk-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Geben Sie alternativ die Netzwerkbits ein, um anzugeben, wie viele Bits der IP-Adresse die Netzwerkadresse bereitstellen.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: Analoges Modem

Füllen Sie diese Felder aus, wenn Sie eine Analogmodem-Verbindung konfigurieren. Da Cisco SDM nur PPP-Kapselung über eine Analogmodem-Verbindung unterstützt, kann die angezeigte Kapselung nicht bearbeitet werden.

Kapselung

PPP ausgewählt.

Remote-Telefonnummer

Geben Sie die Telefonnummer für das Ziel der Analogmodem-Verbindung ein.

Optionen

Klicken Sie auf diese Option, um ACLs zu einer Dialer-Liste zuzuweisen, interessanten Datenverkehr zu identifizieren oder Timer-Einstellungen festzulegen.

Beim Identifizieren von interessantem Datenverkehr wird die DFÜ-Verbindung des Routers beendet, und der Router erstellt nur dann eine aktive Verbindung, wenn dieser interessanten Datenverkehr ermittelt.

Einstellungen für Zeitwerte veranlassen den Router dazu, einen Anruf automatisch zu unterbrechen, wenn sich die Leitung für die angegebene Zeitdauer im Ruhezustand befindet.

Leitung freigeben

Klicken Sie auf diese Schaltfläche, um die Leitung freizugeben. Sie sollten eine Leitung freigeben, nachdem Sie eine Async-Verbindung erstellt haben, sodass die Verbindung durch interessanten Datenverkehr aktiviert werden kann.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse**, **Keine IP-Nummerierung** oder **ausgehandelt**. Wenn Sie **Geben Sie eine IP-Adresse an** wählen, füllen Sie die folgenden Felder aus.

IP-Adresse

Geben Sie die IP-Adresse für diese Point-to-Point-Unterschnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Netzwerk-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Geben Sie alternativ die Netzwerkbits ein, um anzugeben, wie viele Bits der IP-Adresse die Netzwerkadresse bereitstellen.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Verbindung: (Zusätzliche Sicherung)

Füllen Sie diese Felder aus, wenn Sie eine asynchrone DFÜ-Verbindung über den Konsolenport konfigurieren, der als alternativer Port für einen Cisco 831 oder 837 Router eingesetzt werden soll. Wenn Sie die Informationen in diesem Fenster eingegeben haben, klicken Sie auf **Sicherungsdetails**, und geben Sie die Dial-Backup-Informationen ein, die für diesen Verbindungstyp erforderlich sind. Beachten Sie, dass die angezeigte Kapselung nicht bearbeitet werden kann, da Cisco SDM nur PPP-Kapselung über eine Analogmodem-Verbindung unterstützt.

Die Option zur Konfiguration des zusätzlichen Ports als Wählverbindung wird nur für die Cisco 831- und 837-Router angezeigt. Diese Option ist nicht für diese Router verfügbar, wenn eine der folgenden Bedingungen zutrifft:

- Der Router nutzt keine Zutswang Cisco IOS-Version
- Eine primäre WAN-Schnittstelle ist nicht konfiguriert
- Die asynchrone Schnittstelle ist bereits konfiguriert
- Die asynchrone Schnittstelle von Cisco SDM ist nicht konfiguriert, weil sich in der vorhandenen Konfiguration nicht unterstützte Cisco IOS-Befehle befinden.

Kapselung

PPP ausgewählt.

Remote-Telefonnummer

Geben Sie die Telefonnummer für das Ziel der Analogmodem-Verbindung ein.

Optionen

Klicken Sie auf diese Option, um ACLs zu einer Dialer-Liste zuzuweisen, interessanten Datenverkehr zu identifizieren oder Timer-Einstellungen festzulegen.

Beim Identifizieren von interessantem Datenverkehr wird die DFÜ-Verbindung des Routers beendet, und der Router erstellt nur dann eine aktive Verbindung, wenn dieser interessanten Datenverkehr ermittelt.

Einstellungen für Zeitwerte veranlassen den Router dazu, einen Anruf automatisch zu unterbrechen, wenn sich die Leitung für die angegebene Zeitdauer im Ruhezustand befindet.

Leitung freigeben

Klicken Sie auf diese Schaltfläche, um die Leitung freizugeben. Sie sollten eine Leitung freigeben, nachdem Sie eine Async-Verbindung erstellt haben, sodass die Verbindung durch interessanten Datenverkehr aktiviert werden kann.

IP-Adresse

Wählen Sie entweder **Statische IP-Adresse**, **Keine IP-Nummerierung** oder **ausgehandelt**. Wenn Sie **Geben Sie eine IP-Adresse an** wählen, füllen Sie die folgenden Felder aus.

IP-Adresse

Geben Sie die IP-Adresse für diese Point-to-Point-Unterschnittstelle ein. Lassen Sie sich diese Information vom Netzwerkadministrator oder Ihrem Service-Provider geben. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Die Subnetzmaske gibt den Teil der IP-Adresse an, der die Netzwerkadresse bereitstellt. Dieser Wert ist mit den Netzwerk-Bits synchronisiert. Den Wert für die Subnetzmaske oder die Netzwerk-Bits erhalten Sie von Ihrem Service-Provider oder Netzwerkadministrator.

Subnetz-Bits

Geben Sie alternativ die Netzwerkbits ein, um anzugeben, wie viele Bits der IP-Adresse die Netzwerkadresse bereitstellen.

Sicherungsdetails

Klicken Sie auf diese Option, um das Fenster Sicherungskonfiguration anzuzeigen, in dem Sie Dial-Backup-Informationen für diese Verbindung konfigurieren können. Diese Informationen sind für diesen Verbindungstyp erforderlich, und es wird eine Fehlermeldung angezeigt, wenn Sie versuchen, die Verbindungskonfiguration abzuschließen, ohne die Dial-Backup-Konfigurationsinformationen einzugeben.

Authentifizierung

Klicken Sie hier, um die CHAP- oder PAP-Authentifizierungsinformationen einzugeben.

Dynamische DNS

Wählen Sie dynamisches DNS aus, wenn Sie Ihre DNS Server automatisch aktualisieren wollen, sobald sich die WAN Schnittstellen-IP-Adressen ändern.

Hinweis Diese Funktion steht nur zur Verfügung, wenn sie von der Cisco IOS-Version auf Ihrem Router unterstützt wird.

Um eine dynamische DNS Methode auszuwählen, müssen Sie einen der nachfolgenden Möglichkeiten ausführen:

- Geben Sie den Namen einer existierenden dynamischen DNS Methode ein.

  Geben Sie den Namen in das Feld Dynamische DNS Methode genau so ein, wie er in der Liste unter **Konfigurieren > Zusätzliche Aufgaben > Dynamische DNS Methode** aufgeführt wird.

- Wählen Sie aus der Liste eine dynamische DNS Methode aus.

  Klicken Sie auf das Dropdown-Menü und wählen Sie eine existierende Methode aus. Ein Fenster mit einer Liste der existierenden dynamischen DNS Methoden wird geöffnet. Diese Menüwahl steht nur zur Verfügung, wenn es existierende dynamische Methoden gibt.

- Erstellen Sie eine neue dynamische DNS Methode.

  Klicken Sie auf das Dropdown-Menü und wählen Sie den Punkt **eine neue dynamische DNS Methode erstellen** aus.

Um die verknüpfte dynamische DNS Methode von der Schnittstelle zu löschen, wählen Sie aus dem Dropdown-Menü **Keine** aus.

Authentifizierung

Diese Seite wird angezeigt, wenn Sie PPP für eine serielle Verbindung oder PPPoE als Kapselung für eine ATM- oder Ethernet-Verbindung aktiviert haben, oder wenn Sie dabei sind, eine ISDN BRI- oder Analogmodem-Verbindung zu konfigurieren. Ihr Service-Provider oder Netzwerkadministrator kann ein CHAP-Kennwort (CHAP = Challenge Handshake Authentication Protocol) oder ein PAP-Kennwort (PAP = Password Authentication Protocol) verwenden, um die Verbindung zwischen den Geräten zu sichern. Dieses Kennwort sichert sowohl den eingehenden als auch den ausgehenden Zugriff.

CHAP/PAP

Aktivieren Sie das Kontrollkästchen für den Authentifizierungstypen, den Ihr Service-Provider verwendet. Wenn Sie nicht wissen, welchen Typ Ihr Service-Provider verwendet, können Sie beide Kästchen aktivieren: der Router probiert dann beide Authentifizierungstypen aus und hat bei einem Versuch Erfolg.

Die CHAP-Authentifizierung ist sicherer als die PAP-Authentifizierung.

Anmeldename

Der Anmeldename, den Sie von Ihrem Service-Provider erhalten haben, wird als Benutzername für die CHAP/PAP-Authentifizierung verwendet.

Kennwort

Geben Sie das Kennwort auf exakt die gleiche Weise ein, wie Sie es von Ihrem Service-Provider erhalten haben. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. So ist das Kennwort *test* zum Beispiel nicht identisch mit dem Kennwort *TEST*.

Kennwort wiederholen.

Geben Sie hier dasselbe Kennwort wie in das vorhergehende Feld ein.

SPID-Details

Einige Service-Provider verwenden Service-Provider-ID-Nummern (SPIDs), um die Dienste zu definieren, die vom ISDN-Gerät abonniert wurden, das auf den ISDN-Service-Provider zugreift. Der Service-Provider weist beim erstmaligen Abonnieren des Dienstes das ISDN-Gerät einem oder mehreren SPIDs zu. Wenn Sie einen Service-Provider nutzen, für den SPIDs erforderlich sind, kann Ihr ISDN-Gerät keine Anrufe tätigen oder empfangen, bevor eine gültige, zugewiesene SPID an den Service-Provider gesendet wurde, wenn auf den Switch für die Initialisierung der Verbindung zugegriffen wird.

SPIDs nur für die Switch-Typen DMS-100 und NI erforderlich. SPIDs werden vom AT&T 5ESS-Switch-Typ wahrscheinlich unterstützt, wir empfehlen jedoch die Einrichtung dieses ISDN-Dienstes ohne SPIDs. Darüber hinaus sind SPIDs nur in der lokalen Schnittstelle für den ISDN-Zugriff von Bedeutung. Remote-Router empfangen die SPID niemals.

Eine SPID ist normalerweise eine siebenstellige Telefonnummer mit einigen optionalen Nummern. Service-Provider verwenden jedoch möglicherweise unterschiedliche Nummerierungschemata. Dem Switch-Typ DMS-100 sind zwei SPIDs zugeordnet, eine für jeden B-Kanal.

SPID1

Geben Sie die SPID für den ersten BRI B-Kanal ein, die Sie von Ihrem Internet-Service-Provider erhalten haben.

SPID2

Geben Sie die SPID für den zweiten BRI B-Kanal ein, die Sie von Ihrem Internet-Service-Provider erhalten haben.

Dialer-Optionen

Sowohl ISDN BRI- als auch Analogmodem-Schnittstellen können für Dial-on-Demand-Routing (DDR) konfiguriert werden, wodurch die Ausgangs-Verbindung beendet und nur unter bestimmten Bedingungen aktiv wird, um Verbindungszeit und -kosten einzusparen. In diesem Fenster können Sie Optionen zum Starten oder Beenden von ISDN BRI- oder Analogmodem-Verbindungen konfigurieren.

Verknüpfung der Dialer-Liste

Über die Dialer-Liste können Sie die ISDN BRI- oder Analogmodem-Verbindung mit einer ACL verknüpfen, um *interessanten Datenverkehr* zu identifizieren. Beim Identifizieren von interessantem Datenverkehr wird die DFÜ-Verbindung der Schnittstelle beendet, und der Router erstellt nur dann eine aktive Verbindung, wenn dieser interessanten Datenverkehr ermittelt.

Allen IP-Datenverkehr zulassen

Wählen Sie diese Option aus, wenn die Schnittstelle die Ausgangs-Verbindung aufbauen und eine Verbindung herstellen soll, sobald IP-Datenverkehr über die Schnittstelle gesendet wird.

Filter Traffic Based on Selected ACL (Datenverkehr auf der Basis der ausgewählten ACL filtern)

Aktivieren Sie diese Option, um eine ACL, die unter Verwendung der Regelschnittstelle erstellt werden muss, mit der Schnittstelle zu verknüpfen. Nur wenn Datenverkehr auftritt, der mit dem in der ACL angegebenen Datenverkehr übereinstimmt, wird die DFÜ-Verbindung der Schnittstelle beendet, und eine neue Verbindung wird hergestellt.

Sie können die ACL-Nummer eingeben, um sie der Dialer-Schnittstelle zur Kennzeichnung überwachungswürdiger Datenübertragungen zuzuweisen, oder Sie klicken auf die Schaltfläche neben dem Feld, um die Liste mit den ACLs zu durchstöbern bzw. eine neue ACL zu definieren und auszuwählen.

Einstellungen für Zeitwerte

Mit den Einstellungen für Zeitwerte können Sie festlegen, wie lange eine Verbindung, in der kein Datenverkehr auftritt, maximal aktiv bleiben soll. Wenn Sie die Zeitwerte konfigurieren, werden Ihre Verbindungen automatisch getrennt, um Verbindungszeit und -kosten einzusparen.

Idle timeout (Timeout im Ruhezustand)

Geben Sie die Anzahl von Sekunden an, wie lange gewartet werden soll, bevor eine Verbindung im Ruhezustand (eine Verbindung, in der kein Datenverkehr auftritt), beendet wird.

Fast Idle Timeout (Schnelles Timeout im Ruhezustand)

Das Fast Idle-Timeout wird benutzt, wenn eine Verbindung aktiv ist, während eine zweite Verbindung darauf wartet, aufgebaut zu werden. Das Fast-Idle-Timeout legt die maximale Anzahl von Sekunden fest, in der kein interessanter Verkehr fließt, bevor die aktive Verbindung beendet wird und die zweite Verbindung aufgebaut wird.

Dies tritt auf, wenn die Schnittstelle über eine aktive Verbindung zu einer Next Hop-IP-Adresse verfügt und die Schnittstelle interessanten Datenverkehr mit einem anderen Next Hop-IP-Ziel empfängt. Da es sich bei der Dialer-Verbindung um eine Point-to-Point-Verbindung handelt, kann das konkurrierende Paket nicht gesendet werden, bevor die aktuelle Verbindung beendet wird. Der Zeitwert legt fest, wie lange gewartet werden muss, während sich die erste Verbindung im Ruhezustand befindet, bevor diese Verbindung beendet und die konkurrierende Verbindung aufgebaut wird.

Multilink-PPP aktivieren

Mit Multilink-PPP können Sie einen Lastausgleich bei der Datenübertragung über mehrere ISDN BRI B-Kanäle und asynchrone Schnittstellen aktivieren. Bei der Verwendung von Multilink-PPP wird nur ein B-Kanal für die Verbindung genutzt, wenn ursprünglich eine ISDN-Verbindung erstellt wurde. Wenn die Datenverkehrslast auf der Verbindungsleitung den vorgegebenen Schwellwert überschreitet (wird als Prozentsatz zur gesamten Bandbreite angegeben), wird eine Verbindung zu einem zweiten B-Kanal aufgebaut, und der Datenverkehr wird auf beide Verbindungen aufgeteilt. Das hat den Vorteil, dass Verbindungszeit und -kosten eingespart werden, wenn das Datenaufkommen gering ist, Sie jedoch bei Bedarf Ihre gesamte ISDN BRI-Bandbreite nutzen können.

Aktivieren Sie dieses Kontrollkästchen, wenn Multilink-PPP aktiviert werden soll. Deaktivieren Sie anderenfalls dieses Feld.

Auslastungsschwellenwert

Verwenden Sie dieses Feld, um den Prozentwert der Bandbreite zu konfigurieren, der in einem einzelnen ISDN BRI-Kanal auftreten muss, bevor eine andere ISDN BRI-Kanalverbindung erstellt wird, um Lastausgleich für den Datenverkehr zu erreichen. Geben Sie einen Wert zwischen 1 und 255 ein, wobei 255 einem Prozentwert von 100 Prozent der Bandbreite der ersten verwendeten Verbindung entspricht.

Datenrichtung

Cisco SDM unterstützt Multilink-PPP nur für abgehenden Netzwerkdatenverkehr.

Sicherungskonfiguration

ISDN BRI- und Analogmodem-Schnittstellen können so konfiguriert werden, dass sie als Sicherungsschnittstellen für andere, primäre Schnittstellen fungieren. In diesem Fall wird eine ISDN- oder Analogmodem-Verbindung nur dann hergestellt, wenn die primäre Schnittstelle ausfällt. Wenn die primäre Schnittstelle und Verbindung ausfällt, startet die ISDN- oder Analogmodem-Schnittstelle sofort einen Wählvorgang und versucht, eine Verbindung herzustellen, damit die Netzwerkdienste nicht verloren gehen.

Sicherung aktivieren

Aktivieren Sie diese Option, wenn diese ISDN BRI- oder Analogmodem-Schnittstelle als Reserveverbindung fungieren soll. Deaktivieren Sie dieses Kontrollkästchen, wenn die ISDN BRI- oder Analogmodem-Schnittstelle nicht als Sicherungsschnittstelle verwendet werden soll.

Primäre Schnittstelle

Wählen Sie die Schnittstelle des Routers aus, die die primäre Verbindung halten soll. Eine ISDN BRI- oder Analogmodem-Verbindung wird nur dann hergestellt, wenn die Verbindung auf der gewählten Schnittstelle aus irgendeinem Grund einmal ausfällt.

Verfolgungsdetails

Verwenden Sie diesen Abschnitt, um einen bestimmten Host anzugeben, zu dem die Verbindung beibehalten werden muss. Der Router verfolgt die Anbindung an diesem Host. Stellt der Router fest, dass die Verbindung zu dem angegebenen Host auf der primären Schnittstelle verloren gegangen ist, wird eine Reserveverbindung über die ISDN BRI- oder Analogmodem-Schnittstelle hergestellt.

IP-Adresse oder Hostname, die bzw. der verfolgt werden soll

Geben Sie den Hostnamen oder die IP-Adresse des Zielhosts ein, deren/dessen Verbindung verfolgt werden soll. Geben Sie als zu verfolgenden Standort ein Ziel ein, das nicht so häufig kontaktiert wird.

Verfolgungsobjektnummer

Dies ist ein schreibgeschütztes Feld, das eine interne Objektnummer anzeigt, die von Cisco SDM erstellt und verwendet wird, um die Verbindung zum Remote-Host zu verfolgen.

Next Hop-Weiterleitung

Diese Felder sind optional. Sie können die IP-Adresse angeben, zu der die primären und Sicherungsschnittstellen eine Verbindung herstellen sollen, wenn diese aktiv sind. Diese wird als Next Hop-IP-Adresse bezeichnet. Wenn Sie keine Next Hop-IP-Adressen eingeben, konfiguriert Cisco SDM mit dem Schnittstellennamen statische Routen. Beachten Sie, dass bei der Sicherung von Multipoint-WAN-Verbindungen, wie einer Ethernet-Verbindung, Next Hop-IP-Adressen eingegeben werden müssen, damit die Routing-Aufgaben fehlerfrei ausgeführt werden können. Bei der Sicherung einer PPP-Verbindung sind diese Informationen jedoch nicht erforderlich.

Primäre Next Hop-IP-Adresse

Geben Sie die Next Hop-IP-Adresse der primären Schnittstelle ein.

Next Hop-Sicherungs-IP-Adresse

Geben Sie die Next Hop-IP-Adresse der ISDN BRI- oder Analogmodem-Sicherungsschnittstelle ein.

KAPITEL 6

Firewall erstellen

Eine Firewall ist eine Gruppe von Regeln zum Schutz Ihrer LAN-Ressourcen. Mit diesen Regeln werden die Pakete gefiltert, die beim Router ankommen. Wenn ein Paket nicht die in der Regel angegebenen Kriterien erfüllt, wird es entfernt. Wenn es die Kriterien erfüllt, kann es die Schnittstelle durchlaufen, der die Regel zugeordnet ist. Mit diesem Assistenten können Sie eine Firewall für Ihr LAN erstellen, indem Sie in einer Reihe von Bildschirmen die angeforderten Daten eingeben.

In diesem Fenster wählen Sie den Firewalltyp aus, den Sie erstellen möchten.

Hinweis

- Der Router, den Sie konfigurieren, muss ein Cisco IOS-Abbild verwenden, das den Firewall-Funktionssatz unterstützt, damit Sie Cisco Router and Security Device Manager (Cisco SDM) für die Konfiguration einer Firewall auf dem Router verwenden können.
- Die LAN- und WAN-Konfiguration muss abgeschlossen sein, bevor Sie eine Firewall konfigurieren können.

Basisfirewall

Klicken Sie auf diese Option, wenn Cisco SDM eine Firewall mit Standardregeln erstellen soll. Das Anwendungsszenario zeigt eine typische Netzwerkkonfiguration, in der diese Art von Firewall verwendet wird.

Erweiterte Firewall

Klicken Sie auf diese Option, wenn Cisco SDM Sie durch die Schritte für die Konfiguration einer Firewall führen soll. Sie haben die Möglichkeit, ein DMZ-Netzwerk zu erstellen und eine Prüfregel anzugeben. Das Anwendungsszenario, das Sie bei Auswahl dieser Option sehen, zeigt eine typische Konfiguration für eine Firewall zum Internet.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Veranlassen, dass Cisco SDM eine Firewall erstellt Sie sollten diese Option auswählen, wenn Sie kein DMZ-Netzwerk konfigurieren möchten oder wenn es nur eine äußere Schnittstelle gibt.	Klicken Sie auf **Basisfirewall**. Klicken Sie dann auf **Ausgewählte Aufgabe starten**. Sie werden von Cisco SDM aufgefordert, die Schnittstellen auf Ihrem Router zu identifizieren. Anschließend werden Cisco SDM-Standardzugriffsregeln und -Prüfregeln zum Erstellen der Firewall verwendet.
Erstellen einer erweiterten Firewall mit Unterstützung von Cisco SDM Sie sollten diese Option auswählen, wenn Ihr Router mehrere innere und äußere Schnittstellen hat und Sie eine DMZ konfigurieren möchten.	Wählen Sie **Erweiterte Firewall**. Klicken Sie dann auf **Ausgewählte Aufgabe starten**. Cisco SDM zeigt die Standardprüfregel an, die Sie für die Firewall verwenden können. Sie haben auch die Möglichkeit, eine eigene Prüfregel zu erstellen. Cisco SDM verwendet eine Standardzugriffsregel für die Firewall.

Aufgabe	Vorgehensweise
Abrufen von Informationen zu einer Aufgabe, deren Durchführung vom Assistenten nicht unterstützt wird	Wählen Sie ein Thema aus der folgenden Liste aus. • Wie zeige ich Aktivitäten auf meiner Firewall an? • Wie konfiguriere ich eine Firewall auf einer nicht unterstützten Schnittstelle? • Wie konfiguriere ich eine Firewall, nachdem ich ein VPN konfiguriert habe? • Wie lasse ich bestimmten Datenverkehr über eine DMZ-Schnittstelle zu? • Wie ändere ich eine existierende Firewall, um Datenverkehr von einem neuen Netzwerk oder Host zuzulassen? • Wie konfiguriere ich NAT auf einer nicht unterstützten Schnittstelle? • Wie konfiguriere ich NAT Passthrough für eine Firewall? • Wie lasse ich über eine Firewall Datenverkehr zu meinem Easy VPN-Konzentrator zu? • Wie verknüpfe ich eine Regel mit einer Schnittstelle? • Wie hebe ich die Verknüpfung einer Zugriffsregel mit einer Schnittstelle auf? • Wie lösche ich eine Regel, die mit einer Schnittstelle verknüpft ist? • Wie erstelle ich eine Zugriffsregel für eine Java-Liste? • Wie zeige ich die IOS-Befehle an, die ich an den Router sende? • Wie lasse ich bestimmten Datenverkehr in meinem Netzwerk zu, wenn ich kein DMZ-Netzwerk besitze?

Assistent für die Konfiguration der Basisfirewall

Wenn Sie diese Option auswählen, schützt Cisco SDM das LAN mit einer Standardfirewall. Damit Cisco SDM diese Funktion ausführt, müssen Sie im nächsten Fenster die inneren und äußeren Schnittstellen angeben. Klicken Sie auf **Weiter**, um mit der Konfiguration zu beginnen.

Konfiguration der Basisfirewall-Schnittstelle

Identifizieren Sie die Schnittstellen auf dem Router, damit die Firewall der richtigen Schnittstelle zugeordnet wird.

Äußere (nicht vertrauenswürdige) Schnittstelle

Wählen Sie die Routerschnittstelle aus, die mit dem Internet oder dem WAN ihrer Organisation verbunden ist.

Hinweis Wählen Sie nicht die Schnittstelle, über die Sie auf Cisco SDM zugegriffen haben, als äußere (nicht vertrauenswürdige) Schnittstelle aus. Wenn diese Schnittstelle ausgewählt wird, geht die Verbindung zu Cisco SDM verloren. Da die Software durch eine Firewall geschützt wird, können Sie Cisco SDM nicht von der äußeren (nicht vertrauenswürdigen) Schnittstelle starten, nachdem der Firewall-Assistent abgeschlossen wurde.

Kontrollkästchen „Sicheren Cisco SDM-Zugang von äußeren Schnittstellen zulassen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie Benutzer außerhalb der Firewall den Zugang zum Router mittels Cisco SDM gewähren möchten. Der Assistent zeigt einen Bildschirm an, der es Ihnen ermöglicht, eine Host IP-Adresse oder eine Netzwerkadresse festzulegen. Die Firewall wird so angepasst, dass ein Zugang zur festgelegten Adresse möglich wird. Wenn Sie eine Netzwerkadresse festlegen, werden alle Hosts in diesem Netzwerk von der Firewall zugelassen.

Innere (vertrauenswürdige) Schnittstellen

Aktivieren Sie die physikalischen und logischen Schnittstellen, die mit dem LAN verbunden sind. Sie können mehrere Schnittstellen auswählen.

Konfiguration der Firewall für den Remotezugriff

Das Aufbauen einer Firewall kann dazu führen, dass der Zugang für Fernadministratoren blockiert wird. Sie können die Routerschnittstellen, die für den Remote-Verwaltungszugriff verwendet werden sollen, sowie die Hosts angeben, von denen aus sich der Administrator bei Cisco SDM anmelden kann, um den Router zu verwalten. Die Firewall wird so angepasst, dass ein sicherer Zugang von dem Host oder Netzwerk möglich ist, welches Sie bestimmt haben.

Die äußere Schnittstelle auswählen

Wenn Sie den Assistenten **Erweiterte Firewall** verwenden, wählen Sie die Schnittstelle aus, mit der Benutzer Cisco SDM starten. Dieses Feld erscheint im Basisassistenten für Firewalls nicht.

Quellen-Host/-Netzwerk

Wenn Sie einen einzelnen Hostzugang durch die Firewall zulassen wollen, wählen Sie **Host**-**Adresse** aus und geben Sie die IP-Adresse eines Hosts ein. Wählen Sie **Netzwerkadresse** und geben Sie die Adresse eines Netzwerks und einer Subnetzmaske ein, um den Hosts in diesem Netzwerk den Zugang durch die Firewall zu gestatten. Der Host oder das Netzwerk müssen von der Schnittstelle erreichbar sein, die Sie angegeben haben. Wählen Sie **Irgendwelche** aus, um jedem beliebigen Host einen sicheren Zugang zum Netzwerk zu gestatten, der mit den festgelegten Schnittstellen verbunden ist.

Assistent für die Konfiguration der erweiterten Firewall

Cisco SDM unterstützt Sie bei der Erstellung einer Firewall zum Internet. Sie werden aufgefordert, Informationen über die Schnittstellen auf dem Router anzugeben, ob Sie ein DMZ-Netzwerk konfigurieren und welche Regeln Sie für die Firewall verwenden möchten.

Klicken Sie auf **Weiter**, um mit der Konfiguration zu beginnen.

Erweiterte Firewall-Schnittstellenkonfiguration

Identifizieren Sie die inneren und äußeren Schnittstellen des Routers und die Schnittstelle, die mit dem DMZ-Netzwerk verbunden ist.

Aktivieren Sie **äußere** oder **innere**, um die einzelnen Schnittstellen als äußere oder innere Schnittstelle zu identifizieren. Äußere Schnittstellen sind mit dem WAN Ihrer Organisation oder mit dem Internet verbunden. Innere Schnittstellen sind mit Ihrem LAN verbunden.

Kontrollkästchen „Sicheren Cisco SDM-Zugang von äußeren Schnittstellen zulassen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie Benutzer außerhalb der Firewall den Zugang zum Router mittels Cisco SDM gewähren möchten. Der Assistent zeigt einen Bildschirm an, der es Ihnen ermöglicht eine Host IP-Adresse oder eine Netzwerkadresse festzulegen. Die Firewall wird so angepasst, dass ein Zugang zur festgelegten Adresse möglich wird. Wenn Sie eine Netzwerkadresse festlegen, werden alle Hosts in diesem Netzwerk von der Firewall zugelassen.

DMZ-Schnittstelle

Wählen Sie die Routerschnittstelle aus, die mit einem DMZ-Netzwerk verbunden ist (sofern vorhanden). Ein DMZ-Netzwerk ist eine Pufferzone für die Isolierung von Datenverkehr, der von einem nicht vertrauenswürdigen Netzwerk stammt. Wenn Sie ein DMZ-Netzwerk haben, wählen Sie die Schnittstelle aus, die damit verbunden ist.

Konfiguration erweiterter Firewall-DMZ-Dienste

In diesem Fenster können Sie Regeleinträge anzeigen, die angeben, welche innerhalb der DMZ verfügbaren Dienste Sie über die äußeren Schnittstellen des Routers zur Verfügung stellen möchten. Datenverkehr mit den angegebenen Diensttypen wird über die äußeren Schnittstellen in das DMZ-Netzwerk zugelassen.

DMZ-Dienstkonfiguration

In diesem Bereich werden die DMZ-Diensteinträge angezeigt, die auf dem Router konfiguriert sind.

Start-IP-Adresse

Die erste IP-Adresse in dem Bereich, der die Hosts im DMZ-Netzwerk angibt.

End-IP-Adresse

Die letzte IP-Adresse in dem Bereich, der die Hosts im DMZ-Netzwerk angibt. Wenn in dieser Spalte kein Wert aufgelistet ist, wird davon ausgegangen, dass die IP-Adresse in der Spalte **Start-IP-Adresse** den einzigen Host im DMZ-Netzwerk angibt. Im Bereich können maximal 254 Hosts angegeben werden.

Diensttyp

Der Typ des Dienstes, entweder Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP).

Dienst

Der Name des Dienstes, z. B. Telnet, FTP (File Transfer-Protokoll) oder eine Protokollnummer.

So konfigurieren Sie einen DMZ-Diensteintrag:

Klicken Sie auf **Hinzufügen**, und erstellen Sie den Eintrag im Fenster **DMZ-Dienstkonfiguration**.

So bearbeiten Sie einen DMZ-Diensteintrag:

Wählen Sie den Diensteintrag aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann den Eintrag im Fenster **DMZ-Dienstkonfiguration**.

DMZ-Dienstkonfiguration

Erstellen oder bearbeiten Sie einen DMZ-Diensteintrag in diesem Fenster.

Host-IP-Adresse

Geben Sie den Adressenbereich ein, der die Hosts in der DMZ angibt, für die dieser Eintrag gilt. Die Firewall lässt Datenverkehr für den angegebenen TCP- oder UDP-Dienst zu diesen Hosts zu.

Start-IP-Adresse

Geben Sie die erste IP-Adresse im Bereich ein, z. B. 172.20.1.1. Wenn (NAT) Network Address Translation aktiviert ist, müssen Sie die Adresse in der NAT-Übersetzung angeben, die als *innere globale Adresse* bekannt ist.

End-IP-Adresse

Geben Sie die letzte IP-Adresse im Bereich ein, z. B. 172.20.1.254. Wenn NAT aktiviert ist, müssen Sie die Adresse in der NAT-Übersetzung eingeben.

Dienst

TCP

Klicken Sie auf diese Option, wenn Sie Datenverkehr für einen TCP-Dienst zulassen möchten.

UDP

Klicken Sie auf diese Option, wenn Sie Datenverkehr für einen UDP-Dienst zulassen möchten.

Dienst

Geben Sie den Namen oder die Nummer des Dienstes in dieses Feld ein. Wenn Ihnen der Name oder die Nummer nicht bekannt ist, klicken Sie auf die Schaltfläche, und wählen Sie den Dienst aus der angezeigten Liste aus.

Anwendung Sicherheitsstufe

Cisco SDM bietet voreingestellte Anwendungssicherheitsregeln an, die Sie verwenden können, um Ihr Netzwerk zu schützen. Benutzen Sie den Balken, um die Sicherheitsstufe auszuwählen, die Sie einsetzen wollen und um eine Beschreibung der Sicherheiten anzeigen zu lassen, die diese Sicherheitsstufe gewährt. Der Zusammenfassungsbildschirm des Assistenten zeigt den Regelnamen, SDM_HOCH, SDM_MITTEL oder SDM_NIEDRIG und die Einstellungsbestimmungen der Regel an. Sie können sich die Details der Regel auch anschauen, wenn Sie auf die Registerkarte **Sicherheit** klicken und den Namen der Regel auswählen.

Taste Vorschaubefehle

Klicken Sie auf die Taste, um die IOS-Befehle anzusehen, die diese Regel ausmachen.

Taste Anwendung angepasste Sicherheitsstufe

Diese Taste und das Feld **Regelname** werden sichtbar, wenn Sie den Assistenten für die Fortgeschrittene Firewall abschließen. Wählen Sie diese Option, wenn Sie Ihre eigene Sicherheitsstufe festlegen wollen. Wenn die Regel bereits besteht, geben Sie den Namen in das Feld ein oder klicken Sie auf die Taste an der rechten Seite, wählen dort **Eine bestehende Regel auswählen** aus und wählen die Regel aus. Um eine Regel zu erstellen, klicken Sie auf die Taste, wählen **Neue Regel erstellen** aus und erstellen eine Regel im angezeigten Dialogfeld.

Domainname Serverkonfiguration

Der Router muss mit der IP-Adresse von mindestens einem DNS Server konfiguriert werden, um die Sicherheitsstufe zu aktivieren. Klicken Sie auf die Übersetzung **DNS-basierte-Hostname-an-Adresse** und geben Sie die IP-Adresse des primären DNS Servers ein. Wenn ein sekundärer DNS Server zur Verfügung steht, geben Sie seine IP-Adresse in das Feld **Sekundärer DNS Server** ein.

Die eingegebenen IP-Adressen sind im Fenster **DNS Eigenschaften** unter **Zusätzliche Aufgaben** sichtbar.

Konfiguration des URL-Filter-Servers

URL-Filter-Server können wesentlich mehr Informationen zur URL-Filterung speichern und verwalten als eine Routerkonfigurationsdatei enthalten kann. Wenn es im Netzwerk URL-Filter-Server gibt, können Sie den Router so konfigurieren, dass er sie verwendet. Sie können zusätzliche Parameter für URL-Filter-Server konfigurieren, indem Sie **Konfigurieren > Zusätzliche Aufgaben > URL-Filterung** wählen. Weitere Informationen finden Sie unter URL-Filterung.

HTTP-Anforderung durch URL-Filter-Server filtern

Aktivieren Sie das Kontrollkästchen **HTTP-Anforderung durch URL-Filter-Server filtern**, um die URL-Filterung durch URL-Filter-Server zu aktivieren.

Typ des URL-Filter-Servers

Cisco SDM unterstützt SecureComputing- und Websense-URL-Filter-Server. Wählen Sie entweder **SecureComputing** oder **Websense**, um den Typ des URL-Filter-Servers im Netzwerk anzugeben.

IP-Adresse/Hostname

Geben Sie die IP-Adresse oder den Hostnamen des URL-Filter-Servers ein.

Schnittstellenzone auswählen

Dieses Fenster wird angezeigt, wenn eine andere Routerschnittstelle als die, die Sie konfigurieren, Mitglied einer Zone-Based Policy Firewall Sicherheitszone ist. Weitere Informationen zu diesem Thema finden Sie unter Zonenbasierte Richtlinienfirewall (Zone-Based Policy Firewall).

Zone auswählen

Wählen Sie die Sicherheitszone, der die Schnittstelle angehören soll. Wenn Sie die Schnittstelle keiner Zone zuordnen, ist es sehr wahrscheinlich, dass der Datenverkehr nicht durch die Schnittstelle fließt.

Innere Zonen mit ZPF

Zonen, die Schnittstellen enthalten, die in Generic Routing Encapsulation (GRE)-Tunneln verwendet werden, müssen als innere (vertrauenswürdige) Zonen gekennzeichnet werden, damit GRE-Datenverkehr durch die Firewall passieren kann.

Dieses Fenster listet die konfigurierten Zonen und ihre Mitgliedsschnittstellen auf. Um eine Zone als innere Zone zu kennzeichnen, aktivieren Sie die **innere** (**vertrauenswürdige**) Spalte in der Zeile der Zone.

Übersicht

In diesem Bildschirm werden die Informationen über die Firewall zusammengefasst. Sie können die Informationen in diesem Bildschirm überprüfen und die Taste Zurück benutzen, um in den Assistenten zurückzukehren, damit Sie dort Veränderungen vornehmen können.

Der Bildschirm Zusammenfassung enthält einfache Sprache, um die Konfiguration zu beschreiben. Sie können die CLI Befehle anzeigen, die Cisco SDM an den Router ausgibt, indem Sie **Bearbeiten > Präferenzen** wählen und **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktivieren.

Innere (vertrauenswürdige) Schnittstelle(n)

Cisco SDM listet die logischen und physischen Schnittstellen des Routers auf, die Sie im Assistenten als innere Schnittstellen zusammen mit deren IP-Adressen angegeben haben. Darunter werden für jede Konfiguration Beschreibungen in einfacher Sprache gegeben, die auf die inneren Schnittstellen angewendet werden. Nachfolgend sind Beispiele aufgeführt:

```
Innere (vertrauenswürdige) Schnittstellen:
FastEthernet0/0 (10.28.54.205)
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
Spoofing-Verkehr zu verhindern.
Zugriffsregel für Eingang anwenden, um Datenverkehr abzulehnen, dessen
Quellen Broadcast- und lokale Loopback-Adressen sind.
Zugriffsregel für Eingang anwenden, um gesamten anderen Datenverkehr
zuzulassen
Die Sicherheitsstufe SDM_HOCH in eingehender Richtung anwenden.
```

Dieses Beispiel zeigt die Cisco SDM Anwendungssicherheitsrichtlinie SDM_HIGH, die auf eingehenden Verkehr auf dieser Schnittstelle angewandt wird.

Äußere (nicht vertrauenswürdige) Schnittstelle(n)

Cisco SDM listet die logischen und physischen Schnittstellen des Routers auf, die Sie im Assistenten als äußere Schnittstellen zusammen mit deren IP-Adressen angegeben haben. Darunter werden für jede Konfiguration Beschreibungen in einfacher Sprache gegeben, die auf die äußeren Schnittstellen angewendet werden. Nachfolgend sind Beispiele aufgeführt:

```
FastEthernet0/1 (142.120.12.1)
Schalten Sie die Unicast Umkehrpfadvorwärtsprüfung für Keine-Tunnel
Schnittstellen ein.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um falls
notwendig IPSec Tunnelverkehr zuzulassen.
Beachten Sie ggf. die Eingangszugriffsregel zur Genehmigung von GRE
Tunnelverkehr für Schnittstellen.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um ICMP
Verkehr zuzulassen.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um NTP
Verkehr zuzulassen.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
Spoofing-Verkehr zu verhindern.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
Verkehr zu verhindern, der von Übertragungen, lokalen Loopbacks und
privaten Adressen stammt.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
Service-Verkehr an die DMZ-Schnittstelle zuzulassen.
Service ftp von 10.10.10.1 bis 10.10.10.20
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
sicheren SDM Zugang vom 140.44.3.0 255.255.255.0 Host/Netzwerk
zuzulassen.
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
jeglichen sonstigen Verkehr zu verhindern.
```

Beachten Sie, dass diese Konfiguration den Umkehrpfad einschaltet, ein Merkmal, dass dem Router die Möglichkeit gibt, Pakete abzulegen, die über keine nachprüfbare IP-Quell-Adresse verfügen und ftp-Verkehr an DMZ-Adressen 10.10.10.1 bis 10.10.10.20 zulässt.

DMZ-Schnittstelle

Wenn Sie eine erweiterte Firewall konfiguriert haben, werden in diesem Bereich die angegebene DMZ-Schnittstelle mit ihrer IP-Adresse angezeigt. Darunter beschreibt Cisco SDM, welche Zugriffs- und Prüfregeln mit dieser Schnittstelle verknüpft wurden. Nachfolgend sind Beispiele aufgeführt:

```
FastEthernet (10.10.10.1)
CBAC-Prüfregel für Ausgang anwenden
Wenden Sie die Zugriffsregel auf die eingehende Richtung an, um
jeglichen sonstigen Verkehr zu verhindern.
```

So speichern Sie diese Konfiguration in der aktiven Konfiguration des Routers und verlassen diesen Assistenten:

Klicken Sie auf **Fertig stellen**. Cisco SDM speichert die Konfigurationsänderungen in der aktiven Konfiguration des Routers. Die Änderungen werden sofort wirksam; beim Abschalten des Routers gehen sie jedoch verloren.

Wenn Sie im Fenster **Benutzereinstellungen** die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktiviert haben, wird das Fenster **Konfiguration an Router senden** angezeigt. In diesem Fenster können Sie die CLI-Befehle anzeigen, die an den Router gesendet werden.

SDM-Warnung: SDM-Zugriff

Dieses Fenster wird angezeigt, wenn Sie angegeben haben, dass Cisco SDM von äußeren Schnittstellen auf diesen Router zugreifen können sollte. Es informiert Sie darüber, dass Sie sicherstellen müssen, dass SSH und HTTPS konfiguriert sind und dass mindestens eine der als äußere Schnittstelle gekennzeichneten Schnittstellen mit einer statischen IP-Adresse konfiguriert sein muss. Dazu müssen Sie sicherstellen, dass eine äußere Schnittstelle mit einer statischen IP-Adresse konfiguriert ist, und dann eine Verwaltungsrichtlinie mit der Schnittstelle verknüpfen.

Ermitteln, ob eine äußere Schnittstelle mit einer statischen IP-Adresse konfiguriert ist

Führen Sie die folgenden Schritte aus, um zu ermitteln, ob eine äußere Schnittstelle mit einer statischen IP-Adresse konfiguriert ist.

Schritt 1 Klicken Sie auf **Konfigurieren > Schnittstellen und Verbindungen > Schnittstelle/Verbindung bearbeiten**.

Schritt 2 Prüfen Sie anhand der IP-Spalte in der Schnittstellenlistentabelle, ob eine äußere Schnittstelle über eine statische IP-Adresse verfügt.

Schritt 3 Wenn keine äußere Schnittstelle über eine statische IP-Adresse verfügt, wählen Sie eine aus und klicken auf **Bearbeiten**, um ein Dialogfeld anzuzeigen, über das Sie die Informationen für die IP-Adresse der Schnittstelle neu konfigurieren können.

Wenn es keine äußere Schnittstelle mit einer statischen IP-Adresse gibt, notieren Sie sich den Namen der Schnittstelle und führen die folgenden Schritte aus.

Konfigurieren von SSH und HTTPS

Führen Sie die folgenden Schritte aus, um eine Verwaltungsrichtlinie für SSH und HTTPS auf dem Router zu konfigurieren.

Schritt 1 Klicken Sie auf **Konfigurieren > Zusätzliche Aufgaben > Routerzugriff > Verwaltungszugriff**.

Schritt 2 Wenn es keine Verwaltungsrichtlinie gibt, klicken Sie auf **Hinzufügen**. Wenn Sie eine vorhandene Verwaltungsrichtlinie bearbeiten möchten, wählen Sie die Richtlinie aus und klicken auf **Bearbeiten**.

Hinweis Wenn Sie eine Verwaltungsrichtlinie bearbeiten, muss sie mit einer Schnittstelle verknüpft sein, die über eine statische IP-Adresse verfügt.

Schritt 3 Geben Sie im angezeigten Dialogfeld die Adressinformationen im Feld **Quellhost/-netzwerk** ein. Die eingegebenen Informationen zur IP-Adresse müssen die IP-Adresse des PCs beinhalten, mit dem Sie den Router verwalten werden.

Schritt 4 Wählen Sie im Feld **Verwaltungsschnittstelle** eine äußere Schnittstelle mit einer statischen IP-Adresse. Diese Schnittstelle muss eine Route zur IP-Adresse haben, die Sie im Feld **Quellhost/-netzwerk** angegeben haben.

Schritt 5 Aktivieren Sie im Feld **Verwaltungsprotokolle** die Option **SDM zulassen**.

Schritt 6 Aktivieren Sie **HTTPS** und **SSH**, um diese Protokolle zuzulassen.

Schritt 7 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Schritt 8 Klicken Sie im Fenster, das die Verwaltungszugriffsrichtlinien anzeigt, auf **Änderungen übernehmen**.

Wie gehe ich vor?

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie zeige ich Aktivitäten auf meiner Firewall an?

Aktivitäten auf Ihrer Firewall werden über die Erstellung von Protokolleinträgen überwacht. Wenn Logging auf dem Router aktiviert ist, wird bei jedem Aufruf einer Zugriffs-Regel, die für die Generierung von Protokolleinträgen generiert wurde (wenn z. B. eine Verbindung von einer abgelehnten IP-Adresse versucht wurde), ein Protokolleintrag generiert, der im Monitor-Modus angezeigt werden kann.

Logging aktivieren

Der erste Schritt für die Anzeige von Firewallaktivitäten ist die Aktivierung von Logging auf dem Router. So aktivieren Sie Logging:

Schritt 1 Wählen Sie im linken Bereich **Zusätzliche Aufgaben** aus.

Schritt 2 Klicken Sie im Baum **Zusätzliche Aufgaben** auf **Logging** und dann auf die Schaltfläche **Bearbeiten**.

Schritt 3 Aktivieren Sie im Bildschirm **Syslog** die Option **Logging an Puffer**.

Schritt 4 Geben Sie im Feld **Puffergröße** an, wie viel Routerspeicher für einen Logging-Puffer verwendet werden soll. Der Standardwert ist 4096 Byte. In einem größeren Puffer werden mehr Protokolleinträge gespeichert, aber Sie müssen Ihren Bedarf an einem größeren Logging-Puffer gegen mögliche Probleme bei der Leistung des Routers abwägen.

Schritt 5 Klicken Sie auf **OK**.

Geben Sie die Zugriffsregeln an, für die Sie Protokolleinträge generieren möchten

Neben der Aktivierung des Logging müssen Sie die Zugriffsregeln angeben, für die Sie Protokolleinträge generieren möchten. So konfigurieren Sie Zugriffsregeln für die Generierung von Protokolleinträgen:

Schritt 1 Wählen Sie im linken Bereich **Zusätzliche Aufgaben** aus.

Schritt 2 Klicken Sie im Baum **Zusätzliche Aufgaben** auf **ACL-Editor** und dann auf **Zugriffsregeln**.

Die einzelnen Zugriffsregeln werden in der oberen Tabelle auf der rechten Seite des Bildschirms angezeigt. In der unteren Tabelle werden die spezifischen Quell- und Ziel-IP-Adressen und die Dienste angezeigt, die von dieser Regel zugelassen oder nicht zugelassen werden.

Schritt 3 Klicken Sie in der oberen Tabelle auf die Regel, die Sie ändern möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **Regel bearbeiten** wird angezeigt.

Schritt 5 Im Feld **Regeleintrag** werden die einzelnen Quell-IP/Ziel-IP/Dienst-Kombinationen angezeigt, die von der Regel zugelassen oder nicht zugelassen werden. Klicken Sie auf den Regeleintrag, den Sie für die Generierung von Protokolleinträgen konfigurieren möchten.

Schritt 6 Klicken Sie auf **Bearbeiten**.

Schritt 7 Aktivieren Sie im Dialogfeld für die Regeleingabe das Kontrollkästchen **Entsprechungen für diesen Eintrag protokollieren**.

Schritt 8 Klicken Sie auf **OK**, um die angezeigten Dialogfelder zu schließen.

Mit dem gerade von Ihnen geänderten Regeleintrag werden nun immer dann Protokolleinträge generiert, wenn versucht wird, von dem in der Definition des Regeleintrags aufgeführten IP-Adressenbereich und den aufgeführten Diensten eine Verbindung aufzubauen.

Schritt 9 Wiederholen Sie die Schritte 4 bis 8 für jeden Regeleintrag, den Sie für die Generierung von Protokolleinträgen konfigurieren möchten.

Wenn Sie die Logging-Konfiguration abgeschlossen haben, gehen Sie nach den folgenden Schritten vor, um die Firewall-Aktivitäten anzuzeigen:

Schritt 1 Klicken Sie in der Symbolleiste auf **Monitor-Modus**.

Schritt 2 Wählen Sie im linken Bereich **Firewallstatus** aus.

In der Statistik für die Firewall können Sie verifizieren, dass die Firewall konfiguriert ist, und anzeigen, wie viele Verbindungsversuche nicht zugelassen wurden.

In der Tabelle werden alle von der Firewall generierten Routerprotokolleinträge mit der Zeit und dem Grund für die Generierung angezeigt.

Wie konfiguriere ich eine Firewall auf einer nicht unterstützten Schnittstelle?

Cisco SDM kann eine Firewall auf einem Schnittstellentyp konfigurieren, der nicht von Cisco SDM unterstützt wird. Bevor Sie die Firewall konfigurieren können, müssen Sie die Schnittstelle zunächst mit der CLI des Routers konfigurieren. Die Schnittstelle muss mindestens eine konfigurierte IP-Adresse haben und in Betrieb sein. Weitere Informationen darüber, wie Sie eine Schnittstelle mit der CLI konfigurieren, finden Sie im Softwarekonfigurationshandbuch für Ihren Router.

Um zu überprüfen, ob die Verbindung funktioniert, stellen Sie im Fenster **Schnittstellen und Verbindungen** fest, ob als Schnittstellenstatus **Aktiv** angegeben ist.

Im Folgenden finden Sie einen Auszug aus der Konfiguration einer ISDN-Schnittstelle auf einem Cisco 3620-Router:

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
! This is the data BRI WIC
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 100.100.100.100 name junky 883531601
 dialer hold-queue 10
 isdn switch-type basic-5ess
 isdn tei-negotiation first-call
 isdn twait-disable
 isdn spid1 80568541630101 6854163
 isdn incoming-voice modem
```

Weitere Informationen finden Sie im Softwarekonfigurationshandbuch für Ihren Router.

Nachdem Sie die nicht unterstützte Schnittstelle mit der CLI konfiguriert haben, können Sie die Firewall mit Cisco SDM konfigurieren. In den Feldern, in denen die Routerschnittstellen aufgelistet sind, wird die nicht unterstützte Schnittstelle als **Andere** angezeigt.

Wie konfiguriere ich eine Firewall, nachdem ich ein VPN konfiguriert habe?

Wenn eine Firewall auf eine Schnittstelle angewandt wird, die in einem VPN verwendet wird, muss die Firewall den Datenverkehr zwischen lokalen und Remote-VPN-Peers zulassen. Wenn Sie den Assistenten für die Basisfirewall oder die erweiterte Firewall verwenden, lässt Cisco SDM automatisch Datenverkehr zwischen VPN-Peers zu.

Wenn Sie eine Zugriffsregel im ACL-Editor erstellen, der unter der Option **Zusätzliche Aufgaben** zur Verfügung steht, haben Sie die vollständige Kontrolle über die **permit**- und **deny**-Anweisungen in der Regel. Sie müssen außerdem sicherstellen, dass Datenverkehr zwischen VPN-Peers zugelassen ist. Die folgenden Anweisungen sind Beispiele für die Typen von Anweisungen, die in der Konfiguration enthalten sein sollen, um VPN-Datenverkehr zuzulassen:

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

Wie lasse ich bestimmten Datenverkehr über eine DMZ-Schnittstelle zu?

Gehen Sie nach den folgenden Schritten vor, um den Zugriff über eine Firewall auf einen Webserver in einem DMZ-Netzwerk zu konfigurieren:

Schritt 1 Wählen Sie im linken Bereich **Firewall und ACL** aus.

Schritt 2 Wählen Sie **Erweiterte Firewall**.

Schritt 3 Klicken Sie auf **Ausgewählte Aufgabe starten**.

Schritt 4 Klicken Sie auf **Weiter**.

Der Bildschirm **Erweiterte Firewall-Schnittstellenkonfiguration** wird angezeigt.

Schritt 5 Wählen Sie in der Tabelle **Schnittstelle** aus, welche Schnittstellen mit Netzwerken innerhalb der Firewall und welche Schnittstellen mit Netzwerken außerhalb der Firewall verbunden sind.

Schritt 6 Wählen Sie im Feld **DMZ-Schnittstelle** die Schnittstelle aus, die mit Ihrem DMZ-Netzwerk verbunden ist.

Schritt 7 Klicken Sie auf **Weiter >**.

Schritt 8 Geben Sie im Feld **IP-Adresse** die IP-Adresse oder den Bereich der IP-Adressen Ihres bzw. Ihrer Webserver ein.

Schritt 9 Wählen Sie im Feld **Dienst** die Option **TCP**.

Schritt 10 Geben Sie im Feld **Port** den Wert **80** oder **www** ein.

Schritt 11 Klicken Sie auf **Weiter >**.

Schritt 12 Klicken Sie auf **Fertig stellen**.

Wie ändere ich eine existierende Firewall, um Datenverkehr von einem neuen Netzwerk oder Host zuzulassen?

Sie können die Firewallkonfiguration auf der Registerkarte Firewallrichtlinie bearbeiten ändern, um Datenverkehr von einem neuen Netzwerk oder Host zuzulassen.

Schritt 1 Wählen Sie im linken Bereich **Firewall und ACL** aus.

Schritt 2 Klicken Sie auf die Registerkarte **Firewallrichtlinie bearbeiten**.

Schritt 3 Wählen Sie im entsprechenden Bereich für den Datenverkehr unter **Von** und **Zu** Schnittstellen aus, um den Datenverkehrsfluss anzugeben, auf welche die Firewall angewandt wird, und klicken Sie auf **Start**. Wenn dem Datenverkehrsfluss eine Firewall zugeordnet wurde, wird ein Firewallsymbol in der Routergrafik angezeigt. Wenn der von Ihnen ausgewählte Datenverkehrsfluss nicht die Zugriffsregel anzeigt, die Sie ändern müssen, wählen Sie unter **Von** oder **Zu** eine andere Schnittstelle aus.

Schritt 4 Untersuchen Sie die Zugriffsregel im Bereich **Dienst**. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein Dialogfeld für einen neuen Zugriffsregeleintrag anzuzeigen.

Schritt 5 Geben Sie eine **permit**-Anweisung für das Netzwerk oder den Host an, dem der Zugriff auf das Netzwerk gewährt werden soll. Klicken Sie im Dialogfeld für die Regeleingabe auf **OK**.

Schritt 6 Der neue Eintrag wird im Dienstbereich angezeigt.

Schritt 7 Verwenden Sie die Schaltflächen **Ausschneiden** und **Einfügen** um den Eintrag an eine andere Position in der Liste zu verschieben, wenn dies erforderlich ist.

Wie konfiguriere ich NAT auf einer nicht unterstützten Schnittstelle?

Cisco SDM kann die Network Address Translation (NAT) auf einem Schnittstellentyp konfigurieren, der von Cisco SDM nicht unterstützt wird. Bevor Sie die Firewall konfigurieren können, müssen Sie die Schnittstelle zunächst mit der CLI des Routers konfigurieren. Die Schnittstelle muss mindestens eine konfigurierte IP-Adresse haben und in Betrieb sein. Um zu überprüfen, ob die Verbindung funktioniert, stellen Sie fest, ob als Schnittstellenstatus **Aktiv** angegeben ist.

Nachdem Sie die nicht unterstützte Schnittstelle mit der CLI konfiguriert haben, können Sie NAT konfigurieren. Die nicht unterstützte Schnittstelle wird in der Liste der Routerschnittstellen als **Andere** angezeigt.

Wie konfiguriere ich NAT Passthrough für eine Firewall?

Wenn Sie NAT konfiguriert haben und jetzt die Firewall konfigurieren, müssen Sie sie so konfigurieren, dass sie Datenverkehr von Ihrer öffentlichen IP-Adresse zulässt. Hierzu müssen Sie eine ACL (Access Control List, Zugriffssteuerungsliste) konfigurieren. So konfigurieren Sie eine ACL, die Datenverkehr von Ihrer öffentlichen IP-Adresse zulässt:

Schritt 1 Wählen Sie im linken Bereich **Zusätzliche Aufgaben** aus.

Schritt 2 Klicken Sie im Baum **Regeln** auf **ACL-Editor** und dann auf **Zugriffsregeln**.

Schritt 3 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Regel hinzufügen** wird angezeigt.

Schritt 4 Geben Sie im Feld **Name/Nummer** einen eindeutigen Namen oder eine eindeutige Nummer für die neue Regel ein.

Schritt 5 Wählen Sie aus dem Feld **Typ** die Option **Standardregel**.

Schritt 6 Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der neuen Regel ein, z. B. „NAT Passthrough zulassen“.

Schritt 7 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Standardregeleintrag hinzufügen** wird angezeigt.

Schritt 8 Wählen Sie im Feld **Aktion** die Option **Zulassen** aus.

Schritt 9 Wählen Sie im Feld **Typ** die Option **Host** aus.

Schritt 10 Geben Sie im Feld **IP-Adresse** Ihre öffentliche IP-Adresse ein.

Schritt 11 Geben Sie im Feld **Beschreibung** eine kurze Beschreibung ein, z. B. „Öffentliche IP-Adresse“.

Schritt 12 Klicken Sie auf **OK**.

Schritt 13 Klicken Sie auf **OK**.

Die neue Regel wird jetzt in der Tabelle **Zugriffsregeln** angezeigt.

Wie lasse ich über eine Firewall Datenverkehr zu meinem Easy VPN-Konzentrator zu?

Um Datenverkehr über Ihre Firewall an einen VPN-Konzentrator zuzulassen, müssen Sie Zugriffs-Regeln erstellen oder ändern, die den VPN-Datenverkehr zulassen. So erstellen Sie diese Regeln:

Schritt 1 Wählen Sie im linken Bereich **Zusätzliche Aufgaben** aus.

Schritt 2 Klicken Sie im Baum **Regeln** auf **ACL-Editor** und dann auf **Zugriffsregeln**.

Schritt 3 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Regel hinzufügen** wird angezeigt.

Schritt 4 Geben Sie im Feld **Name/Nummer** einen eindeutigen Namen oder eine eindeutige Nummer für diese Regel ein.

Schritt 5 Geben Sie im Feld **Beschreibung** eine Beschreibung der Regel ein, z. B. „VPN-Konzentrator-Datenverkehr“.

Schritt 6 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Eintrag für erweiterte Regel hinzufügen** wird angezeigt.

Schritt 7 Wählen Sie in der Gruppe **Quellhost/-netzwerk** im Feld **Typ** die Option **Ein Netzwerk**.

Schritt 8 Geben Sie in die Felder **IP-Adresse** und **Platzhaltermaske** die IP-Adresse und die Netzwerkmaske des VPN-Quell-Peers ein.

Schritt 9 Wählen Sie in der Gruppe **Zielhost/-netzwerk** im Feld **Typ** die Option **Ein Netzwerk**.

Schritt 10 Geben Sie in die Felder **IP-Adresse** und **Platzhaltermaske** die IP-Adresse und die Netzwerkmaske des VPN-Ziel-Peers ein.

Schritt 11 Wählen Sie in der Gruppe **Protokoll und Dienst** die Option **TCP**.

Schritt 12 Wählen Sie in den Quell-Port-Feldern **=**, und geben Sie die Portnummer **1023** ein.

Schritt 13 Wählen Sie in den Ziel-Port-Feldern **=**, und geben Sie die Portnummer **1723** ein.

Schritt 14 Klicken Sie auf **OK**.

Der neue Regeleintrag wird in der Liste **Regeleintrag** angezeigt.

Schritt 15 Wiederholen Sie die Schritte 7 bis 15, und erstellen Sie Regeleinträge für die folgenden Protokolle und, sofern erforderlich, Portnummern:

- Protokoll **IP**, IP-Protokoll **GRE**
- Protokoll **UDP**, Quell-Port **500**, Ziel-Port **500**
- Protokoll **IP**, IP-Protokoll **ESP**
- Protokoll **UDP**, Quell-Port **10000**, Ziel-Port **10000**

Schritt 16 Klicken Sie auf **OK**.

Wie verknüpfe ich eine Regel mit einer Schnittstelle?

Wenn Sie den Cisco SDM-Firewall-Assistenten verwenden, werden die von Ihnen erstellten Zugriffs- und Prüfregeln automatisch mit der Schnittstelle verknüpft, für die Sie die Firewall erstellt haben. Wenn Sie unter **Zusätzliche Aufgaben** im **ACL-Editor** eine Regel erstellen, können Sie sie über das Fenster Regel hinzufügen/bearbeiten mit einer Schnittstelle verknüpfen. Wenn Sie die Regel zu diesem Zeitpunkt nicht mit einer Schnittstelle verknüpfen, haben Sie dazu später noch die Möglichkeit.

Schritt 1 Klicken Sie im linken Bereich auf **Schnittstellen und Verbindungen** und dann auf die Registerkarte **Schnittstellen und Verbindungen bearbeiten**.

Schritt 2 Wählen Sie die Schnittstelle aus, mit der Sie eine Regel verknüpfen möchten, und klicken Sie auf **Bearbeiten**.

Schritt 3 Geben Sie auf der Registerkarte **Verknüpfung** im Gruppenfeld **Zugriffsregel** oder **Prüfregel** im Feld **Eingehend** oder **Ausgehend** den Namen oder die Nummer der Regel ein. Wenn mit der Regel Datenverkehr gefiltert werden soll, bevor er in der Schnittstelle anlangt, verwenden Sie das Feld **Eingehend**. Soll mit der Regel Datenverkehr gefiltert werden, der bereits im Router angelangt ist, den Router aber über die ausgewählte Schnittstelle verlassen kann, verwenden Sie das Feld **Ausgehend**.

Schritt 4 Klicken Sie auf der Registerkarte **Verknüpfung** auf **OK**.

Schritt 5 Überprüfen Sie im Fenster **Zugriffsregeln** oder **Prüfregeln** in der Spalte **Verwendet von**, ob die Regel mit der Schnittstelle verknüpft wurde.

Wie hebe ich die Verknüpfung einer Zugriffsregel mit einer Schnittstelle auf?

Es kann passieren, dass Sie die Verknüpfung zwischen einer Zugriffsregel und einer Schnittstelle aufheben müssen. Mit der Entfernung der Verknüpfung wird nicht die Zugriffsregel gelöscht. Sie können sie nach Wunsch mit anderen Schnittstellen verknüpfen. Führen Sie die folgenden Schritte aus, um die Verknüpfung zwischen einer Zugriffsregel und einer Schnittstelle aufzuheben.

Schritt 1 Klicken Sie im linken Bereich auf **Schnittstellen und Verbindungen** und dann auf die Registerkarte **Schnittstellen und Verbindungen bearbeiten**.

Schritt 2 Wählen Sie die Schnittstelle aus, von der Sie die verknüpfte Zugriffsregel entfernen möchten.

Schritt 3 Klicken Sie auf **Bearbeiten**.

Schritt 4 Ermitteln Sie auf der Registerkarte **Verknüpfung** im Gruppenfeld **Zugriffsregel** im Feld **Eingehend** oder **Ausgehend** die Zugriffsregel. Die Zugriffsregel kann einen Namen oder eine Nummer besitzen.

Schritt 5 Klicken Sie in das Feld **Eingehend** oder **Ausgehend** und dann auf die Schaltfläche rechts.

Schritt 6 Klicken Sie auf **Keine (Regelverknüpfung aufheben)**.

Schritt 7 Klicken Sie auf **OK**.

Wie lösche ich eine Regel, die mit einer Schnittstelle verknüpft ist?

Sie können in Cisco SDM keine Regel löschen, die mit einer Schnittstelle verknüpft ist. Sie müssen zunächst die Verknüpfung zwischen der Regel und der Schnittstelle aufheben und dann die Zugriffsregel löschen.

Schritt 1 Klicken Sie im linken Bereich auf **Schnittstellen und Verbindungen** und dann auf die Registerkarte **Schnittstellen und Verbindungen bearbeiten**.

Schritt 2 Wählen Sie die Schnittstelle aus, von der Sie die verknüpfte Regel entfernen möchten.

Schritt 3 Klicken Sie auf **Bearbeiten**.

Schritt 4 Ermitteln Sie auf der Registerkarte **Verknüpfung** die Regel im Feld **Zugriffsregel** oder **Prüfregel**. Die Regel kann einen Namen oder eine Nummer besitzen.

Schritt 5 Suchen Sie die Regel auf der Registerkarte **Verknüpfung**. **Wenn es sich um eine Zugriffsregel handelt,** klicken Sie auf **Keine (Regelverknüpfung aufheben). Klicken Sie bei einer Prüfregel auf Keine**.

Schritt 6 Klicken Sie auf **OK**.

Schritt 7 Klicken Sie im linken Bereich auf **Regeln**. Verwenden Sie den Baum **Regeln**, um zum Fenster **Zugriffsregel** oder **Prüfregel** zu wechseln.

Schritt 8 Wählen Sie die Regel aus, die Sie entfernen möchten, und klicken Sie auf **Löschen**.

Wie erstelle ich eine Zugriffsregel für eine Java-Liste?

Prüfregeln ermöglichen Ihnen die Angabe von Java-Listen. Eine Java-Liste wird verwendet, um Java Applet-Datenverkehr von vertrauenswürdigen Quellen zuzulassen. Die Quellen sind in einer Zugriffsregel definiert, die die Java-Liste referenziert. Um diese Art von Zugriffsregel zu erstellen und sie in einer Java-Liste zu verwenden, gehen Sie folgendermaßen vor:

Schritt 1 Wenn das Prüfregelfenster angezeigt wird und Sie auf **Java-Liste** geklickt haben, klicken Sie jetzt auf die Schaltfläche rechts neben dem Ziffernfeld und dann auf **Neue Regel erstellen (ACL) und auswählen.** Das Fenster **Regel hinzufügen** wird geöffnet.

Wenn Sie sich im Fenster **Zugriffsregeln** befinden, klicken Sie auf **Hinzufügen**, um das Fenster **Regel hinzufügen** zu öffnen.

Schritt 2 Erstellen Sie vom Fenster **Regel hinzufügen** aus eine Standardzugriffsregel, die Datenverkehr von den Adressen zulässt, die für Sie vertrauenswürdig sind. Beispiel: Wenn Sie Java Applets von den Hosts 10.22.55.3 und 172.55.66.1 zulassen möchten, können Sie im Fenster **Regel hinzufügen** die folgenden Zugriffsregeleinträge erstellen:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

Sie können Beschreibungen für die Einträge und eine Beschreibung für die Regel eingeben.

Sie müssen die Regel nicht mit der Schnittstelle verknüpfen, der Sie die Prüfregel zuordnen.

Schritt 3 Klicken Sie im Dialogfeld **Regel hinzufügen** auf **OK**.

Schritt 4 Wenn Sie mit diesem Verfahren im Fenster **Prüfregeln** begonnen haben, klicken Sie im Fenster **Java-Liste** auf **OK**. Sie müssen nicht die Schritte 5 und 6 ausführen.

Schritt 5 Wenn Sie mit diesem Verfahren im Fenster **Zugriffsregeln** begonnen haben, wechseln Sie in das Fenster **Prüfregeln**, wählen Sie die Prüfregel aus, für die Sie eine Java-Liste erstellen möchten, und klicken Sie auf **Bearbeiten**.

Schritt 6 Aktivieren Sie in der Spalte **Protokolle** die Option **http**, und klicken Sie auf **Java-Liste**.

Schritt 7 Geben Sie im Feld **Java-Listennummer** die Nummer der Zugriffsliste ein, die Sie erstellt haben. Klicken Sie auf **OK**.

Wie lasse ich bestimmten Datenverkehr in meinem Netzwerk zu, wenn ich kein DMZ-Netzwerk besitze?

Sie können im Firewall-Assistenten den Datenverkehr angeben, den Sie in der DMZ zulassen möchten. Wenn Sie kein DMZ-Netzwerk besitzen, können Sie trotzdem mit der Funktion „Firewallrichtlinie“ bestimmte Typen von äußerem Datenverkehr in Ihrem Netzwerk zulassen.

Schritt 1 Konfigurieren Sie mit dem Firewall-Assistenten eine Firewall.

Schritt 2 Klicken Sie auf **Firewallrichtlinie/ACL bearbeiten**.

Schritt 3 Um die Zugriffsregel anzuzeigen, die Sie ändern müssen, wählen Sie unter **Von** die äußere (nicht vertrauenswürdige) Schnittstelle und unter **Zu** die innere (vertrauenswürdige) Schnittstelle aus. Es wird die Zugriffsregel angezeigt, die eingehendem Datenverkehr auf der nicht vertrauenswürdigen Schnittstelle zugeordnet ist.

Schritt 4 Um einen bestimmten Typ von Datenverkehr, der nicht bereits zugelassen ist, für das Netzwerk zuzulassen, klicken Sie im Bereich **Dienst** auf **Hinzufügen**.

Schritt 5 Erstellen Sie im Dialogfeld für die Regeleingabe die benötigten Einträge. Sie müssen für jeden Eintrag, den Sie erstellen, auf **Hinzufügen** klicken.

Schritt 6 Die von Ihnen erstellten Einträge werden im Bereich **Dienst** in der Eintragsliste angezeigt.

KAPITEL 7

Firewallrichtlinie

Mit der Funktion **Firewallrichtlinie** können Sie Firewallkonfigurationen – Zugriffsregeln und/oder CBAC-Prüfregeln – im Kontext der Schnittstellen, deren Datenverkehr sie filtern, anzeigen und modifizieren. In einer grafischen Darstellung der Router und ihrer Schnittstellen können Sie verschiedene Schnittstellen auf dem Router auswählen und einsehen, ob der Schnittstelle eine Zugriffs- oder Prüfregel zugeordnet wurde. Sie können außerdem Details der im Fenster **Firewallrichtlinie/ACL bearbeiten** angezeigten Regeln anzeigen.

Firewallrichtlinie/ACL bearbeiten

Zeigen Sie im Fenster **Firewallrichtlinie/ACL bearbeiten** die Zugriffs- und Prüfregeln in einem Kontext an, in dem die Schnittstellen angezeigt werden, mit denen die Regeln verknüpft sind. Verwenden Sie es außerdem zum Ändern der angezeigten Zugriff- und Prüfregeln.

Konfigurieren einer Firewall vor Verwendung der Funktion „Firewallrichtlinie“

Führen Sie folgenden Aufgaben aus, bevor Sie das Fenster **Firewallrichtlinie/ACL bearbeiten** verwenden:

1. **Konfigurieren Sie LAN- und WAN-Schnittstellen.** Sie müssen die LAN- und WAN-Schnittstellen konfigurieren, bevor Sie eine Firewall erstellen können. Sie können den LAN- und den WAN-Assistenten verwenden, um Verbindungen für Ihren Router zu konfigurieren.

2. **Verwenden Sie den Firewall-Assistenten, um eine Firewall und eine DMZ zu konfigurieren.** Der Firewall-Assistent ist die einfachste Möglichkeit, Zugriffsregeln und Prüfregeln den von Ihnen angegebenen inneren und äußeren Schnittstellen zuzuordnen. Mit ihm können Sie außerdem eine DMZ-Schnittstelle konfigurieren und die Dienste angeben, die Sie für das DMZ-Netzwerk zulassen möchten.
3. **Wechseln Sie in das Fenster mit der Firewallrichtlinie, um die von Ihnen erstellte Firewallrichtlinie zu bearbeiten.** Nachdem Sie LAN- und WAN-Schnittstellen konfiguriert und eine Firewall erstellt haben, können Sie dieses Fenster öffnen, um eine grafische Darstellung der Richtlinie in einem Datenverkehrsfluss zu erhalten. Sie können die Zugriffsregel- und Prüfregeleinträge anzeigen und die notwendigen Änderungen vornehmen.

Verwenden der Funktion „Firewallrichtlinienansicht“

Nachdem Sie die Firewall erstellt haben, können Sie das Fenster **Firewallrichtlinienansicht** verwenden, um eine grafische Darstellung der Firewall im Kontext der Routerschnittstellen zu erhalten und sie nach Bedarf zu ändern.

Klicken Sie für weitere Informationen auf die durchzuführende Aktion:

- Wählen eines Datenverkehrsflusses
- Untersuchen des Datenverkehrsdiagramms und Auswählen einer Datenverkehrsrichtung
- Vornehmen von Änderungen an den Zugriffsregeln
- Ändern von Prüfregeln

Ein Anwendungsbeispiel finden Sie unter Beispielszenario zur Verwendung der Firewallrichtlinien.

Hinweis Wenn der Router ein Cisco IOS-Abbild verwendet, das nicht den Firewall-Funktionssatz unterstützt, wird nur der Bereich **Dienste** angezeigt, und Sie können nur Zugriffssteuerungseinträge erstellen.

Schaltfläche „Änderungen übernehmen“

Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie in diesem Fenster vorgenommen haben, an den Router zu senden. Wenn Sie das Fenster **Firewallrichtlinie/ACL bearbeiten** schließen, ohne auf **Änderungen übernehmen** zu klicken, wird in Cisco SDM die Meldung angezeigt, dass Sie die Änderungen entweder übernehmen oder verwerfen müssen.

Schaltfläche „Änderungen nicht übernehmen“

Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie in diesem Fenster vorgenommen haben, zu verwerfen. Mit dieser Schaltfläche können Sie keine Änderungen entfernen, die Sie mit der Schaltfläche **Änderungen übernehmen** an den Router gesendet haben.

Wählen eines Datenverkehrsflusses

Datenverkehrsfluss bezieht sich auf Datenverkehr, der auf einer angegebenen Schnittstelle beim Router eingeht (der *Von*-Schnittstelle) und auf einer angegebenen Schnittstelle des Routers abgeht (der *Zu*-Schnittstelle). Die Cisco SDM-Datenverkehrsfluss-Anzeigesteuerungen befinden sich in einer Zeile oben im Fenster **Firewallrichtlinie/ACL bearbeiten**.

Hinweis Es muss mindestens zwei konfigurierte Schnittstellen auf dem Router geben. Wenn es nur eine gibt, werden Sie in Cisco SDM über eine Meldung aufgefordert, eine weitere Schnittstelle zu konfigurieren.

Die folgende Tabelle definiert die Cisco SDM-Datenverkehrsfluss-Anzeigesteuerungen.

Von	Wählen Sie die Schnittstelle aus, von welcher der Datenverkehrsfluss, der für Sie von Interesse ist, abgeht. Die Firewall schützt das Netzwerk, das mit der Von-Schnittstelle verbunden ist. Die Dropdown-Liste **Von** enthält nur Schnittstellen mit konfigurierten IP-Adressen.
Zu	Wählen Sie die Schnittstelle aus, auf welcher der Datenverkehr vom Router abgeht. Die Dropdown-Liste **Zu** enthält nur Schnittstellen mit konfigurierten IP-Adressen.
	Schaltfläche „Details“. Klicken Sie auf diese Schaltfläche, um Details zur Schnittstelle anzuzeigen. Es werden Details wie IP-Adresse, Kapselungstyp, verknüpfte IPSec-Richtlinie und Authentifizierungstyp angegeben.
Schaltfläche „Start“	Klicken Sie, um das Datenverkehrsflussdiagramm mit den Informationen über die ausgewählten Schnittstellen zu aktualisieren. Das Diagramm wird erst aktualisiert, wenn Sie auf **Start** klicken. Die Schaltfläche **Start** ist deaktiviert, wenn Sie keine Von- oder Zu-Schnittstelle ausgewählt haben oder für **Von** und **Zu** dieselbe Schnittstelle angegeben ist.
Ansichtsoption	Wählen Sie **Von- und Zu-Schnittstelle tauschen**, um die Schnittstellen zu tauschen, die Sie ursprünglich in den Dropdown-Listen **Von** und **Zu** ausgewählt haben. Sie können die Option zum Tauschen verwenden, wenn Sie eine Firewall erstellen möchten, die sowohl das mit der Von-Schnittstelle als auch das mit der Zu-Schnittstelle verbundene Netzwerk schützt. Sie können **Alle ACLs im Datenverkehrsfluss anzeigen** auswählen, wenn für eine von Ihnen ausgewählte Datenverkehrsrichtung der Von-Schnittstelle eine Zugriffsregel und der Zu-Schnittstelle eine andere Zugriffsregel zugeordnet wurde. Die Einträge beider Zugriffsregeln werden in einem weiteren Fenster angezeigt.

Cisco SDM zeigt in den Dropdown-Listen **Von** und **Zu** alle Schnittstellen mit IP-Adressen in alphabetischer Reihenfolge an. Standardmäßig wählt Cisco SDM die erste Schnittstelle in der Liste **Von** und die zweite Schnittstelle in der Liste **Zu** aus. Wählen Sie anhand der Dropdown-Listen **Von** und **Zu** einen unterschiedlichen Datenverkehrsfluss aus. Der ausgewählte Datenverkehrsfluss wird im Datenverkehrsdiagramm unter den Datenverkehrsfluss-Anzeigesteuerungen angezeigt.

Um beispielsweise den Datenverkehrsfluss anzuzeigen, der von einem Netzwerk ausgeht, das mit der Router-Schnittstelle „Ethernet 0“ verbundenen ist, und der auf der Router-Schnittstelle „Seriell 0“ abgeht, befolgen Sie die folgenden Schritte:

Schritt 1 Wählen Sie **Ethernet 0** in der Dropdown-Liste **Von**.

Schritt 2 Wählen Sie **Seriell 0** in der Dropdown-Liste **Zu**.

Schritt 3 Klicken Sie auf **Start**.

Schritt 4 Wenn Sie die Schnittstellen in den Dropdown-Listen **Von** und **Zu** tauschen möchten, wählen Sie **Von- und Zu-Schnittstelle tauschen** aus der Dropdown-Liste **Ansichtsoption**.

Die auf den abgehenden und eingehenden Datenverkehr angewandten Zugriffsregeln können unterschiedlich sein. Wenn Sie mehr darüber erfahren möchten, wie Sie die Anzeige zwischen abgehendem und eingehendem Datenverkehr im Datenverkehrsdiagramm umschalten können, siehe Untersuchen des Datenverkehrsdiagramms und Auswählen einer Datenverkehrsrichtung.

Schritt 5 Klicken Sie auf die Schaltfläche **Details** neben der Dropdown-Liste **Von** oder **Zu**, um ein Fenster zu öffnen, das die IP-Adresse, die IPSec-Richtlinie und andere Informationen einer Schnittstelle zeigt.

Um mit dem Datenverkehrsdiagramm zu arbeiten, siehe Untersuchen des Datenverkehrsdiagramms und Auswählen einer Datenverkehrsrichtung. Wenn Sie zur Beschreibung des Haupt-Firewallrichtlinien-Fensters zurückkehren möchten, siehe Firewallrichtlinie/ACL bearbeiten.

Untersuchen des Datenverkehrsdiagramms und Auswählen einer Datenverkehrsrichtung

Das Datenverkehrsdiagramm zeigt den Router mit den ausgewählten Von- und Zu-Schnittstellen (siehe Wählen eines Datenverkehrsflusses für weitere Informationen). Es zeigt auch die Regeltypen an, die auf den gewählten Datenverkehrsfluss angewandt werden, sowie die Richtung, auf die sie angewandt werden.

Abgehender Datenverkehr

Klicken Sie auf diese Option, um den Datenverkehrsfluss zu markieren, der auf der Von-Schnittstelle beim Router eingeht und beim Router über die Zu-Schnittstelle wieder abgeht. Wenn dieser Bereich hervorgehoben ist, werden die Details der Regeln angezeigt, die in der Richtung des Datenverkehrsflusses angewandt werden.

Eingehender Datenverkehr

Klicken Sie auf diese Option, um den Datenverkehrsfluss zu markieren, der auf der Zu-Schnittstelle beim Router eingeht und beim Router über die Von-Schnittstelle wieder abgeht. Wenn dieser Bereich hervorgehoben ist, werden die Details der Regeln angezeigt, die auf den eingehenden Datenverkehr angewandt werden.

Symbole

Regeln werden im Datenverkehrsfluss durch Symbole dargestellt:

	Ein Filtersymbol gibt an, dass eine Zugriffsregel angewandt wird.
	Eine Lupe gibt an, dass eine Prüfregel angewandt wird.

	Ein Firewallsymbol im Router gibt an, dass auf den abgehenden Datenverkehrsfluss eine Firewall angewandt wird. Cisco SDM zeigt ein Firewallsymbol an, wenn die folgenden Kriterien erfüllt sind: • Dem abgehenden Datenverkehr in der Eingangsrichtung der Von-Schnittstelle ist eine Prüfregel zugeordnet, und der Eingangsrichtung der Zu-Schnittstelle ist eine Zugriffsregel zugeordnet. • Die Zugriffsregel in der Eingangsrichtung der Zu-Schnittstelle ist eine erweiterte Zugriffsregel, und sie enthält mindestens einen Zugriffsregeleintrag. Wenn dem eingehenden Datenverkehr eine Firewall zugeordnet wurde, wird kein Firewallsymbol angezeigt. Wenn die Firewallfunktion verfügbar ist, aber keine Firewall auf den Datenverkehrsfluss angewandt wurde, wird **IOS Firewall: Inaktiv** unter dem Datenverkehrsdiagramm angezeigt.
	Regeln, die dem abgehenden Datenverkehr zugeordnet sind, werden durch einen nach rechts weisenden Pfeil angegeben. Ein Symbol auf der Datenverkehrsleitung der Von-Schnittstelle gibt an, dass eine Regel vorhanden ist, die den eingehenden Datenverkehr des Routers filtert. Ein Symbol, das auf der Datenverkehrsleitung der Zu-Schnittstelle platziert ist, gibt eine Regel an, die den ausgehenden Datenverkehr des Routers filtert. Wenn Sie mit dem Mauszeiger auf dieses Symbol zeigen, zeigt Cisco SDM die Namen der angewandten Regeln an.
	Regeln, die dem eingehenden Datenverkehr zugeordnet sind, werden durch einen nach links weisenden Pfeil angegeben. Ein Symbol auf der Datenverkehrsleitung der Zu-Schnittstelle gibt an, dass eine Regel vorhanden ist, die den eingehenden Datenverkehr des Routers filtert. Ein Symbol auf der Datenverkehrsleitung der Von-Schnittstelle gibt an, dass eine Regel vorhanden ist, die den ausgehenden Datenverkehr des Routers filtert. Wenn Sie den Mauszeiger auf dieses Symbol bewegen, werden die Namen der zugeordneten Regeln angezeigt.

Hinweis Auch wenn die Symbole auf einer bestimmten Schnittstelle im Diagramm angezeigt werden, kann eine Firewallrichtlinie Zugriffssteuerungseinträge enthalten, die sich auf Datenverkehr auswirken, der nicht durch das Diagramm dargestellt wird. Beispiel: Ein Eintrag, der das Platzhaltersymbol in der Spalte für das Ziel enthält (siehe Vornehmen von Änderungen an den Zugriffsregeln), kann für Datenverkehr gelten, der von anderen Schnittstellen als der Schnittstelle abgeht, die durch die aktuell ausgewählte Zu-Schnittstelle dargestellt wird. Das Platzhaltersymbol erscheint als Sternchen und steht für ein beliebiges Netzwerk oder einen beliebigen Host.

Informationen darüber, wie Sie die Zugriffsregel ändern können, finden Sie unter Vornehmen von Änderungen an den Zugriffsregeln. Wenn Sie zur Beschreibung des Haupt-Firewallrichtlinien-Fensters zurückkehren möchten, siehe Firewallrichtlinie/ACL bearbeiten.

Vornehmen von Änderungen an den Zugriffsregeln

Im Richtlinienbereich werden die Details der Regeln angezeigt, die auf den ausgewählten Datenverkehrsfluss angewandt werden. Der Richtlinienbereich wird aktualisiert, wenn die Von- und die Zu-Schnittstelle ausgewählt wird und wenn im Datenverkehrsdiagramm zwischen der Darstellung für den abgehenden Datenverkehr und der Darstellung für den eingehenden Datenverkehr gewechselt wird.

Der Richtlinienbereich ist leer, wenn eine Zugriffsregel ohne Einträge mit einer Schnittstelle verknüpft wurde. Beispiel: Wenn über die CLI ein Regelname mit einer Schnittstelle verknüpft wurde, aber keine Einträge für die Regel erstellt wurden, ist dieser Bereich leer. Wenn der Richtlinienbereich leer ist, können Sie über die Schaltfläche **Hinzufügen** Einträge für die Regel erstellen.

Felder in der Kopfzeile des Dienstbereichs

Firewall-Funktionsverfügbarkeit	Wenn das vom Router verwendete Cisco IOS-Abbild die Firewallfunktion unterstützt, enthält dieses Feld den Wert **Verfügbar**.
Zugriffsregel	Der Name oder die Nummer der Zugriffsregel, deren Einträge angezeigt werden.
Prüfregel	Der Name oder die Nummer der Prüfregel, deren Einträge angezeigt werden.
	Dieses Symbol wird angezeigt, wenn eine Zugriffsregel mit einer Schnittstelle verknüpft wurde, aber keine Zugriffregel mit diesem Namen oder dieser Nummer erstellt wurde. Sie werden in Cisco SDM darüber informiert, dass diese Richtlinie erst wirksam wird, wenn es mindestens einen Zugriffsregeleintrag gibt.

Steuerungen im Dienstbereich

In der folgenden Tabelle werden die Steuerungen im Dienstbereich beschrieben.

Schaltfläche „Hinzufügen“	Klicken Sie auf diese Schaltfläche, um einen Zugriffsregeleintrag hinzuzufügen. Geben Sie an, ob Sie den Eintrag vor oder hinter dem derzeit markierten Eintrag hinzufügen möchten. Erstellen Sie anschließend den Eintrag im Fenster **Add an Entry** (Eintrag hinzufügen) Denken Sie daran, dass die Reihenfolge der Einträge wichtig ist. Cisco SDM zeigt das Eingabedialogfeld **Erweitert** an, wenn Sie einen Eintrag aus dem Fenster **Firewallrichtlinie/ACL bearbeiten** hinzufügen. Wenn Sie einen Standard-Regeleintrag hinzufügen möchten, wählen Sie **Zusätzliche Aufgaben > ACL-Editor > Zugriffsregeln**.

Schaltfläche „Bearbeiten“	Klicken Sie auf diese Schaltfläche, um einen markierten Zugriffsregeleintrag zu bearbeiten. Auch wenn Sie im Fenster **Firewallrichtlinie/ACL bearbeiten** nur erweiterte Regeleinträge hinzufügen können, haben Sie dennoch die Möglichkeit, einen Standardregeleintrag zu bearbeiten, der bereits auf eine ausgewählte Schnittstelle angewandt wurde.
Schaltfläche „Ausschneiden“	Klicken Sie auf diese Schaltfläche, um einen markierten Zugriffsregeleintrag zu entfernen. Der Eintrag wird in die Zwischenablage genommen und kann an einer anderen Position in der Liste oder in eine andere Zugriffsregel eingefügt werden. Wenn Sie einen Eintrag verschieben möchten, können Sie den Eintrag ausschneiden, einen Eintrag vor oder hinter der für den ausgeschnittenen Eintrag gewünschten Position auswählen und auf **Einfügen** klicken. Über das Kontextmenü von **Einfügen** können Sie den Eintrag vor oder hinter dem gewählten Eintrag platzieren.
Schaltfläche „Kopieren“	Markieren Sie einen Regeleintrag, und klicken Sie auf diese Schaltfläche, um den Regeleintrag in die Zwischenablage zu stellen.
Schaltfläche „Einfügen“	Klicken Sie auf diese Schaltfläche, um einen Eintrag von der Zwischenablage in die ausgewählte Regel einzufügen. Sie müssen angeben, ob Sie den Eintrag vor oder hinter dem derzeit markierten Eintrag einfügen möchten. Wenn Cisco SDM ermittelt, dass bereits ein identischer Eintrag in der Zugriffsregel existiert, wird das Fenster **Eintrag für erweiterte Regel hinzufügen** angezeigt, damit Sie den Eintrag ändern können. Doppelte Einträge in derselben Regel sind in Cisco SDM unzulässig.
Dropdown-Liste „Schnittstelle“	Wenn der ausgewählte Datenverkehrsfluss (abgehend oder eingehend) sowohl für die Von- als auch für die Zu-Schnittstelle eine Zugriffsregel enthält, können Sie mit dieser Liste zwischen den beiden Regeln wechseln.

Firewall anwenden	Wenn dem ausgewählten Datenverkehrsfluss keine Firewall zugeordnet ist, können Sie eine Firewall zuordnen, indem Sie **Abgehender Datenverkehr** auswählen und auf die Schaltfläche **Firewall anwenden** klicken. Standardmäßig wird durch Klicken auf **Firewall anwenden** der Eingangsrichtung der Von-Schnittstelle eine Cisco SDM-Standardprüfregel zugeordnet. Der Eingangsrichtung der Zu-Schnittstelle wird eine Zugriffsregel zugeordnet, die keinen Datenverkehr zulässt. Wenn das vom Router verwendete Cisco IOS-Abbild die Firewallfunktion nicht unterstützt, ist diese Schaltfläche deaktiviert. Um beispielsweise eine Firewall zuzuordnen, die das mit Schnittstelle **Ethernet 0** verbundene Netzwerk vor Datenverkehr schützt, der auf der Schnittstelle **Ethernet 1** eingeht, wählen Sie **Ethernet 0** aus der Dropdown-Liste **Von** und **Ethernet 1** aus der Dropdownliste **Zu**. Klicken Sie dann auf **Firewall anwenden**. Wenn Sie eine Firewall zuordnen möchten, die das mit Schnittstelle Ethernet 1 verbundene Netzwerk vor Datenverkehr schützt, der auf der Schnittstelle Ethernet 0 eingeht, wählen Sie **Zusätzliche Aufgaben > ACL-Editor > Zugriffsregeln**.

Die Schaltflächen im Dienstbereich sind deaktiviert, wenn die Regel schreibgeschützt ist. Eine Regel ist schreibgeschützt, wenn sie Syntax enthält, die von Cisco SDM nicht unterstützt wird. Schreibgeschützte Regeln werden durch dieses Symbol gekennzeichnet:  .

Wenn eine Standardregel vorhanden ist, die den eingehenden Datenverkehrsfluss filtert, dem Sie die Firewall zuordnen, werden Sie in Cisco SDM darüber informiert, dass die Standardzugriffsregel in eine erweiterte Regel konvertiert wird.

Eintragsfelder im Dienstbereich

In der folgenden Tabelle werden die Symbole und weitere Daten in den Einträgen im Dienstbereich beschrieben.

Feld	Beschreibung	Symbole	Bedeutung
Aktion	Angabe, ob der Datenverkehr zugelassen oder verweigert wird		Zulassen von Quelldatenverkehr
			Verweigern von Quelldatenverkehr
Quelle/ Ziel	Netzwerk- oder Hostadresse oder ein Host oder Netzwerk		Die Adresse eines Netzwerks
			Die Adresse eines Hosts
			Ein Netzwerk oder ein Host
Dienst	Typ des gefilterten Dienstes		Beispiel: TCP, EIGRP, UDP, GRE Siehe IP-Dienste.
			Beispiel: Telnet, http, FTP Siehe TCP-Dienste.
			Beispiel: SNMP, bootpc, RIP Siehe UDP-Dienste.
			IGMP (Internet Group Management Protocol)
			Beispiel: echo-reply, host-unreachable Siehe ICMP-Meldungstypen.
Protokoll	Angabe, ob verweigerter Datenverkehr protokolliert wird		Protokollieren von verweigertem Datenverkehr Um Logging für Firewalls zu konfigurieren, schauen Sie bitte unter Firewall-Protokoll nach.

Feld	Beschreibung	Symbole	Bedeutung
Option	Optionen, die unter Verwendung der CLI konfiguriert sind	Keine Symbole	
Beschreibung	Entsprechend angegebene Beschreibung	Keine Symbole	

Informationen darüber, wie Sie die Prüfregeln ändern können, finden Sie unter Ändern von Prüfregeln. Wenn Sie zur Beschreibung des Haupt-Firewallrichtlinien-Fensters zurückkehren möchten, siehe Firewallrichtlinie/ACL bearbeiten.

Ändern von Prüfregeln

Der Bereich **Anwendungen** wird angezeigt, wenn das auf dem Router ausgeführte Cisco IOS-Abbild CBAC-Prüfregeln unterstützt. Der Bereich **Anwendungen** zeigt die Prüfregeleinträge an, die den Datenverkehrsfluss filtern, und wird jeweils aktualisiert, wenn ein neuer Datenverkehrsfluss gewählt wird. Es wird die Prüfregel angezeigt, welche sich auf die gewählte Datenverkehrsrichtung auswirkt.

Im Bereich **Anwendungen** wird für den **abgehenden Datenverkehr** eine der folgenden Regeln angezeigt:

- Die Prüfregel, die der Eingangsrichtung der Von-Schnittstelle zugeordnet ist (sofern vorhanden)
- Die Prüfregel, die in ausgehender Richtung der Zu-Schnittstelle zugeordnet ist, wenn der eingehenden Richtung der Von-Schnittstelle keine Prüfregel zugeordnet wurde.

Tauschen der Von- und Zu-Schnittstelle, um andere Regeln anzuzeigen

Prüfregeln, die dem **eingehenden Datenverkehr** zugeordnet sind, werden nicht angezeigt. Sie können eine Prüfregel, die dem **eingehenden Datenverkehr** zugeordnet ist, anzeigen, indem Sie im Menü **Ansichtsoption** auf **Von- und Zu-Schnittstelle tauschen** klicken. Sie können auch Prüfregeln anzeigen, die nicht im Fenster **Firewallrichtlinie/ACL bearbeiten** angezeigt werden, indem Sie das Fenster **Anwendungssicherheit** der Aufgabe **Firewall und ACL** aufrufen.

⚠	Dieses Symbol wird angezeigt, wenn zwei Prüfregeln in der ausgewählten Datenverkehrsrichtung gefunden werden. Cisco SDM zeigt außerdem ein Dialogfeld mit einer Warnung an, und Sie haben die Möglichkeit, die Verknüpfung einer der Prüfregeln mit der Schnittstelle aufzuheben.

Steuerungen im Bereich „Anwendung“

Nachfolgend finden Sie eine Liste der Steuerungen im Bereich **Anwendung**.

Hinzufügen – Klicken Sie auf diese Schaltfläche, um eine Prüfregel hinzuzufügen. Wenn es keine Prüfregel gibt, können Sie die Cisco SDM-Standardprüfregel hinzufügen oder eine benutzerdefinierte Prüfregel erstellen und hinzufügen. Wenn Sie die Cisco SDM-Standardprüfregel zu einem Datenverkehrsfluss ohne Prüfregel hinzufügen, wird sie mit dem eingehenden Datenverkehr zur Von-Schnittstelle verknüpft. Sie können einen Eintrag für eine spezifische Anwendung unabhängig davon hinzufügen, ob bereits eine Prüfregel existiert.

Bearbeiten – Klicken Sie auf diese Schaltfläche, um den gewählten Eintrag zu bearbeiten.

Löschen – Klicken Sie auf diese Schaltfläche, um den gewählten Eintrag zu löschen.

Globale Einstellungen – Klicken Sie auf diese Schaltfläche, um ein Dialogfeld anzuzeigen, mit dem Sie globale Timeouts und Grenzwerte festlegen können.

Übersicht – Klicken Sie auf diese Schaltfläche, um den Anwendungs- oder Protokollnamen und eine Beschreibung für jeden Eintrag anzuzeigen.

Detail – Klicken Sie auf diese Schaltfläche, um den Anwendungs- oder Protokollnamen, die Beschreibung, den Alarmstatus, den Überwachungslistenstatus und die Timeout-Einstellungen für jeden Eintrag anzuzeigen.

Eintragsfelder im Bereich „Anwendungen“

In der folgenden Liste werden die Eintragsfelder im Bereich **Anwendungen** beschrieben.

Anwendungsprotokoll – Zeigt den Namen der Anwendung oder des Protokolls an. Zum Beispiel **vdolive**.

Alarm – Gibt an, ob ein Alarm ein- (Standard) oder ausgeschaltet ist.

Überwachungsliste – Gibt an, ob eine Überwachungsliste ein- oder ausgeschaltet (Standard) ist.

Timeout – Zeigt an, wie lange der Router (in Sekunden) warten soll, bevor eingehender Datenverkehr für dieses Protokoll oder diese Anwendung blockiert wird.

Beschreibung – Zeigt eine kurze Beschreibung an. Zum Beispiel **VDOLive-Protokoll**.

Wenn Sie zur Beschreibung des Haupt-Firewallrichtlinien-Fensters zurückkehren möchten, siehe Firewallrichtlinie/ACL bearbeiten.

Anwendungseintrag für *Anwendungsname* hinzufügen

Fügen Sie in diesem Fenster einen Anwendungseintrag hinzu, der von der Cisco IOS-Firewall geprüft werden soll.

Warnungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (ein)** – Als Standard lassen. Der Standardwert ist **ein**.
- **ein** – Alarm aktivieren.
- **aus** – Alarm deaktivieren.

Prüfungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (aus)** – Als Standard lassen. Der Standardwert ist **aus**.
- **ein** – Überwachungsliste aktivieren.
- **aus** – Überwachungsliste deaktivieren.

Timeout

Geben Sie an, wie lange der Router warten soll, bevor eingehender Datenverkehr für dieses Protokoll oder diese Anwendung blockiert wird. In das Feld ist bereits der Standardwert für das Protokoll oder die Anwendung eingetragen.

Anwendungseintrag für RPC hinzufügen

Fügen Sie in diesem Fenster die Nummer eines RPC-Programms (Remote Procedure Call) hinzu, und geben Sie Warn-, Prüf-, Timeout- und Wartezeiteinstellungen ein.

Warnungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (ein)** – Als Standard lassen. Der Standardwert ist **ein**.
- **ein** – Alarm aktivieren.
- **aus** – Alarm deaktivieren.

Prüfungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (aus)** – Als Standard lassen. Der Standardwert ist **aus**.
- **ein** – Überwachungsliste aktivieren.
- **aus** – Überwachungsliste deaktivieren.

Timeout

Geben Sie an, wie lange der Router warten soll, bevor eingehender Datenverkehr für dieses Protokoll oder diese Anwendung blockiert wird. In das Feld ist bereits der Standardwert eingetragen.

Programmnummer

Geben Sie eine einzelne Programmnummer dieses Feld ein.

Wartezeit

Sie können die Zeitdauer in Minuten angeben, während der nachfolgende RPC-Verbindungen von derselben Quelle zur selben Zieladresse und zum selben Port hergestellt werden dürfen. Die Standardwartezeit ist null Minuten.

Anwendungseintrag für Fragment hinzufügen

In diesem Fenster können Sie einen Fragmenteintrag zu einer Prüfregel hinzufügen, die Sie im Fenster **Firewallrichtlinie/ACL bearbeiten** konfigurieren. Sie können außerdem Warn-, Prüf- und Timeout-Einstellungen vornehmen. Ein Fragmenteintrag legt die maximale Anzahl von nicht wieder zusammengesetzten Paketen fest, die der Router akzeptiert, bevor diese entfernt werden.

Warnungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (ein)** – Als Standard lassen. Der Standardwert ist **ein**.
- **ein** – Alarm aktivieren.
- **aus** – Alarm deaktivieren.

Prüfungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (aus)** – Als Standard lassen. Der Standardwert ist **aus**.
- **ein** – Überwachungsliste aktivieren.
- **aus** – Überwachungsliste deaktivieren.

Timeout

Geben Sie an, wie lange der Router warten soll, bevor eingehender Datenverkehr für dieses Protokoll oder diese Anwendung blockiert wird. In das Feld ist bereits der Standardwert eingetragen.

Bereich (optional)

Geben Sie die maximale Anzahl von nicht wieder zusammengesetzten Paketen ein, die der Router akzeptiert, bevor diese entfernt werden. Der Bereich kann einen Wert zwischen 50 und 10000 haben.

Anwendungseintrag für HTTP hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um eine HTTP-Anwendung zur Prüfregel hinzuzufügen.

Warnungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (ein)** – Als Standard lassen. Der Standardwert ist **ein**.
- **ein** – Alarm aktivieren.
- **aus** – Alarm deaktivieren.

Prüfungsaktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Standard (aus)** – Als Standard lassen. Der Standardwert ist **aus**.
- **ein** – Überwachungsliste aktivieren.
- **aus** – Überwachungsliste deaktivieren.

Timeout

Geben Sie an, wie lange der Router warten soll, bevor eingehender Datenverkehr für dieses Protokoll oder diese Anwendung blockiert wird. In das Feld ist bereits der Standardwert eingetragen.

Host/Netzwerke für Java Applet-Download

Die Quellhosts oder -netzwerke, deren Applet-Datenverkehr geprüft werden soll. Es können mehrere Hosts und Netzwerke angegeben werden.

Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Java Applet-Blockierung** anzuzeigen, in dem Sie ein Host oder Netzwerk angeben können.

Klicken Sie auf **Löschen**, um einen Eintrag aus der Liste zu entfernen.

Java Applet-Blockierung

Geben Sie in diesem Fenster an, ob Java Applets von einem angegebenen Netzwerk oder Host zugelassen oder abgelehnt werden sollen.

Aktion

Wählen Sie eine der folgenden Möglichkeiten:

- **Nicht blockieren (Zulassen)** – Java Applets von diesem Netzwerk oder Host zulassen.
- **Blockieren (Verweigern)** – Java Applets von diesem Netzwerk oder Host ablehnen.

Host/Netzwerk

Geben Sie das Netzwerk oder den Host an.

Typ

Wählen Sie eine der folgenden Möglichkeiten:

- **Ein Netzwerk** – Wenn Sie diese Option wählen, geben Sie eine Netzwerkadresse in das Feld **IP-Adresse** ein. Beachten Sie, dass Sie mit der Platzhaltermaske eine Netzwerknummer eingeben können, die mehrere Subnetze angeben kann.
- **Ein Hostname oder eine IP-Adresse** – Wenn Sie diese Option wählen, geben Sie eine Host-IP-Adresse oder einen Hostnamen im nächsten Feld an.
- **Beliebige IP-Adresse** – Wenn Sie diese Option wählen, wird die von Ihnen angegebene Aktion jedem Host oder Netzwerk zugeordnet.

IP-Adresse/Platzhaltermaske

Geben Sie eine Netzwerkadresse und dann die Platzhaltermaske ein, um anzugeben, wie viele Teile der Netzwerkadresse genau übereinstimmen müssen.

Wenn Sie z. B. die Netzwerkadresse 10.25.29.0 und die Platzhaltermaske 0.0.0.255 eingeben, werden alle Java Applets mit einer Quelladresse, die 10.25.29 enthält, gefiltert. Wenn die Platzhaltermaske 0.0.255.255 lautet, werden alle Java Applets mit einer Quelladresse, die 10.25 enthält, gefiltert.

Hostname/IP

Dieses Feld wird angezeigt, wenn Sie **Ein Hostname oder eine IP-Adresse** als Typ ausgewählt haben. Wenn Sie einen Hostnamen eingeben, stellen Sie sicher, dass sich ein DNS-Server im Netzwerk befindet, der den Hostnamen in eine IP-Adresse auflösen kann.

Cisco SDM-Warnung: Prüfregel

Dieses Fenster wird angezeigt, wenn Cisco SDM zwei Prüfregeln ermittelt, die für eine Richtung in einem Datenverkehrsfluss konfiguriert wurden. Sie haben z. B. eine Prüfregel, die dem eingehenden Datenverkehr auf der Von-Schnittstelle zugeordnet ist, und eine andere Regel, die dem ausgehenden Datenverkehr auf der Zu-Schnittstelle zugeordnet ist. Zwei Prüfregeln beeinträchtigen wahrscheinlich nicht die Funktionen des Routers, können aber unnötig sein. Sie haben in Cisco SDM die Möglichkeit, die Prüfregeln unverändert beizubehalten oder die Regel auf der Von- oder auf der Zu-Schnittstelle zu entfernen.

- **Keine Änderungen vornehmen** – Cisco SDM entfernt keine der Prüfregeln.
- **Prüfregel*name* auf** <Schnittstellenname> beibehalten**, eingehend, und Verknüpfung für Prüfregel*name* auf** <Schnittstellenname> ***aufheben,*** **ausgehend** – Cisco SDM behält eine Prüfregel bei und hebt die Verknüpfung der Regel mit der anderen Schnittstelle auf.
- **Prüfregel*name* auf** <Schnittstellenname> ***beibehalten*****, ausgehend, und Verknüpfung für Prüfregel*name* auf** <Schnittstellenname> ***aufheben,*** **eingehend** – Cisco SDM behält eine Prüfregel bei und hebt die Verknüpfung der Regel mit der anderen Schnittstelle auf.

Bevor Sie eine Auswahl treffen und auf **OK** klicken, sollten Sie auf **Abbrechen** klicken und dann überprüfen, ob Sie Einträge zu der Prüfregel hinzufügen müssen, die Sie beibehalten möchten. Sie können anhand der Schaltfläche **Hinzufügen** in der Symbolleiste des Anwendungsbereichs im Fenster **Firewallrichtlinie/ACL bearbeiten** Einträge hinzufügen.

Cisco SDM-Warnung: Firewall

Dieses Fenster wird angezeigt, wenn Sie im Fenster **Firewallrichtlinie/ACL bearbeiten** auf **Firewall anwenden** klicken. Dieses Fenster enthält eine Liste der Schnittstellen, denen eine Regel zugeordnet wird, und eine Beschreibung der Regel, die zugeordnet wird.

Beispiel:

```
SDM wendet die Firewallkonfiguration auf die folgenden
Schnittstellen an:
Innere (vertrauenswürdige) Schnittstelle: FastEthernet 0/0
* SDM-Standardprüfregel für Eingang anwenden.
* Eingangs-ACL anwenden. Anti-Spoofing, Broadcast, lokales
Loopback usw.

Äußere (nicht vertrauenswürdige) Schnittstelle: Seriell 1/0
* Zugriffssteuerungsliste für Eingang anwenden, um eingehenden
Datenverkehr abzulehnen.
```

Klicken Sie auf **OK**, um diese Änderungen zu übernehmen, oder auf **Abbrechen**, um die Anwendung der Firewall zu beenden.

Firewallrichtlinie bearbeiten

Das Fenster **Firewallrichtlinie bearbeiten** liefert eine grafische Ansicht der Firewallrichtlinien auf dem Router und ermöglicht es Ihnen, ACLs zu Richtlinien hinzuzufügen, ohne das Fenster verlassen zu müssen. Lesen Sie die Vorgehensweisen in den folgenden Abschnitten, um zu erfahren, wie die Informationen in diesem Fenster angezeigt und Regeln hinzugefügt werden.

Auszuführende Schritte vor dem Anzeigen von Informationen in diesem Fenster

Dieses Fenster ist leer, wenn keine Zonen, Zonenpaare oder Richtlinienzuordnungen konfiguriert wurden. Erstellen Sie eine Basiskonfiguration mit diesen Elementen, indem Sie **Konfigurieren > Firewall und ACL > Firewall erstellen** wählen und die Schritte des Assistenten für die erweiterte Firewall befolgen. Nachdem Sie dies getan haben, können Sie zusätzliche Zonen, Zonenpaare und Richtlinien erstellen, indem Sie **Konfigurieren > Zusätzliche Aufgaben > Zonen** wählen, um Zonen zu konfigurieren, oder **Zusätzliche Aufgaben > Zonenpaare** wählen, um weitere Zonenpaare zu konfigurieren. Zum Erstellen der von den Zonenpaaren zu verwendenden Richtlinienzuordnungen wählen Sie **Konfigurieren > Zusätzliche Aufgaben > C3PL**. Klicken Sie auf den Zweig **Richtlinienzuordnung**, um weitere Zweige anzuzeigen, mit denen Sie Richtlinienzuordnungen und Klassenzuordnungen erstellen können, die den Datenverkehr für die Richtlinienzuordnungen definieren.

Ein- und Ausblenden der Anzeige einer Richtlinie

Wenn die Anzeige einer Richtlinie ausgeblendet ist, werden nur der Richtlinienname und die Quell- und Zielzone angezeigt. Um die Anzeige der Richtlinie zu erweitern, sodass die Regeln der Richtlinie angezeigt werden, klicken Sie auf die Schaltfläche **+** links neben dem Richtliniennamen. Die erweiterte Ansicht einer Firewallrichtlinie kann in etwa wie folgt aussehen:

		Datenverkehrsklassifizierung			Aktion	Regeloptionen
	ID	**Quelle**	**Ziel**	**Dienst**		
	clients-servers-policy (Clients zu Servern)					
	1	any	any	tcp	Firewall zulassen	
				udp		
				icmp		
	2	Fehlende Übereinstimmung bei Datenverkehr			Entfernen	

Die Richtlinie namens „clients-servers-policy“ enthält zwei ACLs. Die Regel mit der ID 1 lässt TCP-, UDP- und ICMP-Datenverkehr von jeder Quelle zu jedem Ziel zu. Die Regel mit der ID 2 entfernt unzugeordneten Datenverkehr.

Hinzufügen einer neuen Regel zu einer Richtlinie

Wenn Sie eine neue Regel zu einer Richtlinie hinzufügen möchten, führen Sie die folgenden Schritte aus:

Schritt 1 Klicken Sie an eine beliebige Stelle in der Anzeige der Richtlinie und anschließend auf die Schaltfläche **+ Hinzufügen**.

- Um eine Regel für neuen Datenverkehr in der gewünschten Reihenfolge einzufügen, wählen Sie eine vorhandene Regel aus, klicken auf die Schaltfläche **+ Hinzufügen** und wählen **Einfügen** oder **Dahinter einfügen**. Die Optionen **Einfügen** und **Dahinter einfügen** sind auch über ein Kontextmenü verfügbar, das Sie anzeigen können, indem Sie mit der rechten Maustaste auf eine vorhandene Regel klicken.

- Wenn Sie **Regel für neuen Datenverkehr** wählen, wird die neue Regel automatisch an den Anfang der Liste gestellt.
- Wenn Sie **Regel für existierenden Datenverkehr** wählen, können Sie eine vorhandene Klassenzuordnung auswählen und diese ändern. Dadurch wird die neue Regel automatisch an den Anfang der Liste gestellt.

Schritt 2 Füllen Sie die Felder des angezeigten Dialogfelds aus. Weitere Informationen erhalten Sie, wenn Sie auf Hinzufügen einer neuen Regel klicken.

Neuanordnen von Regeln in einer Richtlinie

Wenn eine Richtlinie mehrere Regeln enthält, die Datenverkehr zulassen, können Sie diese neu anordnen, indem Sie eine Regel auswählen und auf die Schaltfläche **Nach oben** oder **Nach unten** klicken. Die Schaltfläche **Nach oben** ist deaktiviert, wenn Sie eine Regel ausgewählt haben, die sich bereits ganz oben in der Liste befindet, oder wenn Sie die Regel **Fehlende Übereinstimmung bei Datenverkehr** ausgewählt haben. Die Schaltfläche **Nach unten** ist deaktiviert, wenn Sie eine Regel ausgewählt haben, die sich bereits ganz unten in der Liste befindet.

Sie können die Regeln auch mithilfe der Schaltflächen **Ausschneiden** und **Einfügen** neu anordnen. Um eine Regel von der aktuellen Position zu entfernen, markieren Sie sie und klicken auf **Ausschneiden**. Um die Regel an einer neuen Position zu platzieren, markieren Sie eine vorhandene Regel, klicken auf **Einfügen** und wählen **Einfügen** oder **Dahinter einfügen**.

Die Optionen **Nach oben**, **Nach unten**, **Ausschneiden**, **Einfügen** und **Dahinter einfügen** sind auch über ein Kontextmenü verfügbar, das angezeigt wird, wenn Sie mit der rechten Maustaste auf eine Regel klicken.

Kopieren und Einfügen einer Regel

Das Kopieren und Einfügen einer Regel ist nützlich, wenn eine Richtlinie eine Regel enthält, die mit wenigen oder gar keinen Änderungen in einer anderen Richtlinie verwendet werden kann.

Zum Kopieren einer Regel wählen Sie eine Regel aus und klicken auf die Schaltfläche **Kopieren** bzw. klicken mit der rechten Maustaste auf die Regel und wählen **Kopieren**. Um die Regel an einem neuen Ort einzufügen, klicken Sie auf **Einfügen** und wählen **Einfügen** oder **Dahinter einfügen**. Die Schaltflächen **Einfügen** und **Dahinter einfügen** sind auch über das Kontextmenü verfügbar. Wenn Sie eine Regel an einem neuen Ort einfügen, wird das Dialogfeld Hinzufügen einer neuen Regel angezeigt, sodass Sie ggf. Änderungen an der Regel vornehmen können.

Anzeigen des Regelflussdiagramms

Klicken Sie an eine beliebige Stelle in der Firewallrichtlinie, und klicken Sie auf **Regeldiagramm**, um das Regelflussdiagramm für die Richtlinie anzuzeigen. Das Regelflussdiagramm zeigt die Quellzone auf der rechten Seite des Routersymbols und die Zielzone auf der linken Seite des Symbols an.

Übernehmen der Änderungen

Zum Übertragen der Änderungen auf den Router klicken Sie auf **Änderungen übernehmen** unten im Bildschirm.

Verwerfen der Änderungen

Zum Verwerfen der vorgenommenen Änderungen, die noch nicht auf den Router übertragen wurden, klicken Sie auf **Änderungen verwerfen** unten im Bildschirm.

Hinzufügen einer neuen Regel

Definieren Sie einen Datenverkehrsfluss und geben Sie im Fenster **Regel hinzufügen** zu prüfende Protokolle an. Führen Sie die folgenden Schritte aus, um eine neue Regel hinzuzufügen.

Schritt 1 Geben Sie im Feld **Quelle** und **Ziel** an, dass der Datenverkehr zwischen einem Netzwerk und einem anderen Netzwerk fließt, indem Sie **Netzwerk** auswählen. Wenn der Datenverkehr zwischen Einheiten fließt, bei denen es sich um Netzwerke oder einzelne Hosts handeln kann, wählen Sie **Beliebige**.

Schritt 2 Geben Sie in das Feld **Datenverkehrsname** einen Namen für den Datenverkehrsfluss ein.

Schritt 3 Klicken Sie neben den Spalten **Quellnetzwerk** und **Zielnetzwerk** auf **Hinzufügen**, und fügen Sie die Adressen von Quell- und Zielnetzwerk hinzu. Sie können für die Quell- und Zielnetzwerke mehrere Einträge hinzufügen, und Sie können einen vorhandenen Eintrag bearbeiten, indem Sie ihn auswählen und auf **Bearbeiten** klicken.

Schritt 4 Ordnen Sie einen Eintrag ggf. neu an, indem Sie ihn auswählen und auf **Nach oben** oder **Nach unten** klicken. Die Schaltfläche **Nach oben** ist deaktiviert, wenn sich der ausgewählte Eintrag bereits ganz oben in der Liste befindet. Die Schaltfläche **Nach unten** ist deaktiviert, wenn sich der ausgewählte Eintrag bereits ganz unten in der Liste befindet.

Schritt 5 Geben Sie einen Namen ein, der die Protokolle oder Dienste beschreibt, die Sie zur Prüfung im Feld **Dienstname** angeben.

Schritt 6 Fügen Sie einen Dienst hinzu, indem Sie in der linken Spalte auf einen Zweig im Baum klicken, wählen Sie einen Dienst und klicken Sie auf **Hinzufügen>>**. Klicken Sie auf das Symbol **+** neben einem Zweig, um die verfügbaren Dienste dieses Typs anzuzeigen. Um einen Dienst aus der rechten Spalte zu entfernen, markieren Sie ihn und klicken auf **<<Entfernen**.

Schritt 7 Geben Sie an, wie der Datenverkehr behandelt werden soll, indem Sie **Firewall zulassen**, **ACL zulassen** oder **Entfernen** im Feld **Aktion** wählen. Wenn Sie **Firewall zulassen** wählen, können Sie auf **Erweitert** klicken und ein Menüelement auswählen, um die Aktion weiter zu definieren und um so beispielsweise die Protokolle zu prüfen, die Sie im Dienstfeld auswählen. Weitere Informationen finden Sie in den folgenden Hilfethemen:

- Anwendungsprüfung
- URL-Filter
- Quality of Service
- Prüfparameter

Schritt 8 Wenn Sie die Aktion **Entfernen** wählen, können Sie auf **Protokollieren** klicken, um das Ereignis zu protokollieren.

Schritt 9 Klicken Sie auf **OK**, um das Dialogfeld zu schließen und die Änderungen an den Router zu übertragen.

Datenverkehr hinzufügen

Mit dem Dialogfeld **Datenverkehr hinzufügen** erstellen Sie einen Quell- und Zieladresseintrag für eine Regel.

Aktion

Über die Option **Einbeziehen** oder **Ausschließen** geben Sie an, ob die Regel auf den Datenverkehr angewandt werden soll, der zwischen der Quell- und Zieladresse ausgetauscht wird.

Wählen Sie **Einbeziehen**, um diesen Datenverkehr in die Regel einzubeziehen.

Wählen Sie **Ausschließen**, um diesen Datenverkehr von der Regel auszuschließen.

Quell-Host/-Netzwerk und Ziel-Host/-Netzwerk

Geben Sie Quelle und Ziel des Datenverkehrs in diesen Feldern an.

Typ

Wählen Sie einen der folgenden Werte aus:

- Beliebige IP-Adresse – Wählen Sie diese Option, wenn Sie den Quell- oder Zieldatenverkehr nicht auf einen Host oder ein Netzwerk beschränken möchten.
- Ein Netzwerk – Wählen Sie diese Option, wenn Sie eine Netzwerkadresse als Quelle oder Ziel angeben möchten, und geben Sie die Netzwerkadresse in den Feldern **IP-Adresse** und **Platzhaltermaske** an.
- Ein Hostname oder eine IP-Adresse – Wählen Sie diese Option, wenn Sie den Namen oder die IP-Adresse eines Hosts angeben möchten. Geben Sie anschließend den Host im Feld **Hostname/IP** an.

IP-Adresse

Geben Sie die Netzwerkadresse ein. Dieses Feld wird angezeigt, wenn Sie **Ein Netzwerk** im Feld **Typ** gewählt haben.

Platzhaltermaske

Geben Sie die Platzhaltermaske ein, welche die Bits angibt, die für die Netzwerkadresse verwendet werden. Wenn die Netzwerkadresse beispielsweise 192.168.3.0 lautet, geben Sie 0.0.0.255 als Maske an. Dieses Feld wird angezeigt, wenn Sie **Ein Netzwerk** im Feld **Typ** gewählt haben.

Hostname/IP

Geben Sie den Namen oder die IP-Adresse eines Hosts in dieses Feld ein. Wenn Sie einen Namen eingeben, muss der Router eine Verbindung zu einem DNS-Server herstellen können, damit der Name in eine IP-Adresse aufgelöst werden kann. Dieses Feld wird angezeigt, wenn Sie **Ein Hostname oder eine IP-Adresse** im Feld **Typ** wählen.

Anwendungsprüfung

Konfigurieren Sie eine Deep Packet Inspection für die in diesem Bildschirm aufgelisteten Anwendungen oder Protokolle, indem Sie das Kontrollkästchen neben der Anwendung oder dem Protokoll aktivieren, auf die Schaltfläche rechts neben dem Feld klicken und **Erstellen** oder **Auswählen** aus dem Kontextmenü wählen. Wählen Sie **Erstellen**, um eine neue Richtlinienzuordnung zu konfigurieren. Wählen Sie **Auswählen**, um eine vorhandene Richtlinienzuordnung auf den Datenverkehr anzuwenden. Wenn Sie fertig sind, wird der Richtlinienzuordnungsname im Feld angezeigt.

Um beispielsweise eine neue Richtlinienzuordnung für Instant Messaging zu erstellen, aktivieren Sie das Kontrollkästchen neben IM, klicken auf die Schaltfläche neben dem Feld **IM** und wählen **Erstellen**. Anschließend erstellen Sie die Richtlinienzuordnung im Dialogfeld **Deep Packet Inspection konfigurieren**.

URL-Filter

Fügen Sie einen URL-Filter hinzu, indem Sie einen vorhandenen URL-Filter aus der Liste **URL-Filtername** auswählen, oder indem Sie auf **Neu erstellen** klicken und in den angezeigten Dialogfeldern einen neuen URL-Filter erstellen. Die Einstellungen für den gewählten oder erstellten URL-Filter werden in diesem Dialogfeld zusammengefasst.

Quality of Service

Sie können Datenverkehr entfernen, der eine bestimmte Rate pro Sekunde überschreitet, die sog. Überwachungsrate, und Datenverkehr entfernen, der einen bestimmten Burst-Wert übersteigt. Die Überwachungsrate kann einen Wert zwischen 8.000 und 2.000.000.000 Bit pro Sekunde haben. Die Burst-Rate kann einen Wert zwischen 1.000 und 512.000.000 Byte haben.

Prüfparameter

Geben Sie eine vorhandene Parameterzuordnung im Fenster **Prüfparameter** an, indem Sie eine Parameterzuordnung aus der Liste **Prüfparameterzuordnung** auswählen oder auf **Neu erstellen** klicken, um eine neue Parameterzuordnung zu erstellen, die auf die Regel für die Richtlinie, die Sie ändern, angewandt wird. Die Details der angegebenen Parameterzuordnung werden in der unteren Hälfte des Feldes **Vorschau** angezeigt.

Für weitere Informationen über Parameterzuordnungen klicken Sie auf Timeouts und Grenzwerte für Prüfparameterzuordnungen und CBAC.

Auswählen des Datenverkehrs

Wählen Sie eine Klassenzuordnung aus, die den Datenverkehr angibt, den Sie zur Richtlinie hinzufügen möchten. Wenn Sie weitere Informationen zu einer bestimmten Klassenzuordnung anzeigen möchten, wählen Sie die Klassenzuordnung aus und klicken auf **Details anzeigen**.

Wenn Sie auf **OK** klicken, wird das Dialogfeld **Neue Regel hinzufügen** angezeigt. Es enthält Informationen zur von Ihnen gewählten Klassenzuordnung. Sie können an der Klassenzuordnung weitere Änderungen vornehmen oder sie unverändert lassen. Wenn Sie Änderungen vornehmen, können Sie den Namen der Klassenzuordnung ändern, wenn Sie Ihre Änderungen nicht auf andere Richtlinien anwenden möchten, welche die ursprüngliche Klassenzuordnung verwenden.

Regel löschen

Dieses Dialogfeld wird angezeigt, wenn Sie eine Regel löschen, die eine Klassenzuordnung oder ACL enthält, die Sie zusammen mit der Regel löschen möchten oder für die Verwendung in anderen Regeln behalten möchten.

Klassenzuordnungen und ACLs, die von dieser Regel verwendet werden, automatisch löschen

Klicken Sie auf diese Option, wenn Sie die Klassenzuordnungen entfernen möchten, die Teil dieser Regel sind. Sie werden aus der Routerkonfiguration entfernt und stehen nicht für die Verwendung in anderen Regeln zur Verfügung.

Nicht verwendete Klassenzuordnungen und ACL später löschen

Klicken Sie auf diese Option, um die Regel zu entfernen, Klassenzuordnungen und ACLs jedoch beizubehalten. Sie können Sie zur Verwendung in anderen Teilen der Firewallkonfiguration aufheben.

Details anzeigen

Klicken Sie auf **Details anzeigen**, um die Namen der Klassenzuordnungen und ACLs anzuzeigen, die mit der Regel, die Sie löschen, verknüpft sind. Das Dialogfeld wird erweitert, um die Details anzuzeigen. Wenn Sie auf **Details anzeigen** klicken, ändert sich der Schaltflächenname in **Details ausblenden**.

Details ausblenden

Klicken Sie auf **Details ausblenden**, um den Bereich mit den Details auszublenden. Wenn Sie auf **Details ausblenden** klicken, ändert sich der Schaltflächenname in **Details anzeigen**.

Manuelles Löschen von Klassenzuordnungen

Um eine Klassenzuordnung manuell zu löschen, führen Sie die folgenden Schritte aus.

Schritt 1 Wählen Sie **Konfigurieren > Zusätzliche Aufgaben > C3PL > Klassenzuordnungen**.

Schritt 2 Klicken Sie auf den Knoten des Klassenzuordnungstyps, den Sie löschen möchten.

Schritt 3 Wählen Sie den Namen der Klassenzuordnung aus, der im Fenster **Details anzeigen** angezeigt wurde, und klicken Sie auf **Löschen**.

Manuelles Löschen von ACLs

Um eine ACL manuell zu löschen, führen Sie die folgenden Schritte aus.

Schritt 1 Wählen Sie **Konfigurieren > Zusätzliche Aufgaben > ACL-Editor**.

Schritt 2 Klicken Sie auf den Knoten des ACL-Typs, den Sie löschen möchten.

Schritt 3 Wählen Sie den Namen oder die Zahl der ACL aus, die im Fenster **Details anzeigen** angezeigt wurde, und klicken Sie auf **Löschen**.

KAPITEL 8

Anwendungssicherheit

Durch die Anwendungssicherheit können Sie Sicherheitsrichtlinien erstellen, die die Netzwerk- und Web-Anwendungen regeln. Sie können die Richtlinien anwenden, die Sie für spezielle Schnittstellen erstellt haben, eine bestehende Richtlinie klonen, um die Einstellungen für eine neue Richtlinie nutzen und Richtlinien vom Router entfernen.

Dieses Kapitel enthält die folgenden Abschnitte:

Das Anwendungssicherheit-Fenster

Mit den Steuerungen im Anwendungssicherheit-Fenster können Sie Richtlinien und Schnittstellen verbinden, globale Einstellungen vornehmen und Anwendungssicherheitsrichtlinien hinzufügen, löschen und klonen. Mit den Anwendungssicherheitsfächern können Sie schnell zum Anwendungssicherheitsbereich navigieren, in dem Sie die Änderungen eingeben wollen.

Regelnamenliste

Wählen Sie die Richtlinie aus der Liste, die Sie ändern möchten. Wenn keine Richtlinien konfiguriert sind, bleibt diese Liste leer und das Fenster **Anwendungssicherheit** zeigt eine Meldung an, dass keine Richtlinien auf dem Router verfügbar sind. Um eine Richtlinie zu erstellen, klicken Sie auf die Schaltfläche **Aktion**, und wählen Sie **Hinzufügen**.

Schaltflächen der Anwendungssicherheit

- Schaltfläche **Aktion** - Klicken Sie auf diese Schaltfläche, um eine Richtlinie hinzuzufügen, die ausgewählte Richtlinie zu löschen oder zu duplizieren. Falls auf dem Router keine Richtlinien konfiguriert sind, ist **Hinzufügen** die einzige, verfügbare Aktion.
- Schaltfläche **Associate** (Verknüpfen) - Klicken Sie auf diese Schaltfläche, um ein Dialogfeld anzuzeigen, mit dem Sie die Richtlinie mit einer Schnittstelle verknüpfen können. Mit dem Dialog können Sie die Schnittstelle wählen und die Richtung des Datenverkehrs angeben, auf die diese Richtlinie zutreffen soll.
- Schaltfläche **Globale Einstellungen** – Klicken Sie auf diese Schaltfläche, um Einstellungen an Werten für Timeout und Schwellenwert vorzunehmen, die für alle Richtlinien gelten. Klicken Sie auf **Globale Einstellungen**, um weitere Informationen zu erhalten.

E-Mail Fach

Klicken Sie hier, um Änderungen an den Sicherheitseinstellungen der E-Mail-Anwendung vorzunehmen. Weitere Informationen erhalten Sie, wenn Sie auf E-mail klicken.

Instant Messaging-Fach

Klicken Sie hier, um Änderungen an den Sicherheitseinstellungen Yahoo Messenger, MSN Messenger und weiteren Instant-Messaging-Anwendungen vorzunehmen. Weitere Informationen erhalten Sie, wenn Sie auf Instant Messaging klicken.

Fach Peer-to-Peer

Klicken Sie hier, um Änderungen an den Sicherheitseinstellungen für KaZa A, eDonkey und weiteren Peer-to-Peer-Anwendungen vorzunehmen. Weitere Informationen erhalten Sie, wenn Sie auf Anwendungen/Protokolle klicken.

Fach URL-Filterung

Klicken Sie hier, um eine Liste mit URLs hinzuzufügen, die von der Richtlinie zur Anwendungssicherheit gefiltert werden sollen. Sie können auch Filterungsserver hinzufügen.

HTTP-Fach

Klicken Sie hier, um Änderungen an den HTTP-Sicherheitseinstellungen vorzunehmen. Weitere Informationen erhalten Sie, wenn Sie auf HTTP klicken.

Anwendungs-/Protokollfach

Klicken Sie hier, um Änderungen an den Sicherheitseinstellungen anderer Anwendungen und Protokolle vorzunehmen. Weitere Informationen erhalten Sie, wenn Sie auf Anwendungen/Protokolle klicken.

Keine Anwendungssicherheit-Regel

Cisco SDM zeigt dieses Fenster an, wenn Sie auf die Registerkarte **Anwendungssicherheit** klicken, jedoch keine Richtlinie zur Anwendungssicherheit auf dem Router konfiguriert wurde. Sie können in diesem Fenster eine Richtlinie erstellen und die globalen Einstellungen anzeigen, die Standardwerte für die Parameter liefern, die Sie beim Erstellen von Richtlinien festlegen können.

Richtlinienname:

Diese Liste ist leer, wenn auf dem Router keine Richtlinie konfiguriert wurde. Wenn Sie im Menü Aktionskontext Hinzufügen auswählen, können Sie einen Regelnamen erstellen und beginnen, Einstellungen für eine Regel einzugeben.

Vorgang

Wenn auf dem Router keine Richtlinie konfiguriert ist, können Sie aus dem Kontextmenü die Option **Hinzufügen** wählen, um eine Richtlinie zu erstellen. Wenn eine Richtlinie konfiguriert wurde, sind die Aktionen **Bearbeiten** und **Löschen** verfügbar.

Zuordnen

Wenn keine Richtlinie konfiguriert wurde, ist diese Schaltfläche deaktiviert. Wenn eine Richtlinie erzeugt wurde, können Sie auf diese Schaltfläche klicken, um die Richtlinie einer Schnittstelle zuzuordnen. Weitere Informationen finden Sie unter Ordnen Sie einer Schnittstelle die Regel zu.

Global Settings

Globale Einstellungen liefern die Standard-Timeouts, -Schwellenwerte und sonstige Werte der Richtlinienparameter. Cisco SDM liefert Standardwerte für jeden Parameter. Sie können jeden Wert ändern, um einen neuen Standardwert zu definieren, der dann angewendet wird, es sei denn, er wird für eine bestimmte Anwendung oder ein Protokoll überschrieben. Wenn Sie eine Regel erstellen, können Sie die Standardwerte für einen bestimmten Parameter akzeptieren oder eine andere Einstellung eingeben. Weil das Konfigurationsfenster der Anwendungssicherheit keine Standardwerte anzeigt, müssen Sie auf diese Schaltfläche klicken, um das Fenster globale Timeouts und Grenzwerte anzuzeigen. Weitere Informationen finden Sie unter Timeouts und Grenzwerte für Prüfparameterzuordnungen und CBAC.

E-mail

Wählen Sie die E-Mailanwendungen aus, die Sie in diesem Fenster prüfen möchten. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Schaltfläche „Bearbeiten“

Klicken Sie hier, um die Einstellungen der gewählten Anwendung zu bearbeiten. Die Einstellungen, die Sie vornehmen, überschreiben die globalen Einstellungen, die auf dem Router konfiguriert sind.

Anwendungsspalte

Der Name der E-Mail-Anwendung, z. B. *bliff*, *esmtp* und *smtp*. Wenn Sie die Einstellungen einer Anwendung bearbeiten möchten, aktivieren Sie das Kontrollkästchen links vom Anwendungsnamen und klicken Sie auf **Bearbeiten**.

Alarme-, Prüfung- und Timeout-Spalten

Diese Spalten enthalten Werte, die ausdrücklich für eine Anwendung eingestellt wurden. Wenn eine Einstellung für eine Anwendung nicht geändert wurde, ist diese Spalte leer. Wenn z. B. eine Überwachung für die bliff-Anwendung aktiviert wurde, an den Einstellungen für Alarm oder Timeout jedoch keine Änderungen vorgenommen wurden, wird der Wert *on* in der Spalte **Prüfung** angezeigt und die Spalten **Alarm** und **Timeout** sind leer.

Optionen-Spalte

Diese Spalte kann Felder enthalten, wenn andere Einstellungen für die gewählte Anwendung vorhanden sind.

Datenfeld MAX

Gibt die maximale Anzahl der Bytes (Daten) an, die in einer einzelnen Simple-Mail-Transport Protokoll (SMTP) Sitzung übertragen werden können. Wenn der maximale Wert überschritten wird, protokolliert die Firewall eine Alarmmeldung und schließt die Sitzung. Standardwert: 20 MB.

Kontrollkästchen Verschlüsselte Anmeldung

Veranlasst einen Benutzer an einem ungesicherten Standort, eine verschlüsselte Authentifizierung einzugeben.

Reset

Setzt die TCP-Verbindung zurück, wenn der Client einen Befehl eingibt, der kein Protokollbefehl ist, bevor die Authentifizierung abgeschlossen wird.

Routerverkehr

Aktiviert die Prüfung des Datenverkehrs, der zu und von einem Router führt. Gilt nur für H.3232, TCP und UDP-Protokolle.

Instant Messaging

Verwenden Sie dieses Fenster zur Steuerung des Verkehrs bei Instant Messaging (IM)-Anwendungen, wie z.B. Yahoo Messenger und MSN-Messenger. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Klicken Sie auf Zulassungs-, Sperr- und Alarmsteuerungen, um zu erfahren, wie Sie die Aktion des Routers angeben, wenn er auf Datenverkehr mit den Eigenschaften trifft, die Sie in dieses Fenster eingegeben haben.

Das folgende Beispiel zeigt gesperrten Datenverkehr für Yahoo Messenger-Verkehr und die Alarme, die erzeugt werden, wenn Verkehr für diese Anwendung eintrifft:

```
Yahoo Messenger        Sperre         Alarm senden (geprüft)
```

Das SDM_HIGH-Profil sperrt IM-Anwendungen. Wenn der Router das SDM_HIGH-Profil verwendet und keine IM-Anwendungen blockiert, dann können diese Anwendungen an einen neuen Server angeschlossen sein, der nicht im Profil angegeben ist. Um den Router so einzustellen, dass er diese Anwendungen blockieren kann, aktivieren Sie das Kontrollkästchen **Alarm senden** neben den IM-Anwendungen, um die Namen der Server anzuzeigen, mit denen die Anwendungen verbunden sind. Dann verwenden Sie das CLI, um den Verkehr von diesen Servern zu blockieren. Das folgende Beispiel verwendet den Servernamen newserver.yahoo.com:

```
Router(config)# appfw Richtlinien-Name SDM_HIGH
Router(cfg-appfw-policy)# Anwendung im yahoo
Router(cfg-appfw-policy-ymsgr)# Server abgewiesener Name
neuerserver.yahoo.com Router(cfg-appfw-policy-ymsgr)# exit
Router(cfg-appfw-policy)# exit
Router(config)#
```

Hinweis

- IM-Anwendungen können über nicht-native Protokollports wie HTTP und über ihre nativen TCP- und UDP-Ports kommunizieren. Cisco SDM konfiguriert Sperr- und Zulassungsaktionen aufgrund des systemeigenen Ports für die Anwendung und blockiert jede Kommunikation über HTTP-Ports.
- Manch IM-Anwendungen, z.B. MSN Messenger 7.0 verwenden HTTP-Ports standardmäßig. Wenn Sie diese Anwendungen zulassen möchten, müssen Sie die IM-Anwendung so konfigurieren, dass sie ihren nativen Port verwendet.

Peer-to-Peer Anwendungen

Diese Seite ermöglicht Ihnen die Erstellung der Richtlinieneinstellungen für Peer-to-Peer-Anwendungen wie Gnutella, BitTorrent und eDonkey. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Klicken Sie auf Zulassungs-, Sperr- und Alarmsteuerungen, um zu erfahren, wie Sie die Aktion des Routers angeben, wenn er auf Datenverkehr mit den Eigenschaften trifft, die Sie in dieses Fenster eingegeben haben.

Das folgende Beispiel zeigt gesperrten Datenverkehr für BitTorrent-Verkehr und die Alarme, die erzeugt werden, wenn Verkehr für diese Anwendung eintrifft:

Beispiel 8-1 Sperren von BitTorrent-Datenverkehr

```
BitTorrent              Sperre
```

Hinweis

- Peer-to-Peer-Anwendungen können über nicht-native Protokollports wie HTTP und über ihre nativen TCP- und UDP-Ports kommunizieren. Cisco SDM konfiguriert Sperr- und Zulassungsaktionen aufgrund des systemeigenen Ports für die Anwendung und blockiert jede Kommunikation über HTTP-Ports.
- Anwendungssicherheitsregeln blockieren keine Dateien, wenn sie von einem bezahlten Service, wie z.B. altnet.com bereitgestellt werden. Dateien, die von Peer-to-Peer-Netzen heruntergeladen wurden, werden blockiert.

URL-Filterung

Mit URL-Filterung können Sie mithilfe von URL-Listen den Benutzerzugriff auf Internet-Websites steuern. In diesen Listen können Sie festlegen, ob eine URL zugelassen oder abgelehnt werden soll. Sie können URL-Filterfunktionen in die Richtlinien zur Anwendungssicherheit aufnehmen, indem Sie in diesem Fenster auf **URL-Filterung aktivieren** klicken.

Sie können eine lokale URL-Liste auf dem Router konfigurieren, die für alle Richtlinien zu Anwendungssicherheit verwendet wird. URL-Listen können auf URL-Filter-Servern gespeichert werden, zu denen der Router eine Verbindung herstellen kann. Informationen zu diesen Servern sind in einer Liste der URL-Filter-Server gespeichert. Sie können eine lokale URL-Filterliste auf dem Router konfigurieren, die für alle Richtlinien zu Anwendungssicherheit verwendet wird.

Die lokale URL-Liste kann in mithilfe der Schaltflächen **URL-Liste hinzufügen**, **URL-Liste bearbeiten** und **URL-Liste importieren** verwaltet werden. Da die Cisco IOS-Software diese Listen mit oder ohne konfigurierte Richtlinie zur Anwendungssicherheit verwalten kann, können Sie diese Listen auch im Fenster **Zusätzliche Aufgaben** verwalten.

Wenn Sie erfahren möchten, wie Sie eine lokale URL-Liste verwalten, klicken Sie auf Liste lokaler URLs.

Wenn Sie erfahren möchten, wie die URL-Filterliste verwaltet wird, klicken Sie auf URL-Filter-Server.

Um Informationen dazu zu erhalten, wie der Router eine lokale URL-Liste in Kombination mit URL-Listen auf URL-Filter-Servern verwendet, klicken Sie auf Vorrang bei der URL-Filterung.

Allgemeine Informationen zur URL-Filterung erhalten Sie durch Klicken auf Fenster URL-Filterung.

HTTP

Geben Sie die allgemeinen Einstellungen für die HTTP-Verkehrsprüfung in diesem Fenster ein. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Klicken Sie auf Zulassungs-, Sperr- und Alarmsteuerungen, um zu erfahren, wie Sie die Aktion des Routers angeben, wenn er auf Datenverkehr mit den Eigenschaften trifft, die Sie in dieses Fenster eingegeben haben.

Genauere Informationen darüber, wie der Router HTTP-Datenverkehr prüfen kann, finden Sie unter *HTTP Inspection Engine* unter dem folgenden Link:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455acb.html

Das Kontrollkästchen „Nicht kompatibler HTTP-Verkehr erkannt“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Cisco SDM den HTTP-Verkehr für Pakete prüft, die nicht mit dem HTTP-Protokoll übereinstimmen. Verwenden Sie die Zulassungs-, Sperr- und Alarmsteuerungen, um die Aktion des Routers anzugeben, wenn er diese Art von Datenverkehr antrifft.

Hinweis Das Sperren von nicht kompatiblem HTTP-Datenverkehr kann dazu führen, dass der Router selbst Datenverkehr von bekannten Websites ablehnt, der dann möglicherweise nicht aufgrund seines Inhalts blockiert wurde, wenn diese Websites nicht mit dem HTTP-Protokoll übereinstimmen.

Das Kontrollkästchen „Tunnelanwendungen erkennen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass Cisco SDM den HTTP-Datenverkehr für Pakete prüft, die mit Tunnelanwendungen erstellt wurden. Verwenden Sie die Zulassungs-, Sperr- und Alarmsteuerungen, um anzugeben, was Cisco SDM tun muss, wenn diese Art von Datenverkehr angetroffen wird.

Das Kontrollkästchen „Maximale URI-Längenprüfung einstellen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine maximale Länge für Universal Resource Indicators (URIs) definieren möchten. Geben Sie die maximale Länge in Byte an, und verwenden Sie dann die Zulassungs-, Sperr- und Alarmsteuerungen, um die Aktion des Routers festzulegen, wenn dieser eine URL antrifft, die länger ist als dieser Wert.

Kontrollkästchen „HTTP-Prüfung aktivieren“

Aktivieren Sie dieses Kontrollkästchen, wenn der Router den HTTP-Datenverkehr prüfen soll. Wenn Sie Datenverkehr von Java-Anwendungen blockieren möchten, können Sie einen Java-Sperrfilter angeben, indem Sie die ...-Schaltfläche anklicken und entweder eine bestehende ACL angeben oder eine neue ACL für die Java-Prüfung erstellen.

Das Kontrollkästchen „HTTPS-Prüfung aktivieren“

Aktivieren Sie dieses Kontrollkästchen, wenn der Router den HTTPS-Datenverkehr prüfen soll.

Das Kontrollkästchen „Timeout-Wert einstellen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie für HTTP-Sitzungen ein Timeout einstellen möchten, und geben Sie in das Timeout-Feld die Zeitspanne in Sekunden ein. Die Sitzungen werden dann nach Ablauf der Zeit beendet.

Überwachungsliste aktivieren

Sie können CBAC-Überwachungslisten für den HTTP-Verkehr einstellen, die die Einstellungen im Fenster globale Timeouts und Grenzwerte überschreiben. **Standard** bedeutet, dass die derzeitigen globalen Einstellungen verwendet werden. **On** aktiviert explizit die CBAC-Überwachungsliste für den HTTP-Datenverkehr und HTTPS-Datenverkehr, falls HTTPS-Prüfung aktiviert ist, und überschreibt die globale Einstellung für den Prüfungspfad. **Off** deaktiviert explizit die CBAC-Überwachungsliste für den HTTP-Datenverkehr und HTTPS-Datenverkehr, falls HTTPS-Prüfung aktiviert ist, und überschreibt die globale Einstellung für den Prüfungspfad.

Header Options

Der Router kann Datenverkehr aufgrund der Länge der HTTP-Kopfleiste und der Anforderungsart in der Kopfzeile zulassen oder ablehnen. Anforderungsarten sind Befehle, die an die HTTP-Server gesendet werden, um URLs und Webseiten aufzurufen und andere Aktionen durchzuführen. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Kontrollkästchen Maximale Kopfleisten-Längenprüfung einstellen

Aktivieren Sie diese Option, wenn der Router Datenverkehr aufgrund der Länge der HTTP-Kopfleiste zulassen bzw. ablehnen soll, und geben Sie die maximale Länge der Kopfzeile für Anforderung und Antwort an. Verwenden Sie die Steuerungen **Zulassung**, **Sperre** und **Alarm**, um anzugeben, was der Router tun muss, wenn die Kopfzeilenlänge den eingegebenen Wert überschreitet.

Die Kontrollkästchen Methode der Erweiterungsanforderung konfigurieren

Aktivieren Sie das Kontrollkästchen neben dieser Anforderungsart, wenn der Router den HTTP-Datenverkehr aufgrund einer Methode der Erweiterungsanforderung zulassen oder ablehnen soll. Verwenden Sie die Steuerungen **Zulassung**, **Sperre** und **Alarm**, um anzugeben, was der Router tun muss, wenn er Datenverkehr mit dieser Anforderungsmethode antrifft.

Die Kontrollkästchen „RFC-Anforderungsmethode konfigurieren“

Wenn Sie möchten, dass der Router den HTTP-Verkehr aufgrund der in RFC 2616, *Hypertext Transfer Protocol - HTTP/1.1*, angegebenen HTTP-Anforderungsmethoden zulässt oder ablehnt, aktivieren Sie das Kontrollkästchen neben dieser Anforderungsmethode. Verwenden Sie die Steuerungen **Zulassung**, **Sperre** und **Alarm**, um anzugeben, was der Router tun muss, wenn er Datenverkehr mit dieser Anforderungsmethode antrifft.

Content-Optionen

Der Router kann Datenverkehr aufgrund des Inhalts des HTTP-Verkehrs überprüfen, und Datenverkehr zulassen oder ablehnen und Alarme erstellen, je nachdem, welche Dinge der Router prüfen soll. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Klicken Sie auf Zulassungs-, Sperr- und Alarmsteuerungen, um zu erfahren, wie Sie die Aktion des Routers angeben, wenn er auf Datenverkehr mit den Eigenschaften trifft, die Sie in diesem Fenster eingegeben haben.

Das Kontrollkästchen „Inhaltsart bestätigen“

Aktivieren Sie diese Option, wenn der Router den Inhalt von HTTP-Paketen bestätigen soll, indem er die Antwort mit der Anforderung vergleicht, einen Alarm für unbekannte Inhaltsarten aktiviert, oder durch beide Methoden. Verwenden Sie die Zulassungs-, Sperr- und Alarmsteuerungen, um anzugeben, welche Aktionen der Router ausführt, wenn die Anforderung nicht mit der Antwort übereinstimmt, und wenn er eine unbekannte Inhaltsart antrifft.

Das Kontrollkästchen Inhaltslänge einstellen

Aktivieren Sie dieses Kontrollkästchen, um die Mindest- und maximale Länge der Daten in einem HTTP-Paket einzustellen und geben Sie die Werte in den bereitgestellten Feldern ein. Verwenden Sie die Zulassung-, Sperr- und Alarmsteuerungen, um anzugeben, welche Aktionen der Router ausführt, wenn die Datenmenge unter die Mindestlänge fällt oder die maximale Länge übersteigt.

Das Kontrollkästchen Übertragungsschlüssel konfigurieren

Aktivieren Sie diese Option, wenn der Router verifizieren soll, wie die Daten in den Paketen codiert sind, und verwenden Sie dann die Genehmigungs-, Sperr- und Alarmsteuerungen, um anzugeben, welche Aktion der Router ausführt, wenn er die von Ihnen gewählten Übertragungscodierungen antrifft.

Kontrollkästchen Chunk

Das in RFC 2616, Hypertext Transfer Protocol - HTTP/1 festgelegte Codierungsformat. Dabei wird der Meldungstext als Serie einzelner Stücke übertragen, wobei jedes Stück eine eigene Größenangabe enthält.

Kontrollkästchen Komprimierung

Das Verschlüsselungsformat, das die UNIX-Einrichtung **Komprimierung** (compress) erzeugt.

Kontrollkästchen Entleeren

Das ZLIB-Format, das in RFC 1950, ZLIB Compressed Data Format Specification version 3.3 (Komprimiertes ZLBI-Datenformatangabe, Version 3.3) definiert wird, zusammen mit dem Entleerungs-Mechanismus in RFC 1951, DEFLATE Compressed Data Format Specification version 1.3 (Entleerung der komprimierten Datenformatsangabe, Version 1.3).

Kontrollkästchen GZip

Das Verschlüsselungsformat, das das GNU-Zip (Gzip) Programm erzeugt.

Kontrollkästchen Identität

Standardverschlüsselung, die anzeigt, dass keine Verschlüsselung durchgeführt wurde.

Anwendungen/Protokolle

Dieses Fenster gestattet Ihnen die Erstellung der Regeleinstellungen für Anwendungen und Protokolle, die nicht in anderen Fenstern gezeigt werden. Weitere Informationen zu den auf der Registerkarte **Anwendungssicherheit** verfügbaren Schaltflächen und Fächern erhalten Sie, indem Sie auf Das Anwendungssicherheit-Fenster klicken.

Anwendungen/Protokoll-Baum

Mit dem Anwendungen/Protokoll-Baum können Sie die Liste rechts entsprechend der Art der Anwendungen und Protokolle filtern, die Sie ansehen möchten. Wählen Sie zunächst den Zweig für die allgemeine Art, die Sie darstellen möchten. Der Rahmen rechts zeigt die verfügbaren Punkte für die gewünschte Art an. Wenn ein Pluszeichen (+) links vom Zweig erscheint, gibt es Unterkategorien, die Sie zur Redefinition des Filters benötigen. Klicken Sie auf das +-Zeichen, um den Zweig zu erweitern und wählen Sie dann die Unterkategorie, die Sie anzeigen möchten. Wenn die Liste zur Rechten leer ist, gibt es keine Anwendungen oder Protokolle für diese Art. Um eine Anwendung auszuwählen, können Sie das Kontrollkästchen daneben im Baum aktivieren oder das Kontrollkästchen daneben auf der Liste.

Beispiel: Wenn Sie alle Cisco-Anwendungen anzeigen möchten, klicken Sie auf den Unterordner **Anwendungen** und dann auf den Ordner **Cisco**. Sie sehen dann Anwendungen wie *clp*, *cisco-net-mgmt* und *cisco-sys*.

Schaltfläche „Bearbeiten“

Klicken Sie auf diese Schaltfläche, um die Einstellungen der gewählten Anwendung zu bearbeiten. Die Einstellungen, die Sie vornehmen, überschreiben die globalen Einstellungen, die auf dem Router konfiguriert sind.

Anwendungsspalte

Der Name der Anwendung oder des Protokolls, z. B. *tcp*, *smtp oder ms-sna*. Wenn Sie die Einstellungen für ein Element bearbeiten möchten, aktivieren Sie das Kontrollkästchen links vom Elementnamen, und klicken Sie auf **Bearbeiten**.

Alarme-, Prüfung- und Timeout-Spalten

Diese Spalten zeigen Werte, die explizit für ein Element eingestellt wurden. Wenn eine Einstellung für ein Element nicht geändert wurde, ist diese Spalte leer. Wenn z. B. eine Überwachung für die Anwendung ms-sna aktiviert wurde, an den Einstellungen für Alarm oder Timeout jedoch keine Änderungen vorgenommen wurden, wird der Wert *On* in der Spalte **Prüfung** angezeigt, die Spalten **Alarm** und **Timeout** sind jedoch leer.

Optionen-Spalte

Diese Spalte kann Felder enthalten, wenn andere Einstellungen für das gewählte Element vorhanden sind.

MAX Daten

Gibt die maximale Anzahl der Bytes (Daten) an, die in einer einzelnen Simple-Mail-Transport Protokoll (SMTP) Sitzung übertragen werden können. Wenn der maximale Wert überschritten wird, protokolliert die Firewall eine Alarmmeldung und schließt die Sitzung. Standardwert: 20 MB.

Verschlüsselte Anmeldung

Veranlasst einen Benutzer an einem ungesicherten Standort, eine verschlüsselte Authentifizierung einzugeben.

Reset

Setzt die TCP-Verbindung zurück, wenn der Client einen Befehl eingibt, der kein Protokollbefehl ist, bevor die Authentifizierung abgeschlossen wird.

Routerverkehr

Aktiviert die Prüfung des Datenverkehrs, der zu und von einem Router führt. Gilt nur für H.3232, TCP und UDP-Protokolle.

Timeouts und Grenzwerte für Prüfparameterzuordnungen und CBAC

Verwenden Sie diese Informationen zum Erstellen oder Bearbeiten einer Parameterzuordnung für Prüfzwecke oder um Context-Based Access Control (CBAC) für globale Timeouts und Grenzwerte einzustellen. CBAC verwendet Timeouts und Grenzwerte, um zu bestimmen, wie lange die Zustandsinformation für eine Sitzung verwaltet werden muss und wann eine Sitzung beendet werden soll, die nicht vollständig aufgebaut werden konnte. Diese Timeouts und Grenzwerte gelten für alle Sitzungen.

Globale Timer-Werte können in Sekunden, Minuten oder Stunden angegeben werden.

Timeout-Wert der TCP-Verbindung

Die Zeitspanne, während der auf die Herstellung einer TCP-Verbindung gewartet wird. Der Standardwert ist 30 Sekunden.

Timeout-Wert der TCP FIN-Verbindung

Die Zeitspanne, über die eine TCP-Sitzung weiterverwaltet wird, nachdem die Firewall einen FIN-Austausch erkennt. Der Standardwert ist 5 Sekunden.

Timeout-Wert der TCP-Verbindung

Die Zeitspanne, die eine TCP-Sitzung weiterverwaltet wird, nachdem keine Aktivität mehr ermittelt wurde. Der Standardwert ist 3600 Sekunden.

Timeout-Wert der UDP-Verbindung

Die Zeitspanne, während der eine User Datagram Protocol (UDP)-Sitzung weiterverwaltet wird, nachdem keine Aktivität mehr ermittelt wurde. Der Standardwert ist 30 Sekunden.

Timeout-Wert des DNS

Die Zeitspanne, während der eine Lookup-Sitzung für DNS (Domain Name System)-Namen weiterverwaltet wird, nachdem keine Aktivität mehr ermittelt wurde. Der Standardwert ist 5 Sekunden.

Grenzwerte des SYN-Flooding DoS-Angriffs

Eine ungewöhnlich hohe Anzahl halboffener Sitzungen kann darauf hindeuten, dass ein Denial-of-Service (DoS)-Angriff vorgeht. DoS-Angriffsgrenzwerte erlauben dem Router, halb geöffnete Sitzungen zu schließen, wenn ihre Gesamtanzahl einen oberen Grenzwert erreicht hat. Durch die Definierung von Grenzwerten können Sie angeben, wann der Router beginnen sollte, halb geöffnete Sitzungen zu löschen und wann er damit wieder aufhören soll.

Schwellenwerte für einminütige Sitzungen. In diesen Feldern können Sie die Schwellenwerte für neue Verbindungsversuche angeben.

Niedrig	Löschen neuer Verbindungen beenden, wenn die Anzahl neuer Verbindungen unter diesen Wert fällt. Der Standardwert ist 400 Sitzungen.
Hoch	Löschen neuer Verbindungen beginnen, wenn die Anzahl neuer Verbindungen diesen Wert überschreitet. Der Standardwert ist 500 Sitzungen.

Schwellenwerte für max. Anz. unvollständiger Sitzungen. In diesen Feldern können Sie die Schwellenwerte für die Gesamtzahl der bestehenden halb geöffneten Sitzungen angeben.

Unterer	Löschen neuer Verbindungen beenden, wenn die Anzahl neuer Verbindungen unter diesen Wert fällt. Der Standardwert beträgt 400 Sitzungen für Cisco IOS-Versionen, die älter als 12.4(11)T sind. Wenn ein niedriger Wert nicht explizit eingestellt ist, hört Cisco IOS auf, neue Sitzungen zu löschen, wenn die Sitzungszahl auf 400 fällt. Für die Cisco IOS-Version 12.4(11)T und neuer lautet der Standardwert unbegrenzt. Wenn ein niedriger Wert nicht explizit eingestellt ist, hört Cisco IOS nicht auf, neue Verbindungen zu löschen.

Hoch	Löschen neuer Verbindungen beginnen, wenn die Anzahl neuer Verbindungen diesen Wert überschreitet. Der Standardwert beträgt 500 Sitzungen für Cisco IOS Versionen, die älter als 12.4(11)T sind. Wenn ein hoher Wert nicht explizit eingestellt ist, beginnt Cisco IOS Sitzungen zu löschen, wenn über 500 neue Sitzungen aufgenommen wurden. Für die Cisco IOS-Version 12.4(11)T und höher lautet der Standardwert unbegrenzt. Wenn ein hoher Wert nicht explizit eingestellt ist, beginnt Cisco IOS nicht, neue Verbindungen zu löschen.

Max. Anz. unvollständiger TCP-Sitzungen pro Host

Der Router beginnt mit dem Löschen halb geöffneter Sitzungen für den Host, wenn die Gesamtzahl für diesen Host diese Zahl überschreitet.
Die standardmäßige Anzahl von Sitzungen ist 50. Wenn Sie das Feld **Blockierzeit** aktivieren und einen Wert in dieses Feld eingeben, blockiert der Router während der in Minuten angegebenen Zeitspanne weiterhin neue Verbindungen für diesen Host.

Globale Prüfung aktivieren

Aktivieren Sie diese Option, wenn Sie für alle Datenverkehrstypen Meldungen für CBAC-Überwachungslisten aktivieren möchten.

Globalen Alarm aktivieren

Aktivieren Sie diese Option, wenn Sie die CBAC-Alarm-Meldungen für alle Arten von Datenverkehr aktivieren möchten.

Ordnen Sie einer Schnittstelle die Regel zu

Wählen Sie in diesem Fenster die Schnittstelle aus, der Sie die gewählte Regel zuordnen möchten. Geben Sie auch an, ob die Regel auf eingehenden, ausgehenden oder beide Verkehrsrichtungen zutreffen soll.

Wenn der Router beispielsweise über FastEthernet 0/0 und FastEthernet 0/1-Schnittstellen verfügt, und Sie die Richtlinie auf die FastEthernet 0/1-Schnittstelle auf Datenverkehr in beide Richtungen anwenden möchten, dann aktivieren Sie die Option neben FastEthernet 0/1 und die Kontrollkästchen in den Spalten für Eingehend und Ausgehend. Wenn nur eingehender Verkehr geprüft werden soll, aktivieren Sie nur das Kontrollkästchen in der Spalte für Eingehend.

Prüfregel bearbeiten

Geben Sie in diesem Fenster die Einstellungen einer benutzerspezifische Prüfungsregel für eine Anwendung an. Die hier eingegebenen Einstellungen, die auf die Routerkonfiguration angewendet werden, überschreiben die globalen Einstellungen.

Klicken Sie im Fenster **Anwendungssicherheit** auf die Schaltfläche **Globale Einstellungen**, um die globalen Einstellungen für die Parameter anzuzeigen, die Sie in diesem Fenster einstellen können. Weitere Informationen finden Sie unter Timeouts und Grenzwerte für Prüfparameterzuordnungen und CBAC.

Alarmfeld

Wählen Sie einen der folgenden Werte aus:

- **Standard** - Verwendung der globalen Einstellungen für Alarme.
- **Ein (on)** - Wenn diese Art des Datenverkehrs angetroffen wird, wird ein Alarm erzeugt.
- **Aus (off)** - Wenn diese Art des Datenverkehrs angetroffen wird, wird kein Alarm erzeugt.

Prüfungsfeld

Wählen Sie einen der folgenden Werte aus:

- **Standard** - Verwendung der globalen Einstellungen für Überwachungslisten.
- **Ein (on)** - Wenn diese Art von Datenverkehr angetroffen wird, wird eine Überwachungsliste generiert.
- **Aus (off)** - Wenn diese Art von Datenverkehr angetroffen wird, wird keine Überwachungsliste generiert.

Timeout-Feld

Geben Sie an, wie viel Sekunden eine Sitzung für diese Anwendung verwaltet werden soll, nachdem keine Aktivität mehr stattfand. Der Timeout-Wert, den Sie eingeben, setzt den TCP-Timeoutwert im Ruhestand, wenn es sich um eine TCP-Anwendung handelt, oder den UDP-Timeout-Wert, falls es eine UDP-Anwendung ist.

Sonstige Optionen:

Gewisse Anwendungen können zusätzliche Optionen haben. Sie finden die Beschreibung der Optionen je nach Anwendung nachstehend.

MAX Datenfeld

Gibt die maximale Anzahl der Bytes (Daten) an, die in einer einzelnen Simple-Mail-Transport Protokoll (SMTP) Sitzung übertragen werden können. Wenn der maximale Wert überschritten wird, protokolliert die Firewall eine Alarmmeldung und schließt die Sitzung. Standardwert: 20 MB.

Das Kontrollkästchen Verschlüsselte Anmeldung

Veranlasst einen Benutzer an einem ungesicherten Standort, eine verschlüsselte Authentifizierung einzugeben.

Das Kontrollkästchen Reset:

Setzt die TCP-Verbindung zurück, wenn der Client einen Befehl eingibt, der kein Protokollbefehl ist, bevor die Authentifizierung abgeschlossen wird.

Das Kontrollkästchen Routerverkehr

Aktiviert die Prüfung des Datenverkehrs, der zu und von einem Router führt. Gilt nur für H.3232, TCP und UDP-Protokolle.

Zulassungs-, Sperr- und Alarmsteuerungen

Verwenden Sie die Zulassungs-, Sperr- und Alarmsteuerungen, um die Aktion des Routers anzugeben, wenn er Datenverkehr mit Eigenschaften antrifft, die Sie angegeben haben. Um eine Regeleinstellung für eine Option mit diesen Steuerungen aufzustellen, aktivieren Sie das Kontrollkästchen daneben. Wählen Sie anschließend in der Aktionsspalte **Zulassen**, um Verkehr in Zusammenhang mit dieser Option zuzulassen, oder wählen Sie **Sperren**, um diesen Datenverkehr abzulehnen. Wenn Sie möchten, dass ein Alarm an das Protokoll gesendet wird, wenn diese Art von Datenverkehr auftritt, aktivieren Sie die Option **Alarm senden**. Die Steuerung **Alarm senden** wird nicht in allen Fenstern verwendet.

Damit die Anwendungssicherheit Alarme ans Protokoll senden kann, muss die Protokollierung aktiviert sein. Weitere Informationen finden Sie unter folgendem Link: Anwendungssicherheitslog.

KAPITEL 9

Site-to-Site-VPN

Die Hilfethemen in diesem Abschnitt beschreiben die Site-to-Site VPN-Konfigurationsbildschirme und die Bildschirme des VPN Design Guide.

VPN Design Guide

Wenn Sie ein Administrator sind, der ein VPN-Netzwerk einrichtet, hilft Ihnen der VPN Design Guide dabei, zu ermitteln, welche Art von VPN konfiguriert werden soll. Sie geben Informationen dazu an, welcher Benutzertyp Sie sind, die Art der Ausrüstung, mit welcher der Router VPN-Verbindungen herstellt, der Datenverkehrstyp, den VPN befördert und zu weiteren Funktionen, die Sie konfigurieren müssen. Nachdem Sie diese Informationen angegeben haben, empfiehlt der VPN Design Guide einen VPN-Typ und erlaubt Ihnen das Starten eines Assistenten, mit dem Sie diesen VPN-Typ konfigurieren können.

Site-to-Site-VPN erstellen

Ein VPN (Virtual Private Network – virtuelles privates Netzwerk) ermöglicht Ihnen den Schutz von Datenverkehr über Leitungen, die sich möglicherweise nicht im Besitz Ihrer Organisation befinden oder von ihr kontrolliert werden. VPNs können über die Leitungen gesendeten Datenverkehr verschlüsseln und Peers authentifizieren, bevor Datenverkehr gesendet wird.

Sie können sich von Cisco SDM (Cisco Router and Security Device Manager) durch eine einfache VPN-Konfiguration führen lassen. Klicken Sie dazu auf das VPN-Symbol. Wenn Sie den Assistenten auf der Registerkarte **Site-to-Site-VPN erstellen** verwenden, gibt Cisco SDM für einige Konfigurationsparameter Standardwerte an, um den Konfigurationsprozess zu vereinfachen.

Wenn Sie mehr über die VPN-Technologie erfahren möchten, erhalten Sie unter dem Link Weitere Informationen zu VPN Hintergrundinformationen.

Erstellen Sie ein Site-to-Site-VPN

Diese Option ermöglicht Ihnen die Erstellung eines VPN-Netzwerks, das zwei Router verbindet.

Erstellen Sie einen sicheren GRE-Tunnel (GRE over IPSec)

Diese Option ermöglicht Ihnen die Erstellung eines GRE-Tunnels (Generic Routing Encapsulation Protocol) zwischen Ihrem Router und einem Peer-System.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Konfigurieren des Routers als Teil eines VPN-Netzwerks, das zwei Router verbindet Wenn Sie ein VPN-Netzwerk zwischen zwei Routern konfigurieren, können Sie kontrollieren, wie der Remote-Router authentifiziert wird, wie Datenverkehr verschlüsselt wird und welcher Datenverkehr verschlüsselt wird.	Wählen Sie die Option **Erstellen Sie ein Site-to-Site-VPN**. Klicken Sie dann auf **Ausgewählte Aufgabe starten**.
Konfigurieren eines GRE-Tunnels zwischen Ihrem Router und einem anderen Router. Sie sollten einen GRE-Tunnel konfigurieren, wenn Sie Netzwerke verbinden müssen, die verschiedene LAN-Protokolle verwenden, oder wenn Sie Routing-Protokolle über die Verbindung an das Remote-System senden müssen.	Wählen Sie die Option **Erstellen Sie einen sicheren GRE-Tunnel (GRE over IPSec)**. Klicken Sie dann auf **Ausgewählte Aufgabe starten**.

Aufgabe	Vorgehensweise
Herausfinden, wie andere VPN-Aufgaben durchgeführt werden, zu denen dieser Assistent keine Anleitungen gibt	Wählen Sie ein Thema aus der folgenden Liste aus. • Wie zeige ich die IOS-Befehle an, die ich an den Router sende? • Wie erstelle ich ein VPN für mehrere Standorte? • Wie konfiguriere ich nach der Konfiguration eines VPN das VPN auf dem Peer-Router? • Wie bearbeite ich einen vorhandenen VPN-Tunnel? • Wie erhalte ich die Bestätigung, dass mein VPN funktioniert? • Wie erhalte ich die Bestätigung, dass mein VPN funktioniert? • Wie konfiguriere ich einen Sicherungs-Peer für mein VPN? • Wie nehme ich mehrere Geräte auf, auf denen VPN in unterschiedlichem Umfang unterstützt wird? • Wie konfiguriere ich ein VPN auf einer nicht unterstützten Schnittstelle? • Wie konfiguriere ich ein VPN, nachdem ich eine Firewall konfiguriert habe? • Wie konfiguriere ich NAT Passthrough für ein VPN? • Wie konfiguriere ich ein DMVPN manuell?

Aufgabe	Vorgehensweise
Konfigurieren eines Easy VPN-Konzentrators Konfigurationsanweisungen für Easy VPN-Server und -Konzentratoren finden Sie unter www.cisco.com.	Unter dem folgenden Link erhalten Sie Anleitungen für die Konfiguration eines Konzentrators der Serie Cisco VPN 3000 für den Betrieb mit einem Easy VPN Remote Phase II-Client sowie weitere Informationen, die möglicherweise für Sie hilfreich sind: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html Über den folgenden Link gelangen Sie zur Dokumentation für die Serie Cisco VPN 3000: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html

Site-to-Site-VPN-Assistent

Sie können veranlassen, dass Cisco SDM für die meisten Konfigurationswerte Standardeinstellungen verwendet, oder sich von Cisco SDM durch die Konfiguration eines VPNs führen lassen.

Was möchten Sie tun?

Aufgabe	Vorgehensweise
Zügiges Konfigurieren eines Site-to-Site-VPNs mit Cisco SDM-Standardwerten	Aktivieren Sie **Schnelleinrichtung**, und klicken Sie dann auf **Weiter**. Cisco SDM gibt automatisch eine Standard-IKE-Richtlinie zur Regelung der Authentifizierung an, weiterhin einen Standardtransformationssatz zur Kontrolle der Datenverschlüsselung und eine Standard-IPSec-Regel, mit der der gesamte Datenverkehr zwischen dem Router und dem Remote-Gerät verschlüsselt wird. Die Schnelleinrichtung ist die beste Methode, wenn sowohl der lokale Router als auch das Remote-System Cisco-Router sind, die Cisco SDM verwenden. Bei der Schnelleinrichtung wird die 3DES-Verschlüsselung konfiguriert, wenn sie vom IOS-Abbild unterstützt wird. Anderenfalls wird die DES-Verschlüsselung konfiguriert. Wenn Sie AES- oder SEAL-Verschlüsselung benötigen, klicken Sie auf **Schritt-für-Schritt-Assistent**.
Anzeigen der Standardwerte für die IKE-Richtlinie, den Transformationssatz und die IPSec-Regel, die für die Konfiguration eines VPNs in einem Schritt verwendet werden	Klicken Sie auf **Standards anzeigen**.
Konfigurieren eines Site-to-Site-VPNs mit von Ihnen angegebenen Parametern	Aktivieren Sie **Schritt-für-Schritt-Assistent**, und klicken Sie dann auf **Weiter**. Sie können eine benutzerdefinierte Konfiguration für das VPN erstellen und die von Ihnen benötigten Cisco SDM-Standardwerte verwenden. Im Schritt-für-Schritt-Assistenten können Sie eine stärkere Verschlüsselung als in der Schnelleinrichtung angeben.

Standards anzeigen

In diesem Fenster werden die Standardwerte für die IKE (Internet Key Exchange)-Richtlinie, der Transformationssatz und die IPSec-Regel angezeigt, die Cisco SDM für die Konfiguration eines Site-to-Site-VPNs in der Schnelleinrichtung verwendet. Wenn Sie eine andere als die in diesem Fenster angezeigte Konfiguration benötigen, aktivieren Sie **Schritt-für-Schritt-Assistent**, damit Sie Konfigurationswerte definieren können.

VPN-Verbindungsinformationen

Verwenden Sie dieses Fenster, um die IP-Adresse oder den Hostnamen des Remote-Standortes anzugeben, der den von Ihnen konfigurierten VPN-Tunnel terminiert, um die zu verwendende Routerschnittstelle anzugeben und um den Pre-Shared Key einzugeben, den beide Router für die gegenseitige Authentifizierung verwenden.

Wählen Sie die Schnittstelle für diese VPN-Verbindung aus

Wählen Sie die Schnittstelle auf dem Router aus, die mit dem Remote-Standort verbunden ist. Der von Ihnen konfigurierte Router wird im Diagramm für das Anwendungsszenario als lokaler Router dargestellt.

Peer-Identität

Geben Sie die IP-Adresse des Remote-IPSec-Peers (IP Security) ein, der den von Ihnen konfigurierten VPN-Tunnel terminiert. Der Remote-IPSec-Peer kann ein anderer Router, ein VPN-Konzentrator oder ein anderes Gateway-Gerät sein, das IPSec unterstützt.

Peer(s) mit dynamischer IP-Adresse

Wählen Sie diese Option aus, wenn die Peers, mit denen der Router verbunden ist, dynamisch zugeordnete IP-Adressen verwenden.

Peer mit statischer IP-Adresse

Wählen Sie diese Option aus, wenn der Peer, mit dem der Router verbunden ist, eine feste IP-Adresse verwendet.

IP-Adresse des Remote-Peers eingeben

(Ist aktiviert, wenn **Peer mit statischer IP-Adresse** ausgewählt ist.) Geben Sie die IP-Adresse des Remote-Peers ein.

Authentifizierung

Klicken Sie auf diese Schaltfläche, wenn die VPN-Peers einen Pre-Shared Key verwenden, um ihre Verbindungen gegenseitig zu authentifizieren. Auf beiden Seiten der VPN-Verbindung muss derselbe Key verwendet werden.

Geben Sie den Pre-Shared Key ein, und geben Sie ihn dann zur Bestätigung noch einmal ein. Tauschen Sie den Pre-Shared Key über eine sichere und praktische Methode mit dem Administrator des Remote-Standorts aus, z. B. über eine verschlüsselte E-Mail. Die Verwendung von Fragezeichen (?) und Leerzeichen ist im Pre-Shared Key nicht zulässig. Der Pre-Shared Key darf maximal 128 Zeichen enthalten.

Hinweis

- Die Zeichen, die Sie für den Pre-Shared Key eingeben, werden während der Eingabe nicht im Feld angezeigt. Es ist hilfreich, den Schlüssel vor der Eingabe zu notieren, damit Sie ihn dem Administrator des Remote-Systems mitteilen können.
- Pre-Shared Keys müssen zwischen allen IPSec-Peer-Paaren ausgetauscht werden, die sichere Tunnel aufbauen müssen. Diese Authentifizierungsmethode eignet sich für ein stabiles Netzwerk mit einer begrenzten Zahl von IPSec-Peers. In einem Netzwerk mit einer großen oder wachsenden Zahl von IPSec-Peers kann sie zu Problemen bei der Skalierbarkeit führen.

Digitales Zertifikat

Wählen Sie diese Option aus, wenn die VPN-Peers digitale Zertifikate für die Authentifizierung verwenden.

Hinweis Der Router muss ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat besitzen, um sich selbst zu authentifizieren. Wenn Sie kein digitales Zertifikat für den Router konfiguriert haben, wechseln Sie zu den VPN-Komponenten, und verwenden Sie den Assistenten für digitale Zertifikate, um sich für ein digitales Zertifikat zu registrieren.

Zu verschlüsselnder Datenverkehr

Wenn Sie im Rahmen der Schnelleinrichtung eine Site-to-Site-VPN-Verbindung konfigurieren, müssen Sie in diesem Fenster das Quell- und das Ziel-Subnetz angeben.

Quelle

Wählen Sie die Schnittstelle auf dem Router, die die Quelle des Datenverkehrs dieser VPN-Verbindung ist. Der gesamte Datenverkehr, der über diese Schnittstelle geht und dessen Ziel-IP-Adresse sich in dem Subnetz befindet, das im Bereich **Ziel** angegeben ist, wird verschlüsselt.

Details

Klicken Sie auf diese Schaltfläche, um Details zu der von Ihnen ausgewählten Schnittstelle zu erhalten. Im Fenster mit den Details sind die Zugriffsregeln, IPSec-Richtlinien, NAT-Regeln (Network Address Translation) und Prüfregeln angezeigt, die mit der Schnittstelle verknüpft sind. Um eine dieser Regeln genauer zu untersuchen, wechseln Sie zu **Zusätzliche Aufgaben - ACL-Editor**, und untersuchen Sie sie in den Fenstern unter **Regeln**.

Ziel

IP-Adresse und Subnetzmaske. Geben Sie die IP-Adresse und die Subnetzmaske des Ziels für diesen Datenverkehr ein. Weitere Informationen zur Eingabe von Werten in diese Felder finden Sie unter IP-Adressen und Subnetzmasken.

Das Ziel wird im Diagramm für das Anwendungsszenario im Hauptfenster des VPN-Assistenten als Remote-Router dargestellt.

IKE-Einstellungen

In diesem Fenster sind alle IKE-Richtlinien (Internet Key Exchange) aufgelistet, die auf dem Router konfiguriert wurden. Wenn keine benutzerdefinierten Richtlinien konfiguriert wurden, wird in diesem Fenster die Cisco SDM-Standard-IKE-Richtlinie angezeigt. IKE-Richtlinien regeln die Methode, mit dem Geräte in einem VPN sich selbst authentifizieren.

Der lokale Router verwendet die in diesem Fenster aufgelisteten IKE-Richtlinien, um die Authentifizierung mit dem Remote-Router auszuhandeln.

Der lokale Router und das Peer-Gerät müssen dieselbe Richtlinie verwenden. Der Router, der die VPN-Verbindung initiiert, bietet zuerst die Richtlinie mit der niedrigsten Prioritätsnummer an. Wenn das Remote-System diese Richtlinie ablehnt, bietet der lokale Router die Richtlinie mit der nächsthöheren Nummer an und fährt auf diese Weise fort, bis das Remote-System eine Richtlinie akzeptiert. Sie und der Administrator des Peer-Systems müssen Ihre Arbeit eng aufeinander abstimmen, damit Sie identische Richtlinien auf beiden Routern konfigurieren können.

Für Easy VPN-Verbindungen werden IKE-Richtlinien nur auf dem Easy VPN-Server konfiguriert. Der Easy VPN-Client sendet Vorschläge, und der Server antwortet gemäß seinen konfigurierten IKE-Richtlinien.

Priorität

Diese ist die Reihenfolge, in der die Richtlinien während der Aushandlung angeboten werden.

Verschlüsselung

Cisco SDM unterstützt unterschiedliche Verschlüsselungstypen, die in der Reihenfolge ihrer Sicherheit aufgeführt werden. Je sicherer ein Verschlüsselungstyp ist, desto mehr Verarbeitungszeit ist für diesen erforderlich.

Hinweis

- Nicht alle Router unterstützen alle Verschlüsselungstypen. Nicht unterstützte Typen werden nicht im Bildschirm angezeigt.
- Nicht alle IOS-Abbilder unterstützen alle von Cisco SDM unterstützten Verschlüsselungstypen. Typen, die nicht vom IOS-Abbild unterstützt werden, werden nicht im Bildschirm angezeigt.
- Wenn die Hardwareverschlüsselung aktiviert ist, werden nur die Verschlüsselungstypen im Bildschirm angezeigt, die von der Hardwareverschlüsselung unterstützt werden.

Cisco SDM unterstützt die folgenden Verschlüsselungstypen:

- DES – Data Encryption Standard. Diese Form unterstützt 56-Bit-Verschlüsselung.
- 3DES – Triple DES. Dies ist eine stärkere Verschlüsselungsform als DES, die 168-Bit-Verschlüsselung unterstützt.
- AES-128 – Advanced Encryption Standard-(AES-)Verschlüsselung mit einem 128-Bit-Schlüssel. AES bietet eine höhere Sicherheit als DES und ist für rechenintensive Aufgaben effizienter als 3DES.
- AES-192 – AES-Verschlüsselung mit einem 192-Bit-Schlüssel.
- AES-256 – AES-Verschlüsselung mit einem 256-Bit-Schlüssel.

Hash

Der Authentifizierungsalgorithmus, der für die Aushandlung verwendet wird. Cisco SDM unterstützt die folgenden Algorithmen:

- SHA_1 – Secure Hash Algorithm. Ein Hash-Algorithmus, der zur Authentifizierung von Paketdaten verwendet wird.
- MD5 – Message Digest 5. Ein Hash-Algorithmus, der zur Authentifizierung von Paketdaten verwendet wird.

D-H-Gruppe

Die Diffie-Hellman-Gruppe – Diffie-Hellman ist ein kryptografisches Public-Key-Protokoll, mit dem zwei Router ein geteiltes Geheimnis über einen nicht sicheren Kommunikationskanal festlegen können. Cisco SDM unterstützt die folgenden Gruppen:

- group1 – D-H-Gruppe 1. 768-Bit-D-H-Gruppe.
- group2 – D-H-Gruppe 2. 1024-Bit-D-H-Gruppe. Diese Gruppe bietet eine höhere Sicherheit als Gruppe 1, erfordert jedoch eine längere Verarbeitungszeit.
- group5 – D-H-Gruppe 5. 1536-Bit-D-H-Gruppe. Diese Gruppe bietet eine höhere Sicherheit als Gruppe 2, erfordert jedoch eine längere Verarbeitungszeit.

Authentifizierung

Die zu verwendende Authentifizierungsmethode. Folgende Werte werden unterstützt:

- PRE_SHARE – Die Authentifizierung wird unter Verwendung von Pre-Shared Keys durchgeführt.
- RSA_SIG – Die Authentifizierung wird mit digitalen Zertifikaten durchgeführt.

Hinweis Sie müssen den Authentifizierungstyp wählen, den Sie bei der Identifizierung der Schnittstellen, die die VPN-Verbindung verwenden, angegeben haben.

Typ

Entweder **Cisco SDM-Standard** oder **Benutzerdefiniert**. Wenn keine benutzerdefinierten Richtlinien auf dem Router erstellt wurden, zeigt dieses Fenster die Standard-IKE-Richtlinie an.

So fügen Sie eine IKE-Richtlinie hinzu oder bearbeiten sie:

Wenn Sie eine IKE-Richtlinie hinzufügen möchten, die nicht in der Liste enthalten ist, klicken Sie auf **Hinzufügen**, und erstellen Sie die Richtlinie in dem angezeigten Fenster. Wenn Sie eine vorhandene Richtlinie bearbeiten möchten, markieren Sie die Richtlinie, und klicken Sie auf **Bearbeiten**.
Cisco SDM-Standardrichtlinien sind schreibgeschützt und können nicht bearbeitet werden.

So übernehmen Sie die Richtlinienliste:

Wenn Sie die IKE-Richtlinie übernehmen und fortfahren möchten, klicken Sie auf **Weiter**.

Transformationssatz

In diesem Fenster werden die Cisco SDM-Standardtransformationssätze und die zusätzlichen Transformationssätze aufgelistet, die auf diesem Router konfiguriert wurden. Diese Transformationssätze können vom VPN oder DMVPN verwendet werden. Ein Transformationssatz stellt eine bestimmte Kombination aus Sicherheitsprotokollen und Algorithmen dar. Während der IPSec Security Association-Aushandlung vereinbaren die Peers, einen bestimmten Transformationssatz zum Schutz eines bestimmten Datenflusses zu verwenden. Eine Transformation beschreibt ein bestimmtes Sicherheitsprotokoll mit seinen entsprechenden Algorithmen.

Sie können nur einen Transformationssatz in diesem Fenster auswählen, können aber auf den Registerkarten für die VPN- oder DMVPN-Bearbeitung weitere Transformationssätze mit der VPN- oder DMVPN-Verbindung verknüpfen.

Transformationssatz auswählen

Wählen Sie aus dieser Liste den Transformationssatz aus, den Sie verwenden möchten.

Details zum ausgewählten Transformationssatz

In diesem Bereich sind Details zum ausgewählten Transformationssatz angegeben. Es müssen nicht alle Verschlüsselungs-, Authentifizierungs- und Kompressionstypen konfiguriert werden. Daher enthalten einige Spalten möglicherweise keine Werte.

Um zu erfahren, welche Werte die einzelnen Spalten enthalten können, klicken Sie auf **Transformationssatz hinzufügen/bearbeiten**.

Name

Der Name, der diesem Transformationssatz zugewiesen wurde.

ESP-Verschlüsselung

Der Typ der verwendeten ESP-Verschlüsselung (Encapsulating Security Protocol). Wenn für den Transformationssatz keine ESP-Verschlüsselung konfiguriert ist, enthält diese Spalte keinen Wert.

ESP-Authentifizierung

Der verwendete ESP-Authentifizierungstyp. Wenn für den Transformationssatz keine ESP-Authentifizierung konfiguriert ist, enthält diese Spalte keinen Wert.

AH-Authentifizierung

Der verwendete AH-Authentifizierungstyp (Authentication Header). Wenn für den Transformationssatz keine AH-Authentifizierung konfiguriert ist, enthält diese Spalte keinen Wert.

IP-Kompression

Wenn für den Transformationssatz IP-Kompression konfiguriert ist, enthält dieses Feld den Wert COMP-LZS.

Hinweis IP-Kompression wird nicht auf allen Routern unterstützt.

Modus

Diese Spalte enthält einen der folgenden Werte:

- Transport – Nur Daten verschlüsseln. Der Transportmodus wird verwendet, wenn beide Endpunkte IPSec unterstützen. Im Transportmodus werden der Authentication Header oder der Encapsulated Security Payload nach dem ursprünglichen IP-Header positioniert; daher wird nur der IP-Payload verschlüsselt. Diese Methode ermöglicht es Benutzern, Netzwerkdienste wie QoS-Steuerelemente (Quality of Service – Dienstgüte) für verschlüsselte Pakete anzuwenden.
- Tunnel – Daten und IP-Header verschlüsseln. Der Tunnelmodus bietet einen stärkeren Schutz als der Transportmodus. Da das gesamte Paket innerhalb von AH oder ESP verschlüsselt ist, wird ein neuer IP-Header angefügt, und das gesamte Datagramm kann verschlüsselt werden. Mit dem Tunnelmodus können Netzwerkgeräte, z. B. Router, als IPSec-Proxy für mehrere VPN-Benutzer fungieren.

Typ

Entweder **Benutzerdefiniert** oder **Cisco SDM-Standard**.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Auswählen eines Transformationssatzes, der im VPN verwendet werden soll	Wählen Sie einen Transformationssatz aus, und klicken Sie auf **Weiter**.
Hinzufügen eines Transformationssatzes zur Routerkonfiguration	Klicken Sie auf **Hinzufügen**, und erstellen Sie den Transformationssatz im Fenster **Transformationssatz hinzufügen**. Klicken Sie dann auf **Weiter**, um mit der VPN-Konfiguration fortzufahren.
Bearbeiten eines vorhandenen Transformationssatzes	Wählen Sie einen Transformationssatz aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann den Transformationssatz im Fenster **Transformationssatz bearbeiten**. Klicken Sie nach der Bearbeitung des Transformationssatzes auf **Weiter**, um mit der VPN-Konfiguration fortzufahren. Cisco SDM-Standard-Transformationssätze sind schreibgeschützt und können nicht bearbeitet werden.
Verknüpfen zusätzlicher Transformationssätze mit dem VPN	Wählen Sie einen Transformationssatz in diesem Fenster aus, und führen Sie den VPN-Assistenten aus. Verknüpfen Sie dann auf der Registerkarte **Bearbeiten** weitere Transformationssätze mit dem VPN.

Zu schützender Datenverkehr

In diesem Fenster können Sie den Datenverkehr definieren, der von diesem VPN geschützt wird. Das VPN kann Datenverkehr zwischen angegebenen Subnetzen oder den Datenverkehr schützen, der in einer von Ihnen ausgewählten IPSec-Regel angegeben ist.

Gesamten Datenverkehr zwischen den folgenden Subnetzen schützen

Geben Sie mit dieser Option ein einzelnes Quell-Subnetz (ein Subnetz im LAN) an, dessen ausgehenden Datenverkehr Sie verschlüsseln möchten, weiterhin ein Ziel-Subnetz, das von dem Peer unterstützt wird, den Sie im Fenster für die VPN-Verbindung angegeben haben.

Der gesamte Datenverkehr zwischen anderen Quell- und Zielpaaren wird unverschlüsselt übertragen.

Quelle

Geben Sie die Adresse des Subnetzes ein, dessen ausgehenden Datenverkehr Sie schützen möchten. Geben Sie außerdem die Subnetzmaske an. Weitere Informationen finden Sie unter Verfügbare Schnittstellenkonfigurationen.

Der gesamte Datenverkehr von diesem Quell-Subnetz, dessen Ziel-IP-Adresse sich im Ziel-Subnetz befindet, wird verschlüsselt.

Ziel

Geben Sie die Adresse des Ziel-Subnetzes ein, und geben Sie die Maske für dieses Subnetz an. Sie können eine Subnetzmaske aus der Liste auswählen oder eine benutzerdefinierte Maske eingeben. Nummer und Maske des Subnetzes müssen im durch Punkte getrennten Dezimalformat eingegeben werden (wie in den vorhergehenden Beispielen dargestellt).

Der gesamte Datenverkehr, der zu den Hosts in diesem Subnetz geht, wird geschützt.

Zugriffsliste für IPSec-Datenverkehr erstellen/auswählen

Verwenden Sie diese Option, wenn Sie mehrere Quellen und Ziele und/oder bestimmte Typen von Datenverkehr angeben müssen, die verschlüsselt werden sollen. Eine IPSec-Regel kann aus mehreren Einträgen bestehen, die unterschiedliche Datenverkehrstypen und unterschiedliche Quellen und Ziele angeben.

Klicken Sie auf die Schaltfläche neben dem Feld, und geben Sie eine vorhandene IPSec-Regel an, die den Datenverkehr definiert, den Sie verschlüsseln möchten. Sie können auch eine IPSec-Regel erstellen, die für dieses VPN verwendet werden soll. Wenn Sie die Nummer der IPSec-Regel kennen, geben Sie sie im rechten Feld ein. Wenn Ihnen die Nummer der Regel nicht bekannt ist, klicken Sie auf die Schaltfläche **...**, und suchen Sie die Regel. Wenn Sie die Regel auswählen, wird die Nummer im Feld angezeigt.

Hinweis Da mit ihnen der Datenverkehrstyp und sowohl Quelle als auch Ziel angegeben werden können, sind IPSec-Regeln erweiterte Regeln. Wenn Sie die Nummer oder den Namen einer Standardregel eingegeben haben, werden Sie in einer Warnmeldung darauf hingewiesen.

Pakete, die die in der IPSec-Regel angegebenen Kriterien nicht erfüllen, werden unverschlüsselt gesendet.

Zusammenfassung der Konfiguration

In diesem Fenster wird die von Ihnen erstellte VPN- oder DMVPN-Konfiguration angezeigt. Sie können die Konfiguration in diesem Fenster überprüfen und, sofern Sie es wünschen, über die Schaltfläche **Zurück** Änderungen vornehmen.

Spoke-Konfiguration

Wenn Sie einen DMVPN-Hub konfiguriert haben, können Sie veranlassen, dass Cisco SDM einen Ablauf generiert, der Sie oder andere Administratoren bei der Konfiguration von DMVPN-Spokes unterstützt. In dieser Prozedur wird erläutert, welche Optionen im Assistenten auszuwählen sind und welche Informationen in den Fenstern für die Spoke-Konfiguration einzugeben sind. Sie können diese Informationen in einer Textdatei speichern, die von Ihnen oder einem anderen Administrator verwendet werden kann.

Konnektivität nach der Konfiguration testen

Klicken Sie auf diese Option, um die gerade von Ihnen konfigurierte VPN-Verbindung zu testen. Die Ergebnisse des Tests werden in einem weiteren Fenster angezeigt.

So speichern Sie diese Konfiguration in der aktiven Konfiguration des Routers und verlassen diesen Assistenten:

Klicken Sie auf **Fertig stellen**. Cisco SDM speichert die Konfigurationsänderungen in der aktiven Konfiguration des Routers. Die Änderungen werden sofort wirksam; beim Abschalten des Routers gehen sie jedoch verloren.

Wenn Sie im Cisco SDM-Fenster **Einstellungen** die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktiviert haben, wird das Fenster **Senden** angezeigt. In diesem Fenster können Sie die CLI-Befehle anzeigen, die an den Router gesendet werden.

Spoke-Konfiguration

Dieses Fenster enthält Informationen, mit denen Sie einem Spoke-Router eine Konfiguration geben können, die mit dem von Ihnen konfigurierten DMVPN-Hub kompatibel ist. In diesem Fenster werden die auszufüllenden Fenster aufgelistet und die Daten angegeben, die Sie in den Fenstern eingeben müssen, damit der Spoke mit dem Hub kommunizieren kann.

In ihm sind die folgenden Daten angegeben, die Sie für die Spoke-Konfiguration eingeben müssen:

- Die öffentliche IP-Adresse des Hubs (die IP-Adresse der Hub-Schnittstelle, die den mGRE-Tunnel unterstützt)
- Die IP-Adresse des mGRE-Tunnels des Hubs
- Die Subnetzmaske, die alle Tunnelschnittstellen im DMVPN verwenden müssen
- Die Informationen zur erweiterten Tunnelkonfiguration
- Das zu verwendende Routing-Protokoll und weitere Informationen zum Protokoll, z. B. die Nummer für ein autonomes System (für EIGRP) und die OSPF-Prozess-ID
- Der Hash, die Verschlüsselung, die D-H-Gruppe und der Authentifizierungstyp der vom Hub verwendeten IKE-Richtlinien, damit auf dem Spoke kompatible IKE-Richtlinien konfiguriert werden können
- Die ESP- und Modusinformationen der vom Hub verwendeten Transformationssätze. Wenn auf dem Spoke keine ähnlichen Transformationssätze konfiguriert wurden, können sie mit diesen Informationen konfiguriert werden.

Sicherer GRE-Tunnel (GRE over IPSec)

GRE (Generic Routing Encapsulation) ist ein Tunneling-Protokoll von Cisco, mit dem eine Vielzahl von Protokollpakettypen in IP-Tunneln gekapselt werden kann. Auf diese Weise wird über ein IP-Verbundnetzwerk eine virtuelle Point-to-Point-Verbindung zu Cisco-Routern an Remote-Punkten erstellt. Durch die Verbindung von Subnetzwerken mit mehreren Protokollen in einer Backbone-Umgebung mit einem einzelnen Protokoll ermöglicht IP-Tunneling mit GRE die Netzwerkerweiterung in einer solchen Umgebung.

Dieser Assistent ermöglicht Ihnen die Erstellung eines GRE-Tunnels mit IPSec-Verschlüsselung. Mit der Erstellung einer GRE-Tunnelkonfiguration erstellen Sie auch eine IPSec-Regel, die die Endpunkte des Tunnels beschreibt.

GRE-Tunnel-Informationen

In diesem Bildschirm werden allgemeine Informationen zum GRE-Tunnel angegeben.

Tunnelquelle

Wählen Sie den Schnittstellennamen oder die IP-Adresse der Schnittstelle, die der Tunnel verwendet. Die IP-Adresse der Schnittstelle muss vom anderen Ende des Tunnels erreichbar sein; daher muss es eine öffentliche, Routing-fähige IP-Adresse sein. Wenn Sie eine IP-Adresse eingeben, die nicht mit einer konfigurierten Schnittstelle verknüpft ist, wird ein Fehler ausgegeben.

Hinweis In der Schnittstellenliste führt Cisco SDM Schnittstellen mit statischen IP-Adressen sowie Schnittstellen auf, die als nicht nummeriert konfiguriert sind. Loopback-Schnittstellen werden nicht in die Liste aufgenommen.

Details

Klicken Sie auf diese Option, um Details zu der von Ihnen ausgewählten Schnittstelle zu erhalten. Im Fenster mit den Details sind die Zugriffsregeln, IPSec-Richtlinien, NAT-Regeln und Prüfregeln angezeigt, die mit der Schnittstelle verknüpft sind. Wenn der Schnittstelle eine NAT-Regel zugeordnet wurde, die die Routing-Fähigkeit der Adresse aufhebt, funktioniert der Tunnel nicht ordnungsgemäß. Um eine dieser Regeln genauer zu untersuchen, wechseln Sie zu **Zusätzliche Aufgaben - ACL-Editor**, und untersuchen Sie sie im Fenster **Regeln**.

Tunnelziel

Geben Sie die IP-Adresse der Schnittstelle auf dem Remote-Router am anderen Ende des Tunnels ein. Dies ist aus der Sicht des anderen Endes des Tunnels die Quellschnittstelle.

Stellen Sie mit dem **ping**-Befehl sicher, dass diese Adresse erreicht werden kann. Den **ping**-Befehl können Sie über das Menü **Extras** aufrufen. Wenn die Zieladresse nicht erreicht werden kann, wird der Tunnel nicht ordnungsgemäß erstellt.

IP-Adresse des GRE-Tunnels

Geben Sie die IP-Adresse des Tunnels ein. Die IP-Adressen beider Enden des Tunnels müssen sich im selben Subnetz befinden. Der Tunnel erhält eine separate IP-Adresse, damit er erforderlichenfalls eine private Adresse sein kann.

IP-Adresse

Geben Sie die IP-Adresse des Tunnels im durch Punkte getrennten Dezimalformat ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske für die Tunneladresse im durch Punkte getrennten Dezimalformat ein.

VPN-Authentifizierungsinformationen

VPN-Peers verwenden einen Pre-Shared Key, um ihre Verbindungen gegenseitig zu authentifizieren. Auf beiden Seiten der VPN-Verbindung muss derselbe Key verwendet werden.

Pre-Shared Key

Klicken Sie auf diese Schaltfläche, wenn die VPN-Peers einen Pre-Shared Key für die Authentifizierung verwenden. Geben Sie dann den Pre-Shared Key ein, und bestätigen Sie ihn durch erneute Eingabe. Tauschen Sie den Pre-Shared Key über eine sichere und praktische Methode mit dem Administrator des Remote-Standorts aus, z. B. über eine verschlüsselte E-Mail. Die Verwendung von Fragezeichen (?) und Leerzeichen ist im Pre-Shared Key nicht zulässig.

Hinweis

- Die Zeichen, die Sie für den Pre-Shared Key eingeben, werden während der Eingabe nicht im Feld angezeigt. Es ist hilfreich, den Schlüssel vor der Eingabe zu notieren, damit Sie ihn dem Administrator des Remote-Systems mitteilen können.
- Pre-Shared Keys müssen zwischen allen IPSec-Peer-Paaren ausgetauscht werden, die sichere Tunnel aufbauen müssen. Diese Authentifizierungsmethode eignet sich für ein stabiles Netzwerk mit einer begrenzten Zahl von IPSec-Peers. In einem Netzwerk mit einer großen oder wachsenden Zahl von IPSec-Peers kann sie zu Problemen bei der Skalierbarkeit führen.

Digitales Zertifikat

Wählen Sie diese Option aus, wenn die VPN-Peers digitale Zertifikate für die Authentifizierung verwenden.

Der Router muss ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat besitzen, um sich selbst zu authentifizieren. Wenn Sie kein digitales Zertifikat für den Router konfiguriert haben, wechseln Sie zu den VPN-Komponenten, und verwenden Sie den Assistenten für digitale Zertifikate, um sich für ein digitales Zertifikat zu registrieren.

Hinweis Wenn Sie eine Authentifizierung mit digitalen Zertifikaten durchführen, wird der VPN-Tunnel eventuell nicht erstellt, wenn der während der IKE-Aushandlung kontaktierte CA-Server (Certificate Authority, Zertifizierungsstelle) nicht für die Beantwortung von CRL-Anfragen (Certification Revocation List – Sperrliste) konfiguriert ist. Wechseln Sie zur Behebung dieses Problems auf die Seite **Digitale Zertifikate**, wählen Sie den konfigurierten Trustpoint aus, und wählen Sie für die Sperrung die Option **Keine** aus.

Sicherungs-GRE-Tunnel-Informationen

Sie können einen GRE-over-IPSec-Sicherungstunnel konfigurieren, den der Router verwenden kann, wenn der primäre Tunnel ausfällt. Dieser Tunnel verwendet dieselbe Schnittstelle, die Sie für den primären Tunnel konfiguriert haben, muss aber mit dem Sicherungs-VPN-Router als Peer konfiguriert werden. Wenn Routing für den primären GRE-over-IPSec-Tunnel konfiguriert ist, wird anhand der vom Routing-Protokoll gesendeten Keepalive-Pakete überprüft, ob der Tunnel noch aktiv ist. Wenn der Router keine weiteren Keepalive-Pakete über den primären Tunnel erhält, wird der Datenverkehr über den Sicherungstunnel gesendet.

Gegen Ausfälle einen Sicherungs-GRE-Tunnel erstellen

Aktivieren Sie dieses Kontrollkästchen, wenn Sie einen Sicherungstunnel erstellen möchten.

IP-Adresse des Ziels des Sicherungs-GRE-Tunnels

Geben Sie die IP-Adresse der Schnittstelle auf dem Remote-Router am anderen Ende des Tunnels ein. (Dies ist aus der Sicht des anderen Endes des Tunnels die Quellschnittstelle.)

Stellen Sie mit dem **ping**-Befehl sicher, dass diese Adresse erreicht werden kann. Den **ping**-Befehl können Sie über das Menü **Extras** aufrufen. Wenn die im Dialogfeld **Ping** angegebene Zieladresse nicht erreicht werden kann, wird der Tunnel nicht ordnungsgemäß erstellt.

IP-Adresse des Tunnels

Geben Sie die IP-Adresse des Tunnels ein. Die IP-Adressen beider Enden des Tunnels müssen sich im selben Subnetz befinden. Der Tunnel erhält eine separate IP-Adresse, damit er erforderlichenfalls eine private Adresse sein kann.

IP-Adresse

Geben Sie die IP-Adresse des Tunnels im durch Punkte getrennten Dezimalformat ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Subnetzmaske

Geben Sie die Subnetzmaske für die Tunneladresse im durch Punkte getrennten Dezimalformat ein.

Routing-Informationen

In diesem Fenster können Sie Routing für den getunnelten Datenverkehr konfigurieren. Informationen, die Sie in diesem Fenster hinzufügen, werden im Fenster **Routing** angezeigt. Änderungen, die Sie im Fenster **Routing** vornehmen, können sich auf das Routing von VPN-Datenverkehr auswirken. Mit der Routing-Konfiguration können Sie die Netzwerke angeben, die am GRE-over-IPSec-VPN teilnehmen. Wenn Sie darüber hinaus einen GRE-over-IPSec-Sicherungstunnel konfigurieren, kann der Router anhand der von Routing-Protokollen gesendeten Keepalive-Pakete bestimmen, ob beim primären Tunnel ein Fehler aufgetreten ist.

Wählen Sie ein Protokoll für dynamisches Routing aus, wenn der Router in einer großen VPN-Bereitstellung mit einer großen Zahl von Netzwerken im GRE over IPSec-VPN verwendet wird. Wählen Sie statisches Routing, wenn wenige Netzwerke am VPN teilnehmen.

EIGRP

Aktivieren Sie dieses Kontrollkästchen, um das EIGRP-Protokoll (Enhanced Interior Gateway Routing Protocol) für das Routing von Datenverkehr zu verwenden. Klicken Sie dann auf **Weiter**, um im Fenster **Routing-Informationen** die Netzwerke anzugeben, die am GRE-over-IPSec-VPN teilnehmen.

OSPF

Aktivieren Sie dieses Kontrollkästchen, um das OSPF-Protokoll (Open Shortest Path First) für das Routing von Datenverkehr zu verwenden. Klicken Sie dann auf **Weiter**, um im Fenster **Routing-Informationen** die Netzwerke anzugeben, die am GRE-over-IPSec-VPN teilnehmen.

RIP

Aktivieren Sie dieses Kontrollkästchen, um das RIP-Protokoll (Routing Information Protocol) für das Routing von Datenverkehr zu verwenden. Klicken Sie dann auf **Weiter**, um im Fenster **Routing-Informationen** die Netzwerke anzugeben, die am GRE-over-IPSec-VPN teilnehmen.

Hinweis Diese Option ist nicht verfügbar, wenn Sie einen GRE-over-IPSec-Sicherungstunnel konfigurieren.

Statisches Routing

Statisches Routing kann in kleineren VPN-Bereitstellungen verwendet werden, in denen nur wenige private Netzwerke am GRE-over-IPSec-VPN teilnehmen. Sie können eine statische Route für jedes Remote-Netzwerk konfigurieren, damit Datenverkehr für die Remote-Netzwerke durch die entsprechenden Tunnel geleitet wird.

Informationen zu statischem Routing

Sie können eine statische Route für jedes Remote-Netzwerk konfigurieren, damit Datenverkehr für die Remote-Netzwerke durch die entsprechenden Tunnel geleitet wird. Konfigurieren Sie die erste statische Route im Fenster **Informationen zu statischem Routing**. Wenn Sie weitere statische Routen konfigurieren müssen, haben Sie dazu im Fenster **Routing** die Möglichkeit.

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine statische Route für den Tunnel angeben möchten, und wählen Sie eine der folgenden Optionen:

- **Gesamten Datenverkehr durch Tunnel** – Der gesamte Datenverkehr wird durch die Tunnelschnittstelle geleitet und verschlüsselt. Cisco SDM erstellt einen Standardeintrag für die statische Route mit der Tunnelschnittstelle als Next Hop.

  Wenn bereits eine Standardroute vorhanden ist, ändert Cisco SDM diese Route dahingehend, dass die Tunnelschnittstelle als Next Hop verwendet wird (und die ursprünglich dort angegebene Schnittstelle ersetzt). Außerdem wird ein neuer statischer Eintrag zum Tunnelzielnetzwerk erstellt, der die Schnittstelle in der ursprünglichen Standardroute als Next Hop angibt.

  Im folgenden Beispiel wird davon ausgegangen, dass das Netzwerk am anderen Ende des Tunnels 200.1.0.0 ist (wie in den Feldern für das Zielnetzwerk angegeben):

  ```
  ! Original entry
  ip route 0.0.0.0  0.0.0.0 FE0
  ! Entry changed by SDM
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ! Entry added by SDM
  ip route 200.1.0.0  255.255.0.0 FE0
  ```

  Wenn keine Standardroute vorhanden ist, erstellt Cisco SDM einfach eine neue und verwendet die Tunnelschnittstelle als Next Hop. Beispiel:

  ```
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ```

- **Split-Tunneling durchführen** – Mit Split-Tunneling kann Datenverkehr, der für das in den Feldern **IP-Adresse** und **Netzwerkmaske** angegebene Netzwerk vorgesehen ist, verschlüsselt und über die Tunnel-Schnittstelle geleitet werden. Der gesamte andere Datenverkehr wird nicht verschlüsselt. Wenn diese Option ausgewählt wird, erstellt Cisco SDM anhand der IP-Adresse und der Netzwerkmaske eine statische Route zum Netzwerk.

  Im folgenden Beispiel wird davon ausgegangen, dass die Netzwerkadresse 10.2.0.0/255.255.0.0 in den Feldern für die Zieladresse angegeben wurde:

  Im folgenden Beispiel wird davon ausgegangen, dass die Netzwerkadresse 10.2.0.0/255.255.0.0 in den Feldern für die Zieladresse angegeben wurde:

  ```
  ip route 10.2.0.0 255.255.0.0 Tunnel0
  ```

  Wenn Tunnelsplit ausgewählt wurde, erscheinen die Felder IP-Adresse und Subnetzmaske, in der Sie die IP-Adresse und Subnetzmaske des Ziel-Peers eingeben müssen. Sie müssen sicherstellen, dass die im Feld **Tunnelziel** im Fenster **GRE-Tunnel-Informationen** eingegebene Ziel-IP-Adresse erreichbar ist. Wenn sie nicht erreichbar ist, wird kein Tunnel aufgebaut.

IP-Adresse

Mit Split-Tunneling aktiviert. Geben Sie die IP-Adresse des Netzwerks am anderen Ende des Tunnels ein. Cisco SDM erstellt einen Eintrag für eine statische Route für die Pakete mit einer Zieladresse in diesem Netzwerk. Dieses Feld ist deaktiviert, wenn **Gesamten Datenverkehr durch Tunnel** ausgewählt wurde.

Bevor Sie diese Option konfigurieren, müssen Sie sicherstellen, dass die in diesem Feld eingegebene IP-Adresse erreicht werden kann. Wenn sie nicht erreichbar ist, wird kein Tunnel aufgebaut.

Netzwerkmaske

Mit Split-Tunneling aktiviert. Geben Sie die Netzwerkmaske ein, die im Netzwerk am anderen Ende des Tunnels verwendet wird. Dieses Feld ist deaktiviert, wenn **Gesamten Datenverkehr durch Tunnel** ausgewählt wurde.

Routing-Protokoll auswählen

Geben Sie in diesem Fenster an, wie andere Netzwerke hinter Ihrem Router für andere Router im Netzwerk angekündigt werden. Wählen Sie eine der folgenden Typen:

- EIGRP – Enhanced Interior Gateway Routing Protocol
- OSPF – Open Shortest Path First
- RIP – Routing Internet Protocol
- Statisches Routing. Diese Option ist aktiviert, wenn Sie einen GRE over IPSec-Tunnel konfigurieren.

Hinweis RIP wird nicht für die DMVPN-Hub-und-Spoke-Topologie unterstützt, ist aber für die vollvermaschte DMVPN-Topologie verfügbar.

Übersicht über die Konfiguration

Dieser Bildschirm fasst die von Ihnen durchgeführte GRE-Konfiguration in einer Übersicht zusammen. Sie können die Informationen in diesem Bildschirm überprüfen und auf die Schaltfläche **Zurück** klicken, um zu einem Bildschirm zurückzukehren, in dem Sie Änderungen vornehmen möchten. Wenn Sie die Konfiguration speichern möchten, klicken Sie auf **Fertig stellen**.

Die GRE-Tunnelkonfiguration erstellt eine IPSec-Regel, die angibt, zwischen welchen Hosts der GRE-Datenverkehr zugelassen ist. Diese IP-Sec-Regel wird in der Übersicht angezeigt.

So speichern Sie diese Konfiguration in der aktiven Konfiguration des Routers und verlassen diesen Assistenten:

Klicken Sie auf **Fertig stellen**. Cisco SDM speichert die Konfigurationsänderungen in der aktiven Konfiguration des Routers. Die Änderungen werden sofort wirksam; beim Abschalten des Routers gehen sie jedoch verloren.

Wenn Sie im Cisco SDM-Fenster **Einstellungen** die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden** aktiviert haben, wird das Fenster **Senden** angezeigt. In diesem Fenster können Sie die CLI-Befehle anzeigen, die an den Router gesendet werden.

Site-to-Site-VPN bearbeiten

VPNs (Virtual Private Networks – virtuelle private Netzwerke) ermöglichen Ihnen den Schutz von Daten zwischen Ihrem Router und einem Remote-System durch die Verschlüsselung von Datenverkehr, damit er nicht von anderen gelesen werden kann, die dasselbe öffentliche Netzwerk verwenden. Sie erhalten praktisch den Schutz eines privaten Netzwerks über öffentliche Leitungen, die von anderen Organisationen verwendet werden können.

Verwenden Sie dieses Fenster, um VPN-Verbindungen zu Remote-Systemen zu erstellen und zu verwalten. Sie können VPN-Verbindungen erstellen, bearbeiten und löschen sowie vorhandene Verbindungen zurücksetzen. Sie können dieses Fenster auch verwenden, um Ihren Router als einen Easy VPN-Client mit Verbindungen zu einem oder mehreren Easy VPN-Servern oder -Konzentratoren zu konfigurieren.

Klicken Sie auf den Link für den Teil des Fensters, für den Sie Hilfe erhalten möchten:

Site-to-Site-VPN-Verbindungen

VPN-Verbindungen, die manchmal als *Tunnel* bezeichnet werden, werden vom Feld **VPN-Verbindungen** aus erstellt und verwaltet. Eine VPN-Verbindung verbindet eine Routerschnittstelle mit einem oder mehreren Peers, die von einer Crypto Map angegeben werden, die wiederum in einer IPSec-Richtlinie (IP Security) definiert ist. Sie können die VPN-Verbindungen in dieser Liste anzeigen, bearbeiten und löschen sowie Verbindungen hinzufügen.

Spalte „Status“

Der Status der Verbindung, der durch die folgenden Symbole angegeben wird:

 Die Verbindung ist aktiv.

 Die Verbindung ist nicht aktiv.

 Die Verbindung wird aufgebaut.

Schnittstelle

Die Routerschnittstelle, die mit den Remote-Peers in dieser VPN-Verbindung verbunden ist. Eine Schnittstelle kann nur mit einer IPSec-Richtlinie verknüpft werden. Ein und dieselbe Schnittstelle wird in mehreren Zeilen angezeigt, wenn mehrere Crypto Maps für die IPSec-Richtlinie definiert wurden, die in dieser Verbindung verwendet wird.

Beschreibung

Eine kurze Beschreibung dieser Verbindung.

IPSec-Richtlinie

Der Name der IPSec-Richtlinie, die in dieser VPN-Verbindung verwendet wird. Die IPSec-Richtlinie gibt an, wie Daten verschlüsselt werden, welche Daten verschlüsselt werden und wohin Daten gesendet werden. Wenn Sie weitere Informationen wünschen, klicken Sie auf Weitere Informationen zu VPN-Verbindungen und IPSec-Richtlinien.

Sequenznummer

Die Sequenznummer für diese Verbindung. Da eine IPSec-Richtlinie in mehreren Verbindungen verwendet werden kann, wird diese VPN-Verbindung durch die Kombination aus der Sequenznummer und dem Namen der IPSec-Richtlinie eindeutig identifiziert. Die Sequenznummer ordnet der VPN-Verbindung keine Priorität zu. Der Router versucht, alle konfigurierten VPN-Verbindungen unabhängig von der Sequenznummer aufzubauen.

Peers

Die IP-Adressen oder Hostnamen der Geräte am anderen Ende der VPN-Verbindung. Wenn eine Verbindung mehrere Peers enthält, werden ihre IP-Adressen oder Hostnamen durch Kommas getrennt. Es können mehrere Peers konfiguriert werden, um alternative Routing-Pfade für die VPN-Verbindung anzugeben.

Transformationssatz

Hier wird der Name des Transformationssatzes angezeigt, der von dieser VPN-Verbindung verwendet wird. Bei mehreren Transformationssätzen werden die Namen durch Kommas getrennt. Ein Transformationssatz gibt die Algorithmen an, die für die Verschlüsselung von Daten, die Gewährleistung der Datenintegrität und die Bereitstellung der Datenkompression verwendet werden. Beide Peers müssen denselben Transformationssatz verwenden, und sie ermitteln über eine Aushandlung, welcher Transformationssatz verwendet wird. Es können mehrere Transformationssätze definiert werden, um sicherzustellen, dass der Router einen Transformationssatz anbieten kann, den der Peer, mit dem die Aushandlung erfolgt, akzeptiert. Die Transformationssätze sind eine Komponente der IPSec-Richtlinie.

IPSec-Regel

Die Regel, die festlegt, welcher Datenverkehr in dieser Verbindung zu verschlüsseln ist. Die IPSec-Regel ist eine Komponente der IPSec-Richtlinie.

Typ

Einer der folgenden Typen:

- Statisch – Dies ist ein statischer Site-to-Site-VPN-Tunnel. Der VPN-Tunnel verwendet statische Crypto Maps.
- Dynamisch – Dies ist ein dynamischer Site-to-Site-VPN-Tunnel. Der VPN-Tunnel verwendet dynamische Crypto Maps.

Schaltfläche „Hinzufügen“

Klicken Sie auf diese Schaltfläche, um eine VPN-Verbindung hinzuzufügen.

Schaltfläche „Löschen“

Klicken Sie auf diese Schaltfläche, um eine ausgewählte VPN-Verbindung zu löschen.

Tunnel testen... (Schaltfläche)

Klicken Sie auf diese Schaltfläche, um einen ausgewählten VPN-Tunnel zu testen. Die Ergebnisse des Tests werden in einem weiteren Fenster angezeigt.

Schaltfläche „Verbindung löschen“

Klicken Sie auf diese Schaltfläche, um eine zu einem Remote-Peer aufgebaute Verbindung zurückzusetzen. Diese Schaltfläche ist deaktiviert, wenn Sie einen dynamischen Site-to-Site-VPN-Tunnel ausgewählt haben.

Schaltfläche „Spiegel generieren“

Klicken Sie auf diese Schaltfläche, um eine Textdatei zu erstellen, in der die VPN-Konfiguration des lokalen Routers erfasst wird, damit ein Remote-Router eine VPN-Konfiguration erhalten kann, mit der er in der Lage ist, eine VPN-Verbindung zum lokalen Router aufzubauen. Diese Schaltfläche ist deaktiviert, wenn Sie einen dynamischen Site-to-Site-VPN-Tunnel ausgewählt haben.

Hinweis Alle von Cisco SDM ermittelten VPN-Verbindungen, die vorher konfiguriert wurden und keine ISAKMP-Crypto Maps verwenden, werden in der Tabelle der VPN-Verbindungen als schreibgeschützte Einträge angezeigt und können nicht bearbeitet werden.

Neue Verbindung hinzufügen

Verwenden Sie dieses Fenster, um eine neue VPN-Verbindung zwischen dem lokalen Router und einem als *Peer* bezeichneten Remote-System hinzuzufügen. Sie erstellen die VPN-Verbindung, indem Sie eine IPSec-Richtlinie mit einer Schnittstelle verknüpfen.

So erstellen Sie eine VPN-Verbindung:

Schritt 1 Wählen Sie aus der Liste **Schnittstelle auswählen** die Schnittstelle aus, die Sie für das VPN verwenden möchten. In dieser Liste werden nur Schnittstellen angezeigt, die nicht in anderen VPN-Verbindungen verwendet werden.

Schritt 2 Wählen Sie aus der Liste **IPSec-Richtlinie auswählen** eine Richtlinie aus. Klicken Sie auf **OK**, um zum Fenster **VPN Connections** zurückzukehren.

Zusätzliche Crypto Maps hinzufügen

Verwenden Sie dieses Fenster, um eine neue Crypto Map zu einer vorhandenen IPSec-Richtlinie hinzuzufügen. In diesem Fenster wird Folgendes angezeigt: die Schnittstelle, die mit der im Fenster **VPN Connections** ausgewählten VPN-Verbindung verknüpft ist, die mit ihr verknüpfte IPSec-Richtlinie und die Crypto Maps, die die Richtlinie bereits enthält.

Die Crypto Map gibt Folgendes an: eine Sequenznummer, das Peer-Gerät am anderen Ende der Verbindung, den Transformationssatz für die Verschlüsselung des Datenverkehrs und die IPSec-Regel, die angibt, welcher Datenverkehr verschlüsselt wird.

Hinweis Das Hinzufügen einer Crypto Map zu einer vorhandenen IPSec-Richtlinie ist die einzige Möglichkeit, einen VPN-Tunnel zu einer Schnittstelle hinzuzufügen, die bereits in einer vorhandenen VPN-Verbindung verwendet wird.

Schnittstelle

Dies ist die Schnittstelle, die in dieser VPN-Verbindung verwendet wird.

IPSec-Richtlinie

Dies ist der Name der IPSec-Richtlinie, die die VPN-Verbindung kontrolliert. Die Crypto Maps, aus denen die IPSec-Richtlinie besteht, werden in der Liste unter diesem Feld angezeigt. Wenn Sie weitere Informationen wünschen, klicken Sie auf Weitere Informationen zu VPN-Verbindungen und IPSec-Richtlinien.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Selbständiges Konfigurieren der Crypto Map	Klicken Sie auf **Neue Crypto Map hinzufügen**, und verwenden Sie das Fenster **Crypto Map hinzufügen**, um die neue Crypto Map zu erstellen. Wenn Sie die Erstellung abgeschlossen haben, klicken Sie auf **OK**. Klicken Sie dann in diesem Fenster auf **OK**.
Hinzufügen einer neuen Crypto Map zu dieser Verbindung mit Unterstützung von Cisco Router and Security Device Manager (Cisco SDM)	Aktivieren Sie das Kontrollkästchen **Hinzufügen-Assistenten verwenden**, und klicken Sie auf **OK**. Cisco SDM führt Sie durch die Schritte für die Erstellung einer neuen Crypto Map und verknüpft sie mit der IPSec-Richtlinie.

Crypto Map-Assistant: Willkommen

Dieser Assistent führt Sie durch die Erstellung einer Crypto Map. Eine Crypto Map gibt die Peer-Geräte am anderen Ende der VPN-Verbindung an, definiert, wie Datenverkehr verschlüsselt wird, und gibt an, welcher Datenverkehr verschlüsselt wird.

Klicken Sie auf **Weiter**, um mit der Erstellung einer Crypto Map zu beginnen.

Crypto Map-Assistant: Übersicht über die Konfiguration

Auf der Übersichtsseite für den Crypto Map-Assistenten werden die Daten angezeigt, die Sie in den Fenstern des Assistenten eingegeben haben. Sie können die Daten überprüfen, auf **Zurück** klicken, um zu einem Bildschirm zurückzukehren und Änderungen vorzunehmen, und dann wieder zum Fenster **Übersicht** wechseln und auf **Fertig stellen** klicken, um die Crypto Map-Konfiguration an den Router zu senden.

Verbindung löschen

Verwenden Sie dieses Fenster, um einen VPN-Tunnel zu löschen oder lediglich seine Verknüpfung mit einer Schnittstelle aufzuheben, die Definition aber für die zukünftige Verwendung beizubehalten.

Löschen Sie die Crypto Map mit der Sequenznummer *n* aus der IPSec-Richtlinie *Richtlinienname*

Klicken Sie auf diese Schaltfläche und dann auf **OK**, um die Definition des VPN-Tunnels zu entfernen. Wenn Sie diesen Schritt ausführen, gehen die Verknüpfungen zwischen der Schnittstelle, der IPSec-Richtlinie und den Peer-Geräten verloren. Wenn mehrere Schnittstellen mit dieser Tunneldefinition verknüpft wurden, werden diese Verknüpfungen ebenfalls gelöscht.

Löschen Sie die dynamische Crypto Map mit der Sequenznummer *n* aus dem Satz *Satzname* mit dynamischen Crypto Maps

Diese Schaltfläche wird angezeigt, wenn Sie einen dynamischen Site-to-Site-VPN-Tunnel ausgewählt haben. Klicken Sie auf diese Schaltfläche und dann auf **OK**, um die Definition des VPN-Tunnels zu entfernen. Wenn Sie diesen Schritt ausführen, gehen die Verknüpfungen zwischen der Schnittstelle, der IPSec-Richtlinie und den Peer-Geräten verloren. Wenn mehrere Schnittstellen mit dieser Tunneldefinition verknüpft wurden, werden diese Verknüpfungen ebenfalls gelöscht.

Heben Sie die Verknüpfung zwischen IPSec-Richtlinie *Richtlinienname* und Schnittstelle *Schnittstellenname* auf, und behalten Sie die IPSec-Richtlinie für eine mögliche erneute Nutzung bei

Klicken Sie auf diese Schaltfläche und dann auf **OK**, um die Tunneldefinition beizubehalten, aber ihre Verknüpfung mit der Schnittstelle aufzuheben. Wenn Sie es wünschen, können Sie diese Definition mit einer anderen Routerschnittstelle verknüpfen.

Ping

In diesem Fenster können Sie einen Ping an ein Peer-Gerät senden. Sie können sowohl die Quelle als auch das Ziel für die Ping-Operation auswählen. Sie sollten einen Ping an einen Remote-Peer senden, nachdem Sie einen VPN-Tunnel zurückgesetzt haben.

Quelle

Wählen Sie die IP-Adresse aus, von der der Ping ausgehen soll, oder geben Sie die Adresse ein. Wenn die Adresse, die Sie verwenden möchten, sich nicht in der Liste befindet, können Sie eine andere in das Feld eingeben. Der Ping kann von jeder Schnittstelle auf dem Router ausgehen. Standardmäßig geht der **ping**-Befehl von der äußeren Schnittstelle mit der Verbindung zum Remote-Gerät aus.

Ziel

Wählen Sie die IP-Adresse aus, an die Sie den Ping senden möchten. Wenn die Adresse, die Sie verwenden möchten, sich nicht in der Liste befindet, können Sie eine andere in das Feld eingeben.

So senden Sie einen Ping an einen Remote-Peer:

Geben Sie die Quelle und das Ziel an, und klicken Sie auf **Ping**. Sie können die Ausgabe des **ping**-Befehls lesen, um festzustellen, ob der Ping-Befehl erfolgreich war.

So löschen Sie die Ausgabe des ping-Befehls:

Klicken Sie auf **Löschen**.

Spiegel generieren...

In diesem Fenster wird die IPSec-Richtlinie angezeigt, die für den VPN-Tunnel zum ausgewählten Peer verwendet wird. Sie haben außerdem die Möglichkeit, die Richtlinie in einer Textdatei zu speichern, die Sie für die Konfiguration der VPN-Verbindung auf dem Peer-Gerät verwenden können.

Peer-Gerät

Wählen Sie die IP-Adresse oder den Hostnamen des Peer-Geräts aus, um die IPSec-Richtlinie anzuzeigen, die für den Tunnel zu diesem Gerät konfiguriert ist. Die Richtlinie wird im Feld unter der Peer-IP-Adresse angezeigt.

So erstellen Sie eine Textdatei der IPSec-Richtlinie:

Klicken Sie auf **Speichern**, und geben Sie einen Namen und einen Speicherort für die Textdatei an. Sie können diese Textdatei der Administration des Peer-Geräts geben, damit diese eine Richtlinie erstellen kann, die die von Ihnen auf dem Router erstellte Richtlinie widerspiegelt. Klicken Sie auf **Wie konfiguriere ich nach der Konfiguration eines VPN das VPN auf dem Peer-Router?**, um zu erfahren, wie die Textdatei für die Erstellung einer Spiegelrichtlinie verwendet wird.

Vorsicht Die von Ihnen generierte Textdatei darf nicht in die Konfigurationsdatei des Remote-Systems kopiert werden, sondern darf nur zur Anzeige der Konfiguration auf dem lokalen Router verwendet werden, damit das Remote-Gerät auf kompatible Weise konfiguriert werden kann. Es werden möglicherweise identische Namen für IPSec-Richtlinien, IKE-Richtlinien und Transformationssätze auf dem Remote-Router verwendet, aber die Richtlinien und Transformationssätze können abweichen. Wenn die Textdatei einfach in die Remote-Konfigurationsdatei kopiert wird, führt dies wahrscheinlich zu Konfigurationsfehlern.

Cisco SDM-Warnung: NAT-Regeln mit ACL

Dieses Fenster wird angezeigt, wenn Sie ein VPN konfigurieren und dazu Schnittstellen mit verknüpften NAT-Regeln verwenden, die wiederum Zugriffsregeln verwenden. Dieser NAT-Regeltyp kann IP-Adressen in Paketen ändern, bevor die Pakete das LAN verlassen oder in das LAN gelangen. Eine NAT-Regel verhindert, dass VPN-Verbindungen ordnungsgemäß funktionieren, wenn sie Quell-IP-Adressen so ändert, dass sie nicht der IPSec-Regel entsprechen, die für das VPN konfiguriert ist. Damit dies nicht passiert, kann Cisco SDM diese in NAT-Regeln konvertieren, die Routenzuordnungen verwenden. Routenzuordnungen geben Subnetze an, die nicht übersetzt werden sollen.

Im Fenster werden die NAT-Regeln angezeigt, die geändert werden müssen, um sicherzustellen, dass die VPN-Verbindung ordnungsgemäß funktioniert.

Ursprüngliche Adresse

Die IP-Adresse, die von NAT übersetzt wird.

Übersetzte Adresse

Die IP-Adresse, durch die NAT die ursprüngliche Adresse ersetzt.

Regeltyp

Der Typ der NAT-Regel, entweder **Statisch** oder **Dynamisch**.

So veranlassen Sie, dass die aufgelisteten NAT-Regeln Routenzuordnungen verwenden:

Klicken Sie auf **OK**.

Wie gehe ich vor?

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie erstelle ich ein VPN für mehrere Standorte?

Sie können mit Cisco SDM mehrere VPN-Tunnel auf einer Schnittstelle des Routers erstellen. Jeder VPN-Tunnel verbindet die ausgewählte Schnittstelle auf dem Router mit einem anderen Subnetz auf dem Zielrouter. Sie können mehrere VPN-Tunnel für die Verbindung mit derselben Schnittstelle, aber anderen Subnetzen auf dem Zielrouter konfigurieren. Es besteht auch die Möglichkeit, mehrere VPN-Tunnel zu konfigurieren, die eine Verbindung zu verschiedenen Schnittstellen auf dem Zielrouter aufbauen.

Zuerst müssen Sie den VPN-Anfangstunnel erstellen. In den folgenden Schritten wird die Erstellung eines solchen Tunnels beschrieben. Wenn Sie bereits einen ersten Tunnel erstellt haben und weitere Tunnel zur selben Schnittstelle hinzufügen müssen, überspringen Sie das erste Verfahren, und führen Sie die Schritte im nächsten Verfahren in diesem Hilfethema aus.

So erstellen Sie den VPN-Anfangstunnel:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie die Option **Erstellen Sie ein Site-to-Site-VPN**.

Schritt 3 Klicken Sie auf **Ausgewählte Aufgabe starten**.

Der VPN-Assistent wird gestartet.

Schritt 4 Klicken Sie auf **Schnelleinrichtung**.

Schritt 5 Klicken Sie auf **Weiter >**.

Schritt 6 Wählen Sie im Feld **Wählen Sie die Schnittstelle für diese VPN-Verbindung aus** die Schnittstelle auf dem Quellrouter aus, auf der der VPN-Tunnel erstellt werden soll. Dies ist auf dem lokalen System im Diagramm für das Anwendungsszenario die mit dem Internet verbundene Schnittstelle.

Schritt 7 Geben Sie im Feld **Peer-Identität** die IP-Adresse der Zielrouterschnittstelle ein.

Schritt 8 Geben Sie in den Feldern unter **Authentifizierung** den Pre-Shared Key ein, den die beiden VPN-Peers verwenden werden, und geben Sie ihn dann noch einmal ein.

Schritt 9 Wählen Sie im Feld **Quelle** die Schnittstelle aus, die mit dem Subnetz verbunden ist, dessen IP-Datenverkehr Sie schützen möchten. Dies ist der lokale Router im Diagramm für das Anwendungsszenario, und es handelt sich in der Regel um eine Schnittstelle, die mit dem LAN verbunden ist.

Schritt 10 Geben Sie in die Zielfelder die IP-Adresse und die Subnetzmaske des Zielrouters ein.

Schritt 11 Klicken Sie auf **Weiter >**.

Schritt 12 Klicken Sie auf **Fertig stellen**.

Erstellen eines zusätzlichen Tunnels von derselben Quellschnittstelle

Nachdem Sie den VPN-Anfangstunnel erstellt haben, gehen Sie nach diesen Schritten vor, um einen zusätzlichen Tunnel von derselben Quellschnittstelle zu einer anderen Zielschnittstelle oder einem anderen Ziel-Subnetz zu erstellen:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie die Option **Erstellen Sie ein Site-to-Site-VPN** aus.

Schritt 3 Klicken Sie auf **Ausgewählte Aufgabe starten**.

Der VPN-Assistent wird gestartet.

Schritt 4 Klicken Sie auf **Schnelleinrichtung**.

Schritt 5 Klicken Sie auf **Weiter >**.

Schritt 6 Wählen Sie im Feld **Wählen Sie die Schnittstelle für diese VPN-Verbindung aus** dieselbe Schnittstelle aus, die Sie für die Erstellung der VPN-Anfangsverbindung verwendet haben.

Schritt 7 Geben Sie im Feld **Peer-Identität** die IP-Adresse der Zielrouterschnittstelle ein. Sie können dieselbe IP-Adresse eingeben, die Sie bei der Erstellung der VPN-Anfangsverbindung eingegeben haben. Dies gibt an, dass diese zweite VPN-Verbindung dieselbe Schnittstelle auf dem Zielrouter wie die VPN-Anfangsverbindung verwenden soll. Wenn Sie nicht möchten, dass beide VPN-Verbindungen zur selben Zielschnittstelle gehen, geben Sie die IP-Adresse einer anderen Schnittstelle auf dem Zielrouter ein.

Schritt 8 Geben Sie in den Feldern unter **Authentifizierung** den Pre-Shared Key ein, den die beiden VPN-Peers verwenden werden, und geben Sie ihn dann noch einmal ein.

Schritt 9 Wählen Sie im Feld **Quelle** dieselbe Schnittstelle aus, die Sie für die Erstellung der VPN-Anfangsverbindung verwendet haben.

Schritt 10 In den Feldern unter **Ziel** stehen Ihnen folgende Optionen zur Verfügung:

- Wenn Sie im Identifizierungsfeld des Peers die IP-Adresse einer anderen Schnittstelle des Zielrouters eingegeben haben und den eingehenden IP-Verkehr von einem bestimmten Subnetz schützen wollen, geben Sie die IP-Adresse und Subnetzmaske dieses Subnetzes in das vorgesehene Feld ein.
- Wenn Sie im Feld **Peer-Identität** die IP-Adresse eingegeben haben, die Sie auch für die VPN-Anfangsverbindung verwendet haben (und damit angeben, dass dieser VPN-Tunnel dieselbe Routerschnittstelle wie der VPN-Anfangstunnel verwendet), geben Sie die IP-Adresse und die Subnetzmaske des neuen Subnetzes, das Sie schützen möchten, in die entsprechenden Felder ein.

Schritt 11 Klicken Sie auf **Weiter >**.

Schritt 12 Klicken Sie auf **Fertig stellen**.

Wie konfiguriere ich nach der Konfiguration eines VPN das VPN auf dem Peer-Router?

Cisco SDM generiert VPN-Konfigurationen auf Ihrem Router. Cisco SDM enthält eine Funktion, mit der eine Textdatei der Konfiguration generiert und diese als Vorlage für die Erstellung einer VPN-Konfiguration für den Peer-Router verwendet werden kann, mit dem der VPN-Tunnel verbunden ist. Diese Textdatei kann nur als Vorlage verwendet werden, die Ihnen die Befehle angibt, die konfiguriert werden müssen. Sie kann nicht unbearbeitet verwendet werden, da sie Daten enthält, die nur auf den lokalen Router zutreffen, den Sie konfiguriert haben.

So generieren Sie eine Vorlagenkonfiguration für den Peer-VPN-Router:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie im VPN-Baum die Option **Site-to-Site-VPN** aus, und klicken Sie dann auf die Registerkarte **Bearbeiten**.

Schritt 3 Wählen Sie die VPN-Verbindung aus, die Sie als Vorlage verwenden möchten, und klicken Sie auf **Spiegel generieren**.

Cisco SDM zeigt den Bildschirm **Spiegel generieren** an.

Schritt 4 Wählen Sie im Feld **Peer-Gerät** die IP-Adresse des Peer-Geräts aus, für das Sie einen Konfigurationsvorschlag generieren möchten.

Der Konfigurationsvorschlag für das Peer-Gerät wird im Bildschirm **Spiegel generieren** angezeigt.

Schritt 5 Klicken Sie auf **Speichern**, um das Windows-Dialogfeld **Datei speichern** anzuzeigen, und speichern Sie die Datei.

Vorsicht Wenden Sie die Spiegelkonfiguration nicht auf das Peer-Gerät an, ohne sie vorher zu bearbeiten! Diese Konfiguration ist eine Vorlage, für die eine zusätzliche manuelle Konfiguration erforderlich ist. Verwenden Sie sie nur als Ausgangspunkt für die Erstellung der Konfiguration des VPN-Peers.

Schritt 6 Wenn Sie die Datei gespeichert haben, nehmen Sie die erforderlichen Änderungen in der Vorlagenkonfiguration in einem Texteditor vor. Unter anderem müssen möglicherweise die folgenden Befehle bearbeitet werden:

- Peer-IP-Adressbefehl(e)
- Transformationsrichtlinienbefehl(e)
- Crypto Map-IP-Adressbefehl(e)
- ACL-Befehl(e)
- Schnittstellen-IP-Adressbefehl(e)

Schritt 7 Wenn Sie die Bearbeitung der Peer-Konfigurationsdatei abgeschlossen haben, senden Sie sie mit einem TFTP-Server (Trivial File Transfer Protocol) an den Peer-Router.

Wie bearbeite ich einen vorhandenen VPN-Tunnel?

So bearbeiten Sie einen existierenden VPN-Tunnel:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie im VPN-Baum die Option **Site-to-Site-VPN** aus, und klicken Sie dann auf die Registerkarte **Bearbeiten**.

Schritt 3 Klicken Sie auf die Verbindung, die Sie bearbeiten möchten.

Schritt 4 Klicken Sie auf **Hinzufügen**.

Schritt 5 Wählen Sie **Static crypto maps to <Regelname>**

Schritt 6 Im Fenster **Statische Crypto Maps hinzufügen** können Sie weitere Crypto Maps zur VPN-Verbindung hinzufügen.

Schritt 7 Wenn Sie Komponenten der Verbindung ändern müssen, z. B. die IPSec-Richtlinie oder die vorhandene Crypto Map, notieren Sie sich die im VPN-Fenster angegebenen Namen dieser Komponenten, und wechseln Sie in die entsprechenden Fenster unter **VPN-Komponenten**, um die Änderungen vorzunehmen.

Wie erhalte ich die Bestätigung, dass mein VPN funktioniert?

Mit dem Monitor-Modus in Cisco SDM können Sie überprüfen, ob Ihre VPN-Verbindung funktioniert. Wenn die VPN-Verbindung funktioniert, wird sie im Monitor-Modus mit den Peer-IP-Adressen für Quelle und Ziel angegeben. Abhängig davon, ob die VPN-Verbindung ein IPSec-Tunnel oder eine IKE-SA (Internet Key Exchange Security Association) ist, wird im Monitor-Modus die Anzahl der über die Verbindung übertragenen Pakete oder der aktuelle Status der Verbindung angezeigt. So zeigen Sie die aktuellen Informationen über eine VPN-Verbindung an:

Schritt 1 Klicken Sie in der Symbolleiste auf **Monitor-Modus**.

Schritt 2 Wählen Sie im linken Bereich **VPN-Status** aus.

Schritt 3 Wählen Sie im Feld **Kategorie auswählen** aus, ob Informationen für IPSec-Tunnel oder IKE-SAs angezeigt werden sollen.

Jede konfigurierte VPN-Verbindung wird als eine Zeile auf dem Bildschirm angezeigt.

Wenn Sie IPSec-Tunneldaten anzeigen, können Sie anhand der folgenden Informationen feststellen, ob Ihre VPN-Verbindung funktioniert:

- Die IP-Adressen für den lokalen und den Remote-Peer sind richtig und geben an, dass die VPN-Verbindung zwischen den richtigen Standorten und Routerschnittstellen besteht.
- Für den Status des Tunnels ist **Aktiv** angegeben. Wenn **Inaktiv** oder **Vom Administrator deaktiviert** angegeben ist, dann ist die VPN-Verbindung nicht aufgebaut.
- Die Anzahl der gekapselten und entkapselten Pakete ist ungleich null; dies gibt an, dass Daten über die Verbindung übertragen wurden und nicht zu viele Sende- und Empfangsfehler aufgetreten sind.

Wenn Sie IKE-SA-Daten anzeigen, können Sie die Funktion der VPN-Verbindung überprüfen, indem Sie feststellen, ob die IP-Adressen für Quelle und Ziel richtig sind und ob als Status „QM_IDLE“ angegeben ist (dies gibt an, dass die Verbindung authentifiziert wurde und Daten übertragen werden können).

Wie konfiguriere ich einen Sicherungs-Peer für mein VPN?

So konfigurieren Sie mehrere VPN-Peers in einer einzelnen Crypto Map:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie im VPN-Baum die Option **VPN-Komponenten** und dann **IPSec-Richtlinien**.

Schritt 3 Klicken Sie in der Tabelle **IPSec-Richtlinien** auf die IPSec-Richtlinie, zu der Sie einen weiteren VPN-Peer hinzufügen möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **IPSec-Richtlinie bearbeiten** wird angezeigt.

Schritt 5 Klicken Sie auf **Hinzufügen**.

Schritt 6 Das Dialogfeld **Crypto Map hinzufügen** wird angezeigt. In ihm können Sie die Werte für die neue Crypto Map festlegen. Verwenden Sie dazu alle vier Registerkarten im Dialogfeld. Die Registerkarte **Peer-Informationen** enthält das Feld **Peers angeben**, in dem Sie die IP-Adresse des Peers eingeben können, den Sie hinzufügen möchten.

Schritt 7 Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf **OK**.

Die Crypto Map mit der neuen Peer-IP-Adresse wird in der Tabelle **Crypto Maps in dieser IPSec-Richtlinie** angezeigt.

Schritt 8 Um weitere Peers hinzuzufügen, wiederholen Sie die Schritte 4 bis 8.

Wie nehme ich mehrere Geräte auf, auf denen VPN in unterschiedlichem Umfang unterstützt wird?

So fügen Sie mehr als einen Transformationssatz zu einer einzelnen Crypto Map hinzu:

Schritt 1 Wählen Sie im linken Bereich **VPN** aus.

Schritt 2 Wählen Sie im VPN-Baum die Option **VPN-Komponenten** und dann **IPSec-Richtlinien**.

Schritt 3 Klicken Sie in der Tabelle **IPSec-Richtlinien** auf die IPSec-Richtlinie mit der Crypto Map, zu der Sie einen weiteren Transformationssatz hinzufügen möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **IPSec-Richtlinie bearbeiten** wird angezeigt.

Schritt 5 Klicken Sie in der Tabelle **Crypto Maps in dieser IPSec-Richtlinie** auf die Crypto Map, zu der Sie einen weiteren Transformationssatz hinzufügen möchten.

Schritt 6 Klicken Sie auf **Bearbeiten**.

Das Dialogfeld **Crypto Map bearbeiten** wird angezeigt.

Schritt 7 Klicken Sie auf die Registerkarte **Transformationssätze**.

Schritt 8 Klicken Sie im Feld **Verfügbare Transformationssätze** auf einen Transformationssatz, den Sie zur Crypto Map hinzufügen möchten.

Schritt 9 Klicken Sie auf **>>**, um den ausgewählten Transformationssatz zur Crypto Map hinzuzufügen.

Schritt 10 Wenn Sie weitere Transformationssätze zu dieser Crypto Map hinzufügen möchten, wiederholen Sie Schritt 9 und Schritt 10, bis Sie alle gewünschten Transformationssätze hinzugefügt haben.

Klicken Sie auf **OK**.

Wie konfiguriere ich ein VPN auf einer nicht unterstützten Schnittstelle?

Cisco SDM kann ein VPN über einen Schnittstellentyp konfigurieren, der nicht von Cisco SDM unterstützt wird. Bevor Sie die VPN-Verbindung konfigurieren können, müssen Sie zunächst mit der Router-CLI die Schnittstelle konfigurieren. Die Schnittstelle muss mindestens eine konfigurierte IP-Adresse haben und in Betrieb sein. Um zu überprüfen, ob die Verbindung funktioniert, stellen Sie fest, ob als Schnittstellenstatus **Aktiv** angegeben ist.

Nachdem Sie die nicht unterstützte Schnittstelle mit der CLI konfiguriert haben, können Sie die VPN-Verbindung mit Cisco SDM konfigurieren. In den Feldern, in denen Sie eine Schnittstelle für die VPN-Verbindung auswählen müssen, wird die nicht unterstützte Schnittstelle angezeigt.

Wie konfiguriere ich ein VPN, nachdem ich eine Firewall konfiguriert habe?

Damit ein VPN mit einer eingerichteten Firewall funktioniert, muss die Firewall so konfiguriert sein, dass sie Datenverkehr zwischen den lokalen und den Remote-Peer-IP-Adressen zulässt. Cisco SDM erstellt diese Konfiguration standardmäßig, wenn Sie eine VPN-Konfiguration erstellen, nachdem Sie bereits eine Firewall konfiguriert haben.

Wie konfiguriere ich NAT Passthrough für ein VPN?

Wenn Sie NAT für die Übersetzung von Adressen von Netzwerken außerhalb Ihres eigenen Netzwerks verwenden und außerdem über VPN eine Verbindung zu einem bestimmten Standort außerhalb Ihres Netzwerks aufbauen, müssen Sie NAT Passthrough für Ihre VPN-Verbindung konfigurieren, damit Netzwerkadressen im VPN-Datenverkehr nicht übersetzt werden. Wenn Sie NAT bereits auf Ihrem Router konfiguriert haben und jetzt mit Cisco SDM eine neue VPN-Verbindung konfigurieren, werden Sie in einer Warnmeldung darüber informiert, dass Cisco SDM NAT so konfiguriert, dass VPN-Datenverkehr nicht übersetzt wird. Sie müssen die Meldung akzeptieren, damit Cisco SDM die ACLs erstellt, die zum Schutz Ihres VPN-Datenverkehrs vor Übersetzung erforderlich sind.

Wenn Sie NAT mit Cisco SDM konfigurieren und bereits eine VPN-Verbindung konfiguriert haben, führen Sie das folgende Verfahren zur Erstellung von ACLs aus.

Schritt 1 Wählen Sie im linken Bereich **Zusätzliche Aufgaben - ACL-Editor** aus.

Schritt 2 Wählen Sie im Baum **Regeln** die Option **Zugriffsregeln** aus.

Schritt 3 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Regel hinzufügen** wird angezeigt.

Schritt 4 Geben Sie im Feld **Name/Nummer** einen eindeutigen Namen oder eine eindeutige Nummer für die neue Regel ein.

Schritt 5 Wählen Sie aus dem Feld **Typ** die Option **Erweiterte Regel**.

Schritt 6 Geben Sie im Feld **Beschreibung** eine kurze Beschreibung der neuen Regel ein.

Schritt 7 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld **Standardregeleintrag hinzufügen** wird angezeigt.

Schritt 8 Wählen Sie im Feld **Aktion** die Option **Zulassen** aus.

Schritt 9 Wählen Sie in der Gruppe **Quellhost/-netzwerk** im Feld **Typ** die Option **Ein Netzwerk**.

Schritt 10 In den Feldern IP-Adresse und Wildcard-Maske geben Sie die IP-Adresse und Subnetzmaske des VPN Quellen-Peers ein.

Schritt 11 Wählen Sie in der Gruppe **Zielhost/-netzwerk** im Feld **Typ** die Option **Ein Netzwerk**.

Schritt 12 Geben Sie in die Felder **IP-Adresse** und **Platzhaltermaske** die IP-Adresse und die Subnetzmaske des VPN-Ziel-Peers ein.

Schritt 13 Geben Sie im Feld **Beschreibung** eine kurze Beschreibung des Netzwerks oder Hosts ein.

Schritt 14 Klicken Sie auf **OK**.

Die neue Regel wird jetzt in der Tabelle **Zugriffsregeln** angezeigt.

KAPITEL 10

Easy VPN Remote

Easy VPN Remote erstellen

Mit Cisco SDM können Sie einen Router als Client eines Easy VPN-Servers oder -Konzentrators konfigurieren. Auf dem Router muss ein Cisco IOS-Softwareimage ausgeführt werden, das Easy VPN Phase II unterstützt.

Damit Sie die Konfiguration durchführen können, müssen Sie die folgenden Informationen bereithalten.

- IP-Adresse oder Hostname des Easy VPN-Servers
- IPSec-Gruppenname
- Schlüssel

Lassen Sie sich diese Informationen von der Easy VPN-Serveradministration geben.

Easy VPN Remote-Client konfigurieren

Dieser Assistent führt Sie durch die Konfiguration eines Easy VPN Remote Phase II-Clients.

Hinweis Wenn der Router kein Cisco IOS-Abbild ausführt, das Easy VPN Remote Phase II oder höher unterstützt, können Sie keinen Easy VPN-Client konfigurieren.

Server-Informationen

Die in diesem Fenster eingegebenen Informationen identifizieren u. a. den Easy VPN-Tunnel und den Easy VPN-Server oder -Konzentrator, zu dem der Router eine Verbindung aufbaut und die Art und Weise mit der der Verkehr zum VPN geroutet werden soll.

Verbindungsname

Geben Sie den Namen ein, den Sie für diese Easy VPN-Verbindung vergeben möchten. Der Name muss innerhalb der Easy VPN-Tunnelnamen für den Router eindeutig sein und darf keine Leerzeichen oder Sonderzeichen wie Fragezeichen (?) enthalten.

Easy VPN-Server

Sie können Informationen für einen primären und einen sekundären Easy VPN-Server eingeben.

Easy VPN-Server 1

Geben Sie die IP-Adresse oder den Hostnamen des primären Easy VPN-Servers oder -Konzentrators ein, zu dem der Router eine Verbindung aufbaut. Wenn Sie einen Hostnamen eingeben, muss sich ein DNS (Domain Name System)-Server im Netzwerk befinden, der den Hostnamen in die richtige IP-Adresse für das Peer-Gerät auflösen kann.

Easy VPN-Server 2

Das Feld **Easy VPN-Server 2** erscheint, wenn das Cisco IOS-Abbild auf dem Router Easy VPN Remote Phase III unterstützt. Das Feld wird nicht angezeigt, wenn das Cisco IOS-Abbild Easy VPN Remote Phase III nicht unterstützt.

Geben Sie die IP-Adresse oder den Hostnamen des sekundären Easy VPN-Servers oder -Konzentrators ein, zu dem der Router eine Verbindung aufbaut. Wenn Sie einen Hostnamen eingeben, muss sich ein DNS-Server im Netzwerk befinden, der den Hostnamen in die richtige IP-Adresse für das Peer-Gerät auflösen kann.

Betriebsmodus

Client- oder Network Extension-Modus auswählen.

Wählen Sie **Client**, wenn die PCs und andere Geräte in den inneren Netzwerken des Routers ein privates Netzwerk mit privaten IP-Adressen bilden sollen. Es werden Network Address Translation (NAT) und Port Address Translation (PAT) verwendet. Geräte außerhalb des LANs können keine Pings an Geräte im LAN senden oder sie direkt erreichen.

Wählen Sie **Network Extension**, wenn die mit den inneren Schnittstellen verbundenen Geräte IP-Adressen haben sollen, die in das Routing einbezogen und vom Zielnetzwerk erreicht werden können. Die Geräte an beiden Enden der Verbindung bilden ein logisches Netzwerk. PAT wird automatisch deaktiviert, damit den PCs und Hosts an beiden Enden der Verbindung ein direkter Zugang ermöglicht wird.

Beraten Sie sich mit dem Administrator des Easy VPN-Servers oder -Konzentrators, bevor Sie diese Einstellung auswählen.

Wenn Sie Network Extension auswählen, können Sie das Fernmanagement des Routers aktivieren, indem Sie das Kontrollkästchen aktivieren, damit eine vom Server zugewiesene IP-Adresse für Ihren Router angefordert wird. Diese IP-Adresse kann für die Verbindung zu Ihrem Router für das Remote Management oder die Fehlerbehebung (ping, Telnet und Secure Shell) benutzt werden. Dieser Modus ist unter dem Namen **Network Extension Plus** bekannt.

Hinweis Wenn auf dem Router kein Cisco IOS-Abbild läuft, das Easy VPN Remote Phase IV oder höher unterstützt, können Sie Network Extension Plus nicht einrichten.

Authentifizierung

Benutzen Sie dieses Fenster, um die Sicherheitsstufe für den Easy VPN Tunnel zu bestimmen.

Geräteauthentifizierung

Wählen Sie Digitale Zertifikate oder Gemeinsamer Schlüssel.

Hinweis Die Option Digitale Zertifikate steht nur zur Verfügung, wenn sie durch das Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

Geben Sie den IPSec-Gruppennamen ein, um einen Pre-Shared Key zu verwenden. Der Gruppenname muss mit dem Gruppennamen übereinstimmen, den Sie auf dem VPN Konzentrator oder Server definiert haben. Lassen Sie sich diese Information von Ihrem Netzwerkadministrator geben.

Geben Sie den IPSec-Gruppenschlüssel ein. Der Gruppenname muss mit dem Gruppennamen übereinstimmen, den Sie auf dem VPN-Konzentrator oder -Server definiert haben. Lassen Sie sich diese Information von Ihrem Netzwerkadministrator geben. Geben Sie den Schlüssel zur Bestätigung der Richtigkeit noch einmal ein.

Benutzerauthentifizierung (XAuth)

Die **Benutzerauthentifizierung (XAuth)** erscheint in diesem Fenster, wenn das Cisco IOS-Abbild auf dem Router Easy VPN Remote Phase III unterstützt. Wenn die Benutzerauthentifizierung nicht erscheint, muss sie von der Befehlszeile der Schnittstelle des Routers eingerichtet werden.

Wählen Sie einen dieser Punkte aus, um den Xauth-Benutzernamen und das Kennwort einzugeben:

- Manuell in einem Webbrowser

  Hinweis Die Option Webbrowser erscheint nur, wenn sie vom Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

- Manuell über die Befehlszeile oder Cisco SDM

- Automatisch durch Speichern des Benutzernamens und Kennworts auf dem Router.

  Der Easy VPN-Server kann XAuth zur Authentifizierung des Routers verwenden. Wenn der Server die Option Kennwort zulässt, brauchen Sie den Benutzernamen und das Kennwort nicht jedes Mal eingeben, wenn der Easy VPN-Tunnel aufgebaut wird. Geben Sie den vom Easy VPN-Serveradministrator zur Verfügung gestellten Benutzernamen und das Kennwort ein. Geben Sie anschließend das Kennwort zur Bestätigung nochmals ein. Die Information wird in der Datei Routerinformationen gespeichert und jedes Mal benutzt, wenn der Tunnel eingerichtet wird.

Vorsicht Das Speichern des XAuth-Benutzernamens und des Kennworts im Speicher des Routers verursacht ein Sicherheitsrisiko, da jeder, der Zugriff auf die Routerkonfiguration hat, an diese Informationen gelangen kann. Wenn Sie die diese Informationen nicht auf dem Router speichern wollen, geben Sie diese nicht an dieser Stelle ein. Der Easy VPN-Server fordert dann einfach den Benutzernamen und das Kennwort bei jedem Verbindungsaufbau vom Router an. Außerdem kann Cisco SDM nicht selbst feststellen, ob der Easy VPN-Server die Option zum Speichern des Kennworts zulässt. Sie müssen feststellen, ob der Server diese Option zulässt. Wenn der Server die Option nicht zulässt, sollten Sie kein Sicherheitsrisiko eingehen, indem Sie die Informationen hier eingeben.

Schnittstellen und Verbindungseinstellungen

In diesem Fenster geben Sie die Schnittstellen an, die in der Easy VPN-Konfiguration verwendet werden.

Schnittstellen

Wählen Sie in diesem Feld die inneren und äußeren Schnittstellen.

Innere Schnittstellen

Markieren Sie die inneren (LAN-) Schnittstellen, die die lokalen Netzwerke bedienen, die Sie in diese Easy VPN-Konfiguration aufnehmen möchten. Sie können mehrere innere Schnittstellen auswählen, indem Sie folgende Beschränkungen beachten:

- Wenn Sie eine Schnittstelle auswählen, die bereits in einer anderen Easy VPN-Konfiguration verwendet wird, werden Sie darüber informiert, dass eine Schnittstelle nicht zu zwei Easy VPN-Konfigurationen gehören kann.
- Wenn Sie Schnittstellen auswählen, die bereits in einer VPN-Konfiguration verwendet werden, dann werden Sie darüber informiert, dass die Easy VPN-Konfiguration, die Sie erstellen, nicht neben der vorhandenen VPN-Konfiguration existieren kann. Sie werden gefragt, ob Sie die vorhandenen VPN-Tunnel dieser Schnittstellen entfernen und ihnen die Easy VPN-Konfiguration zuordnen möchten?
- Eine existierende Schnittstelle erscheint nicht in der Liste der Schnittstellen, wenn sie nicht in einer Easy VPN-Konfiguration verwendet werden kann. So werden z. B. auf dem Router konfigurierte Loopback-Schnittstellen nicht in dieser Liste angezeigt.
- Eine Schnittstelle kann nicht gleichzeitig als innere und äußere Schnittstelle bestimmt werden.

Auf Routern der Serien Cisco 800 und Cisco 1700 werden bis zu drei innere Schnittstellen unterstützt. Im Fenster **Easy VPN Remote bearbeiten** können Sie Schnittstellen aus einer Easy VPN-Konfiguration entfernen.

Äußere Schnittstellen

Wählen Sie in der Schnittstellenliste die äußere Schnittstelle, die mit dem Easy VPN-Server oder -Konzentrator verbunden ist

Hinweis Cisco 800 Router unterstützen nicht die Benutzung einer E 0 Schnittstelle an der äußeren Schnittstelle.

Verbindungseinstellungen

Wählen Sie die automatische, manuelle oder verkehrsabhängige VPN-Tunnelaktivierung aus.

Bei der manuellen Einstellung müssen Sie im Fenster **Easy VPN-Remote bearbeiten** auf die Taste **Verbinden** oder **Trennen** klicken, um den Tunnel aufzubauen oder zu trennen; dafür haben Sie jedoch die volle Kontrolle über den Tunnel und das Fenster **Easy VPN-Remote bearbeiten**. Wenn ein SA-Timeout (Security Association) für den Router eingestellt ist, müssen Sie den VPN-Tunnel bei jedem Timeout manuell neu aufbauen. Sie können SA-Timeout-Einstellungen unter im Fenster Globale VPN-Einstellungen für VPN-Komponenten ändern.

Bei der automatischen Einstellung wird der VPN-Tunnel automatisch eingerichtet, wenn die Easy VPN-Konfiguration an die Konfigurationsdatei des Routers geleitet wird. Sie können aber den Tunnel im Fenster **VPN-Verbindungen** nicht manuell kontrollieren. Die Taste **Verbinden** oder **Trennen** ist deaktiviert, wenn die Easy VPN-Verbindung ausgewählt wurde.

Bei der Einstellung **Verkehrsabhängig** wird der VPN-Tunnel immer eingerichtet, wenn äußerer lokaler (LAN) Datenverkehr festgestellt wird.

Hinweis Die Option Verkehrsabhängig Aktivierung steht nur zur Verfügung, wenn sie durch das Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

Übersicht über die Konfiguration

Dieses Fenster zeigt Ihnen die Easy VPN-Konfiguration an, die Sie eingerichtet haben und ermöglicht Ihnen die Konfiguration zu speichern. Eine Zusammenfassung ähnlich dem nachfolgenden Beispiel erscheint:

```
Easy VPN Tunnel Name:test1
Easy VPN-Server: 222.28.54.7
Gruppe: meineFirma
Schlüssel: 1234
Kontrolle: Auto
Modus: Client
Äußere Schnittstelle: BVI222
Innere Schnittstellen: Dialer0
```

Sie können die Konfiguration in diesem Fenster überprüfen und auf die Schaltfläche **Zurück** klicken, um Elemente zu ändern.

Wenn Sie auf die Schaltfläche **Fertig stellen** klicken, werden die Daten in die aktive Konfiguration des Routers geschrieben. Wenn der Tunnel für den automatischen Betrieb konfiguriert wurde, versucht der Router, eine Verbindung zum VPN-Konzentrator oder -Server aufzubauen.

Wenn Sie die Easy VPN-Konfiguration zu einem späteren Zeitpunkt ändern möchten, können Sie die Änderungen im Fenster **Easy VPN Remote bearbeiten** vornehmen.

Hinweis In vielen Fällen baut der Router eine Verbindung mit dem Easy VPN-Server oder -Konzentrator auf, nachdem Sie auf **Fertig stellen** klicken oder in den Fenstern für VPN-Verbindungen im Fenster **Easy VPN Remote bearbeiten** auf **Verbinden** klicken. Wenn das Gerät jedoch für die Verwendung von XAuth konfiguriert wurde, werden ein Benutzername und ein Kennwort vom Router angefordert. In diesem Fall müssen Sie zunächst eine SSH (Secure Shell)-Anmelde-ID und ein Kennwort für die Anmeldung beim Router und anschließend die XAuth-Anmeldung und das Kennwort für den Easy VPN-Server oder -Konzentrator angeben. Gehen Sie entsprechend diesem Vorgang vor, wenn Sie auf **Fertig stellen** klicken und die Konfiguration an den Router gesendet wird, und wenn Sie die Tunnelverbindung im Fenster **Easy VPN Remote bearbeiten** trennen und dann wieder herstellen. Finden Sie heraus, ob XAuth verwendet wird, und bestimmen Sie den erforderlichen Benutzernamen und das Kennwort.

Die VPN-Konnektivität testen

Wenn Sie die von Ihnen gerade konfigurierte VPN Verbindung testen wollen, werden die Ergebnisse des Tests in einem weiteren Fenster angezeigt.

Easy VPN Remote bearbeiten

Easy VPN-Verbindungen werden von diesem Fenster aus verwaltet. Eine Easy VPN-Verbindung ist eine Verbindung, die zwischen einem Easy VPN-Client und einem Easy VPN-Server oder -Konzentrator konfiguriert wird, um eine sichere Kommunikation mit anderen Netzwerken zu bieten, die der Server oder Konzentrator unterstützt.

In dieser Verbindungsliste werden Informationen über die konfigurierten Easy VPN Remote-Verbindungen angezeigt.

Status

Der Status der Verbindung, der durch die folgenden Symbole und Warntexte angegeben wird:

Die Verbindung ist aktiv. Wenn eine Easy VPN-Verbindung aktiv ist, können Sie die Verbindung mit der Schaltfläche **Trennen** deaktivieren, sofern die manuelle Tunnelkontrolle verwendet wird.

Die Verbindung ist nicht aktiv. Wenn eine Easy VPN-Verbindung deaktiviert ist, können Sie die Verbindung mit der Schaltfläche **Verbinden** aktivieren, sofern die manuelle Tunnelkontrolle verwendet wird.

Die Verbindung wird aufgebaut.

XAuth erforderlich – Für den Easy VPN-Server oder -Konzentrator ist eine XAuth-Anmeldung und ein Kennwort erforderlich. Klicken Sie auf die Schaltfläche **Anmeldung**, um die Anmelde-ID und das Kennwort einzugeben und die Verbindung aufzubauen.

Konfiguration geändert – Die Konfiguration für diese Verbindung wurde geändert und muss an den Router gesendet werden. Wenn die Verbindung die manuelle Tunnelsteuerung benutzt, klicken Sie auf die Taste Verbinden, um die Verbindung aufzubauen.

Name

Der Name, der für diese Easy VPN-Verbindung vergeben wurde.

Modus

Wählen Sie entweder **Client-** oder **Netzwerkerweiterung**. Im **Client-Modus** ordnet der VPN-Konzentrator oder -Server dem gesamten Datenverkehr vom Router eine einzelne IP-Adresse zu. Geräte außerhalb des LANs haben keinen direkten Zugriff auf Geräte im LAN. Im **Netzwerkerweiterungsmodus** ersetzt der VPN-Konzentrator oder -Server keine IP-Adressen und zeigt den Peers am anderen Ende der VPN-Verbindung ein vollständiges und Routing-fähiges Netzwerk.

Details

Wählen Sie eine Easy VPN-Remotesverbindung aus der Liste aus, um die Werte der folgenden Einstellungen für diese Verbindung zu sehen.

Authentifizierung

Wählen Sie digitale Zertifikate oder Gemeinsamer Schlüssel aus. Die Option Gemeinsamer Schlüssel zeigt die Benutzergruppe, die den Schlüssel teilt.

Äußere Schnittstelle

Das ist die Schnittstelle, die mit dem Easy VPN-Server oder -Konzentrator verbunden wird.

Innere Schnittstellen

Dies sind die inneren Schnittstellen, die in diese Easy VPN-Verbindung aufgenommen wurden. Alle Hosts, die mit diesen Schnittstellen verbunden sind, gehören zum VPN.

Easy VPN-Server

Die Namen oder IP-Adressen der Easy VPN-Server oder -Konzentratoren. Wenn das Cisco IOS-Abbild auf Ihrem Router Easy VPN Remote Phase III unterstützt, können Sie während der Konfiguration mit Cisco SDM zwei Easy VPN-Server oder -Konzentratoren identifizieren.

Mehrere Subnet-Unterstützung

Die Adressen der Subnetze, die nicht direkt mit dem Router verbunden sind, die aber den Tunnel benutzen dürfen. Eine ACL definiert die Subnetze, die den Tunnel benutzen dürfen.

Tunnelaktivierung

Wählen Sie automatisch, manuell oder Verkehrsabhängig aus.

Wenn die Verbindung durch die manuelle Einstellung konfiguriert wurde, müssen Sie auf die Taste **Verbinden** klicken, um den Tunnel aufzubauen. Sie können den Tunnel zu jeder Zeit starten oder anhalten, wenn Sie auf die Taste **Verbinden** oder **Trennen** klicken.

Wenn die Verbindung mit der automatischen Einstellung konfiguriert ist, wird der VPN-Tunnel automatisch aufgebaut, wenn die Easy VPN-Konfiguration an die Konfigurationsdatei des Routers übertragen wird. Die Taste **Verbinden** oder **Trennen** ist für diese Verbindung nicht aktiviert.

Wenn die Verbindung durch die Datenverkehrsabhängige Einstellung konfiguriert wurde, wird der VPN-Tunnel automatisch aufgebaut, wenn interner Datenverkehr für äußeres Routing geeignet ist. Die Schaltfläche **Verbinden** bzw. **Trennen** ist für diese Verbindung nicht aktiviert.

Backupverbindung

Eine Easy VPN-Remote Backupverbindung wurde eingerichtet. Backupverbindungen werden in der Aufgabe Cisco SDM Schnittstellen und Verbindungen konfiguriert.

XAuth Antwortmethode

Wenn XAuth aktiviert ist, zeigt der Wert einen der nachfolgenden Punkte an, auf welche Weise die XAuth Anmeldeinformationen gesendet werden:

- Sie müssen über Cisco SDM oder die Routerkonsole eingegeben werden.
- Sie müssen von einem PC-Browser eingegeben werden, wenn dieser aktiv ist.
- Die Anmeldeinformationen werden automatisch gesendet, weil sie auf dem Router abgespeichert wurden.

Die Schaltfläche Hinzufügen

Eine neue Easy VPN-Remote Verbindung hinzufügen

Schaltfläche „Bearbeiten“

Bearbeitet die festgelegte Easy VPN-Remote Verbindung.

Die Schaltfläche Löschen

Löscht die festgelegte Easy VPN-Remote Verbindung.

Taste Verbindung zurücksetzen

Klicken Sie darauf um den Inhalt zu löschen und einen Tunnel mit einem Peer wieder aufzubauen.

Taste Tunneltest

Klicken Sie darauf, um einen festgelegten VPN Tunnel zu testen. Das Ergebnis des Tests erscheint in einem anderen Fenster.

Schaltfläche Verbinden, Trennen oder Anmeldung

Diese Taste hat die Bezeichnung **Verbinden**, wenn alle nachfolgenden Punkte wahr sind:

- Die Verbindung benutzt manuelle Tunnelsteuerung
- Der Tunnel ist unterbrochen
- Die Xauth-Antwort ist *nicht* auf den Abruf durch eine PC-Browsersitzung eingestellt.

Diese Taste hat die Beschriftung Trennen, wenn alle nachfolgenden Punkte wahr sind:

- Die Verbindung benutzt manuelle Tunnelsteuerung
- Der Tunnel ist aufgebaut
- Die Xauth-Antwort ist *nicht* auf den Abruf durch eine PC-Browsersitzung eingestellt.

Diese Taste hat die Beschriftung Login beenden, wenn alle nachfolgenden Punkte wahr sind:

- Der Easy VPN-Server oder -Konzentrator wurde verbunden, um XAuth zu benutzen
- Die XAuth Antwort ist so eingestellt, dass sie von Cisco SDM oder der Routerkonsole angefordert wird.
- Der Tunnel wartet auf die XAuth Anmeldeinformationen (die Verbindung wurde initiiert)

Diese Taste ist deaktiviert, wenn die Verbindung auf automatisch oder Verkehrsabhängige Tunnelsteuerung eingestellt wurde.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Erstellen einer neuen Easy VPN-Verbindung	Klicken Sie im Fenster **Easy VPN Remote bearbeiten** auf **Hinzufügen**. Konfigurieren Sie die Verbindung im Fenster **Easy VPN Remote hinzufügen**, und klicken Sie auf **OK**. Klicken Sie in diesem Fenster anschließend auf **Verbinden**, um eine Verbindung zum Easy VPN-Server aufzubauen.
Ändern einer vorhandenen Easy VPN-Verbindung	Wählen Sie im Fenster **Easy VPN Remote bearbeiten** die Verbindung aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**. Sie sollten auch das folgende Verfahren lesen: • Wie bearbeite ich eine existierende Easy VPN-Verbindung?
Löschen einer vorhandenen Easy VPN-Verbindung	Wählen Sie im Fenster **Easy VPN Remote bearbeiten** die Verbindung, die Sie löschen möchten, und klicken Sie auf **Löschen**.
Zurücksetzen einer zwischen dem Router und einem Remote-VPN-Peer aufgebauten Verbindung Die Verbindung wird getrennt und neu aufgebaut.	Wählen Sie eine aktive Verbindung, und klicken Sie auf **Zurücksetzen**. Im angezeigten Statusfenster wird angegeben, ob das Zurücksetzen erfolgreich war.

Aufgabe	Vorgehensweise
Aufbauen einer Verbindung zu einem Easy VPN-Server, für den der Router eine konfigurierte Verbindung besitzt	Wenn die Verbindung mit der manuellen Tunnelsteuerung arbeitet, wählen Sie die Verbindung, und klicken Sie anschließend auf **Verbinden**. Verbindungen, die die automatische oder verkehrsabhängige Tunnelsteuerung verwenden, können durch Cisco SDM nicht manuell aufgebaut werden. **Hinweis** Wenn der Easy VPN-Server oder -Konzentrator für die Verwendung von XAuth konfiguriert ist, wird statt der Schaltfläche **Verbinden** die Schaltfläche **Anmeldung** angezeigt, und Sie müssen für jeden Verbindungsaufbau einen Benutzernamen und ein Kennwort eingeben. Lassen Sie sich diese Information von der Netzwerkadministration geben. Wenn der Easy VPN Remote-Server oder -Konzentrator diese Authentifizierung anfordert, müssen Sie zunächst eine SSH (Secure Shell)-Anmelde-ID und ein Kennwort für die Anmeldung beim Router und anschließend die XAuth-Anmeldung und das Kennwort für den Easy VPN-Server oder -Konzentrator angeben.
Trennen einer Verbindung zu einem Easy VPN-Server, für den der Router eine konfigurierte Verbindung besitzt	Wenn die Verbindung mit der manuellen Tunnelsteuerung arbeitet, wählen Sie Verbindung, und klicken Sie anschließend auf **Trennen**. Verbindungen, die mit der Einstellung automatische oder verkehrsabhängige Tunnelsteuerung aufgebaut wurden, können über Cisco SDM nicht manuell getrennt werden.
Ermitteln, ob eine Easy VPN-Verbindung aufgebaut wurde	Wenn eine Verbindung aufgebaut wurde, wird das Verbindungssymbol in der Statusspalte angezeigt.

Aufgabe	Vorgehensweise
Konfigurieren eines Easy VPN-Konzentrators Konfigurationsanweisungen für Easy VPN-Server und -Konzentratoren finden Sie unter www.cisco.com.	Über den folgenden Link erhalten Sie Anleitungen für die Konfiguration eines Konzentrators der Serie Cisco VPN 3000 für den Betrieb mit einem Easy VPN Remote Phase II-Client sowie anderen wichtigen Informationen. http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800a8565.html Über den folgenden Link gelangen Sie zur Dokumentation für die Serie Cisco VPN 3000. http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html
Verkehr zu meinem Easy VPN-Remote-Konzentrator durch eine Firewall zulassen.	Siehe Wie lasse ich über eine Firewall Datenverkehr zu meinem Easy VPN-Konzentrator zu?

Easy VPN Remote hinzufügen/bearbeiten

Konfigurieren Sie Ihren Router in diesem Fenster als einen Easy VPN-Client. Ihr Router muss eine Verbindung zu einem Easy VPN-Konzentrator oder -Server im Netzwerk haben.

Hinweis Dieses Fenster wird angezeigt, wenn das Cisco IOS-Abbild auf Ihrem Router Easy VPN Client Phase II unterstützt.

Mit der Easy VPN Remote-Funktion von Cisco wird das Unity-Client-Protokoll von Cisco implementiert. Mit diesem Protokoll können die meisten VPN-Parameter auf einem VPN-Server mit Remote-Zugriff definiert werden. Dieser Server kann ein dediziertes VPN-Gerät sein, z. B. ein VPN 3000-Konzentrator oder eine Cisco PIX Firewall, oder ein Cisco IOS-Router, der das Cisco Unity Client-Protokoll unterstützt.

Hinweis

- Wenn der Easy VPN-Server oder -Konzentrator für die Verwendung von XAuth konfiguriert wurde, wird für jeden Verbindungsaufbau des Routers ein Benutzername und ein Kennwort benötigt. Dies gilt auch, wenn Sie die Konfiguration an den Router senden und die Tunnelverbindung trennen und wieder neu aufbauen. Finden Sie heraus, ob XAuth verwendet wird, und bestimmen Sie den erforderlichen Benutzernamen und das Kennwort.
- Wenn der Router SSH (Secure Shell) verwendet, müssen Sie beim ersten Verbindungsaufbau die SSH-Anmeldung und das Kennwort eingeben.

Name

Geben Sie einen Namen für die Easy VPN-Remotekonfiguration ein.

Modus

Client – Wählen Sie **Client** aus, wenn die PCs und andere Geräte in den inneren Netzwerken des Routers ein privates Netzwerk mit privaten IP-Adressen bilden sollen. Es werden Network Address Translation (NAT) und Port Address Translation (PAT) verwendet. Geräte außerhalb des LANs können keine Pings an Geräte im LAN senden oder sie direkt erreichen.

Netzwerkerweiterung – Wählen Sie **Netzwerkerweiterung**, wenn Sie Geräten, die mit den inneren Schnittstellen verbunden sind, IP-Adressen zuweisen möchten, die geroutet werden können und vom Zielnetzwerk erreichbar sind. Die Geräte an beiden Enden der Verbindung bilden ein logisches Netzwerk. PAT wird automatisch deaktiviert, damit den PCs und Hosts an beiden Enden der Verbindung ein direkter Zugang ermöglicht wird.

Beraten Sie sich mit dem Administrator des Easy VPN-Servers oder -Konzentrators, bevor Sie diese Einstellung auswählen.

Tunnelsteuerung

Wählen Sie entweder **Auto** oder **Manuell**.

Bei der manuellen Einstellung müssen Sie im Fenster **Easy VPN Remote bearbeiten** auf die Schaltfläche **Verbinden** klicken, um den Tunnel aufzubauen; Sie können den Tunnel aber im Fenster für VPN-Verbindungen vollständig manuell steuern. Die Tasten Verbinden und Trennen sind aktiviert, wenn eine VPN-Verbindung mit der Einstellung Manuell Tunnelsteuerung ausgewählt wurde.

Bei der automatischen Einstellung wird der VPN-Tunnel automatisch eingerichtet, wenn die Easy VPN-Konfiguration an die Konfigurationsdatei des Routers geleitet wird. Sie können den Tunnel jedoch im Fenster **VPN-Verbindungen** nicht manuell steuern. Die Taste **Verbinden** oder **Trennen** ist deaktiviert, wenn die Easy VPN-Verbindung ausgewählt wurde.

Easy VPN-Server oder -Konzentrator

Geben Sie den Namen oder die IP-Adresse des VPN-Konzentrators oder –Servers an, zu dem der Router eine Verbindung aufbaut. Wählen Sie **IP-Adresse**, wenn Sie eine IP-Adresse angeben, oder wählen Sie **Hostname,** wenn Sie den Hostnamen des Konzentrators oder Servers angeben. Geben Sie dann den entsprechenden Wert im Feld darunter an. Wenn Sie einen Hostnamen angeben, muss sich ein DNS-Server im Netzwerk befinden, der den Hostnamen in die richtige IP-Adresse auflösen kann. Wenn Sie eine IP-Adresse eingeben, verwenden Sie das Standarddezimalformat mit Punkten, z. B. 172.16.44.1.

Gruppe

Gruppenname

Geben Sie den IPSec-Gruppennamen ein. Der Gruppenname muss mit dem Gruppennamen übereinstimmen, den Sie auf dem VPN Konzentrator oder Server definiert haben. Lassen Sie sich diese Information von der Netzwerkadministration geben.

Gruppenschlüssel

Geben Sie das IPSec-Gruppenkennwort ein. Das Gruppenkennwort muss dem Gruppenkennwort entsprechen, das auf dem VPN-Konzentrator oder -Server definiert ist. Lassen Sie sich diese Information von der Netzwerkadministration geben.

Schlüssel bestätigen

Geben Sie das Gruppenkennwort zur Bestätigung noch einmal ein.

Schnittstellen

Äußere Schnittstelle zu Server oder Konzentrator

Wählen Sie die Schnittstelle, die mit dem Easy VPN-Server oder -Konzentrator verbunden ist.

Hinweis Cisco 800-Router unterstützen nicht die Verwendung einer E 0-Schnittstelle als äußere Schnittstelle.

Innere Schnittstellen

Geben Sie die inneren Schnittstellen an, die Sie in diese Easy VPN-Konfiguration aufnehmen möchten. Alle Hosts, die mit diesen Schnittstellen verbunden sind, gehören zum VPN. Auf Routern der Serien Cisco 800 und Cisco 1700 werden bis zu drei innere Schnittstellen unterstützt.

Hinweis Eine Schnittstelle kann nicht sowohl als innere als auch als äußere Schnittstelle angegeben werden.

Easy VPN Remote hinzufügen oder bearbeiten: Easy VPN-Einstellungen

Konfigurieren Sie Ihren Router in diesem Fenster als einen Easy VPN-Client. Ihr Router muss eine Verbindung zu einem Easy VPN-Konzentrator oder -Server im Netzwerk haben.

Hinweis Dieses Fenster wird angezeigt, wenn das Cisco IOS-Abbild auf Ihrem Router Easy VPN Client Phase III unterstützt.

Mit der Easy VPN Remote-Funktion von Cisco wird das Unity-Client-Protokoll von Cisco implementiert. Mit diesem Protokoll können die meisten VPN-Parameter auf einem VPN-Server mit Remote-Zugriff definiert werden. Dieser Server kann ein dediziertes VPN-Gerät sein, z. B. ein VPN 3000-Konzentrator oder eine Cisco PIX Firewall, oder ein Cisco IOS-Router, der das Cisco Unity Client-Protokoll unterstützt.

Name

Geben Sie einen Namen für die Easy VPN-Remotekonfiguration ein.

Modus

Client – Wählen Sie **Client**, wenn die PCs und andere Geräte in den inneren Netzwerken des Routers ein privates Netzwerk mit privaten IP-Adressen bilden sollen. Es werden Network Address Translation (NAT) und Port Address Translation (PAT) verwendet. Geräte außerhalb des LANs können keine Pings an Geräte im LAN senden oder sie direkt erreichen.

Netzwerkerweiterung – Wählen Sie **Netzwerkerweiterung**, wenn Sie Geräten, die mit den inneren Schnittstellen verbunden sind, IP-Adressen zuweisen möchten, die geroutet werden können und vom Zielnetzwerk erreichbar sind. Die Geräte an beiden Enden der Verbindung bilden ein logisches Netzwerk. PAT wird automatisch deaktiviert, damit den PCs und Hosts an beiden Enden der Verbindung ein direkter Zugang ermöglicht wird.

Nehmen Sie Verbindung mit dem Easy VPN-Serveradministrator oder -Konzentrator auf, bevor Sie diese Einstellung auswählen.

Tunnelsteuerung

Wählen Sie entweder **Auto** oder **Manuell**.

Bei der Einstellung **Manuell** müssen Sie im Fenster **VPN-Verbindungen** auf die Schaltfläche **Verbinden** klicken, um den Tunnel aufzubauen; Sie können den Tunnel aber im Fenster **VPN-Verbindungen** vollständig manuell steuern. Die Tasten Verbinden und Trennen sind aktiviert, wenn eine VPN-Verbindung mit der Einstellung Manuell Tunnelsteuerung ausgewählt wurde.

Bei der automatischen Einstellung wird der VPN-Tunnel automatisch eingerichtet, wenn die Easy VPN-Konfiguration an die Konfigurationsdatei des Routers geleitet wird. Sie können den Tunnel jedoch im Fenster **VPN-Verbindungen** nicht manuell steuern. Die Taste **Verbinden** oder **Trennen** ist deaktiviert, wenn die Easy VPN-Verbindung ausgewählt wurde.

Server

Sie können bis zu zehn Easy VPN-Server nach IP-Adresse oder Hostname angeben, und Sie können die Liste ordnen, um anzugeben, mit welchen Servern der Router zuerst einen Verbindungsaufbau versuchen soll.

Hinzufügen

Klicken Sie auf diese Option, um den Namen oder die IP-Adresse eines VPN-Konzentrators oder -Servers für den Verbindungsaufbau durch den Router anzugeben. Geben Sie in das angezeigte Fenster dann die Adresse oder den Hostnamen ein.

Löschen

Klicken Sie auf diese Option, um eine bestimmte IP-Adresse oder einen bestimmten Hostnamen zu löschen.

Nach oben

Klicken Sie auf diese Option, um eine bestimmte Server-IP-Adresse oder einen bestimmten Server-Hostnamen in der Liste nach oben zu verschieben. Der Router versucht den Verbindungsaufbau mit den Servern in der Reihenfolge, in der sie in der Liste erscheinen.

Nach unten

Klicken Sie auf diese Option, um die festgelegte IP-Adresse oder den festgelegten Hostnamen in der Liste nach unten zu verschieben.

Äußere Schnittstelle zu Server oder Konzentrator

Wählen Sie die Schnittstelle, die mit dem Easy VPN-Server oder -Konzentrator verbunden ist.

Hinweis Cisco 800-Router unterstützen nicht die Verwendung einer E 0-Schnittstelle als äußere Schnittstelle.

Innere Schnittstellen

Geben Sie die inneren Schnittstellen an, die Sie in diese Easy VPN-Konfiguration aufnehmen möchten. Alle Hosts, die mit diesen Schnittstellen verbunden sind, gehören zum VPN. Auf Routern der Serien Cisco 800 und Cisco 1700 werden bis zu drei innere Schnittstellen unterstützt.

Hinweis Eine Schnittstelle kann nicht gleichzeitig als innere und äußere Schnittstelle bestimmt werden.

Easy VPN Remote hinzufügen oder bearbeiten: Authentifizierungsinformationen

Dieses Fenster wird angezeigt, wenn das Cisco IOS-Abbild auf Ihrem Router Easy VPN Client Phase III unterstützt. Wenn das Abbild Easy VPN Client Phase II unterstützt, wird ein anderes Fenster angezeigt.

Benutzen Sie dieses Fenster, um die Informationen einzugeben, die der Router benötigt, um von einem Easy VPN-Server oder -Konzentrator authentifiziert zu werden.

Geräteauthentifizierung

Gruppenname

Geben Sie den IPSec-Gruppennamen ein. Der Gruppenname muss mit dem Gruppennamen übereinstimmen, den Sie auf dem VPN Konzentrator oder Server definiert haben. Lassen Sie sich diese Information von der Netzwerkadministration geben.

Aktueller Schlüssel

In diesem Feld werden Sternchen (*) angezeigt, wenn es einen aktuellen IKE-Schlüsselwert gibt. Das Feld bleibt leer, wenn kein Schlüssel konfiguriert wurde.

Neuer Schlüssel

Geben Sie einen neuen IKE-Schlüssel in dieses Feld ein.

Schlüssel bestätigen

Geben Sie den neuen Schlüssel zur Bestätigung noch einmal ein. Wenn die Werte in den Feldern **Neuer Schlüssel** und **Schlüssel bestätigen** nicht identisch sind, fordert Sie Cisco SDM auf, die Schlüsselwerte nochmals einzugeben.

Benutzerauthentifizierung (XAuth)

Wenn der Easy VPN-Server oder -Konzentrator für die Verwendung von XAuth konfiguriert wurde, werden für jeden Verbindungsaufbau des Routers ein Benutzername und ein Kennwort benötigt. Dies gilt auch, wenn Sie die Konfiguration an den Router senden und die Tunnelverbindung trennen und dann wieder neu aufbauen. Finden Sie heraus, ob XAuth verwendet wird, und lassen Sie sich den erforderlichen Benutzernamen und das Kennwort geben.

Wenn die Benutzerauthentifizierung nicht erscheint, muss sie von der Befehlszeile der Schnittstelle des Routers eingerichtet werden.

Wählen Sie einen dieser Punkte aus, um den Xauth-Benutzernamen und das Kennwort einzugeben:

- Von einem PC

  Geben Sie den Benutzernamen und das Kennwort manuell in einen Webbrowser ein. Wenn Sie diese Option wählen, können Sie das Kästchen aktivieren, mit dem die HTTP-Authentifizierung zugelassen wird, um Webbrowser zu unterstützen, die HTML 4.0 oder JavaScript nicht unterstützen.

  Hinweis Die Option Webbrowser erscheint nur, wenn sie vom Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

- Von Ihrem Router

  Geben Sie den Benutzernamen und das Kennwort manuell über die Befehlszeile oder Cisco SDM ein.

- Automatisch durch Speichern des Benutzernamens und Kennworts auf dem Router.

Der Easy VPN-Server kann XAuth zur Authentifizierung des Routers verwenden. Wenn der Server die Option Kennwort zulässt, brauchen Sie den Benutzernamen und das Kennwort nicht jedes Mal eingeben, wenn der Easy VPN-Tunnel aufgebaut wird. Geben Sie den vom Easy VPN-Serveradministrator zur Verfügung gestellten Benutzernamen und das Kennwort ein. Geben Sie anschließend das Kennwort zur Bestätigung nochmals ein. Die Information wird in der Datei Routerinformationen gespeichert und jedes Mal benutzt, wenn der Tunnel eingerichtet wird.

Vorsicht Das Aufbewahren des XAuth Benutzernamens und Kennworts im Routerspeicher führt zu einem Sicherheitsrisiko, weil jeder, der Zugriff auf die Routerkonfiguration besitzt, diese Informationen erlangen kann. Wenn Sie die diese Informationen nicht auf dem Router speichern wollen, geben Sie diese nicht an dieser Stelle ein. Der Easy VPN-Server fordert dann einfach den Benutzernamen und das Kennwort bei jedem Verbindungsaufbau vom Router an. Außerdem kann Cisco SDM nicht selbst feststellen, ob der Easy VPN-Server die Option zum Speichern des Kennworts zulässt. Sie müssen feststellen, ob der Server diese Option zulässt. Wenn der Server Passwörter nicht speichert, sollten Sie kein Sicherheitsrisiko eingehen, indem Sie die Informationen hier eingeben.

SSH-Anmeldeinformationen eingeben

Wenn der Router-SSH (Secure Shell) verwendet, müssen Sie beim ersten Verbindungsaufbau die SSH-Anmeldung und das Kennwort eingeben. Geben Sie in diesem Fenster SSH- oder Telnet-Anmeldeinformationen ein.

Geben Sie einen gültigen Benutzernamen ein

Geben Sie den Benutzernamen für das SSH- oder Telnet-Benutzerkonto ein, mit dem Sie sich bei diesem Router anmelden.

Geben Sie ein Kennwort ein

Geben Sie das Kennwort ein, das mit dem Benutzernamen für das SSH- oder Telnet-Benutzerkonto verknüpft ist, mit dem Sie sich bei diesem Router anmelden.

Fenster XAuth-Anmeldung

Dieses Fenster wird angezeigt, wenn der Easy VPN-Server eine erweiterte Authentifizierung anfordert. Geben Sie die angeforderten Informationen ein, z. B. den Benutzernamen und das Kennwort für das Konto oder andere Informationen, um den Easy VPN-Tunnel erfolgreich aufzubauen. Wenn Sie sich nicht sicher sind, welche Informationen angegeben werden sollen, wenden Sie sich an Ihren VPN-Administrator.

Easy VPN Remote hinzufügen oder bearbeiten: Allgemeine Einstellungen

In diesem Fenster konfigurieren Sie Ihren Router als einen Easy VPN-Client. Ihr Router muss eine Verbindung zu einem Easy VPN-Konzentrator oder -Server im Netzwerk haben.

Hinweis Dieses Fenster wird angezeigt, wenn das Cisco IOS-Abbild auf Ihrem Router Easy VPN-Client Phase IV unterstützt.

Mit der Easy VPN Remote-Funktion von Cisco wird das Unity-Client-Protokoll von Cisco implementiert. Mit diesem Protokoll können die meisten VPN-Parameter auf einem VPN-Server mit Remote-Zugriff definiert werden. Dieser Server kann ein dediziertes VPN-Gerät sein, z. B. ein VPN 3000-Konzentrator oder eine Cisco PIX Firewall, oder ein Cisco IOS-Router, der das Cisco Unity Client-Protokoll unterstützt.

Name

Geben Sie einen Namen für die Easy VPN-Remotekonfiguration ein.

Server

Sie können bis zu zehn Easy VPN-Server nach IP-Adresse oder Hostname angeben, und Sie können die Liste ordnen, um anzugeben, mit welchen Servern der Router zuerst einen Verbindungsaufbau versuchen soll.

Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Namen oder die IP-Adresse eines VPN-Konzentrators oder -Servers für den Verbindungsaufbau durch den Router anzugeben. Geben Sie in das daraufhin angezeigte Fenster dann die Adresse oder den Hostnamen ein.

Klicken Sie auf die Schaltfläche **Löschen**, um die angegebene IP-Adresse oder den angegebenen Hostnamen zu löschen.

Klicken Sie auf die Taste **Nach Oben**, um die angegebene IP-Serveradresse oder den angegebenen Hostnamen in der Liste nach oben zu verschieben. Der Router versucht den Verbindungsaufbau mit den Servern in der Reihenfolge, in der sie in der Liste erscheinen.

Klicken Sie auf die Taste **Nach Unten**, um die angegebene IP-Serveradresse oder den angegebenen Hostnamen in der Liste nach unten zu verschieben.

Modus

Client – Wählen Sie den Modus **Client**, wenn die PCs und andere Geräte in den inneren Netzwerken des Routers ein privates Netzwerk mit privaten IP-Adressen bilden sollen. Es werden Network Address Translation (NAT) und Port Address Translation (PAT) verwendet. Geräte außerhalb des LANs können keine Pings an Geräte im LAN senden oder sie direkt erreichen.

Netzwerkerweiterung – Wählen Sie **Netzwerkerweiterung**, wenn Sie Geräten, die mit den inneren Schnittstellen verbunden sind, IP-Adressen zuweisen möchten, die geroutet werden können und vom Zielnetzwerk erreichbar sind. Die Geräte an beiden Enden der Verbindung bilden ein logisches Netzwerk. PAT wird automatisch deaktiviert, damit den PCs und Hosts an beiden Enden der Verbindung ein direkter Zugang ermöglicht wird.

Nehmen Sie Verbindung mit dem Easy VPN-Serveradministrator oder -Konzentrator auf, bevor Sie diese Einstellung auswählen.

Wenn Sie Network Extension auswählen, können Sie Nachfolgendes machen:

- Nicht direkt mit dem Router verbundene Subnetze dürfen den Tunnel benutzen.

  Wenn Sie zulassen möchten, dass Subnetze, die nicht direkt mit Ihrem Router verbunden sind, den Tunnel verwenden, klicken Sie auf die Schaltfläche **Optionen**, und konfigurieren Sie die Optionen für die Netzwerkerweiterung.

- Remote Management und Fehlerbehebung auf Ihrem Router aktivieren.

  Sie können die Remote-Verwaltung für den Router aktivieren, indem Sie das Kontrollkästchen aktivieren, mit dem eine vom Server zugewiesene IP-Adresse für Ihren Router angefordert wird. Diese IP-Adresse kann für die Verbindung zu Ihrem Router für das Remote Management oder die Fehlerbehebung (ping, Telnet und Secure Shell) benutzt werden. Dieser Modus lautet **Netzwerkerweiterung Plus**.

Netzwerkerweiterungsoptionen

Um den nicht direkt mit dem Router verbundenen Subnetzen die Erlaubnis zu erteilen, dass Sie den Tunnel benutzen dürfen, befolgen Sie diese Schritte:

Schritt 1 Im Fenster Optionen, aktivieren Sie das Kästchen, um mehrere Subnetze zuzulassen.

Schritt 2 Sie können zwischen der manuellen Eingabe der Subnetze oder der Auswahl einer existierenden Access Control List (ACL) auswählen.

Schritt 3 Wenn Sie die Subnetze manuell eingeben möchten, klicken Sie auf die Schaltfläche **Hinzufügen**, und geben Sie die Subnetzadresse und -maske ein. Cisco SDM generiert automatisch eine ACL.

Hinweis Die von Ihnen eingegebenen Subnetze dürfen *nicht* direkt mit dem Router verbunden sein.

Schritt 4 Um eine existierende ACL hinzuzufügen, geben Sie ihren Namen ein oder wählen sie aus der Dropdown-Liste aus.

Easy VPN Remote hinzufügen oder bearbeiten: Authentifizierungsinformationen

Benutzen Sie dieses Fenster, um die Informationen einzugeben, die der Router benötigt, um von einem Easy VPN-Server oder -Konzentrator authentifiziert zu werden.

Geräteauthentifizierung

Wählen Sie Digitale Zertifikate oder Gemeinsamer Schlüssel.

Wenn Sie einen gemeinsamen Schlüssel verwenden, erhalten Sie den IPSec-Gruppennamen und den IKE-Schlüsselwert von Ihrem Netzwerkadministrator. Der Gruppenname muss mit dem Gruppennamen übereinstimmen, den Sie auf dem VPN Konzentrator oder Server definiert haben.

Geben Sie den IPSec Gruppennamen im Feld Gruppennamen und den neuen IKE Schlüsselwert im Feld Neuer Schlüssel ein. Geben Sie den neuen Schlüssel nochmals zur Bestätigung im Feld Schlüssel bestätigen ein. Wenn die Werte in den Feldern **Neuer Schlüssel** und **Schlüssel bestätigen** nicht identisch sind, fordert Sie Cisco SDM auf, die Schlüsselwerte nochmals einzugeben.

Das Feld Aktueller Schlüssel wird ausgesternt (*) angezeigt, wenn dort ein aktueller IKE Schlüsselwert eingegeben wurde. Das Feld bleibt leer, wenn kein Schlüssel konfiguriert wurde.

Benutzerauthentifizierung

Wenn der Easy VPN-Server oder -Konzentrator für die Verwendung von XAuth konfiguriert wurde, werden für jeden Verbindungsaufbau des Routers ein Benutzername und ein Kennwort benötigt. Dies gilt auch, wenn Sie die Konfiguration an den Router senden und die Tunnelverbindung trennen und dann wieder neu aufbauen. Finden Sie heraus, ob XAuth verwendet wird, und lassen Sie sich den erforderlichen Benutzernamen und das Kennwort geben.

Wenn der Server die Speicherung des Kennworts zulässt, brauchen Sie den Benutzernamen und das Kennwort nicht jedes Mal eingeben, wenn der Easy VPN-Tunnel durch diese Option eingerichtet wird. Die Information wird in der Datei Routerinformationen gespeichert und jedes Mal benutzt, wenn der Tunnel eingerichtet wird.

Wählen Sie einen dieser Punkte aus, um den Xauth-Benutzernamen und das Kennwort einzugeben:

- Manuell in einem Webbrowser

Hinweis Die Option Webbrowser erscheint nur, wenn sie vom Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

- Manuell über die Befehlszeile oder Cisco SDM
- Automatisch durch Speichern des Benutzernamens und Kennworts auf dem Router.

  Der Easy VPN-Server kann XAuth zur Authentifizierung des Routers verwenden. Wenn der Server die Speicherung des Kennworts zulässt, brauchen Sie den Benutzernamen und das Kennwort nicht jedes Mal eingeben, wenn der Easy VPN-Tunnel durch diese Option eingerichtet wird. Geben Sie den vom Easy VPN-Serveradministrator zur Verfügung gestellten Benutzernamen und das Kennwort ein. Geben Sie anschließend das Kennwort zur Bestätigung nochmals ein.

Hinweis Das Feld Aktueller Schlüssel wird ausgesternt (*) angezeigt, wenn dort ein aktuelles Kennwort eingegeben wurde. Das Feld bleibt leer, wenn kein Kennwort konfiguriert wurde.

Die Information wird in der Datei Routerinformationen gespeichert und jedes Mal benutzt, wenn der Tunnel eingerichtet wird.

Vorsicht Das Aufbewahren des XAuth Benutzernamens und Kennworts im Routerspeicher führt zu einem Sicherheitsrisiko, weil jeder, der Zugriff auf die Routerkonfiguration besitzt, diese Informationen erlangen kann. Wenn Sie die diese Informationen nicht auf dem Router speichern wollen, geben Sie diese nicht an dieser Stelle ein. Der Easy VPN-Server fordert dann einfach den Benutzernamen und das Kennwort bei jedem Verbindungsaufbau vom Router an. Außerdem kann Cisco SDM nicht selbst feststellen, ob der Easy VPN-Server die Option zum Speichern des Kennworts zulässt. Sie müssen feststellen, ob der Server diese Option zulässt. Wenn der Server Passwörter nicht speichert, sollten Sie kein Sicherheitsrisiko eingehen, indem Sie die Informationen hier eingeben.

Easy VPN Remote hinzufügen oder bearbeiten: Schnittstellen und Verbindungen

In diesem Fenster können Sie die inneren und äußeren Schnittstellen einrichten und festlegen, wie der Tunnel aufgebaut werden soll.

Innere Schnittstellen

Wählen Sie die innere (LAN) Schnittstelle aus, um sie mit der Easy VPN-Konfiguration zu verknüpfen. Sie können mehrere innere Schnittstellen auswählen, indem Sie folgende Beschränkungen beachten:

- Wenn Sie eine Schnittstelle auswählen, die bereits in einer anderen Easy VPN-Konfiguration verwendet wird, werden Sie darüber informiert, dass eine Schnittstelle nicht zu zwei Easy VPN-Konfigurationen gehören kann.
- Wenn Sie Schnittstellen auswählen, die bereits in einer Standard-VPN Konfiguration verwendet werden, dann werden Sie darüber informiert, dass die Easy VPN-Konfiguration nicht neben der vorhandenen VPN-Konfiguration bestehen kann. Cisco SDM wird Sie fragen, ob Sie die existierenden VPN-Tunnel von diesen Schnittstellen entfernen und auf die Easy VPN-Konfiguration anwenden möchten.
- Eine existierende Schnittstelle erscheint nicht in der Liste der Schnittstellen, wenn sie nicht in einer Easy VPN-Konfiguration verwendet werden kann. So werden z. B. auf dem Router konfigurierte Loopback-Schnittstellen nicht in dieser Liste angezeigt.
- Eine Schnittstelle kann nicht gleichzeitig als innere und äußere Schnittstelle bestimmt werden.

Auf Routern der Serien Cisco 800 und Cisco 1700 werden bis zu drei innere Schnittstellen unterstützt. Im Fenster **Easy VPN Remote bearbeiten** können Sie Schnittstellen aus einer Easy VPN-Konfiguration entfernen.

Äußere Schnittstelle

Wählen Sie die äußere Schnittstelle, die mit dem Easy VPN-Server oder -Konzentrator verbunden ist

Hinweis Cisco 800 Router unterstützen nicht die Benutzung einer E 0 Schnittstelle an der äußeren Schnittstelle.

Virtuelle Tunnelschnittstelle

Aktivieren Sie diese Option, wenn Sie eine virtuelle Tunnelschnittstelle (VTI) für diese Verbindung verwenden möchten. Wenn die VTIs in der Liste von anderen VPN-Verbindungen verwendet werden, klicken Sie auf **Hinzufügen**, um eine neue zu erstellen.

Verbindungssteuerung

Wählen Sie für die VPN-Tunnelaktivierung **Automatisch**, **Manuell** oder **Interessanter Datenverkehr** aus.

Bei der manuellen Einstellung müssen Sie im Fenster **Easy VPN-Remote bearbeiten** auf die Taste **Verbinden** oder **Trennen** klicken, um den Tunnel aufzubauen oder zu trennen; dafür haben Sie jedoch die volle Kontrolle über den Tunnel und das Fenster **Easy VPN-Remote bearbeiten**. Wenn ein SA-Timeout (Security Association) für den Router eingestellt ist, müssen Sie den VPN-Tunnel bei jedem Timeout manuell neu aufbauen. Sie können SA-Timeout-Einstellungen unter im Fenster Globale VPN-Einstellungen für VPN-Komponenten ändern.

Bei der automatischen Einstellung wird der VPN-Tunnel automatisch eingerichtet, wenn die Easy VPN-Konfiguration an die Konfigurationsdatei des Routers geleitet wird. Sie können aber den Tunnel im Fenster **VPN-Verbindungen** nicht manuell kontrollieren. Die Taste **Verbinden** (bzw. **Trennen**) ist deaktiviert, wenn Sie diese Easy VPN-Verbindung auswählen.

Bei der Einstellung für interessanten, verkehrsabhängigen Datenverkehr wird der VPN-Tunnel immer eingerichtet, wenn äußerer lokaler (LAN Side) Verkehr festgestellt wird. Die Taste **Verbinden** (bzw. **Trennen**) ist deaktiviert, wenn Sie diese Easy VPN-Verbindung auswählen.

Hinweis Die Option **Interessanter Datenverkehr** wird nur angezeigt, wenn sie vom Cisco IOS-Abbild auf Ihrem Router unterstützt wird.

Wie mache ich...

In diesem Abschnitt werden Ihnen Prozesse für Aufgaben erklärt, bei denen Sie vom Assistenten keine Hilfe bekommen.

Wie bearbeite ich eine existierende Easy VPN-Verbindung?

Gehen Sie folgendermaßen vor, um eine vorhandene Easy VPN Remote-Verbindung zu bearbeiten:

Schritt 1 Wählen Sie im linken Bereich die Option **VPN**.

Schritt 2 Wählen Sie in der VPN-Baumstruktur die Option **Easy VPN Remote**.

Schritt 3 Klicken Sie auf die Registerkarte **Easy VPN Remote bearbeiten**, und wählen Sie die Verbindung aus, die Sie bearbeiten möchten.

Schritt 4 Klicken Sie auf **Bearbeiten**.

Das Fenster Easy VPN Remote bearbeiten wird angezeigt.

Schritt 5 Klicken Sie im Fenster Easy VPN-Remote bearbeiten auf die Registerkarten, um die Werte anzuzeigen, die Sie ändern möchten.

Schritt 6 Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf **OK**.

Wie konfiguriere ich ein Backup für eine Easy VPN-Verbindung?

Um ein Backup für eine Easy VPN-Verbindung zu konfigurieren, muss Ihr Router über eine ISDN-, eine asnyc- oder eine analoge Modemschnittstelle für das Backup verfügen.

Wenn die ISDN-, asynch- oder analoge Modemschnittstelle nicht konfiguriert wurde, gehen Sie folgendermaßen vor.

Schritt 1 Klicken Sie im linken Bereich auf die Registerkarte **Schnittstellen und Verbindungen**.

Schritt 2 Klicken Sie auf die Registerkarte **Verbindung erstellen**.

Schritt 3 Wählen Sie eine ISDN-, async- oder analoge Modemschnittstelle aus der Liste aus.

Schritt 4 Klicken Sie auf die Schaltfläche **Neue Verbindung erstellen**, und verwenden Sie den Assistenten, um die neue Schnittstelle zu konfigurieren.

Schritt 5 Stellen Sie im entsprechenden Fenster des Assistenten die neue Schnittstelle als Backup für eine Easy VPN Remote-Verbindung ein.

Klicken Sie auf Schnittstellen und Verbindungen auf der linken Seite des Rahmens.

Schritt 1 Klicken Sie im linken Bereich auf die Registerkarte **Schnittstellen und Verbindungen**.

Schritt 2 Klicken Sie auf die Registerkarte **Schnittstelle/Verbindung bearbeiten**.

Schritt 3 Klicken Sie auf die Taste Bearbeiten.

Schritt 4 Klicken Sie auf die Schaltfläche **Bearbeiten**.

Schritt 5 Klicken Sie auf die Registerkarte **Backup**, und konfigurieren Sie das Backup für eine Easy VPN Remote-Verbindung.

Schritt 6 Wenn Sie die Konfiguration des Backup abgeschlossen haben, klicken Sie auf **OK**.

KAPITEL 11

Easy VPN-Server

Mit der Funktion Easy VPN-Server wird Serverunterstützung für Softwareclients für Cisco VPN Client 3.x und höher und für Cisco VPN-Hardwareclients eingeführt. Diese Funktion ermöglicht einem Remote-Benutzer die Kommunikation mit einem Cisco IOS-VPN-Gateway (Virtual Private Network) unter Verwendung von IPSec (IP Security). Zentral verwaltete IPSec-Richtlinien werden vom Server auf den Client übertragen, womit für den Endbenutzer ein Minimum an Konfiguration anfällt.

Genauere Informationen finden Sie unter den folgenden Links:

http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html

Easy VPN-Server erstellen

Dieser Assistent führt Sie durch die Schritte, die erforderlich sind, um einen Easy VPN-Server auf diesem Router zu konfigurieren.

Dieser Assistent führt Sie durch die folgenden Aufgaben, damit Sie den Easy VPN-Server auf diesem Router erfolgreich konfigurieren können.

- Auswählen der Schnittstelle, auf der die Client-Verbindungen beendet werden, sowie der für den Server und die Easy VPN-Clients verwendete Authentifizierungsmethode
- Konfigurieren von IKE-Richtlinien
- Konfigurieren eines IPSec-Transformationssatzes
- Konfigurieren der Gruppenautorisierung und der Gruppenrichtlinien-Lookup-Methode

- Konfigurieren der Benutzerauthentifizierung
- Konfigurieren externer RADIUS-Server
- Konfigurieren von Richtlinien für Remote-Benutzer, die sich über Easy VPN-Clients verbinden

Easy VPN-Server erstellen

Klicken Sie auf diese Option, um eine Easy VPN-Serverkonfiguration auf Ihrem Router zu erstellen.

Schaltfläche Den Easy VPN-Server-Assistenten starten

Klicken Sie auf diese Schaltfläche, um den Assistenten zu starten.

Willkommen beim Easy VPN-Server-Assistenten

Dieses Fenster fasst die Aufgaben zusammen, die Sie bei der Verwendung des Assistenten durchführen werden.

Schnittstelle und Authentifizierung

In diesem Fenster können Sie die Schnittstelle wählen, auf der Sie den Easy VPN-Server konfigurieren möchten.

Wenn Sie eine Schnittstelle wählen, die bereits mit einer Site-to-Site IPSec-Richtlinie konfiguriert wurde, zeigt Cisco SDM eine Meldung an, dass auf dieser Schnittstelle bereits eine IPSec-Richtlinie existiert. Cisco SDM verwendet die bestehende IPSec-Richtlinie zur Konfiguration des Easy VPN-Servers.

Falls die gewählte Schnittstelle Teil einer Easy VPN-Remote-, GREoIPSec- oder DMVPN-Schnittstelle ist, zeigt Cisco SDM die Meldung, dass Sie eine andere Schnittstelle auswählen müssen.

Details

Klicken Sie auf diese Schaltfläche, um Details zu der von Ihnen gewählten Schnittstelle zu erhalten. Im Detailfenster werden die Zugriffsregeln, IPSec-Richtlinien, NAT-Regeln und Prüfregeln angezeigt, die mit der Schnittstelle verknüpft sind.

Diese Schaltfläche erscheint ausgeblendet, wenn keine Schnittstelle ausgewählt wurde.

Authentifizierung

Wählen Sie gemeinsame Schlüssel, digitale Zertifikate oder beides.

Wenn Sie gemeinsame Schlüssel verwenden, müssen Sie bei der Konfiguration des allgemeinen Setup-Fensters Gruppenrichtlinie hinzufügen einen Schlüsselwert eingeben.

Wenn Sie digitale Zertifikate wählen, erscheint das Feld Gemeinsame Schlüssel nicht im allgemeinen Setup-Fenster Gruppenrichtlinie hinzufügen.

Wenn Sie gemeinsame Schlüssel und digitale Zertifikate wählen, können Sie im allgemeinen Setup-Fenster Gruppenrichtlinie hinzufügen einen Wert eingeben oder auch nicht.

Gruppenautorisierung und Gruppenrichtlinien-Lookup

In diesem Fenster können Sie für die AAA-Autorisierung eine neue Netzwerkmethodenliste für Gruppenrichtlinien-Lookup definieren oder eine vorhandene Netzwerkmethodenliste auswählen.

Nur Lokal

Mit dieser Option können Sie eine Methodenliste nur für die lokale Datenbank erstellen.

Nur RADIUS

Mit dieser Option können Sie eine Methodenliste für eine RADIUS-Datenbank erstellen.

Nur RADIUS und Lokal

Mit dieser Option können Sie eine Methodenliste für eine RADIUS- und eine lokale Datenbank erstellen.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Definieren einer AAA-Methodenliste für RADIUS und die lokale Datenbank Wenn Sie sowohl für RADIUS als auch für die lokale Datenbank Methodenlisten definieren, fragt der Router für die Gruppenauthentifizierung zunächst den RADIUS-Server und dann die lokale Datenbank ab.	Wählen Sie **Nur RADIUS und Lokal**. Klicken Sie dann auf **Weiter**.
Definieren einer AAA-Methodenliste nur für die lokale Datenbank Wenn Sie eine AAA-Methodenliste für die lokale Datenbank definieren, fragt der Router für die Gruppenauthentifizierung die lokale Datenbank ab.	Wählen Sie **Nur Lokal**. Klicken Sie dann auf **Weiter**.
Wählen Sie eine der vorhandenen Methodenlisten für die Gruppenauthentifizierung aus. Wenn Sie AAA-Methodenlisten definieren möchten, könnte auch die Auswahl einer bereits vorhandenen Methodenliste für Sie in Betracht kommen.	Wählen Sie **Vorhandene AAA-Methodenliste auswählen**. Klicken Sie dann auf **Weiter**.

Benutzerauthentifizierung (XAuth)

Sie können die Benutzerauthentifizierung auf einem Easy VPN-Server konfigurieren. Details zur Benutzerauthentifizierung können Sie auf einem externen Server, z. B. einem RADIUS-Server, in einer lokalen Datenbank oder sowohl auf einem Server als auch in einer Datenbank speichern. Eine Methodenliste für die AAA-Anmeldungsauthentifizierung wird verwendet, um zu entscheiden, welche Benutzerauthentifizierungsdetails durchsucht werden soll.

Nur Lokal

Mit dieser Option können Sie Details zur Benutzerauthentifizierung nur für die lokale Datenbank hinzufügen.

Nur RADIUS und Lokal

Mit dieser Option können Sie Details zur Benutzerauthentifizierung für RADIUS und die lokale Datenbank hinzufügen.

Vorhandene AAA-Methodenliste auswählen

Mit dieser Option können Sie eine Methodenliste aus einem Verzeichnis aller Methodenlisten auswählen, die auf dem Router konfiguriert sind.

Die gewählte Methodenliste wird zur erweiterten Authentifizierung verwendet.

Die Schaltfläche Benutzer-Anmeldeinformationen hinzufügen

Klicken Sie auf diese Schaltfläche, um ein Benutzerkonto hinzuzufügen.

Benutzerkonten für XAuth

Fügen Sie ein Konto für einen Benutzer hinzu, den Sie authentifizieren möchten, nachdem das Gerät durch IKE authentifiziert wurde.

Benutzerkonten

In diesem Feld sind die Benutzerkonten aufgeführt, die XAuth authentifiziert. Angezeigt werden der Kontoname und die Berechtigungsstufe.

Schaltflächen Hinzufügen und Bearbeiten

Verwenden Sie diese Schaltflächen, um Benutzerkonten hinzuzufügen und zu bearbeiten. Benutzerkonten können im Fenster **Zusätzliche Aufgaben > Routerzugriff > Benutzerkonten/Ansicht** gelöscht werden.

Hinweis Vorhandene CLI-Ansicht-Benutzerkonten können über dieses Fenster nicht bearbeitet werden. Wenn Sie Benutzerkonten bearbeiten müssen, wechseln Sie zu **Zusätzliche Aufgaben > Routerzugriff > Benutzerkonto/CLI-Ansicht**.

RADIUS-Server hinzufügen

In diesem Fenster können Sie einen neuen RADIUS-Server hinzufügen oder einen bereits bestehenden RADIUS-Server bearbeiten oder pingen.

Hinzufügen

Einen neuen RADIUS-Server hinzufügen.

Bearbeiten

Die Konfiguration eines bestehenden RADIUS-Servers bearbeiten.

Ping

Die Konfiguration eines bestehenden oder eines neu konfigurierten RADIUS-Servers pingen.

Gruppenautorisierung: Benutzergruppenrichtlinien

In diesem Fenster können Sie Benutzergruppenrichtlinien zur lokalen Datenbank hinzufügen, darin bearbeiten oder duplizieren oder daraus löschen.

Es sind bereits konfigurierte Gruppenrichtlinien aufgelistet.

Gruppenname

Der Name, der für die Benutzergruppe vergeben wurde.

Pool

Der Name des IP-Adressenpools, aus dem eine IP_Adresse einem Benutzer zugeordnet wird, der sich von dieser Gruppe aus anschließt.

DNS

Domänennamensystem (DNS)-Adresse der Gruppe.

Diese DNS-Adresse wird zu den Benutzern, die sich dieser Gruppe anschließen, ge-pusht.

WINS

Windows Internet Naming Service (WINS)-Adresse der Gruppe.

Diese WINS-Adresse wird zu den Benutzern, die sich dieser Gruppe anschließen, ge-pusht.

Domainname

Der Domänenname der Gruppe.

Dieser Domänenname wird zu den Benutzern, die sich dieser Gruppe anschließen, ge-pusht.

ACL teilen

Die Zugriffssteuerungsliste (ACL), die geschützte Sub-Netze für Split-Tunneling-Verfahren darstellt.

Ruhestand-Timer

Easy VPN-Server laufen wirtschaftlicher, wenn im Ruhestand befindliche VPN-Tunnels abgeschaltet werden und ungenutzte Ressourcen zurückgerufen werden.

Klicken Sie auf das Kontrollkästchen zum Konfigurieren des Leerlauf-Timers, und geben Sie einen Wert für die maximale Zeitspanne an, die ein VPN-Tunnel ungenutzt bleibt, bevor er getrennt wird. Geben Sie im linken Feld die Stunden ein, die Minuten im mittleren Feld und rechts die Sekunden. Die zulässige Mindestzeitspanne ist 1 Minute.

Allgemeine Gruppeninformationen

In diesem Fenster können Sie Gruppenrichtlinien konfigurieren, bearbeiten und duplizieren.

Bitte geben Sie einen Namen für diese Gruppe ein

Geben Sie den Gruppennamen in das angezeigte Feld ein. Wenn diese Gruppenrichtlinie bearbeitet wird, ist dieses Feld deaktiviert. Wenn Sie eine Gruppenrichtlinie duplizieren, müssen Sie einen neuen Wert in dieses Feld eingeben.

Gemeinsamer Schlüssel

Geben Sie den gemeinsamen Schlüssel in das angezeigte Feld ein.

Das Feld **aktueller Schlüssel** kann nicht geändert werden.

Hinweis Sie brauchen keinen gemeinsamen Schlüssel eingeben, wenn Sie digitale Zertifikate zur Gruppenauthentifizierung verwenden. Digitale Zertifikate werden auch zur Benutzerauthentifizierung verwendet.

Pool-Informationen

Gibt einen lokalen Pool von IP-Adressen an, die für die Zuordnung von IP-Adressen zu Clients verwendet werden.

Neuen Pool erstellen

Geben Sie im Feld IP-Adressenbereich den Bereich der IP-Adressen für den lokalen IP-Adressen-Pool ein.

Aus einem existierenden Pool auswählen

Wählen Sie den IP-Adressenbereich aus dem existierenden Pool mit IP-Adressen aus.

Hinweis Dieses Feld kann nicht bearbeitet werden, wenn es keine vordefinierten IP-Adressenpools gibt.

Subnetzmaske (Optional)

Geben Sie eine Subnetmaske ein, die mit der IP-Adress zu den zugeordneten Clients dieser Gruppe gesendet wird.

Maximal zulässige Verbindungen

Geben Sie die maximale Anzahl der Client-Verbindungen von dieser Gruppe zum Easy VPN-Server an.

Cisco SDM unterstützt maximal 5000 Verbindungen pro Gruppe.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Authentifizieren der mit der Gruppe verknüpften Clients	Geben Sie den Schlüssel in das Feld **Gemeinsamer Schlüssel** ein.
Erstellen Sie einen lokalen IP-Adressenpool, der den Clients zugeordnet wird.	Geben Sie im Bereich Pool-Informationen im Feld Neuen Pool erstellen den IP-Adressenbereich ein.
Auswählen eines Bereichs mit IP-Adressen aus dem existierenden Pool für die Zuordnung zu den Clients.	Wählen Sie den IP-Adressenbereich aus dem Feld **Aus einem existierenden Pool auswählen** im Bereich **Pool-Informationen** aus.

DNS und WINS Konfiguration

In diesem Fenster können Sie die Informationen des Domain Name Service (DNS) und des Windows Internet Naming Service (WINS) angeben.

DNS

Geben Sie die primäre und sekundäre IP-Adresse des DNS-Servers in die bereitgestellten Felder ein. Ob Sie eine sekundäre DNS-Serveradresse eingeben, ist optional.

WINS

Geben Sie die primäre und sekundäre IP-Adresse des WINS-Servers in die bereitgestellten Felder ein. Ob Sie eine sekundäre WINS-Serveradresse eingeben, ist optional.

Domainname

Geben Sie den Domänennamen an, der an den Easy VPN-Client übertragen werden soll.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Konfigurieren eines DNS-Servers.	Aktivieren Sie die Option **DNS**. Geben Sie anschließend die primären und sekundären IP-Adressen des DNS-Servers in die bereitgestellten Felder ein.
Konfigurieren eines WINS-Servers.	Aktivieren Sie die Option **WINS**. Geben Sie die primären und sekundären IP-Adressen des WINS-Servers in die bereitgestellten Felder ein.
Angeben eines Namens, der an den Easy VPN-Client übertragen werden soll	Geben Sie in das Feld **Domänenname** den Domänennamen ein.

Split-Tunneling

In diesem Fenster können Sie Split-Tunneling für die Benutzergruppe aktivieren, die Sie hinzufügen.

Split-Tunneling bezeichnet die Möglichkeit, über einen sicheren Tunnel zum zentralen Standort und gleichzeitig über Klartexttunnel zum Internet zu verfügen. Der gesamte Datenverkehr vom Client wird beispielsweise durch den VPN-Tunnel zum Ziel-Subnetz gesendet.

Sie können auch angeben, welche Gruppen von ACLs für das Split-Tunneling geschützte Subnetze darstellen.

Split-Tunneling aktivieren

Dieses Feld ermöglicht Ihnen das Hinzufügen von geschützten Subnetzen und ACLs für das Split-Tunneling.

Geschützte Subnetze eingeben

Sie können Subnetze hinzufügen oder entfernen, für die Pakete von den VPN-Clients ge-tunnelt werden.

Split-Tunneling-ACL auswählen

Wählen Sie die ACL aus, die für das Split-Tunneling verwendet werden soll.

Split DNS

Geben Sie die Internet-Domänennamen ein, die von Ihrem Netzwerk-DNS-Server aufgelöst werden sollen. Es gelten folgende Beschränkungen:

- Es sind maximal 10 Einträge erlaubt.
- Die Einträge müssen mit Kommas unterteilt werden.
- Verwenden Sie keine Leerstellen in der Eintragsliste.
- Doppelte Einträge oder Einträge mit ungültigen Formaten werden nicht akzeptiert.

Hinweis Diese Funktion erscheint nur, wenn sie von der IOS-Ausgabe Ihres Cisco-Servers unterstützt wird.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Aktivieren von Split-Tunneling	Aktivieren Sie die Option **Split-Tunneling aktivieren**.
Hinzufügen eines geschützten Subnetzes.	Wählen Sie **Geschützte Subnetze eingeben**, und klicken Sie dann auf **Hinzufügen**.
Löschen eines geschützten Subnetzes.	Wählen Sie **Geschützte Subnetze eingeben**, und klicken Sie dann auf **Löschen**.

Aufgabe	Vorgehensweise
Auswählen der ACL, die für das Split-Tunneling verwendet werden soll.	Wählen Sie **Split-Tunneling-ACL auswählen** und anschließend die ACL aus den verfügbaren Optionen aus.
Verwenden Sie den DNS-Server Ihres Netzwerks zum Auflösen bestimmter Domänennamen.	Aktivieren Sie die Option **Split-Tunneling aktivieren**, und geben Sie die Domänennamen in das dafür vorgesehene Feld ein. Sie müssen auch Subnetze einrichten oder eine ACL wählen.

Clienteinstellungen

In diesem Fenster können Sie zusätzliche Eigenschaften für die Sicherheitsrichtlinien konfigurieren, z.B. einen Backup-Server, Firewall-Are-U-There und Include-Local-LAN (lokales LAN einschließen) hinzufügen oder löschen.

Hinweis Manche der nachstehend beschriebenen Funktionen erscheinen nur, wenn sie von der IOS-Ausgabe Ihres Cisco-Servers unterstützt werden.

Backup-Server

Sie können bis zu zehn Server mit IP-Adresse oder Hostname als Backup für den Easy VPN-Server angeben und die Liste sortieren, um zu kontrollieren, mit welchen Servern der Router zuerst einen Verbindungsaufbau versuchen soll, wenn die primäre Verbindung zum Easy VPN-Server fehlschlägt.

Hinzufügen

Klicken Sie auf diese Option, um den Namen oder die IP-Adresse eines Easy VPN-Servers anzugeben, mit dem der Router eine Verbindung aufbaut, wenn die primäre Verbindung fehlschlägt. Geben Sie in das daraufhin angezeigte Fenster die Adresse oder den Hostnamen ein.

Löschen

Klicken Sie auf diese Option, um eine bestimmte IP-Adresse oder einen bestimmten Hostnamen zu löschen.

Konfigurationsübertragung

Sie können eine Easy VPN-Client Konfigurationsdatei mit einer URL und Versionsnummer angeben. Der Easy VPN-Server sendet die URL und Versionsnummer zu den Easy VPN-Hardware-Clients, die diese Information anfordern. Nur Easy VPN-Hardware-Clients, die zu der Gruppenrichtlinie gehören, die Sie konfigurieren, können die URL und Versionsnummer anfordern, die sie in diesem Fenster eingeben.

Geben Sie die URL der Konfigurationsdatei im URL-Feld ein. Die URL sollte mit einem entsprechenden Protokoll beginnen und kann Benutzernamen und Passwörter enthalten. Im Folgenden finden Sie URL-Beispiele zum Downloaden einer Aktualisierungsdatei sdm.exe:

- http://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- https://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- ftp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- tftp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- scp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- rcp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/sdm.exe
- cns:
- xmodem:
- ymodem:
- null:
- flash:sdm.exe
- nvram:sdm.exe
- usbtoken[0-9]:sdm.exe

  Der Bereich für die USB-Token-Portnummer ist 0-9. So ist die URL für einen USB-Token, der an USB-Port 0 angeschlossen ist, beispielsweise **usbtoken0:sdm.exe**.

- usbflash[0-9]:sdm.exe

  Der Bereich für die USB-Flash-Portnummer ist 0-9. So lautet die URL für ein USB-Flash, das an USB-Port 0 angeschlossen ist, beispielsweise **usbflash0:sdm.exe**.

- disk[0-1]:sdm.exe

  Die Disk-Nummer ist 0 oder 1. So lautet die URL für Disk Nummer 0 zum Beispiel **disk0:sdm.exe**.

- archive:sdm.exe
- tar:sdm.exe
- system:sdm.exe

In diesen Beispielen ist *Benutzername* der Benutzername und *Kennwort* das Kennwort des Standorts.

Geben Sie die Versionsnummer der Datei im Versionsfeld ein. Die Versionsnummer muss sich in einem Bereich von 1 bis 32767 befinden.

Browser Proxy

Sie können die Brower Proxy-Einstellungen für Easy VPN-Software-Clients angeben. Der Easy VPN-Server sendet die Browser-Proxy-Einstellungen zu den Easy VPN-Softwareclients, die diese Information anfordern. Nur Easy VPN-Softwareclients, die zu der Gruppenrichtlinie gehören, die Sie konfigurieren, können die Browser Proxy-Einstellungen anfordern, die Sie in diesem Fenster eingeben.

Geben Sie den Namen ein, unter dem die Browser Proxy-Einstellungen gespeichert wurden oder wählen Sie folgendes aus dem Dropdown-Menü:

- Wählen Sie eine bestehende Einstellung…

  Öffnet ein Fenster mit einer Liste existierender Browser Proxy-Einstellungen.

- Erstellen Sie eine neue Einstellung und wählen Sie...

  Öffnet ein Fenster, in dem Sie neue Browser Proxy-Einstellungen erstellen können.

- Keine

  Löscht alle Browser Proxy-Einstellungen, die der Gruppe zugeordnet sind.

Firewall-Are-U-There

Sie können VPN-Verbindungen auf Clients beschränken, die Black Ice oder Zone Alarm Personal Firewalls ausführen.

Include Local LAN (lokales LAN einschließen)

Sie können zulassen, dass eine Verbindung, die keine Split-Tunneling-Verbindung ist, zur gleichen Zeit wie der Client auf das lokale Subnetzwerk zugreift.

Perfect Forward Secrecy (PFS)

Aktivieren Sie PFS, wenn dies von der IPSec-Sicherheitsverbindung gefordert wird, die Sie verwenden.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen eines Sicherungsservers	Klicken Sie im Bereich **Sicherungsserver** auf **Hinzufügen**. Fügen Sie im daraufhin angezeigten Fenster die IP-Adresse oder den Hostnamen des Sicherungsservers hinzu.
Löschen eines Sicherungsservers	Wählen Sie im Bereich **Sicherungsserver** den zu löschenden Sicherungsserver aus, und klicken Sie auf **Löschen**.
Ändern der Reihenfolge der Sicherungsserver	Löschen Sie Backup-Server und erstellen Sie sie neu in der gewünschten Reihenfolge.
Aktivieren Sie Firewall-Are-U-There.	Aktivieren Sie die Option **Firewall-Are-U-There**.
Aktivieren Sie **Include Local LAN** (lokales LAN einschließen).	Aktivieren Sie die Option **Include-Local-LAN** (Lokales LAN einschließen).
Geben Sie die maximale Anzahl der zulässigen Client-Verbindungen für die Gruppe ein, die Sie erstellen.	Geben Sie die Anzahl in das Feld **In dieser Gruppe zugelassene maximale Anzahl von Verbindungen** ein.

Wählen Sie die Browser Proxy-Einstellungen

Wählen Sie aus der Dropdown-Liste die Browser Proxy-Einstellungen, die Sie mit der Gruppe verbinden möchten.

Hinweis Um neue Einstellungen hinzuzufügen, wählen Sie im Fenster **Client-Einstellungen** aus dem Dropdown-Menü der Browser-Einstellungen die Option **Browsereinstellungen hinzufügen**, oder wechseln Sie zu **VPN-Komponenten > Easy VPN-Server > Browser Proxy-Einstellungen**, und klicken Sie auf **Hinzufügen**. Um Einstellungen zu löschen, wechseln Sie zu **VPN-Komponenten > Easy VPN-Server > Browser Proxy-Einstellungen**, und klicken Sie auf **Löschen**.

Browser Proxy-Einstellungen hinzufügen oder bearbeiten

In diesem Fenster können Sie Browser Proxy-Einstellungen hinzufügen oder bearbeiten.

Name der Browser Proxy-Einstellung

Wenn Sie Browser Proxy-Einstellungen hinzufügen, geben sie einen Namen ein, der auf der Dropdown-Menüliste der Browser Proxy-Einstellungen erscheint. Wenn Sie Browser Proxy-Einstellungen bearbeiten, ist das Feld schreibgeschützt.

Proxy-Einstellungen

Wählen Sie eine der folgenden Möglichkeiten:

- Kein Proxy-Server

  Sie möchten *nicht*, dass die Clients in dieser Gruppe einen Proxy-Server einsetzen, wenn sie den VPN-Tunnel verwenden.

- Einstellung automatisch erfassen

  Sie möchten, dass die Clients in dieser Gruppe einen Proxy-Server automatisch erkennen, wenn sie den VPN-Tunnel verwenden.

- Manuelle Proxy-Konfiguration

  Sie möchten den Proxy-Server für die Clients dieser Gruppe manuell konfigurieren.

Falls Sie die manuelle Proxy-Konfiguration wählen, befolgen Sie diese Schritte, um den Proxy-Server manuell zu konfigurieren:

Schritt 1 Geben Sie in das Feld Proxy-Server IP-Adresse die Server IP-Adresse ein.

Schritt 2 Geben Sie im Feld Port die Portnummer ein, die der Proxy-Server zum Empfangen der Proxy-Anforderungen verwendet.

Schritt 3 Geben Sie eine Liste der IP-Adressen ein, für die Clients *keine* Proxy-Server verwenden sollen.

Separieren Sie die Adressen mit Kommas und geben Sie keine Leerstellen ein.

Schritt 4 Wenn Sie verhindern möchten, dass Clients den Proxy-Server für lokale (LAN) Adressen verwenden, aktivieren Sie das Kontrollkästchen **Proxy-Server für lokale Adressen übergehen**.

Schritt 5 Klicken Sie auf **OK**, um die Browser Proxy-Einstellungen zu speichern.

Benutzerauthentifizierung (XAuth)

Auf diese Weise können Sie zusätzliche Eigenschaften für die Benutzerauthentifizierung konfigurieren, z.B. Gruppensperren und Kennwort speichern Eigenschaften.

XAuth Banner

Geben Sie den Text für ein Banner ein, das die Benutzer bei Xauth-Anforderungen sehen.

Hinweis Diese Funktion erscheint nur, wenn sie von der IOS-Ausgabe Ihres Cisco-Servers unterstützt wird.

Maximal zulässige Anmeldungen pro Benutzer:

Geben Sie die maximale Anzahl der Verbindungen an, die ein Benutzer gleichzeitig aufbauen darf. Cisco SDM unterstützt maximal zehn Anmeldungen pro Benutzer.

Gruppensperre

Sie können einen Client so einschränken, dass er nur von der angegebenen Benutzergruppe zum Easy VPN-Server verbinden kann.

Kennwort speichern

Sie können den Benutzernamen und das Kennwort für die erweiterte Authentifizierung lokal auf Ihrem Easy VPN-Client speichern.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Beschränken von Benutzerverbindungen auf die angegebene Benutzergruppe	Aktivieren Sie die Option **Gruppensperre aktivieren**.
Speichern von Benutzernamen und Kennwort	Aktivieren Sie die Option **Kennwort speichern aktivieren**.
Geben Sie die maximale Anzahl der Verbindungen an, die ein Benutzer gleichzeitig zum Easy VPN-Server haben darf.	Geben Sie die Anzahl in das Feld **Maximal zulässige Anmeldungen pro Benutzer** ein.

Clientaktualisierung

In diesem Fenster können Sie die Aktualisierungsmeldungen der Client-Software oder –Firmware einstellen und die bestehenden Client-Aktualisierungseinträge einsehen. Sie können bestehende Client-Aktualisierungseinträge zur Bearbeitung und zum Löschen auswählen.

Nachdem eine neue oder bearbeitete Client-Aktualisierung gespeichert wurde, werden automatisch Benachrichtigungen an die Clients gesendet. Clients, die bereits verbunden sind, müssen manuell benachrichtigt werden. Um eine manuelle IKE-Benachrichtigung über die Verfügbarkeit einer Aktualisierung zu senden, wählen Sie im Fenster **Gruppenrichtlinien** eine Gruppenrichtlinie aus, und klicken Sie auf die Schaltfläche **Aktualisierung senden**. Die Gruppen-Clients, welche die Kriterien für die Aktualisierung erfüllen, erhalten eine Benachrichtigung.

Hinweis Das Fenster Client-Aktualisierung ist nur verfügbar, wenn es von der IOS-Ausgabe Ihres Cisco-Servers unterstützt wird.

Spalte Client-Art

Zeigt die Art des Clients, für den die Revision gedacht ist.

Revisions-Spalte

Zeigt, welche Revisionen verfügbar sind.

URL-Spalte

Gibt den Speicherort der Revisionen an.

Die Schaltfläche Hinzufügen

Klicken Sie diese an, wenn Sie einen neuen Client-Aktualisierungseintrag konfigurieren möchten.

Schaltfläche „Bearbeiten“

Klicken Sie auf diese Schaltfläche, wenn Sie den angegebenen Client-Aktualisierungseintrag bearbeiten möchten.

Die Schaltfläche Löschen

Klicken Sie auf diese Schaltfläche, wenn Sie den angegebenen Client-Aktualisierungseintrag löschen möchten.

Den Client-Aktualisierungseintrag hinzufügen oder bearbeiten

In diesem Fenster können Sie einen neuen Client-Aktualisierungseintrag konfigurieren.

Clienttyp

Geben Sie eine Client-Art ein oder wählen Sie eine aus dem Dropdown-Menü aus. Für Client-Artnamen muss die Groß-/Kleinschreibung berücksichtigt werden.

Für Software-Clients ist der Client-Typ normalerweise das Betriebssystem, z. B. *Windows*. Für Hardware-Clients ist der Client-Typ normalerweise die Modellnummer, z. B. *vpn3002*.

Wenn Sie den Client-Aktualisierungseintrag bearbeiten, ist die Client-Art schreibgeschützt.

URL

Geben Sie die URL ein, die zur neuesten Software- oder Firmware-Revision führt. Die URL sollte mit einem entsprechenden Protokoll beginnen und kann Benutzernamen und Passwörter enthalten.

Im Folgenden finden Sie URL-Beispiele zum Downloaden einer Aktualisierungsdatei vpnclient-4-6.exe:

- http://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- https://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- ftp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- tftp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- scp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- rcp://*Benutzername*:*Kennwort*@www.cisco.com/go/vpn/vpnclient-4.6.exe
- cns:
- xmodem:
- ymodem:
- null:
- flash:vpnclient-4.6.exe
- nvram:vpnclient-4.6.exe
- usbtoken[0-9]:vpnclient-4.6.exe

  Der Bereich für die USB-Token-Portnummer ist 0-9. So lautet die URL für einen USB-Token, der an USB-Port 0 angeschlossen ist, beispielsweise **usbtoken0:vpnclient-4.6.exe**.
- usbflash[0-9]:vpnclient-4.6.exe

  Der Bereich für die USB-Flash-Portnummer ist 0-9. So lautet die URL für ein USB-Flash, das an USB-Port 0 angeschlossen ist, beispielsweise **usbflash0:vpnclient-4.6.exe**.
- disk[0-1]:vpnclient-4.6.exe

  Die Disk-Nummer ist 0 oder 1. So lautet die URL für Disk Nummer 0 zum Beispiel **disk0:vpnclient-4.6.exe**.

- archive:vpnclient-4.6.exe
- tar:vpnclient-4.6.exe
- system:vpnclient-4.6.exe

In diesen Beispielen ist *Benutzername* der Benutzername und *Kennwort* das Kennwort des Standorts.

Revisionen

Geben Sie die Revisionsnummer der neuesten Aktualisierung ein. Sie können mehrere Versionsnummern eingeben und durch Kommata voneinander abtrennen, zum Beispiel *4.3,4.4,4.5*. Sie dürfen keine Leerzeichen verwenden.

Übersicht

In diesem Fenster wird die von Ihnen erstellte Easy VPN-Serverkonfiguration angezeigt, und Sie können die Konfiguration speichern. Sie können die Konfiguration in diesem Fenster überprüfen und auf die Schaltfläche **Zurück** klicken, um Elemente zu ändern.

Wenn Sie auf **Beenden** klicken, werden die Informationen in die aktive Konfiguration des Routers geschrieben. Wenn der Tunnel für automatischen Modus konfiguriert wurde, versucht der Router zusätzlich, den VPN-Konzentrator oder -Server zu kontaktieren.

Wenn Sie die Easy VPN-Serverkonfiguration zu einem späteren Zeitpunkt ändern möchten, können Sie die Änderungen im Bereich Den Easy VPN-Server hinzufügen oder bearbeiten vornehmen.

Wenn Sie diese Konfiguration in der aktiven Routerkonfiguration speichern und diesen Assistenten schließen möchten, klicken Sie auf **Fertig stellen**. Die Änderungen treten sofort in Kraft.

Testen der VPN-Konnektivität nach der Konfiguration

Klicken Sie zum Testen der VPN-Verbindung, die Sie gerade konfiguriert haben. Die Testergebnisse werden in einem separaten Fenster angezeigt.

Browser Proxy-Einstellungen

In diesem Fenster werden die Browser Proxy-Einstellungen aufgeführt, in denen Sie die Konfigurationen sehen können. Sie können Browser Proxy-Einstellungen hinzufügen, bearbeiten oder löschen. Verwenden Sie die Konfiguration der Gruppenrichtlinien, um die Browser Proxy-Einstellungen den Clientgruppen zuzuordnen.

Name

Der Name der BrowserProxy-Einstellungen.

Einstellungen

Zeigt eine der folgenden Möglichkeiten an:

- Kein Proxy-Server

  Kein Proxy-Server kann von Clients verwendet werden, wenn Sie über den VPN-Tunnel verbinden.

- Einstellung automatisch erfassen

  Clients versuchen, einen Proxy-Server automatisch zu erkennen.

- Manuelle Proxy-Konfiguration

  Die Einstellungen werden manuell konfiguriert.

Serverdetails

Zeigt die verwendete IP-Adresse des Proxy-Servers und die Portnummer an.

Lokale Adressen übergehen

Wenn eingestellt, verhindert dies, dass Clients den Proxy-Server für lokale (LAN) Adressen verwenden.

Ausnahmeliste

Eine Liste der IP-Adressen, für die Clients *keine* Proxy-Server verwenden sollen.

Die Schaltfläche Hinzufügen

Neue Browser Proxy-Einstellungen konfigurieren.

Schaltfläche „Bearbeiten“

Die angegebenen Browser Proxy-Einstellungen bearbeiten.

Die Schaltfläche Löschen

Löscht die angegebenen Browser Proxy-Einstellungen. Browser Proxy-Einstellungen, die mit einer oder mehr Gruppenrichtlinien verbunden sind, können *nicht* gelöscht werden, bevor diese Verbindungen gelöscht wurden.

Den Easy VPN-Server hinzufügen oder bearbeiten

In diesem Fenster können Sie die Easy VPN-Serververbindungen ansehen und verwalten.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um einen neuen Easy VPN-Server hinzuzufügen.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um eine vorhandene Easy VPN-Serverkonfiguration zu bearbeiten.

Löschen

Klicken Sie auf **Löschen**, um eine angegebene Konfiguration zu löschen.

Spalte „Name“

Der Name der IPSec-Richtlinie, die mit dieser Verbindung verknüpft ist.

Spalte Schnittstelle

Der Name der Schnittstelle, die für diese Verbindung verwendet wird.

Spalte Gruppenautorisierung

Der Name der Methodenliste, die für Gruppenrichtlinien-Lookup verwendet wird.

Spalte Benutzerauthentifizierung

Der Name der Methodenliste, die für Benutzerauthentifizierungs-Lookup verwendet wird.

Moduskonfiguration

Zeigt eine der folgenden Möglichkeiten an:

- Einleiten

  Der Router ist konfiguriert, um Verbindungen mit den Easy VPN-Remote-Clients aufzubauen.

- Antworten

  Der Router ist konfiguriert, um auf Anforderungen von den Easy VPN-Remote-Clients zu warten, bevor er eine Verbindung aufbaut.

Schaltfläche „VPN-Server testen“

Klicken Sie zum Testen des gewählten VPN-Tunnels. Die Testergebnisse werden in einem separaten Fenster angezeigt.

Schaltfläche beschränkter Zugriff

Klicken Sie auf diese Schaltfläche, um Gruppenzugriff auf die angegebene Easy VPN-Serververbindung zu beschränken.

Diese Schaltfläche ist nur aktiv, wenn die folgenden beiden Voraussetzungen erfüllt sind:

- Mehr als eine Easy VPN-Serververbindung verwendet die lokale Datenbank zur Benutzerauthentifizierung.
- Es ist mindestens eine lokale Gruppenrichtlinie konfiguriert.

Easy VPN-Serververbindung hinzufügen/bearbeiten

In diesem Fenster können Sie die Easy VPN-Serververbindungen hinzufügen oder bearbeiten.

Wählen Sie eine Schnittstelle aus

Wenn Sie eine Verbindung hinzufügen, wählen Sie die zu verwendende Schnittstelle aus dieser Liste aus. Wenn Sie die Verbindung bearbeiten, ist diese Liste deaktiviert.

IPSec-Richtlinie auswählen

Wenn Sie eine Verbindung hinzufügen, wählen Sie die zu verwendende IPSec-Richtlinie aus dieser Liste aus. Wenn Sie die Verbindung bearbeiten, ist diese Liste deaktiviert.

Methodenliste für Gruppenrichtlinien-Lookup

Wählen Sie aus dieser Liste die Methodenliste aus, die für das Gruppenrichtlinien-Lookup verwendet werden soll. Klicken Sie zum Konfigurieren von Methodenlisten in der Cisco SDM-Taskleiste auf **Zusätzliche Aufgaben** und dann auf den AAA-Knoten.

Benutzerauthentifizierung aktivieren

Aktivieren Sie dieses Kästchen, wenn die Benutzer sich authentifizieren müssen.

Methodenliste für Benutzerauthentifizierung

Wählen Sie aus dieser Liste die Methodenliste aus, die für die Benutzerauthentifizierung verwendet werden soll. Klicken Sie zum Konfigurieren von Methodenlisten in der Cisco SDM-Taskleiste auf **Zusätzliche Aufgaben** und dann auf den AAA-Knoten.

Moduskonfiguration

Aktivieren Sie **Initiieren**, wenn der Router Verbindungen mit Easy VPN Remote-Clients initiieren soll.

Aktivieren Sie **Antworten**, wenn der Router auf Anforderungen von Easy VPN Remote-Clients warten soll, bevor er Verbindungen aufbaut.

Beschränkter Zugriff

In diesem Fenster können Sie angeben, welche Gruppenrichtlinien eine Easy VPN-Serververbindung verwenden dürfen.

Sie lassen einer Gruppe den Zugriff zur Easy VPN-Serververbindung zu, indem Sie sein Kontrollkästchen aktivieren. Sie verweigern einer Gruppe den Zugriff zur Easy VPN-Serververbindung zu, indem Sie sein Kontrollkästchen deaktivieren.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Beschränken Sie eine Gruppenrichtlinie auf eine bestimmte Easy VPN-Server-Verbindung, und verweigern Sie gleichzeitig allen anderen Gruppenrichtlinien die Verwendung dieser Verbindung.	Wählen Sie die bestimmte Easy VPN-Server-Verbindung, und klicken Sie auf die Schaltfläche **Beschränkter Zugriff**. Aktivieren Sie das Kontrollkästchen der Zielgruppe, und deaktivieren Sie die Kontrollkästchen aller anderen Gruppen. Verweigern Sie der Zielgruppe den Zugriff auf alle anderen Easy VPN-Server-Verbindungen, indem Sie das entsprechende Kontrollkästchen im Fenster **Beschränkter Zugriff** für jede dieser Verbindungen deaktivieren.

Konfiguration von Gruppenrichtlinien

In diesem Fenster können Sie Gruppenrichtlinien zum Bearbeiten oder Löschen ansehen, hinzufügen, klonen und auswählen. Gruppenrichtlinien werden zur Identifizierung der Ressourcen für Easy VPN-Remote-Clients verwendet.

Schaltfläche „Gemeinsamer Pool“

Klicken Sie auf diese Schaltfläche, um einen vorhandenen Pool als gemeinsamen Pool anzugeben, der von allen Gruppenrichtlinien verwendet wird. Wenn keine lokalen Pools konfiguriert wurden, ist diese Schaltfläche inaktiv. Sie können Pools konfigurieren, indem Sie auf **Zusätzliche Aufgaben > Lokale Pools** klicken oder die Easy VPN-Serververbindungen konfigurieren.

Schaltflächen „Hinzufügen“, „Bearbeiten“, „Duplizieren“ und „Löschen“

Verwenden Sie diese Schaltflächen für die Verwaltung von Gruppenrichtlinien auf dem Router. Durch Klicken auf **Duplizieren** werden die Registerkarten für die Gruppenrichtlinienbearbeitung angezeigt.

Schaltfläche Aktualisierung senden

Klicken Sie diese Schaltfläche, um eine IKE-Benachrichtigung über Software- oder Hardware-Aktualisierungen an die aktiven Clients der gewählten Gruppe zu senden. Falls diese Schaltfläche inaktiv ist, dann ist für die gewählte Gruppe keine Client-Aktualisierung konfiguriert.

Um die Benachrichtigungen über die Client-Aktualisierung für die gewählte Gruppe einzustellen, klicken Sie auf die Schaltfläche **Bearbeiten** und dann auf die Registerkarte **Client-Aktualisierung**.

Spalte „Gruppenname“

Der Name der Gruppenrichtlinie.

Spalte „Pool“

Der IP-Adressenpool, der von den Clients in dieser Gruppe verwendet wird.

Spalte „DNS“

Von den Clients in dieser Gruppe verwendete DNS-Server.

Spalte „WINS“

Von den Clients in dieser Gruppe verwendete WINS-Server.

Spalte „Domänenname“

Der Domänenname, der von den Clients in dieser Gruppe verwendet wird.

Spalte „ACL“

Wenn Split-Tunneling für diese Gruppe angegeben ist, kann diese Spalte den Namen einer ACL enthalten, die definiert, welcher Datenverkehr verschlüsselt werden soll.

Fenster Details

Im Detailfenster sehen Sie ein Liste der Funktionseinstellungen und ihre Werte für die gewählte Gruppenrichtlinie. Funktionseinstellungen werden nur dann dargestellt, wenn Sie von der IOS-Version Ihres Cisco Routers unterstützt werden. Die folgenden Funktionseinstellungen können auf der Liste dargestellt werden:

- Authentifizierung

  Die Werte geben einen gemeinsamen Schlüssel an, sofern einer konfiguriert ist, oder ein digitales Zertifikat, falls kein gemeinsamer Schlüssel konfiguriert wurde.

- Maximal zulässige Verbindungen

  Zeigt die maximal zulässige Anzahl gleichzeitiger Verbindungen. Cisco SDM unterstützt maximal 5000 gleichzeitige Verbindungen pro Gruppe.

- Zugriffsbeschränkung

  Zeigt die Art des Client, für den die Revision gedacht ist.

- Backup-Server

  Zeigt die IP-Adressen der konfigurierten Backup-Server.

- Firewall-Are-U-There

  Beschränkt die Verbindungen an Geräte mit einer Black Ice oder Zone Alarm Firewall.

- **Include Local LAN** (lokales LAN einschließen)

  Ermöglicht einer Verbindung *ohne* Split-Tunneling den Zugriff auf das lokale Sub-Netzwerk zur gleichen Zeit wie der Client.

- PFS (Perfect Forward Secrecy)

  PFS ist für IPSec erforderlich.

- Konfiguration Push, URL und Version

  Der Server sendet eine Konfigurationsdatei von der angegebenen URL und mit der angegebenen Versionsnummer an einen Client.

- Gruppensperre

  Clients sind auf ihre Gruppe beschränkt.

- Kennwort speichern

  XAuth-Anmeldeinformationen können auf dem Client gespeichert werden.

- Maximale Anmeldungen

  Die maximale Anzahl von Verbindungen, die der Benutzer gleichzeitig aufbauen kann. Cisco SDM unterstützt maximal 10 gleichzeitige Anmeldungen pro Benutzer.

- XAuth Banner

  Die Textmeldung, die den Clients bei der XAuth-Anforderung angezeigt wird.

IP-Pools

In diesem Fenster sind die für Gruppenrichtlinien auf dem Router konfigurierten IP-Adressenpools aufgelistet. Abhängig vom Cisco SDM-Bereich, in dem Sie arbeiten, sind möglicherweise die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen** verfügbar und das Fenster hat je nach dem Cisco SDM-Bereich, in dem Sie arbeiten, einen anderen Namen. Sie können diese Schaltflächen zur Verwaltung von lokalen IP-Pools auf dem Router verwenden.

Spalte „Pool-Name“

Der Name des IP-Adressenpools.

Spalte „IP-Adressenbereich“

Der IP-Adressenbereich für den ausgewählten Pool. Ein Bereich von 2.2.2.0 bis 2.2.2.254 bietet 255 Adressen.

Spalte „Cache-Größe“

Die Cache-Größe für diesen Pool.

Spalte „Gruppenname“

Wird ein lokaler Pool mithilfe der CLI mit der Gruppenoption konfiguriert, so wird der Name der Gruppe in der Spalte **Gruppenname** angezeigt. Diese Spalte wird nicht in allen Cisco SDM-Bereichen angezeigt.

Hinweis Mit Cisco SDM können Sie keine lokalen Pools mit der Gruppenoption konfigurieren.

Lokalen IP-Pool hinzufügen/bearbeiten

In diesem Fenster können Sie einen lokalen IP-Adressenpool erstellen oder bearbeiten.

Pool-Name

Wenn Sie einen Pool erstellen, geben Sie den Namen des Pools ein. Wenn Sie einen Pool bearbeiten, ist dieses Feld deaktiviert.

IP-Adressenbereich

Geben Sie in diesem Bereich die IP-Adressenbereiche für den Pool ein, oder bearbeiten Sie sie. Ein Pool kann mehrere IP-Adressenbereiche enthalten. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um zusätzliche Bereiche zu erstellen, Bereiche zu bearbeiten und IP-Adressenbereiche zu löschen.

Cache-Größe

Geben Sie in diesem Feld die Cache-Größe für diesen Pool ein, oder bearbeiten Sie den Wert.

IP-Adressenbereich hinzufügen

In diesem Fenster können Sie einem bestehenden Pool einen IP-Adressenbereich hinzufügen.

Start-IP-Adresse

Geben Sie die niedrigste IP-Adresse im Bereich ein.

End-IP-Adresse

Geben Sie die höchste IP-Adresse im Bereich ein.

KAPITEL 12

Enhanced Easy VPN

In den folgenden Abschnitten werden die Konfigurationsbildschirme des Cisco Router and Security Device Managers für Enhanced Easy VPN beschrieben.

Schnittstelle und Authentifizierung

Geben Sie die Routerschnittstelle an, für die bei der virtuellen Vorlagenschnittstelle keine Nummerierung erfolgt, und geben Sie die zu verwendende Authentifzierungsmethode in diesem Fenster an.

Schnittstelle

Eine virtuelle Vorlagenschnittstelle muss für eine Routerschnittstelle ohne Nummerierung konfiguriert sein, damit eine IP-Adresse bezogen werden kann.

Cisco empfiehlt, für mehr Flexibilität keine Nummerierung der virtuellen Vorlagenschnittstelle für eine Loopback-Adresse vorzunehmen. Dazu klicken Sie auf **Keine Nummerierung für neue Loopback-Schnittstelle** und geben eine IP-Adresse und Subnetzmaske für die Loopback-Schnittstelle ein. Eine Beispiel-Loopback-IP-Adresse und Subnetzmaske lautet 127.0.0.1, 255.255.255.0.

Um die virtuelle Vorlagenschnittstelle für eine andere Schnittstelle ohne Nummerierung zu konfigurieren, klicken Sie auf **Keine Nummerierung für** und wählen die Schnittstelle. Sie sollten die Schnittstelle wählen, die den Tunnel auf dem Router beendet. Klicken Sie auf **Details**, um IP-Adresse, Authentifizierung, Richtlinie und andere Informationen über die Schnittstelle anzuzeigen, die Sie wählen.

Authentifizierung

Wählen Sie die Methode, die Easy VPN-Clients verwenden sollen, um sich bei dem auf dem Router konfigurierten Easy VPN Server zu authentifizieren. Pre-Shared Keys erfordern, dass Sie den Schlüssel den Administratoren der Easy VPN Clients mitteilen. Bei digitalen Zertifikaten ist dies nicht erforderlich; jeder Client muss sich jedoch für ein digitales Zertifikat registrieren und ein solches erhalten.

RADIUS-Server

Geben Sie die RADIUS-Server, die der Router für die Autorisierung und das Gruppenrichtlinien-Lookup verwendet, sowie die auf den RADIUS-Servern konfigurierten VPN-Gruppen im Fenster **RADIUS-Server** an.

RADIUS-Client-Quelle

Das Konfigurieren der RADIUS-Quelle ermöglicht Ihnen, die Quell-IP-Adresse festzulegen, die in Paketen an den RADIUS-Server gesendet wird. Zum Anzeigen der IP-Adresse und anderer Informationen über eine Schnittstelle wählen Sie die Schnittstelle und klicken auf die Schaltfläche **Details**.

Die Quell-IP-Adresse in den RADIUS-Paketen, die vom Router gesendet werden, muss als NAD-IP-Adresse in der Cisco Access Control Server (ACS) Version 3.3 oder höher konfiguriert werden.

Wenn Sie **Router wählt Quelle aus** aktivieren, ist die Quell-IP-Adresse in den RADIUS-Paketen die Adresse der Schnittstelle, über die die RADIUS-Pakete den Router verlassen.

Wenn Sie eine bestimmte Routerschnittstelle wählen, ist die Quell-IP-Adresse in den RADIUS-Paketen die Adresse dieser Schnittstelle.

Hinweis Cisco IOS-Software gestattet die Konfiguration einer Single-RADIUS-Quellschnittstelle auf dem Router. Wenn der Router bereits eine RADIUS-Quelle konfiguriert hat und Sie eine andere Quelle auswählen, ändert sich die IP-Adresse, die in den Paketen an den RADIUS-Server steht, in die IP-Adresse der neuen Quelle und kann dann eventuell nicht mehr mit der NAD-IP-Adresse auf dem konfigurierten Cisco ACS übereinstimmen.

Spalten „Server-IP“, „Parameter“ und „Auswählen“

Diese Spalten enthalten die wesentlichen Informationen über die RADIUS-Server, die der Router verwendet. Die Spalte **Server-IP** führt die IP-Adressen aller konfigurierten Server auf. Die Spalte **Parameter** führt die Autorisierungs- und Kontozuordnungs-Ports für jeden Server auf. Die Spalte **Auswählen** enthält ein Kontrollkästchen für jeden konfigurierten Server. Aktivieren Sie das Kontrollkästchen neben jedem Server, den Sie verwenden möchten. Die folgende Tabelle enthält Beispieldaten.

Server-IP-Adresse	Parameter	Auswählen
192.168.108.14	Autorisierungs-Port 1645; Kontozuordnungs-Port 1646	Aktivieren
192.168.108.15	Autorisierungs-Port 3005; Kontozuordnungs-Port 3006	

Bei dieser Konfiguration verwendet der RADIUS-Server bei 192.168.108.14 die Standard-Autorisierungs- und Kontozuordnungs-Ports 1645 bzw. 1646. Der Router verwendet diesen Server sowohl für die Authentifizierung als auch für die Autorisierung. Der Router verwendet bei 192.168.108.15 nicht standardmäßige Authentifizierungs- und Autorisierungs-Ports. Der Router kontaktiert diesen Server nicht, da das Kontrollkästchen **Auswählen** nicht aktiviert ist.

Klicken Sie auf **Hinzufügen**, um einen Eintrag für einen RADIUS-Server zu erstellen. Wählen Sie einen Servereintrag aus, und klicken Sie auf **Bearbeiten**, um die Informationen, die der Router für den Server gespeichert hat, zu ändern. Wählen Sie einen Servereintrag aus, und klicken Sie auf **Ping**, um die Verbindung zwischen Router und RADIUS-Server zu testen.

VPN-Gruppen im RADIUS-Server

Geben Sie die auf dem RADIUS-Server konfigurierten VPN-Gruppen ein, auf die diese Verbindung Zugriff gewähren soll. Trennen Sie die Einträge durch Kommata voneinander. Es folgt eine Gruppe von Beispieleinträgen:

```
WGP-1, WGP-2, ACCTG, CSVC
```

Diese Namen müssen den Gruppennamen entsprechen, die auf dem RADIUS-Server konfiguriert sind. Zur leichteren Administration sollten sie auch den Gruppennamen entsprechen, die Sie für die Easy VPN-Clients konfigurieren.

Gruppenautorisierungs- und Gruppenbenutzerrichtlinien

Sie können Benutzergruppen erstellen, die jeweils ihren eigenen IP-Adressenpool, eine Client-Aktualisierungskonfiguration, eine Split Tunneling-Konfiguration und andere benutzerdefinierte Einstellungen haben. Diese Gruppenattribute werden auf den Client in der Gruppe geladen, wenn sie eine Verbindung zum Easy VPN-Server herstellen. Derselbe Gruppenname muss auf den Clients konfiguriert werden, die Mitglieder der Gruppe sind, um sicherzustellen, dass die richtigen Gruppenattribute geladen werden.

Wenn bereits Gruppenrichtlinien konfiguriert wurden, erscheinen sie in der Liste in diesem Fenster, und Sie können sie für diese Verbindung auswählen, indem Sie das Kontrollkästchen **Auswählen** links neben dem Gruppennamen aktivieren.

Der Gruppenname, der Name des IP-Adressenpools, die DNS- und WINS-Server-Namen und der Domänenname jeder konfigurierten Gruppe werden in der Liste angezeigt. Wenn Sie auf **Hinzufügen** klicken, um Einstellungen für eine neue Gruppe zu konfigurieren, oder auf **Bearbeiten** klicken, um die Einstellungen zu ändern, erscheinen die Änderungen in dieser Liste. Wenn Sie Einstellungen für eine vorhandene Gruppe als Grundlage für eine neue Gruppenkonfiguration verwenden möchten, wählen Sie die vorhandene Gruppe aus und klicken auf **Duplizieren**. Die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Duplizieren** zeigen Dialogfelder an, mit denen Sie die Gruppeneinstellungen konfigurieren können.

Ruhestand-Timer konfigurieren

Aktivieren Sie **Configure Idle Timer** (Ruhestand-Timer konfigurieren), wenn Sie in den Feldern für den Ruhestand-Timer angeben möchten, wie lange eine Verbindung für Clients im Ruhezustand aufrechterhalten werden soll. Geben Sie Zeitwerte im Format HH:MM:SS ein. Wenn Sie beispielsweise 3 Stunden, 20 Minuten und 32 Sekunden eingeben möchten, geben Sie die folgenden Werte in die Felder ein:

```
03:20:32
```

Der Timeout-Wert gilt für alle Gruppen, die für diese Verbindung konfiguriert sind.

Hinzufügen oder Bearbeiten eines Easy VPN-Servers: Registerkarte „Allgemein“

Geben Sie in diesem Dialogfeld allgemeine Informationen zur Easy VPN-Server-Verbindung ein.

Name für diese Verbindung

Geben Sie einen Namen ein, um diese Verbindung zu kennzeichnen. Der eingegebene Name wird im Fenster **Easy VPN-Server bearbeiten** angezeigt.

IP-Adresse der virtuellen Tunnelschnittstelle

Klicken Sie auf Schnittstelle und Authentifizierung, um eine Beschreibung der Felder für die IP-Adresse der virtuellen Tunnelschnittstelle zu erhalten.

Tunnelmodus

Wählen Sie **IPSec-IPV4** im Feld für den Tunnelmodus. Die Option IPSec-IPV4 ermöglicht das Erstellen eines IPSec-Tunnels der IP-Version 4.

Beschreibung

Sie können eine Beschreibung eingeben, die für Administratoren in Ihrem Netzwerk nützlich ist, wenn Sie Konfigurationen ändern oder Fehler im Netzwerk beheben.

Hinzufügen oder Bearbeiten eines Easy VPN-Servers: Registerkarte „IKE“

Das Dialogfeld IKE in den Dialogfeldern **Easy VPN-Server hinzufügen** ermöglicht es Ihnen, ein IKE-Profil für diese Verbindung zu erstellen.

Identitätstyp abgleichen

Das IKE-Profil enthält Übereinstimmungskriterien, mit denen der Router eingehende und abgehende Verbindungen identifizieren kann, auf welche die IKE-Verbindungsparameter anzuwenden sind. Übereinstimmungskriterien können derzeit auf VPN-Gruppen angewandt werden. Im Feld **Identitätstyp abgleichen** ist automatisch **Gruppe** voreingestellt.

Klicken Sie auf **Hinzufügen**, um eine Liste der Gruppen zu erstellen, die Sie in die Übereinstimmungskriterien einbeziehen möchten.

Wählen Sie **Externen Gruppennamen hinzufügen**, um den Namen einer Gruppe hinzuzufügen, die nicht auf dem Router konfiguriert ist, und geben Sie den Namen im angezeigten Dialogfeld ein.

Wählen Sie **Aus lokalen Gruppen auswählen**, um den Namen einer Gruppe hinzuzufügen, die nicht auf dem Router konfiguriert ist. Aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen neben der Gruppe, die Sie hinzufügen möchten. Wenn alle lokalen Gruppen in anderen IKE-Profilen verwendet werden, informiert Sie der SDM, dass alle Gruppen ausgewählt wurden.

Moduskonfiguration

Wählen Sie **Antworten** im Feld **Moduskonfiguration**, wenn der Easy VPN-Server auf Moduskonfigurationsanforderungen antworten soll.

Wählen Sie **Einleiten** im Feld **Moduskonfiguration**, wenn der Easy VPN-Server Moduskonfigurationsanforderungen einleiten soll.

Wählen Sie **Beide** im Feld **Moduskonfiguration**, wenn der Easy VPN-Server auf Moduskonfigurationsanforderungen antworten und diese einleiten soll.

Autorisierungsrichtlinie für Gruppenrichtlinien-Lookup

Sie müssen eine Autorisierungsrichtlinie angeben, die den Zugriff auf Gruppenrichtlinien-Informationen auf dem AAA-Server steuert. Wählen Sie **Standard**, wenn Sie Zugriff auf Gruppenrichtlinien-Lookup-Informationen gewähren möchten. Um eine Richtlinie anzugeben, wählen Sie eine vorhandene Richtlinie in der Liste aus oder klicken auf **Hinzufügen**, um im angezeigten Dialogfeld eine Richtlinie zu erstellen.

Benutzerauthentifizierungsrichtlinie

Sie können eine Benutzerauthentifizierungsrichtlinie angeben, die für XAuth-Anmeldungen verwendet wird. Wählen Sie **Standard**, wenn Sie XAuth-Anmeldungen zulassen möchten. Um eine Richtlinie für die Steuerung von XAuth-Anmeldungen anzugeben, wählen Sie eine vorhandene Richtlinie in der Liste aus oder klicken auf **Hinzufügen**, um im angezeigten Dialogfeld eine Richtlinie zu erstellen.

Dead Peer-Erkennung

Klicken Sie auf **Dead Peer-Erkennung**, um dem Router zu ermöglichen, Meldungen zu Dead Peer-Erkennungen (Dead Peer Discovery, DPD) an Easy VPN Remote-Clients zu senden. Wenn ein Client nicht auf DPD-Meldungen reagiert, wird die Verbindung zu diesem aufgehoben.

Geben Sie die Anzahl der Sekunden zwischen DPD-Meldungen im Feld **Keepalive-Intervall** an. Der zulässige Bereich liegt zwischen 10 und 3600 Sekunden.

Geben Sie im Feld **Wiederholungen** die Anzahl der Sekunden zwischen Wiederholungsversuchen an, wenn DPD-Meldungen fehlschlagen. Der zulässige Bereich liegt zwischen 2 und 60 Sekunden.

Die Dead Peer-Erkennung hilft dabei, Verbindungen ohne Administratoreingriff zu verwalten, generiert jedoch auch zusätzliche Pakete, die beide Peers verarbeiten müssen, damit die Verbindung aufrechterhalten wird.

Hinzufügen oder Bearbeiten eines Easy VPN-Servers: Registerkarte „IPSec“

Geben Sie die Informationen ein, um in diesem Dialogfeld ein IPSec-Profil zu erstellen. Ein IPSec-Profil gibt die zu verwendenden Transformationssätze an, legt fest, wie die Security Association (SA)-Gültigkeitsdauer bestimmt wird und liefert weitere Informationen.

Spalte „Transformationssatz“

Verwenden Sie die zwei Spalten oben im Dialogfeld, um die Transformationssätze anzugeben, die Sie in das Profil einbeziehen möchten. Die Spalte auf der linken Seite enthält die Transformationssätze, die auf dem Router konfiguriert sind. Um einen konfigurierten Transformationssatz zum Profil hinzuzufügen, klicken Sie auf die Schaltfläche **>>**. Wenn sich in der linken Spalte keine Transformationssätze befinden oder wenn Sie einen Transformationssatz benötigen, der noch nicht erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen den Transformationssatz im angezeigten Dialogfeld.

Zeitbasierte IPSec SA-Gültigkeitsdauer

Klicken Sie auf **Zeitbasierte IPSec SA-Gültigkeitsdauer**, wenn nach Ablauf einer festgelegten Zeitspanne eine neue SA erstellt werden soll. Geben Sie die Zeitspanne in den Feldern HH:MM:SS auf der rechten Seite ein. Der zulässige Bereich liegt zwischen 0:2:0 (2 Minuten) und 24:0:0 (24 Stunden).

Datenverkehrvolumen-basierte IPSec SA-Gültigkeitsdauer

Klicken Sie auf **Datenverkehrvolumen-basierte IPSec SA-Gültigkeitsdauer**, wenn eine neue SA erstellt werden soll, nachdem eine bestimmte Menge Datenverkehr durch den IPSec-Tunnel geströmt ist. Geben Sie die Zahl in Kilobyte ein, die durch den Tunnel strömen sollte, bevor eine vorhandene aufgehoben und eine neue eingerichtet wird. Der zulässige Bereich liegt zwischen 2560 KB und 536870912 KB.

IPSec SA-Ruhezustand

Klicken Sie auf **IPSec SA-Ruhezustand**, wenn eine neue SA erstellt werden soll, nachdem der Peer eine gewisse Zeit untätig war. Geben Sie die Ruhezustandszeit in den Feldern HH:MM:SS auf der rechten Seite ein. Der zulässige Bereich liegt zwischen 0:1:0 (eine Minute) und 24:0:0 (24 Stunden).

Perfect Forward Secrecy

Klicken Sie auf **Perfect Forwarding Secrecy**, wenn IPSec Perfect Forwarding Secrecy (PFS) anfordern sollt, wenn es neue Security Associations für diese virtuelle Vorlagenschnittstelle anfordert oder PFS bei vom Peer erhaltenen Anforderungen PFS anfordern sollt. Sie können die folgenden Werte angeben:

- group1 – Die 768-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.
- group2 – Die 1024-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.
- group5 – Die 1536-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.

Virtuelle Tunnelschnittstelle erstellen

Geben Sie in diesem Dialogfeld die Informationen für eine virtuelle Tunnelschnittstelle ein.

Schnittstellentyp

Wählen Sie **Standard** oder **Tunnel** als Schnittstellentyp. Wenn Sie eine virtuelle Tunnelschnittstelle bearbeiten, wird der konfigurierte Wert angezeigt und das Feld ist schreibgeschützt.

IP-Adresse der Schnittstelle konfigurieren

Die IP-Adresse der virtuellen Tunnelschnittstelle kann für eine andere Schnittstelle ohne Nummerierung sein oder keine IP-Adresse aufweisen. Wählen Sie **Keine IP-Nummerierung**, und wählen Sie einen Schnittstellennamen im Feld **Keine Nummerierung für**, oder wählen Sie **Keine IP-Adresse**.

Tunnelmodus

Cisco SDM unterstützt derzeit den IPSec-IPv4-Tunnelmodus, der voreingestellt ist.

Zone auswählen

Dieses Feld wird angezeigt, wenn der Router ein Cisco IOS-Abbild ausführt, das eine Zone-Policy Based Firewall (ZPF) unterstützt, und eine Zone auf dem Router konfiguriert wurde. Wenn diese virtuelle Tunnelschnittstelle ein Zonenmitglied sein soll, klicken Sie auf die Schaltfläche rechts neben dem Feld. Klicken Sie auf **Zone auswählen**, und wählen Sie die Zone, der die Schnittstelle angehören soll, oder klicken Sie auf **Zone erstellen**, um eine neue Zone für diese Schnittstelle zu erstellen.

Hinweis Die virtuelle Zonenschnittstelle muss kein Mitglied einer Zone sein. Der Router leitet jedoch keinen Datenverkehr zwischen einer Schnittstelle, die einer Zone angehört, und Schnittstellen, die keiner Zone angehören, weiter.

KAPITEL 13

DMVPN

Diese Hilfethemen liefern Informationen über DMVPN-Konfigurationsbildschirme (DMVPN = Dynamic Multipoint Virtual Private Network).

Dynamic Multipoint VPN

Dieser Assistent unterstützt Sie bei der Konfiguration des Routers als DMVPN-Hub (Dynamic Multipoint VPN) oder -Spoke. Eine typische VPN-Verbindung ist ein Point-to-Point-IPSec-Tunnel, der zwei Router verbindet. DMVPN ermöglicht Ihnen die Einrichtung eines Netzwerks mit einem zentralen Hub, der mit einem GRE over IPSec-Tunnel andere Remote-Router verbindet, die als Spokes bezeichnet werden. IPSec-Datenverkehr wird über den Hub an die Spokes im Netzwerk geleitet. Mit Cisco SDM haben Sie die Möglichkeit, einen Router als primären oder sekundären DMVPN-Hub oder als Spoke-Router in einem DMVPN-Netzwerk zu konfigurieren.

Über den folgenden Link erhalten Sie weitere Informationen über DMVPN (CCO-Anmelde-ID erforderlich).

Multipoint IPSec VPNs

Cisco SDM unterstützt die Konfiguration eines Hub-und-Spoke-DMVPNs, in dem die Verschlüsselung mit IPSec-Profilen definiert wird. Sie können ein vollvermaschtes DMVPN konfigurieren und Crypto Maps verwenden, um die Verschlüsselung im DMVPN unter Verwendung der CLI zu definieren. Vollvermaschte DMVPNs und DMVPNs, die Crypto Maps verwenden, werden über die CLI verwaltet und geändert. Cisco SDM unterstützt die DMVPN-Konfiguration ab IOS-Version 12.2(13)T.

Cisco SDM unterstützt die Konfiguration eines Einzel-DMVPNs auf einem Router.

Identifizieren Sie Ihren Router in diesem Bildschirm als Hub oder Spoke im DMVPN-Netzwerk.

Es ist wichtig, zuerst die Hub-Konfiguration vorzunehmen, da Spokes, die die Hub-Informationen verwenden, konfiguriert sein müssen. Wenn Sie einen Hub konfigurieren, können Sie mit der Spoke-Konfigurationsfunktion, die im Übersichtfenster zur Verfügung steht, ein Verfahren generieren und dieses an Spoke-Administratoren senden, damit diese die Spokes mit den richtigen Hub-Informationen konfigurieren können. Bevor Sie mit der Konfiguration eines Spokes beginnen, müssen Sie über die korrekten Informationen zum Hub verfügen.

Spoke (Client) in einem DMVPN erstellen

Wählen Sie diese Option aus, wenn Ihr Router ein Spoke im DMVPN-Netzwerk ist. Spokes sind die logischen Endpunkte im Netzwerk. Vor Beginn der Konfiguration sollten Sie mit einem Ping an den Hub die Konnektivität sicherstellen, und Ihnen sollten alle erforderlichen Informationen über die Hub-Konfiguration vorliegen. Diese Informationen sind im Abschnitt Dynamic Multipoint VPN (DMVPN) Spoke-Assistent aufgelistet.

Hub (Server oder Kopfstelle) in einem DMVPN erstellen

Wählen Sie diese Option aus, wenn Ihr Router ein Hub im DMVPN-Netzwerk ist. Der Hub ist der logische Mittelpunkt eines DMVPN-Netzwerks und ist über eine Point-to-Point-IPSec-Verbindung mit jedem Spoke-Router verbunden. Der Hub kann IPSec-Datenverkehr zwischen den Spoke-Routern im Netzwerk leiten.

Dynamic Multipoint VPN (DMVPN) Hub-Assistent

Dieser Assistent unterstützt Sie bei der Konfiguration Ihres Routers als DMVPN-Hub. Konfigurieren Sie den Hub vor den Spokes, damit Sie Spoke-Administratoren die Informationen geben können, die sie für die Konfiguration ihrer Spoke-Router benötigen.

Im Anwendungsfenster wird erläutert, was Sie konfigurieren werden. Nach Abschluss der Konfiguration müssen Sie Spoke-Administratoren die folgenden Informationen über den Hub geben:

- Die IP-Adresse der physikalischen Schnittstelle des Hub-Routers
- Die IP-Adresse der mGRE-Tunnelschnittstelle des Hubs
- Das Protokoll für dynamisches Routing, das für das Senden von Routing-Aktualisierungen an das DMVPN verwendet wird, und die zu verwendende Nummer für ein autonomes System (AS-Nummer, für EIGRP) oder Prozess-ID (für OSPF)

Mit der Cisco SDM-Funktion für die Spoke-Konfiguration können Sie eine Textdatei mit den Informationen über die Hub-Konfiguration erstellen, die Spoke-Administratoren benötigen. Diese Funktion steht im Fenster **Übersicht** dieses Assistenten zur Verfügung.

Sie müssen außerdem den Spoke-Administratoren mitteilen, welche Subnetzmaske verwendet werden soll, und jedem Spoke eine IP-Adresse aus dem Subnetz des Hubs zuordnen, damit keine Adresskonflikte auftreten.

Hub-Typ

DMVPN-Netzwerke können mit einem einzelnen Hub oder mit einem primären und einem Sicherungs-Hub konfiguriert werden. Geben Sie an, als welchen Hub-Typ Sie Ihren Router konfigurieren.

Primärer Hub

Aktivieren Sie dieses Kontrollkästchen, wenn der Router der primäre Hub im DMVPN-Netzwerk ist.

Sicherungs-Hub

Aktivieren Sie dieses Kontrollkästchen, wenn der Router ein Sicherungs-Hub in einem vollvermaschten DMVPN-Netzwerk ist.

Pre-Shared Key konfigurieren

DMVPN-Peers können einen Pre-Shared Key oder digitale Zertifikate verwenden, um Verbindungen gegenseitig zu authentifizieren. Wenn Pre-Shared Keys verwendet werden, müssen alle Hub- und Spoke-Router denselben Pre-Shared Key verwenden.

Pre-Shared Keys sollten über eine sichere und praktische Methode mit dem Administrator des Remote-Standorts ausgetauscht werden, z. B. über eine verschlüsselte E-Mail-Nachricht. Die Verwendung von Fragezeichen (?) und Leerzeichen ist im Pre-Shared Key nicht zulässig. Der Pre-Shared Key darf maximal 128 Zeichen enthalten.

Pre-Shared Key

Geben Sie den Pre-Shared Key ein, der im DMVPN-Netzwerk verwendet wird. Die Verwendung von Fragezeichen (?) und Leerzeichen ist im Pre-Shared Key nicht zulässig. Der Pre-Shared Key darf maximal 128 Zeichen enthalten.

Digitale Zertifikate

Wählen Sie diese Option aus, wenn Ihr Router digitale Zertifikate für die Authentifizierung verwendet. Digitale Zertifikate werden unter „VPN-Komponenten“ > „Public-Key-Infrastruktur“ konfiguriert.

Pre-Shared Key bestätigen

Geben Sie den Schlüssel zur Bestätigung noch einmal ein. Wenn die Werte in diesem Feld und im Feld **Pre-Shared Key** nicht übereinstimmen, werden Sie in Cisco SDM aufgefordert, sie erneut einzugeben.

Konfiguration der Hub-GRE-Tunnelschnittstelle

Multipoint Generic Routing Encapsulation (mGRE) wird in einem DMVPN-Netzwerk verwendet, damit eine einzelne GRE-Schnittstelle auf einem Hub einen IPSec-Tunnel zu jedem Spoke-Router unterstützen kann. Dadurch wird die DMVPN-Konfiguration erheblich vereinfacht. GRE ermöglicht das Senden von Routing-Aktualisierungen über IPSec-Verbindungen.

Schnittstelle für die Internetverbindung auswählen

Wählen Sie die Routerschnittstelle für die Internetverbindung aus. Der GRE-Tunnel geht von dieser Schnittstelle aus.

Wenn Sie eine Schnittstelle, die eine DFÜ-Verbindung verwendet, auswählen, kann dies dazu führen, dass die Verbindung ständig aktiv ist. Sie können unterstützte Schnittstellen in **Schnittstellen und Verbindungen** überprüfen, um festzustellen, ob eine DFÜ-Verbindung vorliegt. In der Regel werden Schnittstellen wie ISDN oder asynchrone serielle Schnittstellen für eine DFÜ-Verbindung konfiguriert.

IP-Adresse

Geben Sie die IP-Adresse für die mGRE-Schnittstelle ein. Dies muss eine private Adresse sein, und sie muss sich im selben Subnetz wie die GRE-Schnittstellen der anderen Router im Netzwerk befinden. Beispiel: Die GRE-Schnittstellen verwenden gemeinsam das Subnetz 10.10.6.0, und ihnen sind IP-Adressen im Bereich zwischen 10.10.6.1 und 10.10.6.254 zugeordnet.

Subnetzmaske

Geben Sie die Maske für das Subnetz ein, in dem sich die GRE-Schnittstellen befinden. Die Maske für das Subnetz 10.10.6.0 könnte 255.255.255.0 lauten. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Schaltfläche „Erweitert“

Cisco SDM liefert Standardwerte für erweiterte Tunneleinstellungen. Die Hub-Administration muss jedoch über die Tunneleinstellungen entscheiden und sie an die Mitarbeiter geben, die die Spoke-Router verwalten, damit sie entsprechende Einstellungen vornehmen können.

Erweiterte Konfiguration für die Tunnelschnittstelle

Verwenden Sie dieses Fenster zur Konfiguration von GRE-Tunnelparametern. Cisco SDM liefert Standardwerte, Sie müssen sich jedoch die richtigen Werte von der Hub-Administration geben lassen und sie hier eingeben.

Die Standardwerte sind in diesem Hilfethema angegeben. Wenn Sie die Standardwerte geändert haben und sie wiederherstellen müssen, lesen Sie dieses Hilfethema.

NHRP-Authentifizierungsstring

Geben Sie den String ein, mit dem DMVPN Hubs und Spokes sich für NHRP-Transaktionen authentifizieren müssen. Dieser String kann bis zu 8 Zeichen lang sein. Sonderzeichen wie Leerzeichen und Fragezeichen (?) sind unzulässig. Alle Geräte im DMVPN müssen mit demselben Authentifizierungsstring konfiguriert werden.

Cisco SDM-Standard: DMVPN_NW

NHRP-Netzwerk-ID

Geben Sie die NHRP-Netzwerk-ID ein. Die Netzwerk-ID ist ein global eindeutiger 32-Bit-Netzwerk-Identifier für ein NBMA-Netzwerk (Nonbroadcast, Multiaccess). Der Bereich liegt zwischen 1 und 4294967295.

Cisco SDM-Standard: 100000

NHRP-Haltezeit

Geben Sie an, für wie viele Sekunden NHRP-Netzwerk-IDs als gültig angekündigt werden sollen.

Cisco SDM-Standard: 360

Tunnelschlüssel

Geben Sie den Schlüssel ein, der für diesen Tunnel verwendet werden soll. Dieser Schlüssel sollte für alle mGRE-Tunnel im Netzwerk gleich sein.

Cisco SDM-Standard: 100000

Bandbreite

Geben Sie die vorgesehene Bandbreite in Kilobyte pro Sekunde (kbps) ein. Standardwerte für die Bandbreite werden während der Einrichtung eingestellt. Die Bandbreitenwerte können mit dem EXEC-Befehl show interfaces angezeigt werden. 1000 ist eine typische Bandbreiteneinstellung in DMVPN-Konfigurationen.

Cisco SDM-Standard: 1000

MTU

Geben Sie die maximal zulässige Datenmenge in Byte für ein Paket ein, das über den Tunnel übertragen wird.

Cisco SDM-Standard: 1400

Tunneldurchsatzverzögerung

Stellen Sie einen Verzögerungswert für eine Schnittstelle in Zehntelmikrosekunden ein.

Cisco SDM-Standard: 1000

Primärer Hub

Wenn der von Ihnen konfigurierte Router der Sicherungs-Hub im DMVPN-Netzwerk ist, müssen Sie den primären Hub durch die Eingabe seiner öffentlichen und privaten IP-Adresse identifizieren.

Öffentliche IP-Adresse

Geben Sie die IP-Adresse der Schnittstelle auf dem primären Hub an, der für diesen Tunnel verwendet wird. Dies sollte eine statische IP-Adresse sein. Lassen Sie sich diese Information von der Hub-Administration geben.

IP-Adresse der mGRE-Tunnelschnittstelle des Hubs

Geben Sie die IP-Adresse der mGRE-Tunnelschnittstelle auf dem primären Hub ein. Lassen Sie sich diese Information von der Hub-Administration geben.

Routing-Protokoll auswählen

Geben Sie in diesem Fenster an, wie andere Netzwerke hinter Ihrem Router für andere Router im Netzwerk angekündigt werden. Wählen Sie eine der folgenden Typen:

- EIGRP – Enhanced Interior Gateway Routing Protocol
- OSPF – Open Shortest Path First
- RIP – Routing Internet Protocol
- Statisches Routing. Diese Option ist aktiviert, wenn Sie einen GRE over IPSec-Tunnel konfigurieren.

Hinweis RIP wird nicht für die DMVPN-Hub-und-Spoke-Topologie unterstützt, ist aber für die vollvermaschte DMVPN-Topologie verfügbar.

Routing-Informationen

Fügen Sie in diesem Fenster Routing-Informationen über hinter dem Router liegende Netzwerke hinzu, die Sie für die anderen Router im Netzwerk ankündigen möchten, oder bearbeiten Sie diese Informationen. Die Felder in diesem Fenster variieren je nach angegebenem Routing-Protokoll.

Weitere Informationen zu RIP-Parametern finden Sie unter RIP-Route hinzufügen/bearbeiten.

Weitere Informationen zu EIGRP-Parametern finden Sie unter EIGRP-Route hinzufügen oder bearbeiten.

Weitere Informationen zu OSPF-Parametern finden Sie unter OSPF-Route hinzufügen oder bearbeiten.

Wählen Sie die zu aktivierende RIP-Version

Geben Sie die RIP-Version 1 oder 2 an.

Wählen Sie eine bestehende OSPF-Prozess-ID/EIGRP AS-Nummer

Sie können eine bestehende Prozess-ID für OSPF oder eine bestehende AS-Nummer für EIGRP wählen, sofern diese bereits konfiguriert wurde. Siehe Empfehlungen zur Konfiguration von Routing-Protokollen für DMVPN.

Erstellen Sie eine neue OSPF-Prozess-ID/EIGRPAS-Nummer

Wenn keine Prozess-IDs vorhanden sind oder Sie eine andere verwenden möchten, können Sie in diesem Feld eine Prozess-ID konfigurieren.

OSPF Area ID für Tunnelnetzwerk

Geben Sie eine neue OSPF Area ID für das Netzwerk ein. Diese Bereichs-ID wird für das Tunnelnetzwerk verwendet. Cisco SDM fügt das Tunnelnetzwerk anhand dieser Bereichs-ID automatisch zu diesem Prozess hinzu.

Mit <*Protokollname*> angekündigte private Netzwerke

In diesem Bereich werden die mit dem ausgewählten Routing-Protokoll angekündigten Netzwerke angezeigt. Wenn Sie das in diesem Assistenten angegebene Routing-Protokoll bereits konfiguriert haben, werden die Netzwerke, die Sie für die Ankündigung vorgesehen haben, in dieser Liste angezeigt.

Fügen Sie alle privaten Netzwerke hinzu, die Sie mit diesem Routing-Prozess für die DMVPN-Peers ankündigen möchten. Der DMVPN-Assistent fügt automatisch das Tunnelnetzwerk zu diesem Prozess hinzu.

Netzwerk – Eine Netzwerkadresse. Sie können die Adresse eines spezifischen Netzwerks eingeben und die Platzhaltermaske verwenden, um die Ankündigung allgemein zu fassen.

Platzhaltermaske – (EIGRP- und OSPF-Protokoll). Eine Bitmaske, die angibt, wie viele Stellen der Netzwerkadresse der in der Netzwerkspalte angegebenen Adresse entsprechen müssen. Mit dieser Maske kann der Router dazu veranlasst werden, auf Grundlage der angegebenen Adresse Netzwerke in einem bestimmten Bereich anzukündigen. Ein 0-Bit gibt an, dass das Bit in der Netzwerkadresse dem entsprechenden Bit in der angegebenen Netzwerkadresse entsprechen muss.

Wenn beispielsweise die Netzwerkadresse 172.55.10.3 lautet und für die Platzhaltermaske 0.0.255.255 angegeben ist, kündigt der Router alle Netzwerke an, die mit 172.55 beginnen, nicht nur das Netzwerk 172.55.10.3.

Bereich – Wenn OSPF ausgewählt ist, wird die OSPF-Bereichsnummer für das Netzwerk angezeigt. Jeder Router in einem bestimmten OSPF-Bereich verwaltet eine topologische Datenbank für diesen Bereich.

Hinzufügen – Klicken Sie auf diese Schaltfläche, um ein Netzwerk oder eine Gruppe von Netzwerken zur Ankündigung hinzuzufügen.

Bearbeiten – Klicken Sie auf diese Schaltfläche, um die Daten für ein angekündigtes Netzwerk oder eine angekündigte Gruppe von Netzwerken zu bearbeiten. Diese Schaltfläche ist für Einträge aktiviert, die Sie während der aktuellen Instanz des Assistenten erstellt haben.

Löschen – Klicken Sie auf diese Schaltfläche, um die Daten für das ausgewählte Netzwerk oder die ausgewählte Gruppe von Netzwerken zu löschen. Diese Schaltfläche ist für Einträge aktiviert, die Sie während der aktuellen Instanz des Assistenten erstellt haben.

Dynamic Multipoint VPN (DMVPN) Spoke-Assistent

Dieser Assistent unterstützt Sie bei der Konfiguration Ihres Routers als Spoke in einem DMVPN-Netzwerk. Vor Beginn der Konfiguration sollten Sie mit einem Ping an den Hub sicherstellen, dass Ihr Router Daten an ihn senden kann. Darüber hinaus sollten Ihnen vor Beginn alle erforderlichen Informationen über den Hub vorliegen. Ein Hub-Administrator, der den Hub mit Cisco SDM konfiguriert, kann eine Textdatei mit den Hub-Informationen erstellen, die Spoke-Administratoren benötigen.

Sie müssen sich vor Beginn die folgenden Informationen geben lassen:

- Die IP-Adresse der physikalischen Schnittstelle des Hubs
- Die IP-Adresse der mGRE-Tunnelschnittstelle des Hubs
- Die IP-Adresse und die Subnetzmaske, die Sie nach Anweisung der Hub-Administration für den Spoke verwenden sollen. Die Hub-Administration muss den einzelnen Spokes Adressen zuordnen, um sicherzustellen, dass alle Router im DMVPN sich im selben Subnetz befinden und alle eine eindeutige Adresse verwenden.
- Das zu verwendende Routing-Protokoll und die AS-Nummer (EIGRP) oder Prozess-ID (OSPF), die zum Senden von Routing-Aktualisierungen im DMVPN verwendet werden soll

DMVPN-Netzwerktopologie

Wählen Sie den Typ des DMVPN-Netzwerks aus, zu dem dieser Router gehört.

Hub-und-Spoke-Netzwerk

Wählen Sie diese Option aus, wenn Sie den Router in einem Netzwerk konfigurieren, in dem jeder Spoke-Router über eine Point-to-Point-Verbindung mit GRE over IPSec zum DMVPN-Hub verfügt und Daten für andere Spokes über den Hub sendet. Wenn Sie diese Option auswählen, werden in der Grafik Verbindungen von den Spokes zum Hub angezeigt.

Vollvermaschtes Netzwerk

Wählen Sie diese Option, wenn Sie einen Router als Spoke konfigurieren, der einen direkten IPSec-Tunnel zu anderen Spokes im Netzwerk aufbauen kann. Zur Unterstützung dieser Funktion wird auf dem Spoke ein Multipoint-GRE-Tunnel konfiguriert. Wenn Sie diese Option auswählen, werden in der Grafik Verbindungen von den Spokes zum Hub sowie zwischen den Spokes angezeigt.

Im Bildschirm für den Assistenten werden die IOS-Abbilder aufgeführt, die zur Unterstützung eines vollvermaschten DMVPN-Netzwerks erforderlich sind.

Hub-Informationen angeben

Geben Sie in diesem Fenster die erforderlichen Informationen über den Hub im DMVPN an.

IP-Adresse der physikalischen Schnittstelle des Hubs

Geben Sie die IP-Adresse der Schnittstelle auf dem Hub an. Lassen Sie sich diese Adresse von der Hub-Administration geben. Diese Adresse wird als Tunnelziel verwendet.

IP-Adresse der mGRE-Tunnelschnittstelle des Hubs

Geben Sie die IP-Adresse der mGRE-Tunnelschnittstelle auf dem Hub ein. Die mGRE-Tunneladressen für den Hub und die Spokes müssen sich im selben Subnetz befinden.

Spoke-GRE-Tunnelschnittstellen-Konfiguration

Mit den in diesem Fenster eingegebenen Informationen wird eine Point-to-Point-Verbindung für diesen Spoke erstellt.

Schnittstelle für die Internetverbindung auswählen

Wählen Sie die Routerschnittstelle für die Internetverbindung aus. Der GRE over IPSec-Tunnel geht von dieser Schnittstelle aus.

Wenn Sie eine Schnittstelle, die eine DFÜ-Verbindung verwendet, auswählen, kann dies dazu führen, dass die Verbindung ständig aktiv ist. Sie können über das Fenster **Schnittstellen und Verbindungen** die unterstützten Schnittstellen untersuchen, um zu ermitteln, ob eine DFÜ-Verbindung, wie beispielsweise eine ISDN- oder Async-Verbindung, für die von Ihnen ausgewählte physikalische Schnittstelle konfiguriert wurde.

Registrieren Sie sich erneut beim Hub, wenn die IP-Adresse von *Schnittstellenname* sich ändert – Diese Option ist verfügbar, wenn die ausgewählte Schnittstelle eine dynamische IP-Adresse über DHCP oder IPCP erhält. Wenn Sie diese Option angeben, kann der Spoke sich neu beim Hub registrieren, wenn er eine neue IP-Adresse erhält.

IP-Adresse

Geben Sie die IP-Adresse für die GRE-Schnittstelle zu diesem Hub ein. Dies muss eine private Adresse sein, und sie muss sich im selben Subnetz wie die GRE-Schnittstellen der anderen Router im Netzwerk befinden. Beispiel: Die GRE-Schnittstellen verwenden gemeinsam das Subnetz 10.10.6.0, und ihnen sind IP-Adressen im Bereich zwischen 10.10.6.1 und 10.10.6.254 zugeordnet.

Wenn Sie einen Spoke-Router konfigurieren, müssen Sie die IP-Adresse verwenden, die die Hub-Administration Ihrem Router zugeordnet hat. Wenn Sie sie nicht verwenden, kann dies zu Adresskonflikten führen.

Subnetzmaske

Geben Sie die Maske für das Subnetz ein, in dem sich die GRE-Schnittstellen befinden. Diese Maske muss von der Hub-Administration zugeordnet werden und für alle Router im DMVPN gleich sein. Beispiel: Die Maske für das Subnetz 10.10.6.0 könnte 255.255.255.0 sein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Schaltfläche „Erweitert“

Klicken Sie auf diese Schaltfläche, um NHRP- und Tunnelparameter für diese Verbindung anzugeben.

Cisco SDM liefert Standardwerte für erweiterte Tunneleinstellungen. Die Hub-Administration muss jedoch über die Tunneleinstellungen entscheiden und sie an die Mitarbeiter geben, die die Spoke-Router verwalten, damit sie entsprechende Einstellungen vornehmen können. Wenn Sie einen Spoke-Router konfigurieren, lassen Sie sich die Tunneleinstellungen von der Hub-Administration geben. Klicken Sie dann auf diese Schaltfläche, und geben Sie die Einstellungen im angezeigten Dialogfeld ein.

Cisco SDM-Warnung: DMVPN Dependency (DMVPN-Abhängigkeit)

Dieses Fenster wird angezeigt, wenn die Schnittstelle, die Sie für die DMVPN-Tunnelquelle ausgewählt haben, eine Konfiguration besitzt, mit der sie nicht für DMVPN eingesetzt werden kann. Sie werden in Cisco SDM über den Konflikt informiert und können auswählen, ob Cisco SDM die Konfiguration so ändern soll, dass der Konflikt gelöst wird.

Firewall

Wenn der als Tunnelquelle angegebenen Schnittstelle eine Firewall zugeordnet wurde, kann Cisco SDM Zugriffsregeleinträge zur Konfiguration hinzufügen, damit GRE-, IPSec- und ISAKMP-Datenverkehr über die Firewall zugelassen wird.

Details anzeigen

Klicken Sie auf diese Schaltfläche, um die Zugriffssteuerungseinträge anzuzeigen, die Cisco SDM zur Zugriffsregel hinzufügt, wenn Sie **GRE-, IPSec- und ISAKMP-Datenverkehr über die Firewall zulassen** auswählen.

Diese Einträge lassen beide Arten von ISAKMP-Datenverkehr, GRE-Datenverkehr, ESP (Encapsulating Security Protocol) und AHP (Authentication Header Protocol) zu.

Dynamic Multipoint VPN (DMVPN) bearbeiten

In diesem Fenster werden die vorhandenen DMVPN-Tunnelkonfigurationen angezeigt. DMVPN ermöglicht Ihnen die Einrichtung eines Netzwerks mit einem zentralen Hub, der andere Remote-Router verbindet, die als Spokes bezeichnet werden. Cisco SDM unterstützt eine Hub-und-Spoke-Netzwerktopologie, in der GRE over IPSec-Datenverkehr durch den Hub geleitet wird. Cisco SDM ermöglicht es Ihnen, Ihren Router als primären oder sekundären DMVPN-Hub oder als Spoke-Router in einem DMVPN-Netzwerk zu konfigurieren.

Über den folgenden Link erhalten Sie weitere Informationen über DMVPN (CCO-Anmelde-ID erforderlich). Multipoint IPSec VPNs

Cisco SDM unterstützt die Konfiguration eines Hub-und-Spoke-DMVPNs, in dem die Verschlüsselung mit IPSec-Profilen definiert wird. Sie können ein vollvermaschtes DMVPN konfigurieren und Crypto Maps verwenden, um die Verschlüsselung im DMVPN unter Verwendung der CLI zu definieren. Vollvermaschte DMVPNs und DMVPNs, die Crypto Maps verwenden, werden über die CLI verwaltet und geändert.

Cisco SDM unterstützt die Konfiguration eines Einzel-DMVPNs auf einem Router.

Der Hub sollte zuerst konfiguriert werden, um die Hub-IP-Adressen und die Routing-Parameter festzulegen, mit denen die *Spokes* konfiguriert werden müssen. Weitere Empfehlungen zum Konfigurieren der Router in einem DMVPN finden Sie unter Empfehlungen zur DMVPN-Konfiguration.

Schnittstelle

Die physikalische Schnittstelle, von der dieser Tunnel ausgeht.

IPSec-Profil

Das IPSec-Profil, das der Tunnel verwendet. Das IPSec-Profil definiert die Transformationssätze, mit denen Datenverkehr auf dem Tunnel verschlüsselt wird. Cisco SDM unterstützt für die Definition der Verschlüsselung in einem DMVPN nur die Verwendung von IPSec-Profilen. Wenn Sie Crypto Maps verwenden möchten, konfigurieren Sie das DMVPN mit der CLI.

IP-Adresse

Die IP-Adresse des GRE-Tunnels. Der GRE-Tunnel wird zum Senden von Routing-Aktualisierungen an das DMVPN verwendet.

Beschreibung

Eine Beschreibung dieses Tunnels.

Bereich „Details“

Im Bereich **Details** werden die Werte für die gesamte Konfiguration des DMVPN-Tunnels angezeigt.

Warum werden einige Tunnelschnittstellen als schreibgeschützt angezeigt?

Eine Tunnelschnittstelle wird als schreibgeschützt angezeigt, wenn sie bereits mit Crypto Map-Verknüpfungen und NHRP-Parametern konfiguriert wurde. Sie können NHRP-Parameter und Routing-Informationen über dieses Fenster ändern, müssen aber die IP-Adresse, die Tunnelquelle und das Tunnelziel über das Fenster **Schnittstellen und Verbindungen** bearbeiten.

Hinzufügen

Klicken Sie auf diese Option, um eine neue DMVPN-Tunnelkonfiguration hinzuzufügen.

Bearbeiten

Klicken Sie auf diese Option, um eine ausgewählte DMVPN-Tunnelkonfiguration zu bearbeiten.

Löschen

Klicken Sie auf diese Option, um eine DMVPN-Tunnelkonfiguration zu löschen.

Bereich „Allgemein“

Fügen Sie in diesem Bereich allgemeine Konfigurationsparameter für den DMVPN-Tunnel hinzu, oder bearbeiten Sie diese Parameter.

IP-Adresse

Geben Sie die IP-Adresse des Tunnels ein. Dies muss eine private Adresse sein, und sie muss sich im selben Subnetz wie die anderen Tunneladressen im DMVPN befinden. Wenn Sie einen Spoke konfigurieren, müssen Sie die Adresse verwenden, die die Hub-Administration Ihrem Router zugeordnet hat, damit keine Adresskonflikte entstehen.

Maske

Geben Sie die Subnetzmaske ein, die die Hub-Administration dem DMVPN zugeordnet hat. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Tunnelquelle

Wählen Sie die Schnittstelle aus, die der Tunnel verwenden soll, oder geben Sie die IP-Adresse dieser Schnittstelle ein. Lesen Sie den Abschnitt Verwenden von Schnittstellen mit DFÜ-Konfigurationen, bevor Sie eine Schnittstelle auswählen, die für eine DFÜ-Verbindung konfiguriert ist.

Tunnelziel

Klicken Sie auf **Dies ist ein Multipoint-GRE-Tunnel**, wenn es sich um einen DMVPN-Tunnel in einem vollständig vermaschten Netzwerk handelt. Klicken Sie auf **IP/Hostname**, und geben Sie eine IP-Adresse oder einen Hostnamen ein, wenn es sich um ein Hub-und-Spoke-Netzwerk handelt.

IPSec-Profil

Wählen Sie ein konfiguriertes IPSec-Profil für diesen Tunnel aus. Das IPSec-Profil definiert die Transformationssätze, mit denen Datenverkehr in diesem Tunnel verschlüsselt wird.

MTU

Geben Sie die maximal zulässige Datenmenge in Byte für ein Paket ein, das über den Tunnel übertragen wird.

Bandbreite

Geben Sie die vorgesehene Bandbreite in Kilobyte pro Sekunde (kbps) ein. Standardwerte für die Bandbreite werden während der Einrichtung eingestellt. Die Bandbreitenwerte können mit dem EXEC-Befehl show interfaces angezeigt werden. Der Wert 1000 ist eine typische Bandbreiteneinstellung in DMVPN-Konfigurationen.

Verzögerung

Stellen Sie einen Verzögerungswert für eine Schnittstelle in Zehntelmikrosekunden ein. Der Wert 1000 ist eine typische Verzögerungseinstellung in DMVPN-Konfigurationen.

Tunnelschlüssel

Geben Sie den Schlüssel ein, der für diesen Tunnel verwendet werden soll. Dieser Schlüssel sollte für alle mGRE-Tunnel im Netzwerk gleich sein.

Dies ist ein Multipoint-GRE-Tunnel

Aktivieren Sie dieses Kontrollkästchen, wenn die Schnittstelle eine mGRE-Tunnelschnittstelle sein soll (eine Schnittstelle, die Verbindungen zu mehreren Peers verwalten kann). Wenn der Router als DMVPN-Hub konfiguriert wird, müssen Sie dieses Kontrollkästchen aktivieren, damit der Hub Verbindungen mit allen Spokes aufbauen kann. Wenn der Router als Spoke konfiguriert wird, aktivieren Sie dieses Kontrollkästchen, wenn Sie ein vollvermaschtes DMVPN konfigurieren. Auf diese Weise kann ein Spoke eine Verbindung zum Hub aufbauen, um Datenverkehr zu senden und Next Hop-Informationen für die direkte Verbindung zu allen anderen Spokes im DMVPN zu erhalten.

Bereich „NHRP“

Geben Sie in diesem Bereich NHRP-Konfigurationsparameter an.

Authentifizierungsstring

Geben Sie den String ein, mit dem DMVPN Hubs und Spokes sich für NHRP-Transaktionen authentifizieren müssen. Dieser String kann bis zu 8 Zeichen lang sein. Alle NHRP-Stationen im DMVPN müssen mit demselben Authentifizierungsstring konfiguriert werden.

Haltezeit

Geben Sie an, für wie viele Sekunden NHRP-Netzwerk-IDs als gültig angekündigt werden sollen.

Netzwerk-ID

Geben Sie die NHRP-Netzwerk-ID ein. Die Netzwerk-ID ist ein global eindeutiger 32-Bit-Netzwerk-Identifier für ein NBMA-Netzwerk (Nonbroadcast, Multiaccess). Der Bereich liegt zwischen 1 und 4294967295. Die Netzwerk-ID muss für jede NHRP-Station eindeutig sein.

Next Hop-Server

In diesem Bereich sind die IP-Adressen der Next Hop-Server aufgelistet, die der Router kontaktieren kann. Wenn der Router ein Spoke-Router ist, muss dieser Bereich die IP-Adresse des primären und des sekundären Hubs enthalten. Ist der Router ein Hub, muss dieser Bereich die IP-Adressen der anderen Hub-Router im DMVPN enthalten.

Klicken Sie auf **Hinzufügen**, um die IP-Adresse eines Next Hop-Servers einzugeben. Markieren Sie einen Server, und klicken Sie auf **Löschen**, um ihn aus der Liste zu löschen.

NHRP-Zuordnung

In diesem Bereich sind die verfügbaren IP-NBMA-Adresszuordnungen aufgelistet. Klicken Sie auf **Hinzufügen**, um eine neue Zuordnung zu erstellen. Nachdem Sie die Zuordnung erstellt haben, wird sie zu dieser Liste hinzugefügt. Klicken Sie auf **Bearbeiten**, um eine ausgewählte Zuordnung zu ändern. Klicken Sie auf **Löschen**, um eine ausgewählte Zuordnungskonfiguration zu entfernen.

Konfiguration der NHRP-Zuordnung

Erstellen oder bearbeiten Sie in diesem Fenster eine Zuordnung zwischen IP- und NBMA-Adressen.

IP-NBMA-Adresszuordnung von IP-Zielen, die mit einem NBMA-Netzwerk verbunden sind, statisch konfigurieren.

Klicken Sie auf diese Schaltfläche, wenn Sie einen Spoke in einem vollvermaschten Netzwerk konfigurieren. Cisco SDM behandelt Sicherungs-Hubs als Spokes von primären Hubs; klicken Sie also auch auf diese Schaltfläche, wenn Sie einen Sicherungs-Hub konfigurieren. In diesem Teil des Fensters geben Sie die Adressinformationen an, die der Spoke oder Sicherungs-Hub benötigt, um eine Verbindung zum primären Hub aufzubauen.

Ziel über NBMA-Netzwerk erreichbar – Geben Sie die IP-Adresse des mGRE-Tunnels ein, der auf dem primären Hub konfiguriert ist. Spokes und Sicherungs-Hubs verwenden diese Tunnelinformationen, um einen Kontakt zum Hub aufzubauen und einen mGRE-Tunnel zu ihm zu erstellen. Spokes verwenden den Tunnel, um verschlüsselte Daten an den Hub zu senden und auf ihm Next Hop-Informationen für andere Spokes abzufragen.

NBMA-Adresse direkt erreichbar – Geben Sie die statische IP-Adresse der Schnittstelle auf dem primären Hub ein, der den mGRE-Tunnel unterstützt.

NBMA-Adressen konfigurieren, die verwendet werden als Ziele für Broadcast- oder Multicast-Pakete, die über ein Tunnelnetzwerk gesendet werden

Geben Sie in diesem Bereich des Fensters Informationen an, die von Routing-Protokollen verwendet werden.

IP-Adressen der Spokes dynamisch in den Multicast-Cache des Hubs aufnehmen – Konfigurieren Sie diese Option, wenn Sie einen primären oder einen Sicherungs-Hub konfigurieren. Diese Option wird vom Hub benötigt, um Routing-Aktualisierungen an alle verbundenen DMVPN-Spokes zu senden.

IP-Adresse der NBMA-Adresse direkt erreichbar – Wenn Sie einen Spoke in einem vollvermaschten DMVPN oder einen Sicherungs-Hub konfigurieren, aktivieren Sie dieses Kontrollkästchen, und geben Sie die statische IP-Adresse der Schnittstelle auf dem primären Hub an, der den mGRE-Tunnel unterstützt.

Bereich „Routing“

Konfigurieren Sie in diesem Bereich Routing-Informationen für die DMVPN-Wolke.

Routing-Protokoll

Wählen Sie das Protokoll für dynamisches Routing, das der Hub und die Spoke-Router in diesem DMVPN für das Routing verwenden. Beachten Sie, dass alle Router im DMVPN für das Routing-Protokoll konfiguriert werden müssen, das Sie auswählen.

- RIP – Routing Internet Protocol
- OSPF – Open Shortest Path First
- EIGRP – Enhanced Interior Gateway Routing Protocol

RIP-Felder

Wenn Sie RIP als Protokoll für dynamisches Routing ausgewählt haben, wählen Sie **Version 1**, **Version 2** oder **Standard**. Wenn Sie **Version 2** auswählen, nimmt der Router die Subnetzmaske in die Routing-Aktualisierung auf. Wenn Sie **Standard** auswählen, versendet der Router Version-2-Aktualisierungen, ist aber in der Lage, RIP-Version-1- oder -Version-2-Aktualisierungen zu empfangen.

Split Horizon deaktivieren – Wenn der Router der Hub-Router ist, aktivieren Sie dieses Kontrollkästchen, um Split Horizon für die mGRE-Tunnelschnittstelle zu deaktivieren. Durch Deaktivieren von Split Horizon ist der Router in der Lage, die Routen, die er über die Tunnelschnittstelle erhalten hat, über dieselbe Schnittstelle anzukündigen.

OSPF-Felder

Wenn Sie OSPF ausgewählt haben, müssen die folgenden Felder ausgefüllt werden:

OSPF-Prozess-ID – Geben Sie die Prozess-ID ein. Dieser Wert identifiziert den OSPF-Prozess für andere Router. Siehe Empfehlungen zur Konfiguration von Routing-Protokollen für DMVPN.

OSPF-Netzwerktyp – Wählen Sie Point-To-Multipoint oder Broadcast. Point-To-Multipoint bewirkt, dass OSPF Routen zu den Routing-Tabellen auf Spoke-Routern hinzufügt. Wenn Sie das vermeiden möchten, können Sie Broadcast auswählen.

OSPF-Priorität – Die OSPF-Priorität identifiziert diesen Router als Hub oder Spoke. Wenn es sich um einen Hub-Router handelt, geben Sie den Prioritätswert 2 ein. Handelt es sich um einen Spoke-Router, geben Sie den Prioritätswert 0 ein.

EIGRP-Felder

Wenn Sie EIGRP ausgewählt haben, müssen die folgenden Felder ausgefüllt werden:

Autonomes System Nummer – Geben Sie die Nummer für das autonome System für die Gruppe von Routern ein, die EIGRP verwenden. Router mit derselben Nummer für das autonome EIGRP-System verwalten eine topologische Datenbank von Routern in der Region, die durch diese Nummer identifiziert wird. Siehe Empfehlungen zur Konfiguration von Routing-Protokollen für DMVPN.

Split Horizon deaktivieren – Wenn der Router der Hub-Router ist, aktivieren Sie dieses Kontrollkästchen, um Split Horizon für die mGRE-Tunnelschnittstelle zu aktivieren. Lassen Sie es deaktiviert, um Split Horizon zu deaktivieren. Durch Deaktivieren von Split Horizon ist der Router in der Lage, die Routen, die er über die Tunnelschnittstelle erhalten hat, über dieselbe Schnittstelle anzukündigen.

Ursprüngl. nächsten Hop verwenden – Wenn der Router ein DMVPN-Hub ist, kündigt EIGRP ihn als nächsten Hop an. Aktivieren Sie dieses Kontrollkästchen, damit EIGRP beim Ankündigen von Routen für die DMVPN-Spoke-Router den ursprünglichen Next Hop für IP verwendet.

Wie konfiguriere ich ein DMVPN manuell?

Sie können Ihren Router im VPN-Komponentenfenster oder im Fenster **Dynamic Multipoint VPN (DMVPN) bearbeiten** als DMVPN-Hub oder -Spoke konfigurieren. Hierzu müssen Sie die folgenden Aufgaben durchführen:

- Konfigurieren Sie ein IPSec-Profil. Sie können erst eine DMVPN-Verbindung konfigurieren, wenn Sie mindestens ein IPSec-Profil konfiguriert haben.
- Konfigurieren Sie die DMVPN-Verbindung.
- Geben Sie die Netzwerke an, die Sie für die DMVPN-Wolke ankündigen möchten.

Die Verfahren für diese Aufgaben sind im Folgenden beschrieben:

So konfigurieren Sie ein IPSec-Profil:

Sie müssen eine IPSec-Richtlinie und dann einen DMVPN-Tunnel konfigurieren.

Schritt 1 Klicken Sie im linken Bereich auf **VPN**, und klicken Sie dann auf **VPN-Komponenten**.

Schritt 2 Klicken Sie auf den Zweig **IPSec-Profile** und dann im Fenster **IPSec-Profile** auf **Hinzufügen**.

Schritt 3 Vergeben Sie im Fenster **IPSec-Profil hinzufügen** einen Namen für das Profil, und wählen Sie die Transformationssätze aus, die es enthalten soll. Wenn Sie es wünschen, können Sie eine kurze Beschreibung eingeben.

Schritt 4 Klicken Sie auf **OK**.

So konfigurieren Sie eine DMVPN-Verbindung:

Schritt 1 Klicken Sie im Baum **VPN** auf den Zweig **Dynamic Multipoint VPN**.

Schritt 2 Klicken Sie auf **Dynamic Multipoint VPN (DMVPN) bearbeiten**.

Schritt 3 Klicken Sie auf **Hinzufügen**.

Schritt 4 Geben Sie im Fenster **DMVPN-Tunnelkonfiguration** Daten in die Registerkarten **Allgemein**, **NHRP** und **Routing** ein, um einen DMVPN-Tunnel zu erstellen. Weitere Informationen zu einem bestimmten Feld erhalten Sie in der Onlinehilfe.

So geben Sie die Netzwerke an, die Sie für das DMVPN ankündigen möchten:

Wenn es Netzwerke hinter dem Router gibt, die Sie für das DMVPN ankündigen möchten, können Sie dazu die Netzwerknummern in den Fenstern unter **Routing** hinzufügen.

Schritt 1 Klicken Sie im linken Bereich auf **Routing**.

Schritt 2 Wählen Sie im Fenster **Routing** das Routing-Protokoll aus, das Sie in der DMVPN-Konfiguration angegeben haben, und klicken Sie auf **Bearbeiten**.

Schritt 3 Fügen Sie die Nummern der Netzwerke hinzu, die Sie ankündigen möchten.

KAPITEL 14

Globale VPN-Einstellungen

In diesen Hilfethemen werden die Fenster unter **Globale VPN-Einstellungen** beschrieben.

Globale VPN-Einstellungen

In diesem Fenster werden die globalen VPN-Einstellungen für den Router angezeigt.

Schaltfläche „Bearbeiten“

Klicken Sie auf die Schaltfläche **Bearbeiten**, um globale VPN-Einstellungen hinzuzufügen oder zu ändern.

IKE aktivieren

Der Wert ist **Wahr**, wenn IKE aktiviert ist, und **Falsch**, wenn IKE deaktiviert ist.

Hinweis Wenn IKE deaktiviert ist, funktionieren VPN-Konfigurationen nicht.

Aggressive-Modus aktivieren

Der Wert ist **Wahr**, wenn der Aggressive-Modus aktiviert ist, und **Falsch**, wenn er deaktiviert ist. Mit dem Aggressive-Modus können Sie RADIUS-Tunnelattribute für einen IPSec-Peer angeben und eine IKE-Agressive-Modus-Aushandlung mit den Tunnelattributen initiieren.

XAuth-Timeout

Die Anzahl der Sekunden, die der Router auf die Antwort eines Systems auf eine XAuth-Anforderung warten soll.

IKE-Identität

Entweder der Hostname des Routers oder die IP-Adresse, mit der der Router sich selbst bei IKE-Aushandlungen identifiziert.

Dead-Peer-Erkennung (DPD)

DPD ermöglicht es einem Router, einen inaktiven Peer zu ermitteln und in diesem Fall die IPSec- und die IKE-Security-Associations (Sicherheitsverknüpfungen) mit diesem Peer zu löschen.

IKE-Keepalive (Sek.)

Der Wert ist die Anzahl der Sekunden, die der Router zwischen dem Senden von IKE-Keepalive-Paketen wartet.

IKE Retry (Sek.)

Der Wert ist die Anzahl der Sekunden, die der Router zwischen den Versuchen wartet, eine IKE-Verbindung mit dem Remote-Peer aufzubauen. Standardmäßig wird **2** Sekunden angezeigt.

DPD-Typ

Entweder **Bei Bedarf** oder **Periodisch**.

Ist die Funktion auf **Bei Bedarf** eingestellt, werden DPD-Nachrichten auf der Grundlage von Datenverkehrsmustern gesendet. Wenn ein Router beispielsweise abgehenden Datenverkehr senden muss und die Aktivität des Peers fragwürdig ist, sendet der Router eine DPD-Nachricht, um den Status des Peers abzufragen. Muss der Router keine Daten weiterleiten, sendet er auch keine DPD-Nachricht.

Ist die Funktion auf **Periodisch** eingestellt, sendet der Router in dem Intervall DPD-Nachrichten, das durch den IKE Keepalive-Wert festgelegt ist.

IPSec Security Association-(SA-)Gültigkeitsdauer (Sek.)

Der Zeitraum, nachdem IPSec Security Associations (SAs) ablaufen und neu generiert werden. Der Standard ist 3600 Sekunden (1 Stunde).

IPSec Security Association-(SA-)Gültigkeitsdauer (Kilobyte)

Die Anzahl an Kilobyte, die der Router über die VPN-Verbindung senden kann, bevor die IPSec SA abläuft. Die SA wird nach Erreichen der kürzesten Gültigkeitsdauer erneuert.

Globale VPN-Einstellungen: IKE

In diesem Fenster können Sie globale Einstellungen für IKE und IPSec angeben.

IKE aktivieren

Lassen Sie dieses Kontrollkästchen aktiviert, wenn Sie VPN verwenden möchten.

Vorsicht Wenn IKE deaktiviert ist, funktionieren VPN-Konfigurationen nicht.

Aggressive-Modus aktivieren

Mit dem Aggressive-Modus können Sie RADIUS-Tunnelattribute für einen IPSec-Peer angeben und eine IKE-Agressive-Modus-Aushandlung mit den Tunnelattributen initiieren.

Identität (dieses Routers)

In diesem Feld ist angegeben, wie der Router sich selbst identifiziert. Wählen Sie entweder **IP-Adresse** oder **Hostname**.

XAuth-Timeout

Die Anzahl der Sekunden, die der Router auf die Antwort eines Systems warten soll, für das eine XAuth-Authentifizierung erforderlich ist.

Dead Peer Detection (DPD) aktivieren

DPD ermöglicht es einem Router, einen inaktiven Peer zu ermitteln und in diesem Fall die IPSec- und die IKE-Security-Associations (Sicherheitsverknüpfungen) mit diesem Peer zu löschen.

Das Kontrollkästchen **Dead Peer Detection aktivieren** ist deaktiviert, wenn das vom Router verwendete Cisco IOS-Image DPD nicht unterstützt.

Keepalive

Geben Sie an, wie viele Sekunden der Router eine Verbindung beibehalten soll, wenn sie nicht verwendet wird.

Erneut versuchen

Geben Sie an, wie viele Sekunden der Router zwischen den Versuchen warten soll, eine IKE-Verbindung mit einem Peer aufzubauen. Der Standardwert ist 2 Sekunden.

DPD-Typ

Wählen Sie **Bei Bedarf** oder **Periodisch**.

Ist die Funktion auf **Bei Bedarf** eingestellt, werden DPD-Nachrichten auf der Grundlage von Datenverkehrsmustern gesendet. Wenn ein Router beispielsweise abgehenden Datenverkehr senden muss und die Aktivität des Peers fragwürdig ist, sendet der Router eine DPD-Nachricht, um den Status des Peers abzufragen. Muss der Router keine Daten weiterleiten, sendet er auch keine DPD-Nachricht.

Ist die Funktion auf **Periodisch** eingestellt, sendet der Router in dem Intervall DPD-Nachrichten, das durch den IKE Keepalive-Wert festgelegt ist.

Globale VPN-Einstellungen: IPSec

In diesem Fenster können Sie die globalen IPSec-Einstellungen bearbeiten.

Neuen Schlüssel authentifizieren und generieren nach jeweils

Aktivieren Sie dieses Kontrollkästchen, und geben Sie das Zeitintervall an, in dem der Router einen neuen Schlüssel authentifizieren und generieren soll. Wenn Sie keinen Wert angeben, authentifiziert und generiert der Router stündlich einen neuen Schlüssel.

Neuen Schlüssel generieren, nachdem der aktuelle Schlüssel das folgende Volumen verschlüsselt hat

Aktivieren Sie dieses Kontrollkästchen, und geben Sie an, wie viel Kilobyte mit dem aktuellen Schlüssel verschlüsselt werden sollen, bevor der Router einen neuen Schlüssel authentifiziert und generiert. Wenn Sie keinen Wert angeben, authentifiziert und generiert der Router einen neuen Schlüssel, nachdem der aktuelle Schlüssel 4.608.000 Kilobyte verschlüsselt hat.

Einstellungen für VPN-Schlüssel-Verschlüsselung

Das Fenster **Einstellungen für VPN-Schlüssel-Verschlüsselung** wird angezeigt, wenn das Cisco IOS-Abbild auf Ihrem Router die Typ-6-Verschlüsselung unterstützt, die auch als *VPN-Schlüssel-Verschlüsselung* bezeichnet wird. Sie können in diesem Fenster einen Master-Schlüssel angeben, der bei der Verschlüsselung von VPN-Schlüsseln (z. B. Pre-Shared Keys, Easy VPN-Schlüsseln und XAuth-Schlüsseln) verwendet werden soll. Wenn diese Schlüssel verschlüsselt sind, können sie nicht von jemandem gelesen werden, der die Konfigurationsdatei des Routers anzeigt.

VPN-Schlüssel-Verschlüsselung aktivieren

Aktivieren Sie dieses Kontrollkästchen, um die Verschlüsselung dieser Schlüssel zu aktivieren.

Aktueller Master-Schlüssel

Dieses Feld enthält Sternchen (*), wenn ein Master-Schlüssel konfiguriert wurde.

Neuer Master-Schlüssel

Geben Sie einen Master-Schlüssel in dieses Feld ein. Master-Schlüssel müssen mindestens 8 Zeichen lang sein und dürfen bis zu 128 Zeichen umfassen.

Master-Schlüssel bestätigen

Geben Sie den Master-Schlüssel zur Bestätigung in dieses Feld noch einmal ein. Wenn die Werte in diesem Feld und im Feld **Neuer Master-Schlüssel** nicht übereinstimmen, werden Sie von Cisco SDM aufgefordert, den Schlüssel erneut einzugeben.

KAPITEL 15

IP Security

IP Security (IPSec) ist ein Framework offener Standards, das Datenvertraulichkeit, Datenintegrität und Datenauthentifizierung zwischen teilnehmenden Peers bietet. IPSec stellt diese Sicherheitsdienste in der IP-Schicht bereit und setzt IKE ein, um auf der Grundlage der lokalen Richtlinie Protokolle und Algorithmen auszuhandeln und die Verschlüsselungs- und Authentifizierungsschlüssel zu generieren, die von IPSec verwendet werden sollen.

Mit Cisco SDM können Sie IPSec-Transformationssätze, -Regeln und -Richtlinien konfigurieren.

Verwenden Sie die IPSec-Baumstruktur, um zu den gewünschten IPSec-Konfigurationsfenstern zu wechseln.

IPSec-Richtlinien

Dieses Fenster zeigt die im Router konfigurierten IPSec-Richtlinien und die mit jeder Richtlinie verknüpften Crypto Maps an. IPSec-Richtlinien werden verwendet, um VPN-Verbindungen zu definieren. Weitere Informationen zu den Beziehungen zwischen IPSec-Richtlinien, Crypto Maps und VPN-Verbindungen finden Sie unter Weitere Informationen zu VPN-Verbindungen und IPSec-Richtlinien.

Symbol

Wenn dieses Symbol neben der IPSec-Richtlinie angezeigt wird, ist diese schreibgeschützt und kann nicht bearbeitet werden. Eine IPSec-Richtlinie kann schreibgeschützt sein, wenn sie Befehle enthält, die von Cisco SDM nicht unterstützt werden.

Name

Der Name dieser IPSec-Richtlinie.

Typ

Einer der folgenden Typen:

- ISAKMP – IKE wird für Erstellung der IPSec-Security-Verknüpfungen verwendet, um den in diesem Crypto Map-Eintrag definierten Datenverkehr zu schützen. Cisco SDM unterstützt folgende Crypto Maps: Internet Security Association- und Schlüsselverwaltungsprotokoll (Internet Security Association and Key Management Protocol, ISAKMP).
- **Manuell** – IKE wird nicht für die Verwendung von IPSec-Security-Association verwendet, um den in diesem Crypto Map-Eintrag definierten Datenverkehr zu schützen.

  Cisco SDM unterstützt nicht die Erstellung manueller Crypto Maps. Cisco SDM behandelt alle manuellen Crypto Maps als schreibgeschützt, die mit der Befehlszeilenschnittstelle (Command Line Interface, CLI) erstellt wurden.
- **Dynamisch** – Gibt an, dass sich dieser Crypto Map-Eintrag auf eine vorher bestehende dynamische Crypto Map bezieht. Dynamische Crypto Maps sind Richtlinienvorlagen, die bei der Verarbeitung von Aushandlungsanforderungen von einem Peer-IPSec-Gerät aus verwendet werden.

  Cisco SDM unterstützt nicht die Erstellung dynamischer Crypto Maps. Cisco SDM behandelt alle dynamischen Crypto Maps als schreibgeschützt, die mit der CLI erstellt wurden.

Crypto Maps in dieser IPSec-Richtlinie

Name

Der Name der IPSec-Richtlinie, deren Bestandteil die Crypto Map ist.

Seq.-Nr.

Wenn eine IPSec-Richtlinie in einer VPN-Verbindung verwendet wird, identifiziert die Kombination aus der Sequenznummer und dem Namen der IPSec-Richtlinie die Verbindung eindeutig.

Peers

Diese Spalte listet die IP-Adressen oder Hostnamen der in der Crypto Map angegebenen Peer-Geräte auf. Mehrere Peers werden durch Kommas getrennt.

Transformationssatz

Diese Spalte listet die in der Crypto Map verwendeten Transformationssätze auf.

Sätze mit dynamischen Crypto Maps in dieser IPSec-Richtlinie

Name des Satzes mit dynamischen Crypto Maps

Der Name dieses Satzes mit dynamischen Crypto Maps. Mit den Namen können Administratoren Informationen dazu erhalten, wie der Satz mit den Crypto Maps verwendet wird.

Sequenznummer

Die Sequenznummer für diesen Satz mit dynamischen Crypto Maps.

Typ

Der Typ ist immer **Dynamisch**.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen einer IPSec-Richtlinie zur Routerkonfiguration	Klicken Sie auf **Hinzufügen**.
Bearbeiten einer vorhandenen IPSec-Richtlinie	Wählen Sie die Richtlinie aus, und klicken Sie auf **Bearbeiten**.
Entfernen eines Crypto Map-Eintrags aus einer Richtlinie	Wählen Sie die Richtlinie aus, und klicken Sie auf **Bearbeiten**. Wählen Sie in diesem Fenster die Crypto Map aus, die Sie entfernen möchten, und klicken Sie auf **Löschen**. Klicken Sie anschließend auf **OK**, um zu diesem Fenster zurückzukehren.
Entfernen einer IPSec-Richtlinie	Wählen Sie die Richtlinie aus, und klicken Sie auf **Löschen**.

IPSec-Richtlinie hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um eine IPSec-Richtlinie hinzuzufügen oder zu bearbeiten.

Name

Der Name dieser IPSec-Richtlinie. Der Name kann ein beliebiger Satz an alphanumerischen Zeichen sein. Es kann eventuell hilfreich sein, Peer-Namen im Richtliniennamen zu integrieren, oder andere Informationen, die Hinweise für Sie enthalten, hinzuzufügen.

Crypto Maps in dieser IPSec-Richtlinie

Dieses Feld listet die Crypto Maps in dieser IPSec-Richtlinie auf. Die Liste enthält den Namen, die Sequenznummer und den Transformationssatz, aus dem diese Crypto Map besteht. Sie können eine Crypto Map auswählen und diese bearbeiten oder aus der IPSec-Richtlinie löschen.

Wenn Sie eine Crypto Map bearbeiten möchten, klicken Sie auf **Hinzufügen**. Wenn Cisco SDM Sie durch den Prozess leiten soll, aktivieren Sie **Hinzufügen-Assistenten verwenden**, und klicken Sie anschließend auf **Hinzufügen**.

Symbol

Wenn eine Crypto Map schreibgeschützt ist, wird das Symbol für Schreibgeschützt in dieser Spalte angezeigt. Eine Crypto Map kann schreibgeschützt sein, wenn sie Befehle enthält, die von Cisco SDM nicht unterstützt werden.

Sätze mit dynamischen Crypto Maps in dieser IPSec-Richtlinie

Dieses Feld listet die dynamischen Crypto Maps in dieser IPSec-Richtlinie auf. Verwenden Sie die Schaltfläche **Hinzufügen**, um einen bestehenden Satz mit dynamischen Crypto Maps zu der Richtlinie hinzuzufügen. Verwenden Sie die Schaltfläche **Löschen**, um einen ausgewählten Satz mit dynamischen Crypto Maps aus der Richtlinie zu entfernen.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen einer Crypto Map zu dieser Richtlinie	Klicken Sie auf **Hinzufügen**, und erstellen Sie eine Crypto Map in den Bereichen **Crypto Map hinzufügen**. Oder aktivieren Sie **Hinzufügen-Assistenten verwenden**, und klicken Sie anschließend auf **Hinzufügen**. **Hinweis** Mit dem Assistenten können Sie nur einen Transformationssatz zur Crypto Map hinzufügen. Wenn Sie mehrere Transformationssätze in der Crypto Map benötigen, verwenden Sie nicht den Assistenten.
Bearbeiten einer Crypto Map in dieser Richtlinie	Wählen Sie die Crypto Map aus, klicken Sie auf **Bearbeiten**, und bearbeiten Sie die Crypto Map in den Bereichen **Crypto Map bearbeiten**.
Entfernen einer Crypto Map aus dieser Richtlinie	Wählen Sie die Crypto Map aus, und klicken Sie auf **Löschen**.

Crypto Map hinzufügen oder bearbeiten: Allgemeines

Ändern Sie die allgemeinen Crypto Map-Parameter über dieses Fenster. Dieses Fenster enthält die folgenden Felder.

Name der IPSec-Richtlinie

Ein schreibgeschütztes Feld, das den Namen der Richtlinie enthält, der für diese Crypto Map verwendet wird. Dieses Feld wird nicht angezeigt, wenn Sie den Crypto Map-Assistenten verwenden.

Beschreibung

Geben Sie in dieses Feld eine Beschreibung der Crypto Map ein, oder bearbeiten Sie hier eine Beschreibung. Diese Beschreibung wird in der Liste der VPN-Verbindungen angezeigt. Sie kann Sie dabei unterstützten, diese Crypto Map von anderen in derselben IPSec-Richtlinie zu unterscheiden.

Sequenznummer

Eine Nummer, die zusammen mit dem IPSec-Richtliniennamen verwendet wird, um eine Verbindung zu identifizieren. Cisco SDM erstellt die Sequenznummer automatisch. Wenn Sie möchten, können Sie Ihre eigene Sequenznummer eingeben.

Security Association-Gültigkeitsdauer

IPSec Security Associations verwenden gemeinsame Schlüssel. Diese Schlüssel und deren Security Associations haben dieselbe Gültigkeitsdauer. Es gibt zwei Typen der Gültigkeitsdauer: eine zeitbezogene Gültigkeitsdauer und eine datenverkehrsbezogene Gültigkeitsdauer. Die Security Association läuft ab, wenn der erste dieser Gültigkeitszeiträume überschritten wurde.

Sie können dieses Feld verwenden, um eine andere Security Association-Gültigkeitsdauer als die global festgelegte Gültigkeitsdauer für diese Crypto Map anzugeben. Im Feld **Kilobyte** können Sie die Gültigkeitsdauer nach der Anzahl der gesendeten Kilobyte bis zu einem Höchstwert von 4608000 festlegen. In den Feldern **HH:MM:SS** können Sie diese Dauer in Stunden, Minuten und Sekunden angeben. Gleichzeitig können Sie auch eine zeitbezogene und eine datenverkehrsbezogene Gültigkeitsdauer festlegen. Wenn beide Werte angegeben sind, läuft die Gültigkeitsdauer ab, wenn das erste Kriterium zutrifft.

Perfect Forwarding Secrecy aktivieren

Wenn Sicherheitsschlüssel von einem vorher generierten Schlüssel bezogen werden, besteht ein Sicherheitsproblem, denn wenn ein Schlüssel kompromittiert werden kann, bedeutet das, dass auch eine Kompromittierung der anderen Schlüssel möglich ist. Mit Perfect Forwarding Secrecy (PFS) wird sichergestellt, dass jeder Schlüssel unabhängig voneinander abgerufen wird. So wird sichergestellt, dass bei der Kompromittierung eines Schlüssels nicht auch die anderen Schlüssel betroffen sind. Wenn Sie PFS aktivieren, können Sie angeben, dass die Methode **Diffie-Hellman group1**, **group2** oder **group5** verwendet werden soll.

Hinweis Wenn Ihr Router **group5** nicht unterstützt, wird sie nicht in der Liste angezeigt.

Reverse Route Injection aktivieren

Reverse Route Injection (RRI) wird verwendet, um Einträge in der Routingtabelle eines internen Routers zu erstellen, auf dem das Open Shortest Path First-(OSPF-)Protokoll oder das Routing Information-Protokoll (RIP) für Remote-VPN-Clients oder LAN-to-LAN-Sitzungen ausgeführt wird.

Reverse Route Injection fügt dynamisch statische Routen zu den Clients hinzu, die mit dem Easy VPN-Server verbunden sind.

Crypto Map hinzufügen oder bearbeiten: Peer-Informationen

Eine Crypto Map enthält die Hostnamen oder IP-Adressen der Peers, die an der Security Association beteiligt sind. In diesem Bildschirm können Sie Peers, die mit dieser Crypto Map verknüpft sind, hinzufügen und entfernen. Mehrere Peers bieten dem Router mehrere Routen für verschlüsselte Daten.

Aufgabe	Vorgehensweise
Hinzufügen eines Peers zu **Aktuelle Liste**	Geben Sie die IP-Adresse oder den Hostnamen des Peers ein, und klicken Sie auf **Hinzufügen**.
Entfernen eines Peers aus **Aktuelle Liste**	Wählen Sie den Peer aus, und klicken Sie auf **Entfernen**.

Crypto Map hinzufügen oder bearbeiten: Transformationssätze

In diesem Fenster können Sie den Transformationssatz hinzufügen und bearbeiten, der in der Crypto Map verwendet wird. Eine Crypto Map enthält die Hostnamen oder IP-Adressen der Peers, die an der Security Association beteiligt sind. Mehrere Peers bieten dem Router mehrere Routen für verschlüsselte Daten. Die Geräte auf beiden Seiten der VPN-Verbindung müssen allerdings denselben Transformationssatz verwenden.

Verwenden Sie den Crypto Map-Assistenten, wenn die Crypto Map in Ihrem Router mit nur einem Transformationssatz ausreicht.

Verwenden Sie die Option **Neue Crypto Map hinzufügen...**, und deaktivieren Sie **Hinzufügen-Assistenten verwenden**, wenn Sie eine Crypto Map mit mehreren Transformationssätzen (bis zu sechs) manuell konfigurieren und auf diese Weise sicherstellen möchten, dass vom Router wenigstens ein Transformationssatz angeboten wird, der vom Peer, mit dem der Router die Verbindung aushandelt, akzeptiert wird. Wenn Sie sich bereits im Crypto Map-Assistenten befinden, beenden Sie diesen, deaktivieren Sie **Hinzufügen-Assistenten verwenden**, und klicken Sie auf **Neue Crypto Map hinzufügen...**.

Eine Crypto Map können Sie manuell mit mehreren Transformationssätzen konfigurieren und für diese auch eine bestimmte Reihenfolge bestimmen. Diese Reihenfolge beachtet der Router anschließend beim Aushandeln des zu verwendenden Transformationssatzes.

Verfügbare Transformationssätze

Konfigurierte Transformationssätze, die für die Verwendung in Crypto Maps verfügbar sind. Im Crypto Map-Assistenten sind die verfügbaren Transformationssätze in der Dropdown-Liste **Transformationssatz auswählen** untergebracht.

Wenn keine Transformationssätze im Router konfiguriert wurden, werden nur die Standard-Transformationssätze angezeigt, die in Cisco SDM enthalten sind.

Hinweis

- Nicht alle Router unterstützen alle Transformationssätze (Verschlüsselungstypen). Nicht unterstützte Transformationssätze werden in dem Fenster nicht angezeigt.
- Nicht alle IOS-Abbilder unterstützen alle von Cisco SDM unterstützten Transformationssätze. Transformationssätze, die nicht vom IOS-Abbild unterstützt werden, werden in dem Fenster nicht angezeigt.
- Wenn die Hardwareverschlüsselung aktiviert ist, werden nur die Transformationssätze in dem Fenster angezeigt, die sowohl von der Hardwareverschlüsselung als auch vom IOS-Abbild unterstützt werden.

Details zum ausgewählten Transformationssatz (nur Crypto Map-Assistent)

Zeigt den Namen, die Verschlüsselung, Authentifizierungsmerkmale und andere Parameter der gewählten Crypto Map an.

Wenn dieses Symbol neben dem Transformationssatz angezeigt wird, ist er schreibgeschützt und kann nicht bearbeitet werden.

Ausgewählte Transformationssätze in bevorzugter Reihenfolge (nur bei manueller Crypto Map-Konfiguration)

Die Transformationssätze, die für diese Crypto Map gewählt wurden, in der Reihenfolge, in der sie verwendet werden. Während der Aushandlung der Parameter mit einem Peer bietet der Router Transformationssätze in der Reihenfolge an, die von dieser Liste vorgegeben wird. Sie können die Reihenfolge über die nach oben und nach unten gerichteten Pfeilschaltflächen ändern.

Welche Aufgabe möchten Sie ausführen? (Nur Crypto Map-Assistent)

Aufgabe	Vorgehensweise
Verwenden des ausgewählten Transformationssatzes für die Crypto Map	Klicken Sie auf **Weiter**.
Verwenden eines anderen Transformationssatzes	Markieren Sie ihn in der Liste **Transformationssatz auswählen**, und klicken Sie auf **Weiter**.
Verwenden eines neuen Transformationssatzes	Klicken Sie auf **Hinzufügen**, und erstellen Sie den Transformationssatz im Fenster **Transformationssatz hinzufügen**. Kehren Sie dann zu diesem Fenster zurück, und klicken Sie auf **Weiter**.
Bearbeiten des ausgewählten Transformationssatzes	Klicken Sie auf **Bearbeiten**, und bearbeiten Sie den Transformationssatz im Fenster **Transformationssatz bearbeiten**.
Hinzufügen weiterer Transformationssätze zu dieser Crypto Map. Sie sollten auf diese Weise sicherstellen, dass der Router einen Transformationssatz anbieten kann, den der Peer akzeptiert.	Verlassen Sie den Crypto Map-Assistenten, deaktivieren Sie **Hinzufügen-Assistenten verwenden**, und klicken Sie auf **Crypto Map hinzufügen**. Auf der Registerkarte **Transformationssatz** können Sie Transformationssätze hinzufügen und ihre Reihenfolge festlegen.

Welche Aufgabe möchten Sie ausführen? (Nur manuelle Crypto Map-Konfiguration)

Aufgabe	Vorgehensweise
Hinzufügen eines Transformationssatzes zum Feld **Ausgewählte Transformationssätze**	Wählen Sie einen Transformationssatz im Feld **Verfügbare Transformationssätze** aus, und klicken Sie auf die nach rechts gerichtete Pfeilschaltfläche.
Entfernen eines Transformationssatzes aus dem Feld **Ausgewählte Transformationssätze**	Wählen Sie den Transformationssatz, den Sie entfernen möchten, aus, und klicken Sie auf die nach links gerichtete Pfeilschaltfläche.
Ändern der bevorzugten Reihenfolge der ausgewählten Transformationssätze	Wählen Sie einen Transformationssatz aus, und klicken Sie auf die nach oben oder nach unten gerichtete Pfeilschaltfläche.

Aufgabe	Vorgehensweise
Hinzufügen eines Transformationssatzes zur Liste **Verfügbare Transformationssätze**	Klicken Sie auf **Hinzufügen**, und konfigurieren Sie den Transformationssatz im Fenster **Transformationssatz hinzufügen**.
Bearbeiten eines Transformationssatzes in der Liste **Verfügbare Transformationssätze**	Klicken Sie auf **Bearbeiten**, und konfigurieren Sie den Transformationssatz im Fenster **Transformationssatz bearbeiten**.

Crypto Map hinzufügen oder bearbeiten: Schutz des Datenverkehrs

Crypto Map können Sie so einstellen, dass der gesamte Datenverkehr (nur Crypto Map-Assistent) geschützt wird, oder Sie können den Schutz anhand einer IPSec-Regel auf einen bestimmten Datenverkehr beschränken.

Gesamten Datenverkehr zwischen den folgenden Subnetzen schützen (nur Crypto Map-Assistent)

Geben Sie mit dieser Option ein einzelnes Quell-Subnetz (ein Subnetz im LAN) an, dessen Datenverkehr Sie verschlüsseln möchten, weiterhin ein Ziel-Subnetz, das von dem Peer unterstützt wird, den Sie im Fenster **Peers** angegeben haben. Der gesamte Datenverkehr zwischen anderen Quell- und Ziel-Subnetzen wird unverschlüsselt übertragen.

Quelle

Geben Sie die Adresse des Subnetzes ein, dessen ausgehenden Datenverkehr Sie schützen möchten. Geben Sie außerdem die Subnetzmaske an. Sie können eine Subnetzmaske aus der Liste auswählen oder eine benutzerdefinierte Maske eingeben. Die Subnetznummer und die Maske müssen im durch Punkte getrennten Dezimalformat eingegeben werden. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Der gesamte Datenverkehr von diesem Quell-Subnetz, dessen Ziel-IP-Adresse sich im Ziel-Subnetz befindet, wird verschlüsselt.

Ziel

Geben Sie die Adresse des Ziel-Subnetzes ein, und geben Sie die Maske für dieses Subnetz an. Sie können eine Subnetzmaske aus der Liste auswählen oder eine benutzerdefinierte Maske eingeben. Die Subnetznummer und die Maske müssen im durch Punkte getrennten Dezimalformat eingegeben werden.

Der gesamte Datenverkehr, der zu den Hosts in diesem Subnetz geht, wird verschlüsselt.

IPSec-Regel (Zugriffsliste für IPSec-Datenverkehr erstellen/auswählen)

Die in dieser Crypto Map verwendete IPSec-Regel können Sie hinzuzufügen oder bearbeiten. Verwenden Sie diese Option, wenn Sie mehrere Quellen und Ziele und/oder bestimmte Typen von Datenverkehr angeben müssen, die verschlüsselt werden sollen. Eine IPSec-Regel kann aus mehreren Einträgen bestehen, die unterschiedliche Datenverkehrstypen und unterschiedliche Quellen und Ziele angeben. Pakete, die die in der IPSec-Regel angegebenen Kriterien nicht erfüllen, werden unverschlüsselt gesendet.

Hinweis Wenn Sie eine IPSec-Regel für eine VPN-Verbindung hinzufügen, die eine Tunnelschnittstelle verwendet, muss die Regel dieselben Quell- und Zieldaten wie die Tunnelkonfiguration angeben.

Klicken Sie auf die Schaltfläche **…** rechts neben dem Feld **IPSec-Regel**, und wählen Sie eine der folgenden Optionen, um die IPSec-Regel für die Crypto Map hinzuzufügen oder zu ändern.

- **Vorhandene Regel (ACL) auswählen** - Wenn die gewünschte Regel bereits erstellt ist, wählen Sie die Regel aus, und klicken Sie auf **OK**.
- **Neue Regel (ACL) erstellen und auswählen** - Wenn die gewünschte Regel noch nicht erstellt wurde, erstellen Sie sie, und klicken Sie danach auf **OK**.
- **Keine** - Dient zum Aufheben einer Regelverknüpfung. Im Feld **IPSec-Regel** wird der Name der benutzten IPSec-Regel angezeigt. Wenn Sie aber **Keine** auswählen, ist das Feld leer.

Als alternative Möglichkeit zur Eingabe oder Änderung einer IPSec-Regel für diese Crypto Map können Sie die Nummer der IPSec-Regel auch direkt in das Feld **IPSec-Regel** eintragen.

Hinweis IPSec-Regeln müssen erweiterte Regeln sein, Standardregeln sind nicht zulässig. Wenn die von Ihnen eingegebene Nummer bzw. der eingegebene Name eine Standardregel identifiziert, zeigt Cisco SDM eine Warnmeldung an, wenn Sie auf **OK** klicken.

Sätze mit dynamischen Crypto Maps

Dieses Fenster listet die dynamischen Crypto Maps auf, die im Router konfiguriert sind.

Schaltfläche Hinzufügen/Bearbeiten/Löschen

Verwenden Sie diese Schaltflächen, um Crypto Maps im Fenster zu verwenden. Wenn Sie versuchen, einen Satz mit einer Crypto Map, der mit einer IPSec-Richtlinie verknüpft ist, zu löschen, verhindert Cisco SDM diesen Schritt. Sie müssen die Verknüpfung der Crypto Map mit der Richtlinie entfernen, bevor Sie sie löschen können. Dieser Vorgang kann über das Fenster **IPSec-Richtlinien** ausgeführt werden.

Name

Der Name der dynamischen Crypto Map.

Typ

Der Typ ist immer **Dynamisch**.

Satz mit dynamischen Crypto Maps hinzufügen/bearbeiten

In diesem Fenster können Sie einen Satz mit dynamischen Crypto Maps hinzufügen oder bearbeiten.

Name

Wenn Sie eine dynamische Crypto Map hinzufügen, geben Sie den Namen in dieses Feld ein. Wenn Sie einen Satz mit Crypto Maps bearbeiten, ist dieses Feld deaktiviert, und Sie können den Namen nicht ändern.

Crypto Maps in dieser IPSec-Richtlinie

Dieser Bereich listet die Crypto Maps auf, die in diesem Satz verwendet werden. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um Crypto Maps zu dieser Liste hinzuzufügen, aus dieser Liste zu entfernen oder in dieser Liste zu bearbeiten.

Crypto Map mit dieser IPSec-Richtlinie verknüpfen

Sequenznummer

Geben Sie eine Sequenznummer ein, die diesen Satz mit Crypto Maps identifiziert. Diese Sequenznummer darf nicht in einem anderen Satz mit Crypto Maps verwendet werden.

Satz mit dynamischen Crypto Maps auswählen

Wählen Sie den Satz mit dynamischen Crypto Maps aus, den Sie aus dieser Liste hinzufügen möchten.

Crypto Maps in diesem Satz mit dynamischen Crypto Maps

Dieser Bereich listet die Namen, Sequenznummer und Peers in dem von Ihnen ausgewählten Satz mit dynamischen Crypto Maps auf.

IPSec-Profile

Dieses Fenster listet die IPSec-Profile auf, die im Router konfiguriert sind. IPSec-Profile bestehen aus einem oder mehreren konfigurierten Transformationssätzen; die Profile werden auf mGRE-Tunnel angewendet, um anzugeben, wie der Tunneldatenverkehr verschlüsselt wird.

Name

Der Name des IPSec-Profils.

Transformationssatz

Die in diesem Profil verwendeten Transformationssätze.

Beschreibung

Eine Beschreibung des IPSec-Profils.

Hinzufügen

Klicken Sie auf diese Schaltfläche, um ein neues IPSec-Profil hinzuzufügen.

Bearbeiten

Wählen Sie ein vorhandenes Profil aus, und klicken Sie auf **Bearbeiten**, um die Profilkonfiguration zu ändern.

Löschen

Klicken Sie auf diese Schaltfläche, um ein ausgewähltes IPSec-Profil zu bearbeiten. Wenn das Profil, das Sie löschen, derzeit in einem DMVPN-Tunnel verwendet wird, müssen Sie den DMVPN-Tunnel für die Verwendung eines anderen IPSec-Profils konfigurieren.

Details zum IPSec-Profil

Dieser Bereich zeigt die Konfiguration des gewählten IPSec-Profils an. Lesen Sie IPSec-Profil hinzufügen oder bearbeiten, um eine Erläuterung zu den dargestellten Informationen zu erhalten.

IPSec-Profil hinzufügen oder bearbeiten

Geben Sie die Informationen ein, um in diesem Dialogfeld ein IPSec-Profil zu erstellen. Ein IPSec-Profil gibt die zu verwendenden Transformationssätze an, legt fest, wie die Security Association (SA)-Gültigkeitsdauer bestimmt wird und liefert weitere Informationen.

Spalte „Transformationssatz“

Verwenden Sie die zwei Spalten oben im Dialogfeld, um die Transformationssätze anzugeben, die Sie in das Profil einbeziehen möchten. Die Spalte auf der linken Seite enthält die Transformationssätze, die auf dem Router konfiguriert sind. Um einen konfigurierten Transformationssatz zum Profil hinzuzufügen, klicken Sie auf die Schaltfläche **>>**. Wenn sich in der linken Spalte keine Transformationssätze befinden oder wenn Sie einen Transformationssatz benötigen, der noch nicht erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen den Transformationssatz im angezeigten Dialogfeld.

IKE-Profil-Zuordnung

Wenn Sie ein IKE-Profil mit diesem IPSec-Profil verknüpfen möchten, wählen Sie aus der Liste ein vorhandenes Profil aus. Wenn eine IKE-Profil bereits verknüpft wurde, ist dieses Feld schreibgeschützt.

Zeitbasierte IPSec SA-Gültigkeitsdauer

Klicken Sie auf **Zeitbasierte IPSec SA-Gültigkeitsdauer**, wenn eine neue SA erstellt werden soll, nachdem eine festgelegte Zeitspanne abgelaufen ist. Geben Sie die Zeitspanne in den Feldern HH:MM:SS auf der rechten Seite ein.

Datenverkehrvolumen-basierte IPSec SA-Gültigkeitsdauer

Klicken Sie auf **Datenverkehrvolumen-basierte IPSec SA-Gültigkeitsdauer**, wenn eine neue SA erstellt werden soll, nachdem eine bestimmte Menge Datenverkehr durch den IPSec-Tunnel geströmt ist. Geben Sie die Zahl in Kilobyte ein, die durch den Tunnel passieren sollte, bevor eine vorhandene aufgehoben und eine neue eingerichtet wird.

IPSec SA-Ruhezustand

Klicken Sie auf **IPSec SA-Ruhezustand**, wenn eine neue SA erstellt werden soll, nachdem der Peer eine gewisse Zeit untätig war. Geben Sie die Ruhezustandszeit in den Feldern HH:MM:SS auf der rechten Seite ein.

Perfect Forward Secrecy

Klicken Sie auf **Perfect Forwarding Secrecy**, wenn IPSec Perfect Forwarding Secrecy (PFS) anfordern sollte, wenn es neue Security Associations für diese virtuelle Vorlagenschnittstelle anfordert oder PFS bei vom Peer erhaltenen Anforderungen PFS anfordern sollte. Sie können die folgenden Werte angeben:

- group1 – Die 768-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.
- group2 – Die 1024-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.
- group5 – Die 1536-Bit Diffie Hellman-Prime Modulus-Gruppe wird für die Verschlüsselung der PFS-Anforderung verwendet.

IPSec-Profil hinzufügen/bearbeiten und Dynamische Crypto Map hinzufügen

Verwenden Sie dieses Fenster, um ein IPSec-Profil hinzuzufügen oder zu bearbeiten oder um eine dynamische Crypto Map hinzuzufügen.

Name

Geben Sie einen Namen für dieses Profil ein.

Verfügbare Transformationssätze

Diese Spalte listet die in diesem Router konfigurierten Transformationssätze auf. Um einen Transformationssatz aus dieser Liste zu der Spalte **Ausgewählte Transformationssätze** hinzuzufügen, wählen Sie einen Transformationssatz aus, und klicken Sie auf die Schaltfläche mit dem Rechtspfeil (**>>**).

Wenn Sie einen neuen Transformationssatz konfigurieren müssen, klicken Sie in der IPSec-Baumstruktur auf **Transformationssätze**, um zum Fenster **Transformationssätze** zu wechseln. Klicken Sie in diesem Fenster auf **Hinzufügen**, um einen neuen Transformationssatz zu erstellen.

Ausgewählte Transformationssätze

Diese Spalte listet die in diesem Profil verwendeten Transformationssätze auf. Sie können mehrere Transformationssätze auswählen, sodass der von Ihnen konfigurierte Router und der Router am anderen Ende des Tunnels aushandeln können, welcher Transformationssatz verwendet wird.

Transformationssatz

In diesem Bildschirm können Sie Transformationssätze anzeigen, neue hinzufügen und bestehende Transformationssätze bearbeiten oder entfernen. Ein Transformationssatz ist eine bestimmte Kombination aus Sicherheitsprotokollen und Algorithmen. Während der IPSec Security Association-Aushandlung vereinbaren die Peers, einen bestimmten Transformationssatz zum Schutz eines bestimmten Datenflusses zu verwenden.

Sie können mehrere Transformationssätze erstellen und dann einen oder mehrere dieser Sätze in einem Crypto Map-Eintrag angeben. Der im Crypto Map-Eintrag definierte Transformationssatz wird in der IPSec Security Association-Aushandlung verwendet, um die Datenübertragung zu schützen, die von dieser Zugriffsliste des Crypto Map-Eintrags angegeben wird.

Während der IPSec Security Association-Aushandlungen mit IKE suchen die Peers einen Transformationssatz, der für beide Peers identisch ist. Wenn der Transformationssatz gefunden wurde, wird dieser ausgewählt und auf den geschützten Datenverkehr als Teil der IPSec Security Associations beider Peers angewendet.

Name

Name, der dem Transformationssatz zugewiesen ist.

ESP-Verschlüsselung

Cisco SDM erkennt die folgenden ESP-Verschlüsselungstypen:

- ESP_DES – Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES unterstützt 56-Bit-Verschlüsselung.
- ESP_3DES – ESP, Triple DES. Dies ist eine stärkere Verschlüsselungsform als DES, die 168-Bit-Verschlüsselung unterstützt.

- ESP_AES_128 – ESP, Advanced Encryption Standard (AES). Verschlüsselung mit einem 128-Bit-Schlüssel AES bietet eine höhere Sicherheit als DES und ist für rechenintensive Aufgaben effizienter als 3DES.
- ESP_AES_192 – ESP, AES-Verschlüsselung mit einem 192-Bit-Schlüssel.
- ESP_AES_256 – ESP, AES-Verschlüsselung mit einem 256-Bit-Schlüssel.
- ESP_NULL – Null-Verschlüsselungsalgorithmus, es wird jedoch eine Verschlüsselungstransformation verwendet.
- ESP_SEAL – ESP mit dem 160-Bit-Schlüssel mit Verschlüsselungsalgorithmus Software Encryption Algorithm (SEAL). SEAL (Software Encryption Algorithm) ist ein alternativer Algorithmus zum softwarebasierten Data Encryption Standard (DES), Triple DES (3DES) und Advanced Encryption Standard (AES). SEAL-Verschlüsselung verwendet eine 160-Bit-Verschlüsselung und führt im Vergleich zu anderen softwarebasierten Algorithmen zu einer geringeren Auslastung des Prozessors.

ESP-Integrität

Gibt den verwendeten Integritätsalgorithmus an. Diese Spalte enthält einen Wert, wenn der Transformationssatz so konfiguriert ist, dass er sowohl Datenintegrität als auch Verschlüsselung bereitstellt. Diese Spalte enthält einen der folgenden Werte:

- ESP-MD5-HMAC – Message Digest 5, Hashed Message Authentication Codes (HMAC)
- ESP-SHA-HMAC – Security Hash Algorithm, HMAC

AH-Integrität

Gibt den verwendeten Integritätsalgorithmus an. Diese Spalte enthält einen Wert, wenn der Transformationssatz so konfiguriert ist, dass er Datenintegrität, aber keine Verschlüsselung bereitstellt. Diese Spalte enthält einen der folgenden Werte:

- AH-MD5-HMAC – Message Digest 5
- AH-SHA-HMAC – Security Hash Algorithm

IP-Kompression

Gibt an, ob IP-Datenkompression verwendet wird.

Hinweis Wenn Ihr Router keine IP-Kompression unterstützt, ist dieses Feld deaktiviert.

Modus

Diese Spalte enthält einen der folgenden Werte:

- **Tunnel** – Sowohl Header als auch Daten sind verschlüsselt. Der in VPN-Konfigurationen verwendete Modus.
- **Transport** – Nur Daten werden verschlüsselt. Dieser Modus wird verwendet, wenn die Verschlüsselungsendpunkte und die Kommunikationsendpunkte identisch sind.

Typ

Entweder **Benutzerdefiniert** oder **Cisco SDM-Standard**.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen eines neuen Transformationssatzes zur Routerkonfiguration	Klicken Sie auf **Hinzufügen**, und erstellen Sie den Transformationssatz im Fenster **Transformationssatz hinzufügen**.

Aufgabe	Vorgehensweise
Bearbeiten eines vorhandenen Transformationssatzes	Wählen Sie den Transformationssatz aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann den Transformationssatz im Fenster **Transformationssatz bearbeiten**.  **Hinweis** Cisco SDM-Standard-Transformationssätze sind schreibgeschützt und können nicht bearbeitet werden.
Löschen eines vorhandenen Transformationssatzes	Wählen Sie den Transformationssatz aus, und klicken Sie auf **Löschen**.  **Hinweis** Cisco SDM-Standard-Transformationssätze sind schreibgeschützt und können nicht gelöscht werden.

Transformationssatz hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um einen Transformationssatz hinzuzufügen oder zu bearbeiten.

Eine Beschreibung der zulässigen Transformationskombinationen und Beschreibungen der Transformationen erhalten Sie, indem Sie auf **Zulässige Transformationskombinationen** klicken.

Hinweis

- Nicht alle Router unterstützen alle Transformationssätze (Verschlüsselungstypen). Nicht unterstützte Transformationssätze werden nicht im Bildschirm angezeigt.
- Nicht alle IOS-Abbilder unterstützen alle von Cisco SDM unterstützten Transformationssätze. Transformationssätze, die nicht vom IOS-Abbild unterstützt werden, werden nicht im Bildschirm angezeigt.
- Wenn die Hardwareverschlüsselung aktiviert ist, werden nur die Transformationssätze im Bildschirm angezeigt, die sowohl von der Hardwareverschlüsselung als auch vom IOS-Abbild unterstützt werden.
- Easy VPN-Server unterstützen nur den Tunnelmodus. Der Transportmodus wird nicht von Easy VPN-Servern unterstützt.

- Easy VPN-Server unterstützen nur Transformationssätze mit ESP-Verschlüsselung. Easy VPN-Server unterstützten nicht den AH-Algorithmus.
- Easy VPN-Server unterstützen nicht die ESP-SEAL-Verschlüsselung.

Name dieses Transformationssatzes

Dies kann ein beliebiger Name sein. Der Name muss nicht mit dem Namen im Transformationssatz übereinstimmen, den der Peer verwendet, es kann jedoch hilfreich sein, sich entsprechenden Transformationssätzen denselben Namen zu geben.

Datenintegrität und Verschlüsselung (ESP)

Aktivieren Sie dieses Feld, wenn Sie Encapsulating Security Payload-(ESP-)Datenintegrität und -Verschlüsselung bereitstellen möchten.

Integritätsalgorithmus

Wählen Sie eine der folgenden Typen:

- ESP_MD5_HMAC. Message Digest 5.
- ESP_SHA_HMAC. Security Hash Algorithm.

Verschlüsselung

Cisco SDM erkennt die folgenden ESP-Verschlüsselungstypen:

- ESP_DES. Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES unterstützt 56-Bit-Verschlüsselung.
- ESP_3DES. ESP, Triple DES. Dies ist eine stärkere Verschlüsselungsform als DES, die 168-Bit-Verschlüsselung unterstützt.
- ESP_AES_128. ESP, Advanced Encryption Standard (AES). Verschlüsselung mit einem 128-Bit-Schlüssel AES bietet eine höhere Sicherheit als DES und ist für rechenintensive Aufgaben effizienter als 3DES.
- ESP_AES_192. ESP, AES-Verschlüsselung mit einem 192-Bit-Schlüssel.
- ESP_AES_256. ESP, AES-Verschlüsselung mit einem 256-Bit-Schlüssel.

- ESP_SEAL – ESP mit dem 160-Bit-Schlüssel mit Verschlüsselungsalgorithmus Software Encryption Algorithm (SEAL). SEAL (Software Encryption Algorithm) ist ein alternativer Algorithmus zum softwarebasierten Data Encryption Standard (DES), Triple DES (3DES) und Advanced Encryption Standard (AES). SEAL-Verschlüsselung verwendet eine 160-Bit-Verschlüsselung und führt im Vergleich zu anderen softwarebasierten Algorithmen zu einer geringeren Auslastung des Prozessors.
- ESP_NULL. Null-Verschlüsselungsalgorithmus, es wird jedoch eine Verschlüsselungstransformation verwendet.

Hinweis Die verfügbaren Typen der ESP-Verschlüsselung richten sich nach dem Router. Je nach dem Routertyp, den Sie konfigurieren, sind eventuell einer oder mehrere dieser Verschlüsselungstypen nicht verfügbar.

Daten- und Adressintegrität ohne Verschlüsselung (AH)

Dieses Kontrollkästchen und die Felder darunter werden angezeigt, wenn Sie auf **Erweiterte anzeigen** klicken.

Aktivieren Sie dieses Feld, wenn der Router Authentication Header-(AH-)Daten- und Adressintegrität bereitstellen soll. Der Authentication Header wird nicht verschlüsselt.

Integritätsalgorithmus

Wählen Sie eine der folgenden Typen:

- AH_MD5_HMAC – Message Digest 5.
- AH_SHA_HMAC – Security Hash Algorithm.

Modus

Wählen Sie aus, welche Teile des Datenverkehrs verschlüsselt werden sollen:

- **Transport. nur Datenverschlüsseln** – Der Transportmodus wird verwendet, wenn beide Endpunkte IPSec unterstützten. Dieser Modus positioniert den AH oder ESP nach dem ursprünglichen IP-Header, daher wird nur der IP-Payload verschlüsselt. Diese Methode ermöglicht es Benutzern, Netzwerkdienste wie QoS-Steuerelemente (Quality of Service – Dienstgüte) für verschlüsselte Pakete anzuwenden. Der Transportmodus sollte nur dann verwendet werden, wenn das Ziel der Daten immer der Remote-VPN-Peer ist.

- **Tunnel. Daten und IP-Header verschlüsseln** – Der Tunnelmodus bietet einen höheren Schutz als der Transportmodus. Da das gesamte IP-Paket innerhalb von AH oder ESP verschlüsselt ist, wird ein neuer IP-Header angefügt; das gesamte Datagramm kann so verschlüsselt werden. Mit dem Tunnelmodus können Netzwerkgeräte, wie ein Router, als IPSec-Proxy für mehrere VPN-Benutzer fungieren. Für diese Konfigurationen sollte der Tunnelmodus verwendet werden.

IP-Kompression (COMP-LZS)

Aktivieren Sie dieses Kontrollkästchen, wenn Datenkompression verwendet werden soll.

Hinweis Nicht alle Router unterstützen die IP-Kompression. Wenn Ihr Router keine IP-Kompression unterstützt, ist dieses Feld deaktiviert.

IPSec-Regeln

Dieses Fenster zeigt die IPSec-Regeln an, die für diesen Router konfiguriert sind. IPSec-Regeln definieren, welcher Datenverkehr von IPSec verschlüsselt wird. Der obere Bereich des Fensters listet die definierten Zugriffsregeln auf. Der untere Bereich des Fensters zeigt die Zugriffsregeleinträge für die in der Regelliste ausgewählte Zugriffsregel an.

IPSec-Regeln enthalten IP-Adressen- und Diensttypinformationen. Pakete, die die in der Regel angegebenen Kriterien erfüllen, werden verschlüsselt. Pakete, die die in der Regel angegebenen Kriterien nicht erfüllen, werden unverschlüsselt gesendet.

Name/Nummer

Der Name oder die Nummer dieser Regel.

Verwendet von

Gibt an, in welchen Crypto Maps diese Regel verwendet wird.

Typ

IPSec-Regeln müssen sowohl die Quelle als auch das Ziel definieren und müssen den Datenverkehrstyp angeben können, den das Paket enthält. Daher sind IPSec-Regeln erweiterte Regeln.

Beschreibung

Eine Beschreibung der Regel in Textform, falls verfügbar.

Aktion

Entweder **Zulassen** oder **Verweigern**. **Zulassen** bedeutet, dass Pakete, die mit den Kriterien in dieser Regel übereinstimmen, durch eine Verschlüsselung geschützt sind. **Verweigern** bedeutet, dass übereinstimmende Pakete unverschlüsselt gesendet werden. Weitere Informationen finden Sie unter Bedeutung der Schlüsselwörter Zulassen und Verweigern.

Quelle

Eine IP-Adresse oder ein Schlüsselwort, die bzw. das die Quelle des Datenverkehrs angibt. **Alle** gibt an, dass die Quelle eine beliebige IP-Adresse sein kann. Eine IP-Adresse in dieser Spalte kann allein oder gefolgt von einer Platzhaltermaske angezeigt werden. Falls vorhanden, gibt die Platzhaltermaske die Teile der IP-Adresse an, mit der die Quell-IP-Adresse übereinstimmen müssen. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Ziel

Eine IP-Adresse oder ein Schlüsselwort, die bzw. das das Ziel des Datenverkehrs angibt. **Alle** gibt an, dass das Ziel eine beliebige IP-Adresse sein kann. Eine IP-Adresse in dieser Spalte kann allein oder gefolgt von einer Platzhaltermaske angezeigt werden. Falls vorhanden, gibt die Platzhaltermaske die Teile der IP-Adresse an, mit der die Ziel-IP-Adresse übereinstimmen müssen.

Dienst

Der Datenverkehrstyp, den das Paket enthalten muss.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Zugriffsregeleinträge für eine bestimmte Regel anzeigen	Wählen Sie die Regel aus der Regelliste aus. Die Einträge für diese Regel werden im unteren Feld angezeigt.
Hinzufügen einer IPSec-Regel	Klicken Sie auf **Hinzufügen**, und erstellen Sie die Regel im angezeigten Regelfenster.
Löschen einer IPSec-Regel	Wählen Sie die Regel aus der Regelliste aus, und klicken Sie auf **Löschen**.
Löschen eines bestimmten Regeleintrags	Wählen Sie die Regel aus der Regelliste aus, und klicken Sie auf **Bearbeiten**. Löschen Sie dann den Eintrag im angezeigten Regelfenster.
Anwenden einer IPSec-Regel auf eine Schnittstelle	Wenden Sie die Regel im Fenster **Konfiguration der Schnittstelle** an.

KAPITEL 16

Internet Key Exchange

Die Hilfethemen in diesem Abschnitt beschreiben die Internet Key Exchange (IKE) Konfigurationsbildschirme.

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) ist eine Standardmethode für eine sichere, authentifizierte Kommunikation. IKE erstellt Sitzungsschlüssel (und eine verknüpfte kryptografische und Netzwerkkonfiguration) zwischen zwei Hosts im Netzwerk.

Cisco SDM ermöglicht Ihnen die Erstellung von IKE-Richtlinien, die die Identität von Peers während der Authentifizierung schützen. Mit Cisco SDM können Sie darüber hinaus Pre-Shared Keys erstellen, die von den Peers ausgetauscht werden können.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Weitere Informationen zu IKE	Klicken Sie auf **Weitere Informationen zu IKE**.
Aktivieren von IKE Sie müssen IKE für VPN-Verbindungen zur Verwendung von IKE-Aushandlungen aktivieren.	Klicken Sie auf **Globale Einstellungen**, und klicken Sie dann auf **Bearbeiten**, um IKE zu aktivieren und andere globale Einstellungen für IKE vorzunehmen.

Aufgabe	Vorgehensweise
Erstellen einer IKE-Richtlinie Cisco SDM bietet eine Standard-IKE-Richtlinie; es kann jedoch nicht sicher davon ausgegangen werden, dass der Peer über dieselbe Richtlinie verfügt. Sie sollten andere IKE-Richtlinien konfigurieren, sodass der Router eine IKE-Richtlinie bereitstellen kann, die vom Peer akzeptiert wird.	Klicken Sie in der VPN-Baumstruktur auf **IKE-Richtlinie**. Weitere Informationen finden Sie unter IKE-Richtlinien.
Erstellen eines Pre-Shared Key Bei der Verwendung von IKE müssen die Peers an jedem Ende einen Pre-Shared Key austauschen, um eine gegenseitige Authentifizierung vorzunehmen.	Klicken Sie in der VPN-Baumstruktur auf **Pre-Shared Key**. Weitere Informationen finden Sie unter IKE-Pre-shared Keys.
Erstellen Sie ein IKE-Profil.	Klicken Sie in der VPN-Baumstruktur auf den Knoten **IKE-Profil**. Weitere Informationen finden Sie unter IKE-Profile.

IKE-Richtlinien

IKE-Aushandlungen müssen geschützt sein. Daher beginnt jede IKE-Aushandlung damit, dass alle Peers eine gemeinsame (shared) IKE-Richtlinie vereinbaren. Diese Richtlinie gibt an, welche Sicherheitsparameter verwendet werden, um spätere IKE-Aushandlungen zu schützen. Dieses Fenster zeigt die im Router konfigurierten IKE-Richtlinien an und ermöglicht Ihnen, eine IKE-Richtlinie hinzuzufügen, zu bearbeiten oder aus der Routerkonfiguration zu entfernen. Wenn keine IKE-Richtlinien im Router konfiguriert wurden, zeigt dieses Fenster die Standard-IKE-Richtlinie an.

Nachdem zwei Peers eine Richtlinie vereinbart haben, werden die Sicherheitsparameter der Richtlinie von einer Security Association identifiziert, die in jedem Peer eingerichtet wird. Diese Security Associations werden für sämtlichen später erfolgenden IKE-Datenverkehr während der Aushandlung verwendet.

Die IKE-Richtlinien in dieser Liste sind für alle VPN-Verbindungen verfügbar.

Priorität

Ein Wert als ganze Zahl, der die Priorität für diese Richtlinie im Verhältnis zu anderen konfigurierten IKE-Richtlinien angibt. Weisen Sie den IKE-Richtlinien, die der Router bevorzugt verwenden soll, die niedrigsten Nummern zu. Der Router schlägt diese Richtlinien während der Aushandlungen zuerst vor.

Verschlüsselung

Der Verschlüsselungstyp, der verwendet werden soll, um diese IKE-Richtlinie zu übermitteln.

Hash

Der Authentifizierungsalgorithmus für die Aushandlung. Es stehen zwei mögliche Werte zur Verfügung:

- **Secure Hash Algorithm (SHA)**
- **Message Digest 5 (MD5)**

Authentifizierung

Die zu verwendende Authentifizierungsmethode.

- **Pre-SHARE**. Die Authentifizierung wird unter Verwendung von Pre-Shared Keys durchgeführt.
- **RSA_SIG**. Die Authentifizierung wird unter Verwendung von digitalen Signaturen durchgeführt.

Art

Entweder **SDM_DEFAULT** oder **Benutzerdefiniert**. **SDM_DEFAULT**-Richtlinien können nicht bearbeitet werden.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Weitere Informationen zu IKE-Richtlinien	Siehe **Weitere Informationen zu IKE-Richtlinien**.
Hinzufügen einer IKE-Richtlinie zur Routerkonfiguration Cisco SDM bietet eine Standard-IKE-Richtlinie; es kann jedoch nicht sicher davon ausgegangen werden, dass der Peer über dieselbe Richtlinie verfügt. Sie sollten andere IKE-Richtlinien konfigurieren, sodass der Router eine IKE-Richtlinie bereitstellen kann, die vom Peer akzeptiert wird.	Klicken Sie auf **Hinzufügen**, und konfigurieren Sie eine neue IKE-Richtlinie im Fenster **IKE-Richtlinie hinzufügen**.
Bearbeiten einer vorhandenen IKE-Richtlinie	Wählen Sie die IKE-Richtlinie aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann die IKE-Richtlinie im Fenster **IKE-Richtlinie bearbeiten**. Standard-IKE-Richtlinien sind schreibgeschützt. Sie können nicht bearbeitet werden.
Entfernen einer IKE-Richtlinie aus der Routerkonfiguration	Wählen Sie die IKE-Richtlinie aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

IKE-Richtlinie hinzufügen oder bearbeiten

Fügen Sie eine IKE-Richtlinie über dieses Fenster hinzu bzw. bearbeiten Sie diese in diesem Fenster.

Hinweis

- Nicht alle Router unterstützen alle Verschlüsselungstypen. Nicht unterstützte Typen werden nicht im Bildschirm angezeigt.
- Nicht alle IOS-Abbilder unterstützen alle von Cisco SDM unterstützten Verschlüsselungstypen. Typen, die nicht vom IOS-Abbild unterstützt werden, werden nicht im Bildschirm angezeigt.

- Wenn die Hardwareverschlüsselung aktiviert ist, werden nur die Verschlüsselungstypen im Bildschirm angezeigt, die sowohl von der Hardwareverschlüsselung als auch vom IOS-Abbild unterstützt werden.

Priorität

Ein Wert als ganze Zahl, der die Priorität für diese Richtlinie im Verhältnis zu anderen konfigurierten IKE-Richtlinien angibt. Weisen Sie den IKE-Richtlinien, die der Router bevorzugt verwenden soll, die niedrigsten Nummern zu. Der Router schlägt diese Richtlinien während der Aushandlungen zuerst vor.

Verschlüsselung

Der Verschlüsselungstyp, der verwendet werden soll, um diese IKE-Richtlinie zu übermitteln. Cisco SDM unterstützt unterschiedliche Verschlüsselungstypen, die in der Reihenfolge ihrer Sicherheit aufgeführt werden. Je sicherer ein Verschlüsselungstyp ist, desto mehr Verarbeitungszeit ist für diesen erforderlich.

Hinweis Wenn Ihr Router einen Verschlüsselungstyp nicht unterstützt, wird der Typ nicht in der Liste angezeigt.

Cisco SDM unterstützt die folgenden Verschlüsselungstypen:

- Data Encryption Standard (DES) – Diese Verschlüsselungsform unterstützt die 56-Bit-Verschlüsselung.
- Triple Data Encryption Standard (3DES) – Dies ist eine höhere Verschlüsselungsform als DES, die eine 168-Bit-Verschlüsselung unterstützt.
- AES-128 – Advanced Encryption Standard-(AES-)Verschlüsselung mit einem 128-Bit-Schlüssel. AES bietet eine höhere Sicherheit als DES und ist für rechenintensive Aufgaben effizienter als Triple DES.
- AES-192 – Advanced Encryption Standard-(AES-)Verschlüsselung mit einem 192-Bit-Schlüssel.
- AES-256 – Advanced Encryption Standard-(AES-)Verschlüsselung mit einem 256-Bit-Schlüssel.

Hash

Der Authentifizierungsalgorithmus, der für die Aushandlung verwendet wird. Es stehen zwei Optionen zur Verfügung:

- **Secure Hash Algorithm (SHA)**
- **Message Digest 5 (MD5)**

Authentifizierung

Die zu verwendende Authentifizierungsmethode.

- **Pre-SHARE**. Die Authentifizierung wird unter Verwendung von Pre-Shared Keys durchgeführt.
- **RSA_SIG**. Die Authentifizierung wird unter Verwendung von digitalen Signaturen durchgeführt.

D-H-Gruppe

Diffie-Hellman-(D-H-)Gruppe. Diffie-Hellman ist ein kryptografisches Public-Key-Protokoll, mit dem zwei Router gemeinsam genutzte, vertrauliche Informationen über einen nicht sicheren Kommunikationskanal austauschen können. Zu den Optionen gehören:

- group1 – 768-Bit-D-H-Gruppe. D-H-Gruppe 1.
- group2 – 1024-Bit-D-H-Gruppe. D-H-Gruppe 2. Diese Gruppe bietet eine höhere Sicherheit als Gruppe 1, erfordert jedoch eine höhere Verarbeitungszeit.
- group5 – 1536-Bit-D-H-Gruppe. D-H-Gruppe 5. Diese Gruppe bietet eine höhere Sicherheit als Gruppe 2, erfordert jedoch eine höhere Verarbeitungszeit.

Hinweis

- Wenn Ihr Router **group5** nicht unterstützt, wird sie nicht in der Liste angezeigt.
- Easy VPN-Server verfügen über keine Unterstützung für D-H-Gruppe 1.

Gültigkeitsdauer

Dies ist die Gültigkeitsdauer der Sicherheitsverknüpfung in Stunden, Minuten und Sekunden. Der Standard ist ein Tag oder 24:00:00.

IKE-Pre-shared Keys

Über dieses Fenster können Sie IKE-Pre-Shared Keys in der Routerkonfiguration anzeigen, bearbeiten, zur Konfiguration hinzufügen oder daraus entfernen. Ein Pre-Shared Key wird mit einem Remote-Peer während der IKE-Aushandlung ausgetauscht. Beide Peers müssen mit demselben Schlüssel konfiguriert sein.

Icon

Wenn ein Pre-Shared Key schreibgeschützt ist, wird das entsprechende Symbol für Schreibgeschützt in dieser Spalte angezeigt. Ein Pre-Shared Key wird dann als schreibgeschützt markiert, wenn er mit der CLI-Option **no-xauth** konfiguriert ist.

Peer-IP/Name

Eine IP-Adresse oder der Name eines Peers, mit dem dieser Schlüssel gemeinsam verwendet wird. Wenn eine IP-Adresse bereitgestellt wird, kann die Option alle Peers in einem Netzwerk oder Subnetz oder nur einen einzelnen Host angeben. Wenn ein Name angegeben ist, wird der Schlüssel nur mit dem aufgeführten Peer gemeinsam genutzt.

Netzwerkmaske

Die Netzwerkmaske gibt an, zu welchem Teil die Peer-IP-Adresse für die Netzwerkadresse und zu welchem Teil sie für die Hostadresse verwendet wird. Die Netzwerkmaske 255.255.255.255 gibt beispielsweise an, dass die Peer-IP-Adresse eine Adresse für einen bestimmten Host ist. Eine Netzwerkmaske, die die Zahlenwerte Null in den letzten signifikanten Bytes enthält, gibt an, dass die Peer-IP-Adresse eine Netzwerk- oder Subnetzadresse ist. Eine Netzwerkmaske von 255.255.248.0 gibt beispielsweise an, dass die ersten 22 Bits der Adresse für die Netzwerkadresse und die letzten 10 Bits für den Hostteil der Adresse verwendet werden.

Pre-Shared Key

Der Pre-Shared Key kann nicht in den Cisco SDM-Fenstern abgelesen werden. Wenn Sie den Pre-Shared Key sehen müssen, wählen Sie **Aktive > Konfiguration anzeigen**. Dadurch wird die aktive Konfiguration angezeigt. Dieser Schlüssel ist im Befehl **crypto isakmp key** enthalten.

Aufgabe	Vorgehensweise
Hinzufügen eine Pre-Shared Keys zur Routerkonfiguration	Klicken Sie auf **Hinzufügen**, und fügen Sie den Pre-Shared Key im Fenster **Neuen Pre-Shared Key hinzufügen** hinzu.
Bearbeiten eines vorhandenen Pre-Shared Key	Wählen Sie den Pre-Shared Key aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann den Schlüssel im Fenster **Pre-shared Key bearbeiten**.
Entfernen eines vorhandenen Pre-Shared Key	Wählen Sie den Pre-Shared Key aus, und klicken Sie auf **Entfernen**.

Neuen Pre-Shared Key hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um einen Pre-Shared Key hinzuzufügen oder zu bearbeiten.

Schlüssel

Dies ist eine alphanumerische Zeichenfolge, die mit dem Remote-Peer ausgetauscht wird. Derselbe Schlüssel muss im Remote-Peer konfiguriert sein. Dieser Schlüssel sollte nicht einfach zu erraten sein. Die Verwendung von Fragezeichen (?) und Leerzeichen ist im Pre-Shared Key nicht zulässig.

Schlüssel erneut eingeben

Geben Sie dieselbe Zeichenfolge ein, die Sie im Feld **Schlüssel** eingegeben haben, um die Eingabe zu bestätigen.

Peer

Wählen Sie **Hostname**, wenn Sie den Schlüssel auf einen bestimmten Host anwenden möchten. Wählen Sie **IP-Adresse**, wenn Sie ein Netzwerk oder Subnetz angeben möchten, oder wenn Sie die IP-Adresse eines bestimmten Hosts angeben möchten, da kein DNS-Server zur Übersetzung von Hostnamen in IP-Adressen vorhanden ist.

Hostname

Dieses Feld wird angezeigt, wenn Sie **Hostname** im Feld **Peer** ausgewählt haben. Geben Sie den Hostnamen des Peers ein. Es muss ein DNS-Server im Netzwerk verfügbar sein, der den Hostnamen in eine IP-Adresse auflösen kann.

IP-Adresse/Subnetzmaske

Diese Felder werden angezeigt, wenn Sie Feld **Peer** die Option **IP-Adresse** ausgewählt haben. Geben Sie die IP-Adresse eines Netzwerks oder Subnetzes im Feld **IP-Adresse** ein. Der Pre-Shared Key wird auf alle Peers in diesem Netzwerk oder Subnetz angewendet. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Geben Sie eine Subnetzmaske ein, wenn es sich bei der von Ihnen eingegebenen IP-Adresse um eine Subnetzadresse handelt und nicht um die Adresse eines bestimmten Hosts.

Benutzerauthentifizierung [Xauth]

Aktivieren Sie dieses Feld, wenn Site-to-Site-VPN-Peers für die gegenseitige Authentifizierung die Option Xauth verwenden. Wenn Xauth-Authentifizierung unter **Globale VPN-Einstellungen** aktiviert ist, ist diese Option sowohl für Site-to-Site-Peers als auch für Easy VPN-Verbindungen aktiviert.

IKE-Profile

IKE-Profile, auch ISAKMP-Profile genannt, ermöglichen es Ihnen, einen Satz IKE-Profile zu erstellen, den Sie mit einem oder mehreren IPSec-Tunneln verknüpfen können. Ein IKE-Profil wendet Parameter auf eine eingehende IPSec-Verbindung an, die eindeutig über ihr Konzept übereinstimmender Identitätskriterien identifiziert wird. Diese Kriterien basieren auf der IKE-Identität, die von eingehenden IKE-Verbindungen vorgezeigt wird, und beinhaltet eine IP-Adresse, einen voll qualifizierten Domänennamen (Full Qualified Domain Name, FQDN) und eine Gruppe (die Virtual Private Network [VPN]-Remote-Client-Gruppierung).

Weitere Informationen zu ISAKMP-Profilen und dazu, wie diese mit der Cisco IOS CLI konfiguriert werden, finden Sie bei Cisco.com unter diesem Pfad:

Products & Services > Cisco IOS Software > Cisco IOS Security > Cisco IOS IPSec > Product Literature > White Papers > ISAKMP Profile Overview

IKE-Profile

Der Bereich zu den IKE-Profilen des Bildschirms führt die konfigurierten IKE-Profile auf und enthält den Profilnamen, das von ihm verwendete IPSec-Profil und eine Beschreibung des Profils, falls eine solche angegeben wurde. Wenn das gewählte IKE-Profil von keinem IPSec-Profil verwendet wird, wird in der Spalte **Verwendet von** der Wert <Keine> angezeigt.

Wenn Sie mithilfe von SDM eine Easy VPN-Serverkonfiguration erstellen, werden die IKE-Profile automatisch erstellt, von SDM benannt und in dieser Liste angezeigt.

Details zum IKE-Profil

Der Details-Bereich des Bildschirms führt die Konfigurationswerte für das gewählte Profil auf. Sie können ihn verwenden, um Details anzuzeigen, ohne auf die Schaltfläche **Bearbeiten** zu klicken und ein zusätzliches Dialogfenster anzuzeigen. Wenn Sie Änderungen vornehmen müssen, klicken Sie auf **Bearbeiten** und nehmen im angezeigten Dialogfeld die erforderlichen Änderungen vor. Weitere Informationen über die in diesem Bereich angezeigten Informationen finden Sie unter IKE-Profil hinzufügen oder bearbeiten.

IKE-Profil hinzufügen oder bearbeiten

Geben Sie in diesem Dialogfeld Informationen ein, erstellen Sie ein IKE-Profil und verknüpfen Sie es mit einer virtuellen Tunnelschnittstelle.

IKE-Profil-Name

Geben Sie einen Namen für dieses IKE-Profil ein. Wenn Sie ein Profil bearbeiten, ist dieses Feld aktiviert.

Virtuelle Tunnelschnittstelle

Wählen Sie aus der Liste **Virtuelle Tunnelschnittstelle** die virtuelle Tunnelschnittstelle aus, mit der Sie dieses IKE-Profil verknüpfen möchten. Wenn Sie eine virtuelle Tunnelschnittstelle erstellen müssen, klicken Sie auf **Hinzufügen** und erstellen die Schnittstelle im angezeigten Dialogfeld.

Identitätstyp abgleichen

Das IKE-Profil enthält Übereinstimmungskriterien, mit denen der Router eingehende und abgehende Verbindungen identifizieren kann, auf welche die IKE-Verbindungsparameter anzuwenden sind. Übereinstimmungskriterien können derzeit auf VPN-Gruppen angewandt werden. Im Feld **Identitätstyp abgleichen** ist automatisch **Gruppe** voreingestellt.

Klicken Sie auf **Hinzufügen**, um eine Liste der Gruppen zu erstellen, die Sie in die Übereinstimmungskriterien einbeziehen möchten.

Wählen Sie **Externen Gruppennamen hinzufügen**, um den Namen einer Gruppe hinzuzufügen, die nicht auf dem Router konfiguriert ist, und geben Sie den Namen im angezeigten Dialogfeld ein.

Wählen Sie **Aus lokalen Gruppen auswählen**, um den Namen einer Gruppe hinzuzufügen, die nicht auf dem Router konfiguriert ist. Aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen neben der Gruppe, die Sie hinzufügen möchten. Wenn alle lokalen Gruppen in anderen IKE-Profilen verwendet werden, informiert Sie der SDM, dass alle Gruppen ausgewählt wurden.

Moduskonfiguration

Wählen Sie **Antworten** im Feld **Moduskonfiguration**, wenn der Router auf Moduskonfigurationsanforderungen antworten soll.

Wählen Sie **Einleiten** im Feld **Moduskonfiguration**, wenn der Router Moduskonfigurationsanforderungen einleiten soll.

Wählen Sie **Beide** im Feld **Moduskonfiguration**, wenn der Router auf Moduskonfigurationsanforderungen antworten und diese einleiten soll.

Autorisierungsrichtlinie für Gruppenrichtlinien-Lookup

Sie müssen eine Autorisierungsrichtlinie angeben, die den Zugriff auf Gruppenrichtlinien-Informationen auf dem AAA-Server steuert. Wählen Sie **Standard**, wenn Sie Zugriff auf Gruppenrichtlinien-Lookup-Informationen gewähren möchten. Um eine Richtlinie anzugeben, wählen Sie eine vorhandene Richtlinie in der Liste aus oder klicken auf **Hinzufügen**, um im angezeigten Dialogfeld eine Richtlinie zu erstellen.

Benutzerauthentifizierungsrichtlinie

Sie können eine Benutzerauthentifizierungsrichtlinie angeben, die für XAuth-Anmeldungen verwendet wird. Wählen Sie **Standard**, wenn Sie XAuth-Anmeldungen zulassen möchten. Um eine Richtlinie für die Steuerung von XAuth-Anmeldungen anzugeben, wählen Sie eine vorhandene Richtlinie in der Liste aus oder klicken auf **Hinzufügen**, um im angezeigten Dialogfeld eine Richtlinie zu erstellen.

Dead Peer-Erkennung

Klicken Sie auf **Dead Peer-Erkennung**, um dem Router zu ermöglichen, Meldungen zu Dead Peer-Erkennungen (DPD) an Peers zu senden. Wenn ein Peer nicht auf DPD-Meldungen reagiert, wird die Verbindung zu diesem aufgehoben.

Geben Sie die Anzahl der Sekunden zwischen DPD-Meldungen im Feld **Keepalive-Intervall** an. Der zulässige Bereich liegt zwischen 1 und 3600 Sekunden.

Geben Sie im Feld **Wiederholungen** die Anzahl der Sekunden zwischen Wiederholversuchen an, wenn DPD-Meldungen fehlschlagen. Der zulässige Bereich liegt zwischen 2 und 60 Sekunden.

Die Dead Peer-Erkennung hilft dabei, Verbindungen ohne Administratoreingriff zu verwalten, generiert jedoch auch Pakete, die beide Peers verarbeiten müssen, damit die Verbindung aufrechterhalten wird.

Beschreibung

Sie können eine Beschreibung zu dem IKE-Profil hinzufügen, das Sie hinzufügen oder bearbeiten.

KAPITEL 17

Public-Key-Infrastruktur

Über das Fenster **Public-Key-Infrastruktur (PKI)** können Sie Registrierungsanforderungen und RSA-Schlüssel erstellen sowie Schlüssel und Zertifikate verwalten. Sie können den Simple Certificate Enrollment-Prozess (SCEP) verwenden, um eine Registrierungsanforderung und ein RSA-Schlüsselpaar zu erstellen und Zertifikate online zu erhalten, oder um eine Registrierungsanforderung zu erstellen, die Sie offline an einen Zertifizierungsstellenserver (Certificate Authority, CA-Server) weiterleiten können.

Wenn Sie Secure Device Provisioning (SDP) zum Registrieren von Zertifikaten benutzen möchten, lesen Sie weiter unter Secure Device Provisioning.

Zertifikat-Assistenten

In diesem Fenster können Sie den Typ der Registrierung auswählen, die Sie ausführen möchten. Das Fenster zeigt auch Alarmmeldungen an, wenn Sie Konfigurationsaufgaben vornehmen müssen, bevor Sie mit der Registrierung beginnen, oder wenn Sie Aufgaben vor der Registrierung ausführen sollten, die von Cisco empfohlen werden. Wenn Sie diese Aufgaben ausführen, bevor Sie mit dem Registrierungsprozess beginnen, können Sie mögliche Probleme vermeiden.

Wählen Sie die Registrierungsmethode aus, die Cisco SDM verwendet, um eine Registrierungsanforderung zu generieren.

Erforderliche Aufgaben

Wenn Cisco SDM Konfigurationsaufgaben identifiziert, die vorgenommen werden sollten, bevor Sie mit dem Registrierungsprozess beginnen, werden Sie auf diese Aufgaben in diesem Feld durch eine Alarmmeldung hingewiesen. Neben der Alarmmeldung ist ein Link verfügbar, über den Sie zur entsprechenden Stelle in Cisco SDM wechseln können und die Konfiguration fertig stellen können. Wenn Cisco SDM keine fehlenden Konfigurationen feststellt, wird dieses Feld nicht angezeigt. Unter Erforderliche Aufgaben für PKI-Konfigurationen werden mögliche vorausgesetzte Aufgaben beschrieben.

Simple Certificate Enrollment-Protokoll (SCEP)

Klicken Sie auf diese Schaltfläche, um eine direkte Verbindung zwischen Ihrem Router und einem CA-Server herzustellen. Sie müssen über den Registrierungs-URL des Servers verfügen, um diesen Schritt vornehmen zu können. Der Assistent führt folgende Schritte aus:

- Er sammelt Informationen von Ihnen, um einen Trustpoint konfigurieren zu können und diesen an den Router zu senden.
- Er initiiert eine Registrierung mit dem CA-Server, den Sie im Trustpoint angegeben haben.
- Wenn der CA-Server verfügbar ist, zeigt er den Fingerabdruck des CA-Servers an, damit Sie diesen Sie verifizieren können.
- Wenn Sie den Fingerabdruck des CA-Servers akzeptieren, stellt er die Registrierung fertig.

Ausschneiden und einfügen/Von PC importieren

Klicken Sie auf diese Schaltfläche, wenn Ihr Router keine direkte Verbindung zum CA-Server herstellen kann oder wenn Sie eine Registrierungsanforderung generieren und diese an die CA zu einem späteren Zeitpunkt senden möchten. Nach dem Generieren kann die Registrierungsanforderung später an eine CA übermittelt werden. Für das Ausschneiden und Einfügen von Registrierungen müssen Sie den Assistent für digitale Zertifikate aufrufen, um eine Anforderung zu generieren, und diesen erneut aufrufen, wenn Sie die Zertifikate für den CA-Server und für den Router erhalten haben.

Hinweis Cisco SDM unterstützt nur das Ausschneiden und Einfügen für Registrierungen diesen Typs: Base-64-codiertes PKCS#10-type cut. Cisco SDM unterstützt nicht das Importieren von Zertifikatsregistrierungen diesen Typs: PEM und PKCS#12.

Schaltfläche Ausgewählte Aufgabe starten

Klicken Sie auf diese Schaltfläche, um den Assistenten für den von Ihnen ausgewählten Registrierungstyp zu starten. Wenn Cisco SDM eine erforderliche Aufgabe ermittelt hat, die ausgeführt werden muss, bevor die Registrierung gestartet werden kann, ist diese Schaltfläche deaktiviert. Sobald die Aufgabe fertig gestellt wird, ist die Schaltfläche aktiviert.

Willkommen beim SCEP-Assistenten

Dieser Bildschirm zeigt an, dass Sie den SCEP-Assistenten verwenden. Wenn Sie den Simple Certificate Enrollment-Prozess nicht verwenden möchten, klicken Sie auf **Abbrechen**, um diesen Assistenten zu verlassen.

Nachdem der Assistent abgeschlossen wurde und die Befehle an den Router gesendet wurden, versucht Cisco SDM eine Verbindung zum CA-Server herzustellen. Nachdem die Verbindung zum CA-Server aufgebaut wurde, zeigt Cisco SDM ein Mitteilungsfenster mit dem digitalen Zertifikat des Servers an.

Certificate Authority-(CA-)Informationen

Geben Sie in diesem Fenster Informationen an, um den CA-Server identifizieren zu können. Geben Sie darüber hinaus ein Anforderungskennwort an, das zusammen mit der Anforderung gesendet wird.

Hinweis Die von Ihnen in diesem Bildschirm eingegebenen Informationen werden verwendet, um einen Trustpoint zu generieren. Der Trustpoint wird mit einer Standardmethode für die Überprüfung der Sperrung der CRL verwendet. Wenn Sie einen bestehenden Trustpoint mit dem SCEP-Assistenten bearbeiten und eine andere Sperrmethode als CRL, wie beispielsweise OCSP, bereits unter diesem Trustpoint vorhanden ist, ändert Cisco SDM diesen Trustpoint nicht. Wenn Sie die Sperrungsmethode ändern müssen, wechseln Sie zum Fenster **Router-Zertifikate**, wählen Sie den von Ihnen konfigurierten Trustpoint aus, und klicken Sie dann auf die Schaltfläche **Sperrung überprüfen**.

CA-Server-Aliasname

Der CA-Server-Aliasname ist ein Bezeichner für den Trustpoint, den Sie konfigurieren. Geben Sie einen Namen ein, der Ihnen bei der Unterscheidung der einzelnen Trustpoints hilft.

Registrierungs-URL

Wenn Sie eine SCEP-Registrierung abschließen, müssen Sie den Registrierungs-URL für den CA-Server in dieses Feld eingeben. Beispiel:

```
http://CAuthority/enrollment
```

Der URL muss mit der Zeichenfolge http:// beginnen. Stellen Sie sicher, dass eine Verbindung zwischen dem Router und dem CA-Server besteht, bevor Sie den Registrierungsprozess starten.

Dieses Feld wird nicht angezeigt, wenn Sie eine Registrierung durch Ausschneiden und Einfügen abschließen.

Anforderungskennwort und Anforderungskennwort bestätigen

Es kann ein Anforderungskennwort an die CA gesendet werden, das Sie verwenden können, wenn Sie das Zertifikat einmal sperren müssen. Es wird empfohlen, dies zu tun, da einige CA-Server keine Zertifikate ausgeben, wenn kein Anforderungskennwort angegeben wird. Wenn Sie ein Anforderungskennwort verwenden möchten, geben Sie dieses Kennwort ein, und geben Sie es anschließend erneut im Bestätigungsfeld ein. Das Anforderungskennwort wird zusammen mit der Registrierungsanforderung gesendet. Aus Sicherheitsgründen ist das Anforderungskennwort in der Routerkonfigurationsdatei verschlüsselt, daher sollten Sie das Kennwort notieren und an einem sicheren Ort als Erinnerungshilfe aufbewahren.

Dieses Kennwort wird auch als Anforderungskennwort bezeichnet.

Schaltfläche Erweiterte Optionen

Mit den erweiterten Optionen können Sie zusätzliche Informationen angeben, um die Verbindung des Routers zum CA-Server zu aktivieren.

Erweiterte Optionen

Verwenden Sie dieses Fenster, um zusätzliche Informationen für das Aktivieren der Verbindung des Routers zum CA-Server anzugeben.

Quellzertifikatsanforderung von einer bestimmten Schnittstelle

Aktivieren Sie dieses Feld, wenn eine bestimmte Schnittstelle als Quelle für das Zertifikat festlegen wollen.

HTTP-Proxy und HTTP-Port

Wenn die Registrierungsanforderung über einen Proxy-Server gesendet wird, geben Sie die IP-Adresse des Proxy-Servers und die Portnummer ein, die für die Proxy-Anforderungen in diesen Feldern verwendet wird.

Namensattribute für Zertifikatsinhaber

Geben Sie die optionalen Informationen an, die im Zertifikat enthalten sein sollen. Alle von Ihnen in der Zertifikatsanforderung angegebenen Informationen werden im Zertifikat abgelegt und können von allen Parteien, an die der Router das Zertifikat sendet, angezeigt werden.

Vollständig qualifizierten Domänennamen (FQDN) des Routers aufnehmen

Es wird empfohlen, den vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Routers im Zertifikat aufzunehmen. Aktivieren Sie dieses Feld, wenn Cisco SDM den vollständig qualifizierten Domänennamen des Routers in die Zertifikatsanforderung aufnehmen soll.

Hinweis Wenn das vom Router ausgeführte Cisco IOS-Abbild diese Funktion nicht unterstützt, ist dieses Feld deaktiviert.

FQDN

Wenn Sie dieses Feld aktivieren, geben Sie den FQDN des Routers in dieses Feld ein. Ein Beispiel für einen FQDN ist:

```
sjrtr.mycompany.net
```

IP-Adresse des Routers aufnehmen

Aktivieren Sie dieses Feld, wenn eine gültige IP-Adresse, die in Ihrem Router konfiguriert ist, in die Zertifikatsanforderung aufgenommen werden soll. Wenn Sie dieses Feld aktivieren, können Sie eine IP-Adresse manuell eingeben, oder Sie können die Schnittstelle auswählen, deren IP-Adresse verwendet werden soll.

IP-Adresse

Klicken Sie auf diese Option, wenn Sie eine IP-Adresse eingeben möchten, und geben Sie eine IP-Adresse, die im Router konfiguriert ist, in das angezeigte Feld ein. Geben Sie eine IP-Adresse ein, die im Router konfiguriert wurde, oder eine Adresse, die dem Router zugewiesen wurde.

Schnittstelle

Wählen Sie eine Routerschnittstelle aus, deren IP-Adresse, in die Zertifikatsanforderung aufgenommen werden soll.

Router-Seriennummer aufnehmen

Aktivieren Sie dieses Feld, wenn die Seriennummer des Routers in das Zertifikat aufgenommen werden soll.

Weitere Zertifikatsinhaberattribute

Die Informationen, die Sie über dieses Fenster eingeben, werden in die Registrierungsanforderung aufgenommen. CAs verwenden den X.500-Standard, um Informationen für digitale Zertifikate zu speichern und zu verwalten. Alle Felder sind optional, es wird jedoch empfohlen, so viele Informationen wie möglich anzugeben.

Allgemeiner Name (cn)

Geben Sie den allgemeinen Namen (Common Name) ein, der in dieses Zertifikat aufgenommen werden soll. Das wäre dann der Name, der für die Zertifikatsuche im X.500-Verzeichnis herangezogen wird.

Unternehmenseinheit (ou)

Geben Sie die Unternehmenseinheit (Organizational Unit) oder den Abteilungsnamen ein, die bzw. der in diesem Zertifikat verwendet werden soll. Als Unternehmenseinheiten kommen beispielsweise Development (Entwicklung) oder Engineering (Technik) in Frage.

Unternehmen (o)

Geben Sie den Organisationsnamen oder Unternehmensnamen ein. Dies ist der X.500-Unternehmensname.

Bundesland (st)

Geben Sie das Bundesland (State) ein, in dem sich der Router oder das Unternehmen bzw. die Organisation befindet.

Land (c)

Geben Sie das Land (Country) ein, in dem sich der Router oder das Unternehmen bzw. die Organisation befindet.

E-Mail (e)

Geben Sie die E-Mail-Adresse ein, die im Router-Zertifikat aufgenommen werden soll.

Hinweis Wenn das vom Router ausgeführte Cisco IOS-Abbild dieses Attribut nicht unterstützt, ist dieses Feld deaktiviert.

RSA-Schlüssel

Sie müssen einen öffentlichen RSA-Schlüssel in die Registrierungsanforderung aufnehmen. Sobald das Zertifikat erteilt wurde, wird der öffentliche Schlüssel in das Zertifikat aufgenommen, den Peers dann zum Verschlüsseln der Daten verwenden können, die an den Router gesendet werden. Der private Schlüssel verbleibt im Router und wird zum Entschlüsseln der von den Peers gesendeten Daten und zur digitalen Signatur von Transaktionen bei Aushandlungen mit den Peers verwendet.

Neue(s) Schlüsselpaar(e) generieren

Klicken Sie auf diese Schaltfläche, wenn Sie einen neuen Schlüssel zur Verwendung im Zertifikat generieren möchten. Wenn Sie ein neues Schlüsselpaar generieren, müssen Sie das Modul zum Ermitteln der Schlüsselgröße angeben. Dieser neue Schlüssel wird nach Abschluss des Assistenten im Fenster **RSA-Schlüssel** angezeigt.

Modul

Geben Sie den Wert des Schlüsselmoduls ein. Wenn Sie einen Modulwert zwischen 512 und 1024 wünschten, geben Sie einen Ganzzahlwert ein, der ein Vielfaches von 64 ist. Wenn Sie einen Wert über 1024 wünschen, können Sie 1536 oder 2048 eingeben. Wenn Sie einen größeren Wert als 512 eingeben, kann die Generierung des Schlüssels mindestens eine Minute dauern.

Der Modulwert bestimmt die Größe des Schlüssels. Je größer der Modulwert ist, desto sicherer ist der Schlüssel. Die Erstellung von Schlüsseln mit großen Modulwerten beansprucht jedoch mehr Zeit bei der Erstellung, und die Verschlüsselung/Entschlüsselung dauert länger, wenn große Schlüssel verwendet werden.

Getrennte Schlüsselpaare für Verschlüsselung und Signatur generieren

Standardmäßig erstellt Cisco SDM ein allgemeines Schlüsselpaar, das für die Verschlüsselung und für die Signatur verwendet wird. Wenn Cisco SDM separate Schlüsselpaare für die Verschlüsselung und das Signieren von Dokumenten generieren soll, aktivieren Sie dieses Feld. Cisco SDM generiert Verwendungsschlüssel für die Verschlüsselung und die Signatur.

Existierendes RSA-Schlüsselpaar verwenden

Klicken Sie auf diese Schaltfläche, wenn Sie ein existierendes Schlüsselpaar verwenden möchten, und wählen Sie den Schlüssel aus der Dropdown-Liste aus.

Auf USB-Token speichern

Aktivieren Sie das Kontrollkästchen **Schlüssel und Zertifikate auf gesichertes USB-Token speichern**, wenn Sie die RSA-Schlüssel und Zertifikate auf ein mit Ihrem Router verbundenes USB-Medium speichern möchten. Dieses Kästchen erscheint nur, wenn ein USB-Token am Router angeschlossen ist.

Wählen Sie das USB-Token aus dem Dropdown-Menü **USB-Token** aus. Geben Sie die benötigte PIN ein, um sich per **PIN** beim gewünschten USB-Token anzumelden.

Nachdem Sie ein USB-Token ausgewählt und die korrekte PIN eingegeben haben, klicken Sie auf **Anmelden**, um sich beim USB-Token anzumelden.

Übersicht

Dieses Fenster fasst die von Ihnen angegebenen Informationen zusammen. Die von Ihnen angegebenen Informationen werden verwendet, um einen Trustpoint im Router zu konfigurieren und mit der Registrierung zu beginnen. Wenn Sie im Dialogfeld **Einstellungen** die Option **Zeigen Sie die Befehle an, bevor Sie diese an den Router senden** aktiviert haben, können Sie eine Vorschau der CLI-Befehle anzeigen, die an den Router gesendet werden.

Ausführung einer SCEP-Registrierung

Nachdem die Befehle an den Router gesendet wurden, versucht Cisco SDM eine Verbindung zum CA-Server herzustellen. Nachdem die Verbindung zum CA-Server aufgebaut wurde, zeigt Cisco SDM ein Mitteilungsfenster mit dem digitalen Zertifikat des Servers an.

Ausführung einer Registrierung durch Ausschneiden und Einfügen

Nachdem die Befehle an den Router gesendet wurden, generiert Cisco SDM eine Registrierungsanforderung und zeigt diese in einem neuen Fenster an. Sie müssen diese Registrierungsanforderung speichern und diese dem CA-Serveradministrator vorlegen, um das CA-Serverzertifikat und das Zertifikat für den Router zu erhalten. Die Registrierungsanforderung ist mit Base64 codiert und liegt im Format PKCS#10 vor.

Nach dem Erhalt der Zertifikate vom CA-Server müssen Sie den Assistent zum Ausschneiden und Einfügen erneut starten. Wählen Sie dann **Mit nicht abgeschlossener Registrierung fortfahren**, um die Zertifikate in den Router zu importieren.

CA-Serverzertifikat

Cisco SDM zeigt den digitalen Fingerabdruck des CA-Server-Zertifikats an. Wenn Sie die Registrierung fortsetzen wollen, müssen Sie dieses Zertifikat akzeptieren. Wenn Sie das Zertifikat nicht akzeptieren, wird der Registrierungsvorgang nicht fortgesetzt.

Der Zertifikatsfingerabdruck des CA-Servers ist:

Cisco SDM zeigt den Hexadezimalwert des Zertifikats vom CA-Server groß geschrieben an. Beispiel:

E55725EC A389E81E 28C4BE48 12B905ACD

So akzeptieren Sie das Zertifikat des CA-Servers und setzen die Registrierung fort

Klicken Sie auf **Ja, ich akzeptiere dieses Zertifikat** und anschließend auf **Weiter**.

So lehnen Sie das Zertifikat des CA-Servers ab und brechen die Registrierung ab

Klicken Sie auf **Nein, ich akzeptiere dieses Zertifikat nicht** und anschließend auf **Weiter**.

Registrierungsstatus

Dieses Fenster informiert Sie über den Status des Registrierungsprozesses. Wenn bei dem Prozess Fehler auftreten, zeigt Cisco SDM die verfügbaren Informationen über diesen Fehler an.

Wenn der Statusbericht erfolgt ist, klicken Sie auf **Fertig stellen**.

Begrüßungsbildschirm des Assistenten zum Ausschneiden und Einfügen

Mit dem Assistenten zum Ausschneiden und Einfügen können Sie Registrierungsanforderungen generieren und diese in Ihrem PC speichern, um sie offline an die CA zu senden. Da Sie die Registrierung nicht in einer einzelnen Sitzung fertig stellen können, schließt dieser Assistent den Vorgang ab, wenn Sie Trustpoint- und Registrierungsanforderungen generieren und diese im PC speichern.

Nachdem Sie die Registrierungsanforderung manuell an den CA-Server gesendet und das CA-Serverzertifikat und das Zertifikat für Ihren Router empfangen haben, müssen Sie den Assistent zum Ausschneiden und Einfügen erneut starten, um die Registrierung abzuschließen und die Zertifikate in den Router zu importieren.

Registrierungsaufgabe

Geben Sie an, ob Sie eine neue Registrierung starten oder ob Sie eine Registrierung mit einer Registrierungsanforderung, die Sie im PC gespeichert haben, fortsetzen möchten.

Neue Registrierung beginnen

Klicken Sie auf **Neue Registrierung beginnen**, um einen Trustpoint, ein RSA-Schlüsselpaar und eine Registrierungsanforderung zu generieren, die Sie im PC speichern und an den CA-Server senden können. Der Assistent schließt die Registrierung ab, nachdem Sie die Registrierungsanforderung gespeichert haben. Um die Registrierung fertig zu stellen, nachdem Sie das CA-Serverzertifikat und das Zertifikat für den Router erhalten haben, rufen Sie den Assistent zum Ausschneiden und Einfügen erneut auf. Wählen Sie dann **Mit nicht abgeschlossener Registrierung fortfahren**.

Mit nicht abgeschlossener Registrierung fortfahren

Klicken Sie auf diese Schaltfläche, um einen Registrierungsprozess fortzusetzen. Sie können Zertifikate, die Sie vom CA-Server erhalten haben, importieren und bei Bedarf eine neue Registrierungsanforderung für einen Trustpoint generieren.

Registrierungsanforderung

Dieses Fenster zeigt die Registrierungsanforderung des Base-64-codierten PKCS#10-Typs an, die der Router generiert hat. Speichern Sie die Registrierungsanforderung im PC. Senden Sie sie dann an die CA, um Ihr Zertifikat zu erhalten.

Speichern

Durchsuchen Sie den PC nach dem Verzeichnis, in dem die Textdatei mit der Registrierungsanforderung gespeichert werden soll, geben Sie einen Namen für die Datei ein, und klicken Sie auf **Speichern**.

Mit nicht abgeschlossener Registrierung fortfahren

Wenn Sie mit einer nicht abgeschlossenen Registrierung fortfahren, müssen Sie den Trustpoint auswählen, der mit der nicht abgeschlossenen Registrierung verknüpft ist, und anschließend den Teil des Registrierungsprozesses angeben, den Sie abschließen müssen. Wenn Sie ein CA-Serverzertifikat oder ein Router-Zertifikat importieren, muss das Zertifikat in Ihrem PC verfügbar sein.

CA-Server-Aliasname (Trustpoint) auswählen

Wählen Sie den Trustpoint aus, der mit der Registrierung verknüpft ist, die Sie abschließen.

CA- und Router-Zertifikat(e) importieren

Wählen Sie diese Option, wenn Sie das CA-Serverzertifikat und das Router-Zertifikat zugleich in einer Sitzung importieren möchten. Beide Zertifikate müssen im PC verfügbar sein.

Diese Option ist deaktiviert, wenn das CA-Zertifikat bereits importiert wurde.

CA-Zertifikat importieren

Wählen Sie diese Option, um ein CA-Serverzertifikat zu importieren, das im PC gespeichert ist. Nach dem Import des Zertifikats zeigt Cisco SDM den digitalen Fingerabdruck des Zertifikats an. Sie können dann das Zertifikat überprüfen und akzeptieren oder ablehnen.

Diese Option ist deaktiviert, wenn das CA-Zertifikat bereits importiert wurde.

Router-Zertifikat(e) importieren

Wählen Sie diese Option, um ein Zertifikat für den Router zu importieren, das im PC gespeichert ist. Nach dem Import des Router-Zertifikats zeigt Cisco SDM einen Bericht über den Status des Registrierungsprozesses an.

Hinweis Sie müssen das CA-Serverzertifikat vor dem Import des Router-Zertifikats importieren.

Registrierungsanforderung generieren

Wählen Sie diese Option, wenn Sie eine Registrierungsanforderung für den ausgewählten Trustpoint generieren müssen. Der Router generiert eine Registrierungsanforderung, die Sie im PC speichern und an die CA senden können.

Cisco SDM generiert eine Registrierungsanforderung, die mit Base64 codiert ist und im Format PKCS#10 vorliegt.

CA-Zertifikat importieren

Wenn ein CA-Serverzertifikat auf der Festplatte gespeichert ist, können Sie danach suchen und dieses dann über dieses Fenster in den Router importieren. Sie können den Zertifikatstext auch kopieren und in den Textbereich dieses Fensters einfügen.

Schaltfläche Durchsuchen

Klicken Sie auf diese Schaltfläche, um nach der Zertifikatsdatei im PC zu suchen.

Router-Zertifikat(e) importieren

Wenn ein Zertifikat oder mehrere Zertifikate von der CA für Ihren Router auf der Festplatte gespeichert sind, können Sie danach suchen und diese in Ihren Router importieren.

Weitere Zertifikate importieren

Wenn Sie getrennte RSA-Schlüsselpaare für die Verschlüsselung und die Signatur generiert haben, erhalten Sie zwei Zertifikate für den Router. Verwenden Sie diese Schaltfläche, wenn Sie mehr als ein Router-Zertifikat importieren müssen.

Zertifikate entfernen

Klicken Sie auf die Registerkarte des Zertifikats, das Sie entfernen möchten, und klicken Sie auf **Entfernen**.

Durchsuchen

Führen Sie einen Suchvorgang nach dem Zertifikat aus, und importieren Sie es in den Router.

Digitale Zertifikate

Über dieses Fenster können Sie Informationen über die im Router konfigurierten digitalen Zertifikate anzeigen.

Trustpoints

Dieser Bereich zeigt eine Übersicht der Informationen zu den im Router konfigurierten Trustpoints an und ermöglicht Ihnen Details zu den Trustpoints anzuzeigen, Trustpoints zu bearbeiten und zu ermitteln, ob ein Trustpoint gesperrt wurde.

Schaltfläche Details

Die Liste der Trustpoints zeigt nur den Namen, den Registrierungs-URL und den Registrierungstyp für einen Trustpoint an. Klicken Sie auf diese Schaltfläche, um alle Informationen zum ausgewählten Trustpoint anzuzeigen.

Schaltfläche „Bearbeiten“

Ein Trustpoint kann bearbeitet werden, wenn es sich um einen SCEP-Trustpoint handelt und wenn sowohl das CA-Serverzertifikat als auch das Router-Zertifikat nicht erfolgreich importiert werden konnte. Wenn es sich bei dem Trustpoint nicht um einen SCEP-Trustpoint handelt oder wenn sowohl das CA-Serverzertifikat als auch das Router-Zertifikat, das mit einem SCEP-Trustpoint verknüpft ist, importiert wurde, ist diese Schaltfläche deaktiviert.

Schaltfläche „Löschen“

Klicken Sie auf diese Schaltfläche, um den ausgewählten Trustpoint zu löschen. Wenn Sie einen Trustpoint löschen, werden alle Zertifikate vernichtet, die Sie von der dazugehörigen CA erhalten haben.

Schaltfläche Sperrung überprüfen

Klicken Sie auf diese Schaltfläche, um zu überprüfen, ob das ausgewählte Zertifikat gesperrt wurde. Cisco SDM zeigt ein Dialogfeld an, in dem Sie die Methode auswählen können, um die Sperrung zu überprüfen. Weitere Informationen dazu finden Sie unter Überprüfung der Sperrung und Überprüfung der Sperrung, nur CRL.

Name	Name des Trustpoints
CA-Server	Der Name oder die IP-Adresse des CA-Servers
Registrierungstyp	Einer der folgenden Typen: • SCEP – Simple Certificate Enrollment Protocol. Die Registrierung wurde durchgeführt, indem eine direkte Verbindung zum CA-Server erstellt wurde. • Ausschneiden und Einfügen – Die Registrierungsanforderung wurde vom PC importiert. • TFTP – Die Registrierungsanforderung wurde unter Verwendung eines TFTP-Servers durchgeführt.

Zertifikatskette für Trustpoint-*Namen*

Dieser Bereich zeigt Details zu den mit dem ausgewählten Trustpoint verknüpften Zertifikaten an.

Schaltfläche Details

Klicken Sie auf diese Schaltfläche, um das ausgewählte Zertifikat anzuzeigen.

Schaltfläche Aktualisieren

Klicken Sie auf diese Schaltfläche, um den Zertifikatskettenbereich zu aktualisieren, wenn Sie einen anderen Trustpoint in der Liste der Trustpoints auswählen.

Typ	Einer der folgenden Typen: • RA KeyEncipher Certificate – Verschlüsselungszertifikat Rivest Adelman • RA Signature Certificate – Rivest Adelman-Signaturzertifikat • CA Certificate – Das Zertifikat der CA-Organisation • Certificate – Das Zertifikat des Routers

Verwendung	Einer der folgenden Typen: • General Purpose – Ein Zertifikat für allgemeine Zwecke, das der Router verwendet, um sich bei Remote-Peers zu authentifizieren. • Signature – CA-Zertfikate sind Signaturzertifikate.
Seriennummer	Die Seriennummer des Zertifikats
Aussteller	Der Name der CA, die das Zertifikat ausgestellt hat
Status	Einer der folgenden Typen: • Available – Das Zertifikat kann verwendet werden. • Pending – Das Zertifikat wurde angefordert, ist jedoch nicht für die Verwendung verfügbar.
Expires (Days)	Die Anzahl an Tagen, für die das Zertifikat genutzt werden kann, bevor es abläuft
Expiry Date	Das Datum, an dem das Zertifikat abläuft

Trustpoint-Informationen

Die im Fenster **Router-Zertifikate** aufgelisteten Trustpoints zeigen die Schlüsselinformationen über jeden Trustpoint im Router an. Dieses Fenster zeigt alle Informationen an, die für die Erstellung eines Trustpoints bereitgestellt werden.

Details zum Zertifikat

Dieses Fenster zeigt die Trustpoint-Details an, die nicht im Fenster **Zertifikate** aufgeführt werden.

Überprüfung der Sperrung

Geben Sie an, wie der Router überprüfen soll, ob ein Zertifikat in diesem Fenster gesperrt wurde.

Überprüfung der Sperrung

Konfigurieren Sie, wie der Router die Überprüfung von Sperrungen vornehmen soll, und bringen Sie die Methoden in die bevorzugte Reihenfolge. Der Router kann mehrere Methoden verwenden.

Verwenden/Methode/Nach oben/Nach unten

Aktivieren Sie die Methoden, die verwendet werden sollen, und bringen Sie diese über die Schaltflächen **Nach oben** und **Nach unten** in die für die Verwendung gewünschte Reihenfolge.

- OCSP – Der Status eines Zertifikats wird ermittelt, indem eine Verbindung mit einem Online Certificate Status Protocol-Server hergestellt wird.
- CRL – Die Zertifikatssperre (Certificate Revocation List) wird über eine Zertifikatssperrliste überprüft.
- Keine – Es findet keine Überprüfung der Sperrung statt.

CRL-Abfrage-URL

Verfügbar, wenn **CRL** ausgewählt wurde. Geben Sie den URL ein, unter dem sich die Zertifikatssperrliste befindet. Geben Sie den URL nur dann ein, wenn das Zertifikat X.500 DN unterstützt.

OCSP-URL

Verfügbar, wenn **OCSP** ausgewählt wurde. Geben Sie den URL des OCSP-Servers ein, mit dem Sie eine Verbindung herstellen möchten.

Überprüfung der Sperrung, nur CRL

Geben Sie an, wie der Router überprüfen soll, ob ein Zertifikat in diesem Fenster gesperrt wurde.

Verifizierung

Einer der folgenden Typen:

- Keine – Überprüfen Sie den im Zertifikat eingebetteten CRL-Verteilungspunkt (Sperrlistenverteilungspunkt, Certificate Revocation List Distribution Point).

- Best-Effort – Laden Sie die CRL vom CRL-Server herunter, falls verfügbar. Wenn diese nicht verfügbar ist, wird das Zertifikat akzeptiert.
- Optional – Überprüfen Sie die CRL nur, wenn sie bereits in den Cache-Speicher manuell heruntergeladen wurde.

CRL-Abfrage-URL

Geben Sie den URL ein, unter dem sich die Zertifikatssperrliste befindet. Geben Sie den URL nur dann ein, wenn das Zertifikat X.500 DN unterstützt.

Fenster „RSA-Schlüssel“

RSA-Schlüssel bieten ein elektronisches Verschlüsselungs- und Authentifizierungssystem, das einen Algorithmus verwendet, der von Ron Rivest, Adi Shamir und Leonard Adleman entwickelt wurde. Das RSA-System ist der am häufigsten verwendete Verschlüsselungs- und Authentifizierungsalgorithmus und ist Teil des Cisco IOS. Für die Verwendung des RSA-Systems generiert der Netzwerkhost ein Schlüsselpaar. Ein Schlüssel wird als *öffentlicher Schlüssel* und der andere als *privater Schlüssel* bezeichnet. Der öffentliche Schlüssel wird an jede Partei ausgegeben, die verschlüsselte Daten an den Host senden möchte. Der private Schlüssel wird nicht verteilt. Wenn ein Remote-Host Daten versenden möchte, werden diese mit dem öffentlichen Schlüssel verschlüsselt, der gemeinsam mit dem lokalen Host verwendet wird. Der lokale Host entschlüsselt die gesendeten Daten mit dem privaten Schlüssel.

Auf dem Router konfigurierte RSA-Schlüssel

Name	Der Schlüsselname. Schlüsselnamen werden automatisch von Cisco SDM zugewiesen. Der Schlüssel **HTTPS_SS_CERT_KEYPAIR** und **HTTPS_SS_CERT_KEYPAIR.server** wird als schreibgeschützt angezeigt. Sämtliche Schlüssel, die im Router gesperrt/verschlüsselt sind, werden ebenso mit Symbolen angezeigt, die ihren Status angeben.

Verwendung	Entweder **Allgemein** oder **Verwendung**. Allgemeine Schlüssel werden verwendet, um Daten zu verschlüsseln und um das Zertifikat zu signieren. Wenn getrennte Schlüssel für die Verschlüsselung von Daten und für die Signatur von Zertifikaten konfiguriert sind, werden diese Schlüssel als **Verwendungsschlüssel** bezeichnet.
Exportierbar	Wenn diese Spalte mit einem Häkchen versehen ist, kann der Schlüssel in einen anderen Router exportiert werden, wenn dieser Router die Rolle eines lokalen Routers übernehmen soll.

Schlüsseldaten

Klicken Sie auf diese Schaltfläche, um einen ausgewählten RSA-Schlüssel anzuzeigen.

Schaltfläche Schlüssel auf PC speichern

Klicken Sie auf diese Schaltfläche, um die Daten des ausgewählten Schlüssels im PC zu speichern.

RSA-Schlüsselpaar generieren

Verwenden Sie dieses Fenster, um ein neues RSA-Schlüsselpaar zu generieren.

Bezeichnung

Geben Sie die Bezeichnung für den Schlüssel in dieses Feld ein.

Modul

Geben Sie den Wert des Schlüsselmoduls ein. Wenn Sie einen Modulwert zwischen 512 und 1024 wünschten, geben Sie einen Ganzzahlwert ein, der ein Vielfaches von 64 ist. Wenn Sie einen Wert über 1024 wünschen, können Sie 1536 oder 2048 eingeben. Wenn Sie einen größeren Wert als 512 eingeben, kann die Generierung des Schlüssels mindestens eine Minute dauern.

Je größer der Modulwert ist, desto sichererer ist der Schlüssel. Schlüssel mit größeren Modulgrößen benötigen jedoch länger, um generiert und ausgetauscht zu werden.

Typ

Wählen Sie den zu generierenden Schlüsseltyp aus: **Allgemein** oder **Verwendung**. Allgemeine Schlüssel werden sowohl für die Verschlüsselung als auch für die Signatur von Zertifikaten verwendet. Wenn Sie Verwendungsschlüssel generieren, wird ein Schlüsselsatz für die Verschlüsselung und ein anderer Schlüsselsatz für die Signatur von Zertifikaten verwendet.

Kontrollkästchen Schlüssel ist exportierbar

Aktivieren Sie dieses Kontrollkästchen, wenn der Schlüssel exportierbar sein soll. Ein exportierbares Schlüsselpaar kann an einen Remote-Router gesendet werden, wenn dieser Router die Funktionen eines lokalen Routers übernehmen muss.

Auf USB-Token speichern

Aktivieren Sie das Kontrollkästchen **Schlüssel auf gesichertes USB-Token speichern**, wenn Sie die RSA-Schlüssel auf ein am Router angeschlossenes USB-Token speichern möchten. Dieses Kästchen erscheint nur, wenn ein USB-Token am Router angeschlossen ist.

Wählen Sie das USB-Token aus dem Dropdown-Menü **USB-Token** aus. Geben Sie die benötigte PIN ein, um sich per **PIN** beim gewünschten USB-Token anzumelden.

Nachdem Sie ein USB-Token ausgewählt und die korrekte PIN eingegeben haben, klicken Sie auf **Anmelden**, um sich beim USB-Token anzumelden.

USB-Token Anmeldeinformationen

Dieses Fenster erscheint, wenn Sie Anmeldeinformationen hinzufügen oder löschen, z.B. ein RSA-Schlüsselpaar oder digitale Zertifikate, die auf ein USB-Token gespeichert wurden. Damit Sie löschen können, müssen Sie den USB-Tokennamen und die PIN eingeben.

Wählen Sie das USB-Token aus dem Dropdown-Menü **USB-Token** aus. Geben Sie die benötigte PIN ein, um sich per **PIN** beim gewünschten USB-Token anzumelden.

USB Token

In diesem Fenster können Sie USB-Tokenanmeldungen konfigurieren. Dieses Fenster zeigt auch eine Liste der USB-Tokenanmeldungen an, die Sie konfigurieren möchten. Wenn ein USB-Token an Ihren Cisco-Router angeschlossen ist, verwendet Cisco SDM die passende Anmeldung, um sich beim Token anzumelden.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um eine neue USB-Tokenanmeldung hinzuzufügen.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um eine bestehende USB-Tokenanmeldung zu bearbeiten. Geben Sie die zu bearbeitende Anmeldung an, indem Sie sie aus der Liste wählen.

Löschen

Klicken Sie auf **Löschen**, um eine bestehende USB-Tokenanmeldung zu löschen. Geben Sie die Anmeldung an, die Sie löschen möchten, indem Sie sie aus der Liste wählen.

Token Name

Zeigt den Namen an, der zur Anmeldung beim USB-Token verwendet wird.

Benutzer PIN

Zeigt die PIN an, der zur Anmeldung beim USB-Token verwendet wird.

Maximale PIN-Neuversuche

Zeigt an, wie oft Cisco SDM maximal versucht, sich mit der angegebenen PIN beim USB-Token anzumelden. Wenn die Versuche von Cisco SDM nach der angegebenen Anzahl nicht erfolgreich sind, werden die Anmeldeversuche für das USB-Token abgebrochen.

Timeout nach Entfernen

Zeigt die Anzahl an Sekunden an, während derer Cisco SDM maximal versucht, die vom USB-Token erhaltenen Internet Key Exchange (IKE)-Anmeldeinformationen zu verwenden, nachdem das Token vom Router entfernt wurde.

Wenn Timeout nach Entfernen leer ist, wird das Standard-Timeout verwendet. Das Standard-Timeout wird abgerufen, wenn ein neuer Zugriffsversuch auf die IKE-Anmeldeinformationen stattfindet.

Sekundäre Konfigurationsdatei

Zeigt die Konfigurationsdatei an, die Cisco SDM auf dem USB-Token sucht. Die Konfigurationsdatei kann eine CCCD-Datei oder eine.cfg-Datei sein.

CCCD bezieht sich auf eine Boot-Konfigurationsdatei. Eine CCCD-Datei wird mit der TMS-Software auf USB-Token geladen.

USB-Token hinzufügen oder bearbeiten

In diesem Fenster können Sie USB-Tokenanmeldungen hinzufügen und bearbeiten.

Token Name

Wenn Sie eine USB-Tokenanmeldung hinzufügen, geben Sie den USB-Tokennamen ein. Der eingegebene Name muss mit dem Namen des Tokens übereinstimmen, bei dem Sie sich anmelden möchten.

Ein Tokenname wird vom Hersteller eingestellt. USB-Token, die von Aladdin Knowledge Systems hergestellt wurden, heißen beispielsweise eToken.

Sie können auch den Namen **usbtoken*x*** eingeben, wobei *x* die Nummer auf dem USB-Port ist, an den das USB-Token angeschlossen ist. Ist das USB-Token z. B. an USB-Port 0 angemeldet, lautet der Name usbtoken0.

Wenn Sie eine USB-Tokenanmeldung bearbeiten, kann das Feld Tokenname nicht geändert werden.

Aktuelle PIN

Wenn Sie eine USB-Tokenanmeldung hinzufügen oder bearbeiten möchten, die keine PIN hat, ist im Feld **Aktuelle PIN** der Wert <Keine> eingetragen. Wenn Sie eine USB-Tokenanmeldung bearbeiten, die eine PIN hat, dann zeigt das Feld Aktuelle PIN ******.

Neue PIN eingeben

Geben Sie eine neue PIN für das USB-Token ein. Die neue PIN muss mindestens 4 Ziffern lang sein und mit dem Namen des Tokens übereinstimmen, bei dem Sie sich anmelden wollen. Wenn Sie eine USB-Tokenanmeldung bearbeiten, wird die aktuelle PIN durch die neue ersetzt.

Neue PIN erneut eingeben

Geben Sie die neue PIN nochmals ein, um sie zu bestätigen.

Maximale PIN-Neuversuche

Wählen Sie aus, wie oft Cisco SDM maximal versuchen soll, sich mit der angegebenen PIN beim USB-Token anzumelden. Wenn die Versuche von Cisco SDM nach der angegebenen Anzahl nicht erfolgreich sind, werden die Anmeldeversuche für das USB-Token abgebrochen.

Timeout nach Entfernen

Geben Sie die Anzahl an Sekunden ein, während derer Cisco SDM maximal versuchen soll, die vom USB-Token erhaltenen Internet Key Exchange (IKE)-Anmeldeinformationen zu verwenden, nachdem das Token vom Router entfernt wurde. Die Anzahl der Sekunden muss sich in einem Bereich von 0 bis 480 befinden.

Wenn Sie keine Zahl eingeben, wird das Standard-Timeout verwendet. Das Standard-Timeout wird abgerufen, wenn ein neuer Zugriffsversuch auf die IKE-Anmeldeinformationen stattfindet.

Sekundäre Konfigurationsdatei

Geben Sie eine Konfigurationsdatei an, die auf dem USB-Token besteht. Die Datei kann eine teilweise oder vollständige Konfigurationsdatei sein. Die Dateierweiterung muss.cfg sein.

Wenn Cisco SDM sich beim USB-Token anmelden kann, führt es die angegebene Konfigurationsdatei mit der laufenden Konfiguration des Routers zusammen.

Firewall öffnen

Dieser Bildschirm wird angezeigt, wenn Cisco SDM eine oder mehrere Firewalls auf Schnittstellen ermittelt, die zurücklaufenden Datenverkehr blockieren würden, der beim Router eingehen muss. Zwei Situationen, in denen dieser Bildschirm anzeigt werden kann, sind beispielsweise die Fälle, in denen die Firewall DNS- oder PKI-Datenverkehr blockiert und verhindert, dass der Router die entsprechenden Daten von den Servern erhält. Cisco SDM kann diese Firewalls ändern, sodass die Server mit dem Router kommunizieren können.

Firewall ändern

Dieser Bereich listet die ausgehenden Schnittstellen und ACL-Namen auf. Sie können hier auswählen, welche Firewalls von Cisco SDM geändert werden sollen. Wählen Sie die Firewalls in der Spalte **Aktion** aus, die Cisco SDM ändern soll. Cisco SDM nimmt Änderungen an diesen Firewalls vor, um SCEP- oder DNS-Datenverkehr vom Server zum Router zuzulassen.

Hinweis zu SCEP-Datenverkehr:

- Cisco SDM ändert nicht die Firewall für CRL/OCSP-Server, wenn diese nicht ausdrücklich auf dem Router konfiguriert sind. Um die Kommunikation mit CRL/OCSP-Servern zuzulassen, müssen Sie die erforderlichen Informationen beim CA-Serveradministrator anfordern und die Firewalls im Fenster **Firewallrichtlinie/ACL bearbeiten** ändern.

- Cisco SDM geht davon aus, dass der vom CA-Server an den Router gesendete Datenverkehr durch dieselben Schnittellen in den Router eintritt, über die Datenverkehr vom Router an den CA-Server gesendet wurde. Wenn der zurücklaufende Datenverkehr vom CA-Server über eine andere als die von Cisco SDM angegebene Schnittstelle in den Router eintritt, müssen Sie die Firewall unter Verwendung des Fensters **Firewallrichtlinie/ACL bearbeiten** öffnen. Das kann vorkommen, wenn asymmetrisches Routing verwendet wird, bei dem Datenverkehr vom Router an den CA-Server den Router über eine Schnittstelle verlässt und zurücklaufender Datenverkehr durch eine andere Schnittstelle in den Router eintritt.
- Cisco SDM ermittelt die ausgehenden Schnittstellen im Router, wenn der Passthrough-ACE hinzugefügt wird. Wenn ein Protokoll für dynamisches Routing für die Ermittlung der Routen zum CA-Server verwendet wird und sich eine Route ändert – die ausgehende Schnittstelle ändert sich für SCEP-Datenverkehr, der für den CA-Server bestimmt ist – müssen Sie für die Schnittstellen ausdrücklich einen Passthrough-ACE über das Fenster **Firewallrichtlinie/ACL bearbeiten** hinzufügen.
- Cisco SDM fügt Passthrough-ACEs für SCEP-Datenverkehr hinzu. SDM fügt keine Passthrough-ACEs für gesperrten Datenverkehr wie CRL-Datenverkehr und OCSP-Datenverkehr hinzu. Sie müssen Passthrough-ACEs ausdrücklich für diesen Datenverkehr über das Fenster **Firewallrichtlinie/ACL bearbeiten** hinzufügen.

Schaltfläche Details

Klicken Sie auf diese Schaltfläche, um den Zugriffssteuerungseintrag anzuzeigen, den Cisco SDM zur Firewall hinzufügt, wenn Sie die Änderung zulassen.

Details zu „Firewall öffnen“

Dieses Fenster zeigt den Access Control Entry (ACE) an, den Cisco SDM einer Firewall hinzufügen würde, um verschiedene Arten von Datenverkehr an den Router zu aktivieren. Dieser Eintrag wird erst dann hinzugefügt, wenn Sie im Fenster **Firewall öffnen** die Option **Ändern** aktivieren und den Assistenten abschließen.

KAPITEL 18

Certificate Authority-Server

Sie können einen Cisco IOS-Router konfigurieren, der als Certificate Authority (CA)-Server dient. Ein CA-Server verarbeitet Zertifikatsregistrierungsanforderungen von Clients und kann digitale Zertifikate ausstellen und sperren.

Um einen CA-Server zu erstellen, zu sichern, wiederherzustellen oder zu bearbeiten, wählen Sie **Konfigurieren > VPN > Public-Key-Infrastruktur > Certificate Authority > CA-Server erstellen**.

Um Zertifikate auf einem vorhandenen CA-Server zu verwalten, wählen Sie **Konfigurieren > VPN > Public-Key-Infrastruktur > Certificate Authority > CA-Server verwalten**.

Wenn Sie einen CA-Server überwachen möchten, wählen Sie **Monitor > VPN-Status > CA-Server**.

CA-Server erstellen

Über dieses Fenster können Sie einen Assistenten aufrufen, um einen Certificate Authority (CA)-Server zu erstellen oder einen CA-Server wiederherzustellen. Es kann jeweils nur ein CA-Server auf einem Cisco IOS-Router eingerichtet werden.

Der CA-Server sollte verwendet werden, um im privaten Netzwerk Zertifikate für Hosts auszustellen, sodass sie die Zertifikate nutzen können, um sich gegenseitig zu authentifizieren.

Erforderliche Aufgaben

Wenn Cisco SDM feststellt, dass es Konfigurationsaufgaben gibt, die vorgenommen werden sollten, bevor Sie mit der Konfiguration des CA-Servers beginnen, werden Sie in diesem Feld durch eine Alarmmeldung auf diese Aufgaben hingewiesen. Neben der Alarmmeldung ist ein Link verfügbar, über den Sie zur entsprechenden Stelle in Cisco SDM wechseln können und die Konfiguration fertig stellen können. Wenn Cisco SDM keine fehlenden Konfigurationen feststellt, wird dieses Feld nicht angezeigt. Unter Erforderliche Aufgaben für PKI-Konfigurationen werden mögliche vorausgesetzte Aufgaben beschrieben.

Erstellen eines Certificate Authority (CA)-Servers

Klicken Sie auf diese Schaltfläche, um einen CA-Server auf dem Router zu erstellen. Da auf dem Router nur ein CA-Server konfiguriert werden kann, ist diese Schaltfläche deaktiviert, wenn bereits ein CA-Server konfiguriert ist.

Hinweis Mit dem CA-Server, den Sie mit dem SDM konfigurieren, können Sie Zertifikate ausstellen und sperren. Obwohl der Router die Seriennummern und andere identifizierende Informationen zu den ausgestellten Zertifikaten speichert, speichert er nicht die Zertifikate selbst. Der CA-Server sollte mit einer URL zu einem Registration Authority (RA)-Server konfiguriert werden, der die vom CA-Server ausgestellten Zertifikate speichern kann.

Wiederherstellen eines Certificate Authority (CA)-Servers

Wenn auf dem Router bereits ein CA-Server betrieben wird, können Sie die CA-Server-Konfiguration und die Informationen wiederherstellen. Wenn auf dem Router kein CA-Server konfiguriert ist, ist diese Option deaktiviert.

Erforderliche Aufgaben für PKI-Konfigurationen

Bevor Sie eine Zertifikatsregistrierung oder CA-Serverkonfiguration starten, müssen Sie eventuell erst einige unterstützende Konfigurationsaufgaben durchführen. Der SDM prüft die aktuelle Konfiguration, bevor Sie beginnen können, weist Sie auf vorzunehmende Konfigurationen hin und liefert Links, die Sie zu den Bereichen des SDMs leiten, wo Sie diese Konfigurationen vornehmen können.

Der SDM kann Warnmeldungen zu den folgenden Konfigurationsaufgaben ausgeben:

- SSH-Anmeldeinformationen nicht verifiziert – Cisco SDM benötigt Ihre SSH-Anmeldeinformationen, bevor Sie mit der Registrierung beginnen können.
- NTP/SNTP nicht konfiguriert – Für die Zertifikatsregistrierung muss die genaue Routerzeit eingestellt sein. Durch die Identifikation eines Network Time Protocol-Servers kann Ihr Router die korrekte Zeit abfragen, und es steht eine Zeitquelle zur Verfügung, die nicht davon beeinträchtigt wird, wenn der Router neu gestartet werden muss. Wenn Ihre Organisation nicht über einen NTP-Server verfügt, empfiehlt es sich, einen öffentlich verfügbaren Server zu verwenden, wie unter der folgenden URL erläutert:

  http://www.eecis.udel.edu/~mills/ntp/clock2a.html
- DNS nicht konfiguriert – Wenn Sie DNS-Server angeben, erhöhen Sie die Wahrscheinlichkeit, dass der Router Kontakt mit dem Zertifizierungsserver aufnehmen kann. Die DNS-Konfiguration ist für den Kontakt mit dem CA-Server und anderen Servern erforderlich, die bei der Registrierung von Zertifikaten eingesetzt werden, wie OCSP-Server oder Speicherorte der CRL (Sperrliste, Certificate Revocation List), wenn diese Server als Namen und nicht als IP-Adressen eingegeben wurden.
- Domäne und/oder Hostname nicht konfiguriert – Es wird empfohlen eine Domäne und einen Hostnamen zu konfigurieren, bevor Sie mit der Registrierung beginnen.

CA-Server-Assistent: Willkommen

Der Certificate Authority (CA)-Server-Assistent führt Sie durch die Konfiguration eines CA-Servers. Halten Sie die folgenden Informationen bereit, bevor Sie beginnen:

- Allgemeine Informationen zum CA-Server – Den Namen, den Sie dem Server geben möchten, den Namen des Zertifikatausstellers, der verwendet werden soll, sowie den Benutzernamen und das Kennwort, das Registrierende eingeben müssen, wenn sie eine Registrierungsanforderung an den Server senden.
- Detailliertere Informationen zum Server – Ob der Server im Registration Authority (RA)-Modus oder Certificate Authority (CA)-Modus betrieben wird, die Informationsstufe zu jedem Zertifikat, das der Server speichert, ob der Server Zertifikate automatisch ausstellen soll sowie die Lebensdauer der ausgestellten Zertifikate und offene Registrierungsanforderungen.
- Unterstützende Informationen – Links zum RA-Server, der die Zertifikate speichert, und zum CRL-Verteilungspunkt (CDP)-Server.

CA-Server-Assistent: Certificate Authority-Informationen

Geben Sie grundlegende Informationen zum CA-Server ein, den Sie in diesem Fenster konfigurieren.

CA-Server-Name

Geben Sie einen Namen ein, um den Server im Feld **CA-Server-Name** zu identifizieren. Dies kann der Hostname des Routers oder ein anderer von Ihnen eingegebener Name sein.

Gewähren

Wählen Sie **Manuell**, wenn Zertifikate manuell gewährt werden sollen. Wählen Sie **Auto**, wenn der Server Zertifikate automatisch gewähren soll. Die vor allem für Debug-Zwecke verwendete Option **Auto** wird nicht empfohlen, weil dadurch Zertifikate für jeden Anfordernden ausgestellt werden, ohne dass Registrierungsinformationen erforderlich sind.

Warnung **Setzen Sie Gewähren nicht auf Auto, wenn Ihr Router mit dem Internet verbunden ist. Gewähren sollte nur für interne Zwecke auf Auto eingestellt werden, z. B. für die Ausführung von Debugging-Vorgängen.**

CDP URL

Geben Sie die URL zu einem CRL-Verteilungspunkt (CDP)-Server in das Feld **CDP URL** ein. Der URL muss ein HTTP URL sein. Es folgt eine Beispiel-URL:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

Die Sperrliste (Certificate Revocation List, CRL) ist die Liste gesperrter Zertifikate. Geräte, die die Gültigkeit eines Zertifikats von einem anderen Gerät überprüfen müssen, rufen die CRL vom CA-Server ab. Da viele Geräte gleichzeitig versuchen können, die CRL abzurufen, empfiehlt es sich, sie auf einem Remote-Gerät abzulegen, vorzugsweise einem HTTP-Server, um die Leistung des Cisco IOS-Routers mit dem CA-Server nicht zu beeinträchtigen. Wenn das überprüfende Gerät keine Verbindung zum CDP herstellen kann, verwendet es als Alternative SCEP, um die CRL vom CA-Server abzurufen.

Ausstellername-Attribute

Allgemeiner Name (cn)

Geben Sie den allgemeinen Namen (Common Name) ein, den Sie für dieses Zertifikat verwenden möchten. Dies kann der CA-Server-Name, der Router-Hostname oder ein anderer Name Ihrer Wahl sein.

Unternehmenseinheit (ou)

Geben Sie die Unternehmenseinheit (Organizational Unit) oder den Abteilungsnamen ein, die bzw. der in diesem Zertifikat verwendet werden soll. Als Unternehmenseinheiten kommen beispielsweise IT-Support oder Engineering (Technik) in Frage.

Unternehmen (o)

Geben Sie den Organisationsnamen oder Unternehmensnamen ein.

Bundesland (st)

Geben Sie das Bundesland (State) ein, in dem sich die Organisation befindet.

Land (c)

Geben Sie das Land (Country) ein, in dem sich die Organisation befindet.

E-Mail (e)

Geben Sie die E-Mail-Adresse ein, die im Router-Zertifikat aufgenommen werden soll.

Erweiterte Optionen

Klicken Sie auf diese Schaltfläche, um erweiterte Optionen für den CA-Server einzugeben.

Erweiterte Optionen

Im Bildschirm **Erweiterte Optionen** können Sie Standardwerte für Servereinstellungen ändern und die URL für die Datenbank angeben, die die Zertifikatsinformationen enthalten soll.

Datenbank

Konfigurieren Sie die Datenbankebene, die Datenbank-URL und das Datenbankformat in diesem Abschnitt des Dialogfensters.

Datenbankebene

Wählen Sie den Datentyp, der in der Datenbank für die Zertifikatsregistrierung gespeichert werden soll:

- **Minimal –** Es werden ausreichend Informationen gespeichert, um neue Zertifikate ohne Konflikte ausstellen zu können. Dies ist die Standardeinstellung.
- **Namen –** Neben den Informationen der Option **Minimal** umfasst dies die Seriennummer und den Betreff jedes Zertifikats.
- **Vollständig –** Neben den Informationen der Optionen **Minimal** und **Namen** wird jedes ausgestellte Zertifikat in der Datenbank festgehalten.

Datenbank-URL

Geben Sie den Ort an, wo der CA-Server Zertifikatsregistrierungsdaten schreibt. Wird kein Ort angegeben, werden die Zertifikatsregistrierungsdaten standardmäßig in den Flash-Speicher geschrieben.

Um Zertifikatsregistrierungsdaten beispielsweise auf einen TFTP-Server zu schreiben, geben Sie tftp://mytftp ein. Um die Datenbank-URL auf Flash-Speicher zurückzusetzen, geben Sie nvram ein.

Datenbankarchiv

Wählen Sie **pem**, um das Archiv im pem-Format zu erstellen, oder **pkcs12**, um das Archiv im pkcs12-Format zu erstellen.

Datenbank-Benutzername

Geben Sie einen Benutzernamen für das Datenbankarchiv im Feld **Datenbank-Benutzername** ein. Der Benutzername und das Kennwort werden verwendet, um den Server in der Datenbank zu authentifizieren.

Datenbank-Kennwort und Kennwort bestätigen

Geben Sie ein Kennwort in das Feld **Datenbank-Kennwort** ein, und geben Sie es in das Feld **Kennwort bestätigen** erneut ein.

Gültigkeitsdauer

Legen Sie die Gültigkeitsdauer oder die Zeit bis zum Ablauf der Elemente fest, die mit dem CA-Server verknüpft sind. Um die Gültigkeitsdauer für ein bestimmtes Element festzulegen, wählen Sie es aus der Dropdown-Liste **Gültigkeitsdauer** aus und geben einen Wert in das gleichnamige Feld ein.

Sie können eine Gültigkeitsdauer für die folgenden Elemente festlegen:

- **Zertifikat** – Vom CA-Server ausgestellte Zertifikate. Die Gültigkeitsdauer wird in Tagen im Bereich von 1 bis 1825 angegeben. Wenn kein Wert eingegeben wird, läuft das Zertifikat nach einem Jahr ab. Wenn ein neuer Wert eingegeben wird, betrifft er nur Zertifikate, die nach dem Inkrafttreten des Wertes erstellt wurden.
- **CRL** – Die Sperrliste (Certificate Revocation List) für vom CA-Server ausgestellte Zertifikate. Die Gültigkeitsdauer wird in Stunden im Bereich von 1 bis 336 angegeben. Wenn kein Wert eingegeben wird, läuft die CRL nach 168 Stunden (eine Woche) ab.

- **Registrierungsanforderung** – Offene Zertifikatsanforderungen in der Registrierungsdatenbank, jedoch ohne über SCEP erhaltene Anforderungen. Die Gültigkeitsdauer wird in Stunden im Bereich von 1 bis 1000 angegeben. Wenn kein Wert eingegeben wird, läuft eine offene Registrierungsanforderung nach 168 Stunden (eine Woche) ab.

CA-Server-Assistent: RSA-Schlüssel

Der CA-Server verwendet öffentliche und private RSA-Schlüssel, um Daten zu verschlüsseln und Zertifikate zu signieren. Der SDM generiert automatisch ein neues Schlüsselpaar und gibt ihm den Namen des CA-Servers. Sie können das Schlüsselmodul und den -typ ändern und den Schlüssel exportierbar machen. Sie müssen eine Passphrase eingeben, die für die Wiederherstellung des CA-Servers zu verwenden ist.

Bezeichnung

Dieses Feld ist schreibgeschützt. Der SDM verwendet den Namen des CA-Servers als Namen des Schlüsselpaars.

Modul

Geben Sie den Wert des Schlüsselmoduls ein. Wenn Sie einen Modulwert zwischen 512 und 1024 wünschten, geben Sie einen Ganzzahlwert ein, der ein Vielfaches von 64 ist. Wenn Sie einen Wert über 1024 wünschen, können Sie 1536 oder 2048 eingeben. Wenn Sie einen größeren Wert als 512 eingeben, kann die Generierung des Schlüssels mindestens eine Minute dauern.

Der Modulwert bestimmt die Größe des Schlüssels. Je größer der Modulwert ist, desto sicherer ist der Schlüssel. Die Erstellung von Schlüsseln mit großen Modulwerten beansprucht jedoch mehr Zeit bei der Erstellung, und die Verschlüsselung/Entschlüsselung dauert länger, wenn große Schlüssel verwendet werden.

Typ

Standardmäßig erstellt Cisco SDM ein allgemeines Schlüsselpaar, das für die Verschlüsselung und für die Signatur verwendet wird. Wenn Cisco SDM separate Schlüsselpaare für die Verschlüsselung und das Signieren von Dokumenten generieren soll, wählen Sie **Verwendungsschlüssel**. Cisco SDM generiert Verwendungsschlüssel für das Verschlüsseln und Signieren.

Schlüssel ist exportierbar

Aktivieren Sie **Schlüssel ist exportierbar**, wenn der CA-Server-Schlüssel exportierbar sein soll.

Passphrase und Passphrase bestätigen

Geben Sie in das Feld **Passphrase** eine Passphrase ein, die verwendet werden soll, wenn der CA-Server von einem Backup wiederhergestellt wird. Geben Sie dieselbe Passphrase in das Feld **Passphrase bestätigen** ein.

Firewall öffnen

Das Fenster **Firewall öffnen** wird angezeigt, wenn eine Firewall-Konfiguration geändert werden muss, um die Kommunikation zwischen CDP-Server und CA-Server zuzulassen. Wählen Sie die Schnittstelle aus, und aktivieren Sie das Kontrollkästchen **Ändern**, um es dem SDM zu erlauben, die Firewall zu ändern, damit dieser Datenverkehr zugelassen wird. Klicken Sie auf **Details**, um den ACE anzuzeigen, der zur Firewall hinzugefügt wird.

CA-Server-Assistent: Übersicht

Das Fenster **Zusammenfassung** zeigt die Informationen an, die Sie in die Bildschirme des Assistenten eingegeben haben, sodass Sie diese nochmals überprüfen können, bevor sie an den Router gesendet werden. Es folgt eine Beispielzusammenfassung:

```
---------------------------------------------------------------
CA-Server-Konfiguration
---------------------------------------------------------------
CA-Server-Name: CASvr-a
Gewähren: Manuell
CDP URL: http://192.27.108.92/snrs.com
Allgemeiner Name (cn): CS1841
Organisationseinheit (ou): IT Support
Organisation (o): Acme Enterprises
Bundesland (st): CA
Land (c): USA
```

```
------------------------------------------------------------
Erweiterte CA-Server-Konfiguration
------------------------------------------------------------
Datenbank-URL: nvram
Datenbankarchiv: pem
Datenbank-Benutzername: bjones
Datenbank-Kennwort: *********

------------------------------------------------------------
RSA-Schlüssel:
------------------------------------------------------------
Der CA-Server generiert automatisch ein RSA-Schlüsselpaar mit den
folgenden Standardwerten:-
Modul: 1024
Schlüsseltyp: Allgemein
Exportierbarer Schlüssel: Nein
Konfigurierte Passphrase: ******


------------------------------------------------------------
Firewall-Passthrough-ACEs für Schnittstelle(n):
------------------------------------------------------------

FastEthernet0/0
    permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

Die Zusammenfassung enthält vier Abschnitte, den Abschnitt für die CA-Server-Konfiguration, für die erweiterte Konfiguration des CA-Servers, für die RSA-Schlüssel und den Firewall-Passthrough. Der Name dieses CA-Servers lautet CAsvr-a. Zertifikate werden manuell gewährt. Die Zertifikatinformationen werden in nvram im Format PEM gespeichert. Der SDM generiert ein allgemeines Schlüsselpaar mit dem Standardmodul 1024. Der Schlüssel ist nicht exportierbar. Es wird ein ACE konfiguriert, damit Datenverkehr zwischen dem Router und dem CDP-Host mit der IP-Adresse 192.27.108.92 zugelassen wird.

CA-Server verwalten

Sie können den CA-Server über dieses Fenster starten und anhalten, Zertifikatsanforderungen gewähren und ablehnen sowie Zertifikate sperren. Wenn Sie die CA-Server-Konfiguration ändern müssen, können Sie den Server über dieses Fenster deinstallieren und zum Fenster **CA-Server erstellen** zurückkehren, um die erforderliche Serverkonfiguration zu erstellen.

Name

Zeigt den Namen des Servers an. Der Name des Servers wurde erstellt, als der Server erstellt wurde.

Statussymbol

Wenn der CA-Server läuft, wird das Wort Läuft und ein grünes Symbol angezeigt. Wenn der CA-Server nicht läuft, wird das Wort Angehalten und ein rotes Symbol angezeigt.

Server starten

Die Schaltfläche **Server starten** wird angezeigt, wenn der Server angehalten wurde. Klicken Sie auf **Server starten**, um den CA-Server zu starten.

Server anhalten

Die Schaltfläche **Server anhalten** wird angezeigt, wenn der Server läuft. Klicken Sie auf **Server anhalten**, wenn Sie den CA-Server anhalten müssen.

Server sichern

Klicken Sie auf **Server sichern**, um die Serverkonfigurationsdaten auf dem PC zu sichern. Geben Sie den Sicherungsort im angezeigten Dialogfeld ein.

Server deinstallieren

Klicken Sie auf diese Schaltfläche, um den CA-Server vom Cisco IOS-Router zu deinstallieren. Alle CA-Server-Konfigurationen und -Daten werden entfernt. Wenn Sie den CA-Server vor der Deinstallation gesichert haben, können Sie dessen Daten nur wiederherstellen, nachdem Sie einen neuen CA-Server erstellt haben. Siehe CA-Server erstellen.

Details zum CA-Server

Die Tabelle **Details zum CA-Server** liefert einen Snapshot der CA-Server-Konfiguration. Die folgende Tabelle zeigt Beispielinformationen.

Elementname	Elementwert
Gültigkeitsdauer des CA-Zertifikats	1095 Tage
CDP URL	http://192.168.7.5
CRL-Gültigkeitsdauer	168 Stunden
Gültigkeitsdauer des Zertifikats	365 Tage
Datenbankebene	Minimal
Datenbank-URL	nvram:
Gültigkeitsdauer der Registrierungsanforderung	168 Stunden
Gewähren	Manuell
Name des Ausstellers	CN=CertSvr
Modus	Certificate Authority
Name	CertSvr

Eine Beschreibung dieser Elemente finden Sie unter CA-Server-Assistent: Certificate Authority-Informationen und Erweiterte Optionen.

CA-Server sichern

Sie können die Dateien, die die Informationen für den CA-Server enthalten, auf Ihrem PC sichern. Das Fenster **CA-Server sichern** führt die Dateien auf, die gesichert werden. Die aufgeführten Dateien müssen im NVRAM des Routers vorhanden sein, damit die Sicherung erfolgreich ist.

Klicken Sie auf **Durchsuchen**, und geben Sie einen Ordner auf dem PC an, in dem die CA-Server-Dateien gesichert werden sollen.

Fenster „CA-Server verwalten: Fenster wiederherstellen“

Wenn Sie einen CA-Server gesichert und deinstalliert haben, können Sie die Serverkonfiguration auf dem Router wiederherstellen, indem Sie auf die Schaltfläche **CA-Server wiederherstellen** klicken. Sie müssen den CA-Server-Namen, die vollständige Datenbank-URL und die Passphrase für die Sicherung angeben können, die während der ursprünglichen Konfiguration verwendet wurde. Wenn Sie den CA-Server wiederherstellen, erhalten Sie die Gelegenheit, die Konfigurationseinstellungen zu ändern.

CA-Server wiederherstellen

Wenn Sie die Konfiguration für einen deinstallierten CA-Server gesichert haben, können Sie diese wiederherstellen, indem Sie die entsprechenden Informationen im Fenster **CA-Server wiederherstellen** eingeben. Sie können die Einstellungen für den Server bearbeiten, indem Sie auf **CA-Server-Einstellungen vor der Wiederherstellung bearbeiten** klicken. Sie müssen den Namen, das Dateiformat, die URL zur Datenbank und die Passphrase angeben, damit der Server gesichert oder die Server-Einstellungen bearbeitet werden können.

CA-Server-Name

Geben Sie den Namen des gesicherten CA-Servers ein.

Dateiformat

Wählen Sie das Dateiformat, das in der Serverkonfiguration angegeben war, entweder PEM oder PKCS12.

Vollständige URL

Geben Sie die Router-Datenbank-URL ein, die bei der Konfiguration des CA-Servers angegeben wurde. Das ist der Ort, an den der CA-Server die Zertifikatsregistrierungsdaten schreibt. Es folgen zwei Beispiel-URLs:

```
nvram:/mycs_06.p12
tftp://192.168.3.2/mycs_06.pem
```

Passphrase

Geben Sie die Passphrase ein, die bei der Konfiguration des CA-Servers eingegeben wurde.

CA-Server-Dateien vom PC kopieren

Aktivieren Sie das Kontrollkästchen **CA-Server-Dateien vom PC kopieren**, wenn Sie die auf dem PC gesicherten Serverinformationen in den nvram des Routers kopieren möchten.

CA-Server-Einstellungen vor der Wiederherstellung bearbeiten

Klicken Sie auf **CA-Server-Einstellungen vor der Wiederherstellung bearbeiten**, wenn Sie die CA-Server-Konfigurationseinstellungen vor der Wiederherstellung des Servers bearbeiten möchten. Weitere Informationen zu den Einstellungen, die Sie ändern können, finden Sie unter CA-Server-Assistent: Certificate Authority-Informationen und CA-Server-Assistent: RSA-Schlüssel.

CA-Server-Einstellungen bearbeiten Registerkarte „Allgemein“

In diesem Fenster bearbeiten Sie die CA-Server-Konfigurationseinstellungen. Sie können den Namen des CA-Servers nicht ändern. Weitere Informationen zu den Einstellungen, die Sie ändern können, finden Sie unter CA-Server-Assistent: Certificate Authority-Informationen.

CA-Server-Einstellungen bearbeiten Registerkarte „Erweitert“

In diesem Fenster können Sie alle erweiterten CA-Server-Einstellungen ändern. Weitere Informationen zu diesen Einstellungen finden Sie unter Erweiterte Optionen.

CA-Server verwalten: CA-Server nicht konfiguriert

Dieses Fenster wird angezeigt, wenn Sie auf **CA-Server verwalten** klicken, jedoch kein CA-Server konfiguriert ist. Klicken Sie auf **CA-Server erstellen** und folgen Sie den Anweisungen des Assistenten, um einen CA-Server auf Ihrem Router zu konfigurieren.

Zertifikate verwalten

Wenn Sie auf **VPN > Public-Key-Infrastruktur > Certificate Authority > Zertifikate verwalten** klicken, wird die Registerkarte **Anstehende Anforderungen** und **Gesperrte Zertifikate** angezeigt. Wenn Sie zu diesen Registerkarten Hilfe-Themen anzeigen möchten, klicken Sie auf die folgenden Links:

- Anstehende Anforderungen
- Gesperrte Zertifikate

Anstehende Anforderungen

Dieses Fenster zeigt eine Liste der vom CA-Server von Clients erhaltenen Zertifikatsregistrierungsanforderungen an. Der obere Teil des Fensters enthält CA-Server-Informationen und Steuerungen. Weitere Informationen zum Anhalten, Starten und Deinstallieren des CA-Servers finden Sie unter CA-Server verwalten.

Sie können eine Zertifikatsregistrierungsanforderung in der Liste auswählen und dafür dann **Ausstellen** (akzeptieren), **Ablehnen** oder **Löschen** wählen. Die verfügbaren Aktionen hängen vom Status der gewählten Zertifikatsregistrierungsanforderung ab.

Alles auswählen

Klicken Sie auf **Alles auswählen**, um alle anstehenden Zertifikatsanforderungen auszuwählen. Wenn alle Zertifikatsanforderungen ausgewählt sind, werden durch Klicken auf **Gewähren** alle Anforderungen gewährt. Wenn Sie auf **Ablehnen** klicken, wenn alle Zertifikate ausgewählt sind, werden alle Anforderungen abgelehnt.

Gewähren

Klicken Sie auf **Gewähren**, um dem anfordernden Client das Zertifikat auszustellen.

Hinweis Das CA-Server-Fenster zeigt nicht die IDs der gewährten Zertifikate. Falls es notwendig sein sollte, ein Zertifikat zu sperren, können Sie die Zertifikats-ID vom Administrator des Clients erhalten, für den das Zertifikat ausgestellt wurde. Der Client-Administrator kann die Zertifikats-ID ermitteln, indem er den Cisco IOS-Befehl „sh crypto pki cert“ eingibt.

Löschen

Klicken Sie auf **Löschen**, um die Zertifikatsregistrierungsanforderung aus der Datenbank zu entfernen.

Ablehnen

Klicken Sie auf **Ablehnen**, um die Zertifikatsregistrierungsanforderung zu verweigern.

Aktualisieren

Klicken Sie auf **Aktualisieren**, um die Zertifikatsregistrierungsanforderungen mit den letzten Änderungen zu aktualisieren.

Bereich für Zertifikatsregistrierungsanforderungen

Der Bereich für die Zertifikatsregistrierungsanforderungen verfügt über die folgenden Spalten:

Anforderungs-ID – Eine eindeutige Nummer, die der Zertifikatsregistrierungsanforderung zugewiesen ist.

Status – Der aktuelle Status der Zertifikatsregistrierungsanforderung. Der Status kann **Anstehend** (keine Entscheidung), **Gewährt** (Zertifikat ausgestellt), **Abgelehnt** (Anforderung abgelehnt) lauten.

Fingerabdruck – Ein eindeutiger digitaler Client-Identifikator.

Betreff – Die Bezeichnung des Betreffs in der Registrierungsanforderung.

Es folgt eine Beispiel-Registrierungsanforderung:

Anforderungs-ID	Status	Fingerabdruck	Betreff
1	anstehend	serialNumber=FTX0850Z0GT+ hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FDB BB5E8BA

Zertifikat sperren

Klicken Sie auf **Zertifikat sperren**, um ein Dialogfeld anzuzeigen, in das Sie die ID des Zertifikats eingeben können, das Sie sperren möchten.

Hinweis Die Zertifikats-ID entspricht nicht immer der in den CA-Server-Fenstern angezeigten Anforderungs-ID. Es kann notwendig sein, die ID des zu sperrenden Zertifikats vom Administrator des Clients zu erfragen, für den das Zertifikat gewährt wurde. Weitere Informationen dazu, wie der Administrator die Zertifikats-ID ermitteln kann, finden Sie unter Anstehende Anforderungen.

Gesperrte Zertifikate

Dieses Fenster zeigt auch eine Liste der ausgestellten und gesperrten Zertifikate an. Es können nur ausgestellte Zertifikate gesperrt werden. Der obere Teil des Fensters enthält CA-Server-Informationen und Steuerungen. Weitere Informationen zum Anhalten, Starten und Deinstallieren des CA-Servers finden Sie unter CA-Server verwalten.

Die Zertifikatsliste enthält folgende Spalten:

- **Certificate Serial Number** (Zertifikatsseriennummer) – Eine eindeutige Nummer, die dem Zertifikat zugewiesen ist. Diese Nummer wird im Hexadezimalformat angezeigt. Die dezimale Seriennummer 1 wird beispielsweise als 0x01 angezeigt.
- **Datum der Sperrung** – Uhrzeit und Datum, wann das Zertifikat gesperrt wurde. Wenn ein Zertifikat am 6. Februar 2007 41 Minuten und 20 Sekunden nach Mitternacht gesperrt wurde, wird das Sperrdatum als 00:41:20 UTC Feb 6 2007 angezeigt.

Zertifikat sperren

Klicken Sie auf **Zertifikat sperren**, um ein Dialogfeld anzuzeigen, in dem Sie die ID des Zertifikats eingeben können, das Sie sperren möchten.

Hinweis Die Zertifikats-ID entspricht nicht immer der in den CA-Server-Fenstern angezeigten Anforderungs-ID. Es kann notwendig sein, die ID des zu sperrenden Zertifikats vom Administrator des Clients zu erfragen, für den das Zertifikat gewährt wurde. Weitere Informationen dazu, wie der Administrator die Zertifikats-ID ermitteln kann, finden Sie unter Anstehende Anforderungen.

Zertifikat sperren

Sie können in diesem Fenster Zertifikate sperren, die vom CA-Server gewährt wurden.

Zertifikats-ID

Geben Sie die ID des Zertifikats ein, das Sie sperren möchten.

Hinweis Die Zertifikats-ID entspricht nicht immer der in den CA-Server-Fenstern angezeigten Anforderungs-ID. Es kann notwendig sein, die ID des zu sperrenden Zertifikats vom Administrator des Clients zu erfragen, für den das Zertifikat gewährt wurde. Weitere Informationen dazu, wie der Administrator die Zertifikats-ID ermitteln kann, finden Sie unter Anstehende Anforderungen.

KAPITEL 19

Cisco IOS SSL VPN

Cisco IOS SSL VPN bietet eine Remote-Zugriff-Konnektivität über ein Secure Socket Layer (SSL)-VPN von fast jedem Internet-fähigen Standort aus. Dazu benötigen Sie nur einen Webbrowser mit der dazugehörigen nativen SSL-Verschlüsselung. Auf diese Weise können Unternehmen ihre sicheren Unternehmensnetzwerke für beliebige autorisierte Benutzer erweitern, indem sie Remote-Zugriff-Konnektivität für Unternehmensressourcen von jedem Internet-fähigen Standort bereitstellen.

Cisco IOS SSL VPN ermöglicht zusätzlich den Zugriff von anderen als den unternehmenseigenen Geräten, einschließlich Heimcomputern, Internet-Kiosks und Wireless-Hotspots, bei denen eine IT-Abteilung die VPN-Client-Software, die für IPSec VPN-Verbindungen erforderlich ist, nicht einfach einsetzen und verwalten kann.

Es gibt drei Modi für den SSL-VPN-Zugriff: Clientless, Thin Client und Full Tunnel-Client. Cisco SDM unterstützt alle drei. Die einzelnen Modi werden nachfolgend beschrieben:

- **Clientless SSL VPN** – Der Clientless-Modus bietet den sicheren Zugriff auf private Web-Ressourcen und ermöglicht den Zugriff auf Web-Inhalte. Dieser Modus ist nützlich für den Zugriff auf die meisten Inhalte, die Sie erwartungsgemäß in einem Webbrowser verwenden, zum Beispiel Intranet-Zugriff und Online-Tools, die eine Web-Oberfläche nutzen.
- **Thin Client SSL VPN** (Java-Applet zur Portweiterleitung) – Der Thin Client-Modus erweitert die Möglichkeiten der Kryptografiefunktionen des Webbrowsers, um den Remote-Zugriff auf TCP-basierte Anwendungen wie POP3, SMTP, IMAP, Telnet und SSH zu ermöglichen.

- **Full Tunnel-Client SSL VPN** – Der Full Tunnel-Client-Modus bietet über seine dynamisch heruntergeladene SSL VPN-Client-Software für Cisco IOS-SSL VPN umfassende Anwendungsunterstützung. Mit dem Full Tunnel-Client für Cisco IOS SSL VPN stellen wir einen leichten, zentral konfigurierten SSL VPN-Tunneling-Client bereit, der einfach zu unterstützen ist und per Netzwerkschicht-Konnektivität den Zugriff auf fast jede Anwendung ermöglicht.

Cisco IOS SSL VPN-Kontexte, Gateways und Richtlinien erläutert, wie die Komponenten einer Cisco IOS SSL VPN-Konfiguration zusammenwirken.

Klicken Sie auf Cisco IOS SSL VPN-Links unter Cisco.com, um Links zu Cisco IOS SSL VPN-Dokumenten anzuzeigen.

Cisco IOS SSL VPN-Links unter Cisco.com

Dieses Hilfethema führt die aktuellen Links auf, die die nützlichsten Informationen zu Cisco IOS SSL VPN enthalten.

Über den folgenden Link gelangen Sie zu Dokumenten, die Cisco IOS SSL VPN beschreiben. Kehren Sie von Zeit zu Zeit zu diesem Link zurück, um die neuesten Informationen abzurufen.

www.cisco.com/go/iosSSLVPN

Unter dem folgende Link wird erläutert, wie ein AAA-Server mit dem RADIUS-Protokoll für Cisco IOS SSL VPN konfiguriert wird.

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

SSL VPN erstellen

Sie können mit den Cisco IOS SSL VPN-Assistenten ein neues Cisco IOS SSL VPN erstellen oder neue Richtlinien oder Funktionen zu einem vorhandenen Cisco IOS SSL VPN hinzufügen.

Klicken Sie auf Cisco IOS SSL VPN, um eine Übersicht über die Funktionen aufzurufen, die Cisco SDM unterstützt. Cisco IOS SSL VPN-Kontexte, Gateways und Richtlinien erläutert, wie die Komponenten einer Cisco IOS SSL VPN-Konfiguration zusammenwirken.

Klicken Sie auf Cisco IOS SSL VPN-Links unter Cisco.com, um Links zu Cisco IOS SSL VPN-Dokumenten anzuzeigen.

Erforderliche Aufgaben

AAA und Zertifikate müssen auf dem Router konfiguriert sein, bevor Sie mit einer Cisco IOS SSL VPN-Konfiguration beginnen können. Wenn eine oder beide dieser Konfigurationen fehlen, wird eine Benachrichtigung in diesem Fensterbereich angezeigt, und es erscheint ein Link, über den Sie die fehlende Konfiguration abschließen können. Wenn alle vorausgesetzten Konfigurationen abgeschlossen sind, können Sie zu diesem Fenster zurückkehren und mit der Konfiguration von Cisco IOS SSL VPN beginnen.

Cisco SDM aktiviert AAA ohne Benutzereingabe. Cisco SDM kann Ihnen beim Generieren von öffentlichen und privaten Schlüsseln für den Router helfen und diese bei einer Zertifizierungsstelle registrieren, um digitale Zertifikate zu erwerben. Weitere Informationen finden Sie unter Public-Key-Infrastruktur. Sie können auch ein dauerhaftes selbst signiertes Zertifikat konfigurieren, für das keine Genehmigung einer Zertifizierungsstelle erforderlich ist. Weitere Informationen zur Funktion für dauerhafte selbst signierte Zertifikate finden Sie in den Informationen unter folgendem Link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Stellen Sie sicher, dass der gesamte URL im Link-Feld Ihres Browsers angezeigt wird.

Create a new SSL VPN (Neues SSL VPN erstellen)

Wählen Sie diese Option, um eine neue Cisco IOS SSL VPN-Konfiguration zu erstellen. Mit diesem Assistenten können Sie ein Cisco IOS SSL VPN mit einer Benutzerrichtlinie und einem eingeschränkten Funktionssatz erstellen. Nachdem Sie diesen Assistenten abgeschlossen haben, können Sie die anderen Assistenten verwenden, um zusätzliche Richtlinien und Funktionen für das Cisco IOS-SSL VPN zu erstellen. Sie können zu diesem Assistenten zurückkehren, um weitere Cisco IOS SSL VPN-Konfigurationen zu erstellen.

Wenn Sie Cisco SDM zum Erstellen der ersten Cisco IOS SSL VPN-Konfiguration auf einem Router verwenden, erstellen Sie einen Cisco IOS SSL VPN-Kontext, konfigurieren ein Gateway und erstellen eine Gruppenrichtlinie. Nachdem Sie den Assistenten abgeschlossen haben, klicken Sie auf **Edit SSL VPN** (SSL VPN bearbeiten), um die Konfiguration anzuzeigen und sich mit der Zusammenarbeit der einzelnen Cisco IOS SSL VPN-Komponenten vertraut zu machen. Dazugehörige Informationen finden Sie unter Cisco IOS SSL VPN-Kontexte, Gateways und Richtlinien.

Add a new policy to an existing SSL VPN for a new group of users (Eine neue Richtline für eine neue Benutzergruppe zu einem vorhandenen SSL VPN hinzufügen)

Wählen Sie diese Option aus, um eine neue Richtlinie zu einer vorhandenen Cisco IOS SSL VPN-Konfiguration für eine neue Benutzergruppe hinzuzufügen. Verschiedene Richtlinien ermöglichen es Ihnen, separate Funktionssätze für verschiedene Benutzergruppen zu definieren. So ist es möglicherweise sinnvoll, eine Richtlinie für Konstruktion und eine separate Richtlinie für den Vertrieb zu definieren.

Configure advanced features for an existing SSL VPN (Erweiterte Funktionen für ein vorhandenes SSL VPN konfigurieren)

Wählen Sie diese Option aus, um zusätzliche Funktionen für eine vorhandene Cisco IOS SSL VPN -Richtlinie zu konfigurieren. Sie müssen den Kontext angeben, unter dem diese Richtlinie konfiguriert wird.

Schaltfläche Ausgewählte Aufgabe starten

Klicken Sie auf diese Schaltfläche, um mit der von Ihnen ausgewählte Konfiguration zu beginnen. Wenn Sie die ausgewählte Aufgabe nicht abschließen können, erhalten Sie eine Warnmeldung. Falls es eine Aufgabe gibt, deren Durchführung vorausgesetzt wird, erhalten Sie Informationen dazu, um welche Aufgabe es sich handelt und wie Sie diese Aufgabe durchführen.

Persistent Self-Signed Certificate (Bleibendes selbst signiertes Zertifikat)

In dieses Dialogfeld können Sie die Informationen für ein bleibendes selbst signiertes Zertifikat eingeben. Mit den von Ihnen angegebenen Informationen generiert der HTTPS-Server ein Zertifikat, das beim SSL-Handshake verwendet wird. Dauerhafte selbst signierte Zertifikate verbleiben auch dann in der Konfiguration, wenn der Router neu geladen wird, und werden während des SSL-Handshake-Vorgangs präsentiert. Neue Benutzer müssen diese Zertifikate manuell übernehmen. Jedoch müssen Benutzer, die dies bereits zuvor getan haben, die Zertifikate nicht erneut übernehmen, wenn der Router neu geladen wurde.

Weitere Informationen zu der Funktion für ein dauerhaftes selbst signiertes Zertifikat finden Sie unter folgendem Link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Stellen Sie sicher, dass der gesamte URL im Link-Feld Ihres Browsers angezeigt wird.

Name

Cisco SDM gibt den Namen **Router_Zertifikat** in dieses Feld ein. Sie können den Namen gegebenenfalls ändern. Dies entspricht dem Namen des Zertifikatsinhabers, der in einer Zertifikatsanforderung verwendet wird.

Länge des RSA-Schlüssels

Cisco SDM gibt den Wert 512 in dieses Feld ein. Sie können gegebenenfalls einen längeren Schlüssel festlegen, zum Beispiel 1024. Die Länge des Schlüssels sollte ein Vielfaches von 64 sein.

Zertifikatsinhaber

Geben Sie die Informationen in die Felder des Bereichs **Zertifikatsinhaber** ein. Weitere Informationen zu diesen Feldern finden Sie unter Weitere Zertifikatsinhaberattribute.

Schaltfläche „Generieren“

Nachdem Sie die erforderlichen Informationen in dieses Fenster eingegeben haben, klicken Sie auf **Generieren**. Daraufhin generiert der Router das dauerhafte selbstsignierte Zertifikat.

Willkommen

Im Willkommensfenster der einzelnen Assistenten werden die Aufgaben aufgeführt, die Sie mit dem Assistenten durchführen können. Verwenden Sie diese Informationen, um sicherzustellen, dass Sie den richtigen Assistenten verwenden. Klicken Sie andernfalls auf **Abbrechen**, um zum Fenster **Create SSL VPN** (Neues SSL VPN erstellen) zurückzukehren, und wählen Sie den gewünschten Assistenten aus.

Wenn Sie alle Informationen eingeben, die der Assistent von Ihnen verlangt, zeigt das Übersichtsfenster die Informationen an, die Sie eingegeben haben. Wenn Sie die Cisco IOS CLI-Befehle anzeigen möchten, die Sie an den Router senden, klicken Sie auf **Abbrechen**, um den Assistenten zu verlassen, wählen Sie **Bearbeiten > Einstellungen**, und aktivieren Sie die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden**. Starten Sie dann den Assistenten erneut, und geben Sie die Informationen an, zu deren Eingabe Sie aufgefordert werden. Wenn Sie die Konfiguration an den Router senden, wird ein zusätzliches Fenster angezeigt, in dem Sie die Cisco IOS CLI-Befehle anzeigen können, die Sie senden.

SSL VPN-Gateways

Ein Cisco IOS SSL VPN-Gateway stellt die IP-Adresse und das digitale Zertifikat für die SSL VPN-Kontexte zur Verfügung, die sie benötigen. In diesem Fenster können Sie die Informationen für ein Gateway sowie die Informationen angeben, mit denen die Benutzer auf ein Portal zugreifen können.

Felder IP-Adresse und Name

In diesen Feldern können Sie die URL erstellen, die die Benutzer für den Zugriff auf das Cisco IOS SSL VPN-Portal eingeben. Die IP-Adressenliste enthält die IP-Adressen von allen konfigurierten Routerschnittstellen sowie alle vorhandenen Cisco IOS SSL VPN-Gateways. Sie können die IP-Adresse einer Routerschnittstelle verwenden, wenn es sich um eine öffentliche Adresse handelt, die von den gewünschten Clients erreicht werden kann. Sie können auch eine andere öffentliche IP-Adresse verwenden, die von den Clients erreicht werden kann.

Wenn Sie eine IP-Adresse verwenden, die nicht bereits für ein Gateway verwendet wurde, erstellen Sie ein neues Gateway.

Kontrollkästchen zum Zulassen des Cisco SDM-Zugriffs über IP-Adresse

Aktivieren Sie dieses Kontrollkästchen, wenn Cisco SDM den Zugriff über diese IP-Adresse fortsetzen soll. Dieses Kontrollkästchen wird angezeigt, wenn Sie die IP-Adresse eingegeben haben, die Sie derzeit für den Zugriff auf Cisco SDM verwenden.

Hinweis Wenn Sie dieses Kontrollkästchen aktivieren, ändert sich die URL, die Sie für den Zugriff auf Cisco SDM verwenden müssen, nachdem Sie die Konfiguration an den Router senden. Die URL, die Sie verwenden müssen, finden Sie im Informationsbereich am unteren Fensterrand. Cisco SDM platziert eine Verknüpfung zu dieser URL auf dem Desktop Ihres PCs, über die Sie künftig auf Cisco SDM zugreifen können.

Digitales Zertifikat

Wenn Sie ein neues Gateway erstellen, wählen Sie das digitale Zertifikat aus, das der Router den Clients präsentieren soll, wenn diese sich beim Gateway anmelden. Wenn Sie die IP-Adresse eines vorhandenen Gateway gewählt haben, verwendet der Router das digitale Zertifikat, das für dieses Gateway konfiguriert wurde, und dieses Feld ist deaktiviert.

Informationsbereich

Wenn Sie die Informationen in die Felder für die IP-Adresse und den Namen eingeben, enthält dieser Bereich den URL, den die Benutzer eingeben. Sie müssen diese URL den Benutzern zur Verfügung stellen, für die Sie dieses Cisco IOS SSL VPN erstellen.

Wenn Sie die Option **Allow Cisco SDM access through *IP address*** (Cisco SDM-Zugriff über IP-Adresse zulassen) aktivieren, wird die URL, die Sie künftig für den Zugriff auf Cisco SDM verwenden, in diesem Bereich angezeigt. Cisco SDM platziert eine Verknüpfung zu dieser URL auf dem Desktop Ihres PCs, nachdem Sie die Cisco IOS SSL VPN-Konfiguration an den Router gesendet haben.

Benutzerauthentifizierung

Geben Sie in diesem Fenster an, wie der Router die Benutzerauthentifizierung durchführen soll. Der Router kann Cisco IOS SSL VPN-Benutzer lokal authentifizieren oder Authentifizierungsanforderungen an Remote-AAA-Server senden.

Schaltfläche „Externe AAA-Server“

Klicken Sie auf diese Schaltfläche, wenn Sie möchten, dass der Router einen AAA-Server für die Authentifizierung von Cisco IOS SSL VPN-Benutzern verwendet. Der Router verwendet die AAA-Server, die in diesem Fenster aufgeführt sind. Wenn keine AAA-Server konfiguriert sind, können Sie sie in diesem Fenster konfigurieren. Zur Verwendung dieser Option muss mindestens ein AAA-Server auf dem Router konfiguriert sein.

Schaltfläche „Lokal auf diesem Router“

Klicken Sie auf diese Schaltfläche, wenn der Router die Benutzer selbst authentifizieren soll. Der Router authentifiziert jeden Benutzer, der in diesem Fenster angezeigt wird. Wenn keine Benutzer auf dem Router konfiguriert sind, können Sie in diesem Fenster Benutzer hinzufügen.

Schaltfläche „Zunächst auf einem externen AAA-Server und dann lokal auf diesem Router“

Klicken Sie auf diese Schaltfläche, wenn der Router die Authentifizierung zunächst über einen AAA-Server durchführen und bei Fehlschlagen der Authentifizierung eine lokale Authentifizierung versuchen soll. Wenn der Benutzer weder auf einem konfigurierten AAA-Server noch lokal auf dem Router konfiguriert ist, schlägt die Authentifizierung für diesen Benutzer fehl.

Schaltfläche „AAA-Authentifizierungsmethodenliste verwenden“

Klicken Sie auf diese Schaltfläche, wenn der Router eine Methodenliste zur Authentifizierung verwenden soll. Eine Methodenliste enthält die Authentifizierungsmethoden, die verwendet werden sollten. Der Router versucht die erste Authentifizierungsmethode in der Liste. Wenn die Authentifizierung fehlschlägt, versucht der Router die nächste Methode in der Liste und fährt fort, bis der Benutzer authentifiziert ist oder das Ende der Liste erreicht ist.

Liste „Für diesen Router konfigurierte AAA-Server“

Diese Liste enthält die AAA-Server, die der Router zur Authentifizierung der Benutzer verwendet. Wenn Sie Benutzer mit AAA-Servern authentifizieren möchten, muss diese Liste den Namen oder die IP-Adresse von mindestens einem Server enthalten. Verwenden Sie die Schaltfläche **Hinzufügen**, um Informationen für einen neuen Server hinzuzufügen. Wenn Sie AAA-Konfigurationen auf dem Router verwalten möchten, beenden Sie den Assistenten, klicken Sie auf **Zusätzliche Aufgaben**, und klicken Sie dann in der Baumstruktur für Zusätzliche Aufgaben auf den AAA-Knoten. Diese Liste wird nicht angezeigt, wenn Sie die Option **Lokal auf diesem Router** gewählt haben.

Erstellen Sie Benutzerkonten lokal auf diesem Router

Geben Sie in diese Liste die Benutzer ein, die der Router authentifizieren soll. Verwenden Sie diese Schaltflächen **Hinzufügen und Bearbeiten** für die Verwaltung der Benutzer auf dem Router. Diese Liste wird nicht angezeigt, wenn Sie die Option **Externe AAA-Server** gewählt haben.

Intranet-Websites konfigurieren

Konfigurieren Sie in diesem Fenster Gruppen von Intranet-Websites, auf welche die Benutzer zugreifen dürfen. Diese Links werden im Portal angezeigt, das den Benutzern von diesem Cisco IOS SSL VPN beim Anmelden angezeigt wird.

Spalten „Vorgang und URL-Liste“

Wenn Sie eine Richtlinie zu einem vorhandenen Cisco IOS SSL VPN-Kontext hinzufügen, sind in der daraufhin angezeigten Tabelle möglicherweise URL-Listen enthalten. Aktivieren Sie die Option **Auswählen**, wenn Sie die angezeigte URL-Liste für die Richtlinie verwenden möchten.

Wenn Sie eine neue Liste erstellen möchten, klicken Sie auf **Hinzufügen**, und geben Sie in das daraufhin angezeigte Dialogfeld die erforderlichen Informationen ein. Verwenden Sie die Schaltflächen **Bearbeiten**, **Löschen**, um URL-Listen in dieser Tabelle zu ändern oder zu löschen.

URL hinzufügen/bearbeiten

In diesem Fenster fügen Sie Informationen für einen Cisco IOS SSL VPN-Link hinzu oder bearbeiten diese.

Bezeichnung

Die Bezeichnungen erscheinen auf dem Portal, das den Benutzern beim Anmelden bei dem Cisco IOS SSL VPN angezeigt wird. So könnten Sie zum Beispiel die Bezeichnung **Gehaltskalender** für einen Link verwenden, den Sie bereitstellen und der die bezahlten Ferientage und Zahltage anzeigt.

URL-Link

Geben Sie die URL für die Website des Unternehmens-Intranets ein, die die Benutzer besuchen dürfen.

Customize SSL VPN Portal (SSL VPN-Portal anpassen)

Die auf dieser Seite vorgenommenen Einstellungen bestimmen das Erscheinungsbild des Portals. Sie können unter den aufgeführten vordefinierten Themen wählen und eine Vorschau des Portals bei Verwendung dieses Themas anzeigen.

Thema

Wählen Sie den Namen eines vordefinierten Themas aus.

Vorschau

In diesem Bereich wird angezeigt, wie das Portal mit dem gewählten Thema aussieht. Unter Umständen empfiehlt es sich, eine Vorschau verschiedener Themen anzuzeigen, um festzulegen, welches verwendet werden soll.

SSL VPN Passthrough-Konfiguration

Damit die Benutzer eine Verbindung zum Intranet herstellen können, müssen Zugriffssteuerungseinträge (Access Control Entries, ACE) zu Firewall- und Network Access Control (NAC)-Konfigurationen hinzugefügt werden, damit der SSL-Datenverkehr das Intranet erreicht. Cisco SDM kann diese ACE für Sie konfigurieren, oder Sie können diese selbst konfigurieren, indem Sie zu **Firewall und ACL > Firewallrichtlinie/ACL bearbeiten** wechseln und die erforderlichen Einstellungen vornehmen.

Wenn Sie mit dem Cisco IOS SSL VPN-Assistenten arbeiten, klicken Sie auf **Zusammenarbeit von SSL VPN mit NAC und Firewall zulassen**, wenn Cisco SDM diese ACEs konfigurieren soll. Klicken Sie auf **Details anzeigen**, um die ACEs anzuzeigen, die Cisco SDM erstellen würde. Ein von Cisco SDM hinzugefügter Eintrag könnte wie im folgenden Beispiel aussehen:

```
permit tcp any host 172.16.5.5 eq 443
```

Wenn Sie einen Cisco IOS SSL VPN-Kontext bearbeiten, zeigt Cisco SDM die betroffene Schnittstelle und die angewendete ACL an. Klicken Sie auf **Ändern**, um zuzulassen, dass Cisco SDM Einträge zur ACL hinzufügt, damit das Passieren des Datenverkehrs durch die Firewall erlaubt wird. Klicken Sie auf **Details**, um den Eintrag anzuzeigen, den Cisco SDM hinzufügt. Der Eintrag ähnelt dem bereits angezeigten.

Benutzerrichtlinie

In diesem Fenster können Sie ein vorhandenes Cisco IOS SSL VPN auswählen und eine neue Richtlinie hinzufügen. So haben Sie beispielsweise ein Cisco IOS SSL VPN mit der Bezeichnung „Unternehmen“ erstellt, und Sie möchten den Intranet-Zugriff für eine neue Benutzergruppe mit dem Namen „Produktion“ definieren.

Select existing SSL VPN (Vorhandenes SSL VPN auswählen)

Wählen Sie das Cisco IOS SSL VPN, für das Sie eine neue Benutzergruppe erstellen möchten. Die bereits für dieses Cisco IOS SSL VPN konfigurierten Richtlinien werden in einem Feld unterhalb der Liste angezeigt. Sie können auf eine beliebige dieser Richtlinien klicken, um Einzelheiten dazu anzuzeigen. Weitere Informationen finden Sie unter Details zur SSL VPN-Gruppenrichtlinie: Richtlinienname.

Name der neuen Richtlinie

Geben Sie den Namen ein, den Sie der neuen Benutzergruppe geben möchten. Im Bereich unterhalb dieses Felds werden die Gruppenrichtlinien angezeigt, die bereits für dieses Cisco IOS SSL VPN vorhanden sind.

Details zur SSL VPN-Gruppenrichtlinie: Richtlinienname

In diesem Fenster werden die Details einer vorhandenen Cisco IOS SSL VPN-Richtlinie angezeigt.

Dienste

In diesem Bereich werden die Dienste, zum Beispiel URL-Mangling und Cisco Secure Desktop, aufgeführt, für die diese Richtlinie konfiguriert wurde.

Den Benutzern angezeigte URLs

In diesem Bereich werden die Intranet-URLs aufgeführt, die den Benutzern angezeigt werden, für die diese Richtlinie gilt.

Den Benutzern angezeigte Server

In diesem Bereich werden die IP-Adressen der Portweiterleitungs-Server aufgelistet, für die diese Richtlinie konfiguriert ist.

WINS-Server

In diesem Bereich werden die IP-Adressen der WINS-Server aufgelistet, für die diese Richtlinie konfiguriert ist.

Select the SSL VPN User Group (SSL VPN-Benutzergruppe auswählen)

Wählen Sie in diesem Fenster das Cisco IOS SSL VPN und die verknüpfte Benutzergruppe aus, für die Sie erweiterte Dienste konfigurieren möchten.

SSL VPN

Wählen Sie in dieser Liste das Cisco IOS SSL VPN aus, mit dem die Benutzergruppe verknüpft ist.

Benutzergruppe

Wählen Sie die Benutzergruppe aus, für die Sie erweiterte Funktionen konfigurieren möchten. Der Inhalt dieser Liste basiert auf dem gewählten Cisco IOS SSL VPN.

Erweiterte Funktionen auswählen

Wählen Sie in diesem Fenster die Funktionen aus, die Sie konfigurieren möchten. Der Assistent zeigt Fenster an, mit deren Hilfe Sie die ausgewählten Funktionen konfigurieren können.

Wenn Sie zum Beispiel auf Thin Client (Portweiterleitung), Cisco Secure Desktop und Common Internet File System (CIFS) klicken, zeigt der Assistent Konfigurationsfenster für diese Funktionen an.

Sie müssen mindestens eine Funktion zum Konfigurieren auswählen.

Thin Client (Portweiterleitung)

Remote-Workstations müssen manchmal Client-Anwendungen ausführen, um mit Intranet-Servern kommunizieren zu können. So erfordern Internet Mail Access Protocol (IMAP)- oder Simple Mail Transfer Protocol (SMTP)-Server unter Umständen, dass Client-Anwendungen auf Workstations ausgeführt werden, um E-Mails senden und empfangen zu können. Die Thin Client-Funktion, auch als Portweiterleitung bekannt, ermöglicht das Herunterladen eines kleinen Applet zusammen mit dem Portal, sodass eine Remote-Workstation mit dem Intranet-Server kommunizieren kann.

Dieses Fenster enthält eine Liste der Server und Portnummern, die für das Intranet konfiguriert wurden. Verwenden Sie die Schaltfläche **Hinzufügen**, um die IP-Adresse und Portnummer eines Servers einzugeben. Verwenden Sie die Schaltflächen **Bearbeiten** und **Löschen**, um Änderungen an den Informationen in dieser Liste vorzunehmen oder Informationen aus dieser Liste zu löschen.

Die von Ihnen erstellte Liste erscheint auf dem Portal, das den Clients bei der Anmeldung angezeigt wird.

Server hinzufügen oder bearbeiten

In diesem Fenster können Sie Serverinformationen hinzufügen oder bearbeiten.

IP-Adresse des Servers

Geben Sie die IP-Adresse oder den Hostnamen des Servers ein.

Serverport, auf dem der Dienst aufgeführt ist

Geben Sie den Port ein, an den der Server für diesen Dienst angeschlossen ist. Dabei kann es sich um eine Standard-Portnummer für den Dienst handeln, zum Beispiel Portnummer 23 für Telnet, oder es kann eine vom Standard abweichende Portnummer sein, für die eine Port-to-Application Map (PAM) erstellt wurde. Wenn Sie zum Beispiel die Telnet-Portnummer auf dem Server zu 2323 geändert und einen PAM-Eintrag für diesen Port auf diesem Server erstellt haben, würden Sie 2323 in dieses Fenster eingeben.

Port auf Client-PC

Cisco SDM gibt in dieses Feld eine Zahl ein, beginnend mit der Zahl 3000. Jedes Mal, wenn Sie einen Eintrag erstellen, erhöht Cisco SDM die Zahl um 1. Verwenden Sie die Einträge, die Cisco SDM in dieses Feld eingegeben hat.

Beschreibung

Geben Sie eine Beschreibung für den Eintrag ein. Wenn Sie zum Beispiel einen Eintrag hinzufügen, mit dem Benutzer eine Telnet-Verbindung zu einem Server unter 10.10.11.2 herstellen können, können Sie „Telnet to 10.10.11.2“ eingeben. Die eingegebene Beschreibung erscheint auf dem Portal.

Weitere Informationen

Weitere Informationen finden Sie unter diesem Link. Sie können diese Informationen jetzt durch Klicken auf Weitere Informationen zu Servern für die Portweiterleitung anzeigen.

Weitere Informationen zu Servern für die Portweiterleitung

Mit Portweiterleitung kann ein Remote-Benutzer von Cisco IOS SSL VPN eine Verbindung zu statischen Ports auf Servern mit privaten IP-Adressen im Unternehmens-Intranet herstellen. So können Sie Portweiterleitung zum Beispiel auf einem Router konfigurieren, um Remote-Benutzern Telnet-Zugriff auf einen Server im Unternehmens-Intranet zu ermöglichen. Zum Konfigurieren der Portweiterleitung benötigen Sie die folgenden Informationen:

- Die IP-Adresse des Servers.
- Die statische Portnummer des Servers.
- Die Remote-Portnummer für den Client-PC. Im Dialogfeld gibt Cisco SDM eine Portnummer an, deren Verwendung sicher ist.

Damit Benutzer über Telnet zum Beispiel eine Verbindung zu einem Server mit der IP-Adresse 10.0.0.100 (Port 23) herstellen können, würden Sie einen Portzuordnungseintrag mit den folgenden Informationen eingeben:

Server IP-Adresse: 10.0.0.100

Serverport, über den der Benutzer eine Verbindung herstellt: 23

Port auf Client-PC: Von Cisco SDM angegebener Wert. In diesem Beispiel 3001.

Beschreibung: SSL VPN-Telnet-Zugriff auf Server-a. Diese Beschreibung wird auf dem Portal angezeigt.

Wenn der Browser eine Verbindung zum Gateway-Router herstellt, wird ein Portal-Applet auf den Client PC heruntergeladen. Dieses Applet enthält die IP-Adresse und statische Portnummer des Servers sowie die Portnummer, die der Client-PC verwenden soll. Das Applet führt folgende Aktionen durch:

- Es wird eine Zuordnung auf dem Client-PC erstellt, welche den Datenverkehr für Port 23 unter 10.0.0.100 der Loopback-IP-Adresse des PCs 127.0.0.1, Port 3001 zuordnet.
- Prüft auf Port 3001, IP-Adresse 127.0.0.1

Wenn der Benutzer eine Anwendung ausführt, die eine Verbindung mit Port 23 unter 10.0.0.100 herstellt, wird die Anforderung an 127.0.0.1 Port 3001 gesendet. Das Portal-Applet, das diesen Port und diese IP-Adresse prüft, erhält die Anforderung und sendet sie über den Cisco IOS SSL VPN-Tunnel an das Gateway. Der Gateway-Router leitet sie an den Server unter 10.0.0.100 weiter und sendet Gegenverkehr zurück an den PC.

Full Tunnel

Full Tunnel-Clients müssen die Full Tunnel-Software herunterladen und eine IP-Adresse vom Router abrufen. Verwenden Sie dieses Fenster, um den IP-Adressenpool zu konfigurieren, von dem Full Tunnel-Clients bei der Anmeldung abrufen, und um den Speicherort des Full Tunnel-Installationspakets festzulegen.

Hinweis Wenn das Software-Installationspaket nicht bereits installiert ist, muss ausreichend Speicherplatz im Router-Flash vorhanden sein, damit Cisco SDM das Paket installieren kann, nachdem Sie diesen Assistenten abgeschlossen haben.

Kontrollkästchen „Full Tunnel aktivieren“

Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass der Router die Full Tunnel Client-Software auf den PC des Benutzers herunterlädt und um die anderen Felder in diesem Fenster zu aktivieren.

IP-Adressenpool

Geben Sie den IP-Adressenpool an, von dem Full Tunnel-Clients abrufen. Sie können den Namen eines vorhandenen Pools in das Feld eingeben, oder Sie klicken auf die Schaltfläche rechts von dem Feld und wählen **Aus einem vorhandenen IP-Pool auswählen,** um durch die Liste der Pools zu blättern. Wählen Sie **Create a new pool** (Neuen Pool erstellen), und füllen Sie das daraufhin angezeigte Dialogfeld aus, um einen neuen Pool zu erstellen. Der ausgewählte oder neu erstellte Adressenpool muss Adressen aus dem Unternehmens-Intranet enthalten.

Kontrollkästchen zum Beibehalten der Installation der Full Tunnel-Client-Software auf Client-PC

Aktivieren Sie dieses Kontrollkästchen, wenn die Full Tunnel-Software nach der Abmeldung auf dem Client-PC verbleiben soll. Wenn Sie dieses Kontrollkästchen nicht aktivieren, laden die Clients die Software bei jedem Verbinden mit dem Gateway herunter.

Kontrollkästchen „Full Tunnel-Client installieren“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Full Tunnel-Client-Software jetzt installieren möchten. Sie können die Client-Software auch installieren, wenn Sie dieses Cisco IOS SSL VPN bearbeiten.

Die Full Tunnel-Client-Software muss auf dem Router installiert sein, damit sie von den Clients heruntergeladen und Full Tunnel-Konnektivität hergestellt werden kann. Wenn die Full Tunnel-Software zusammen mit Cisco SDM installiert wurde, wird der entsprechende Pfad automatisch im Speicherort-Feld angezeigt, wie in Beispiel 19-1 dargestellt.

Beispiel 19-1 Full Tunnel-Paket, auf dem Router installiert

```
flash:sslclient-win-1.0.2.127.pkg
```

In Beispiel 19-1 wird das Full Tunnel-Installationspaket in den Router-Flash geladen. Wenn das Primärgerät Ihres Routers eine Disk oder ein Steckplatz ist, beginnt der angezeigte Pfad mit `Diskn` oder `Steckplatzn`.

Wenn dieses Feld leer ist, müssen Sie nach dem Installationspaket suchen, damit Cisco SDM es auf das Primärgerät des Routers laden kann, oder laden Sie das Software-Installationspaket von Cisco.com herunter, indem Sie auf den Link für die aktuellsten Downloads am unteren Fensterrand klicken. Dieser Link bringt Sie zur folgenden Webseite:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Hinweis Sie benötigen unter Umständen einen CCO-Benutzernamen und ein Kennwort, um Software von den Cisco-Software-Download-Websites herunterzuladen. Diese Anmeldeinformationen erhalten Sie, indem Sie auf **Registrieren** am oberen Rand der Cisco.com-Website klicken und die erforderlichen Informationen eingeben. Ihre Benutzer-ID und das Kennwort wird Ihnen per E-Mail zugeschickt.

Klicken Sie auf Suchen nach dem Installationspaket für Cisco SDM, um zu erfahren, wie Sie nach dem Installationspaket für die Full Tunnel-Software suchen können, und geben Sie einen Pfad für Cisco SDM an.

Schaltfläche „Erweitert“

Klicken Sie auf diese Schaltfläche, um erweiterte Optionen wie Split Tunneling, Split DNS und Microsoft Internet Explorer-Client-Einstellungen zu konfigurieren.

Suchen nach dem Installationspaket für Cisco SDM

Verwenden Sie die folgende Vorgehensweise, um Software-Installationspakete für Cisco SDM zu suchen, damit dieser Speicherort in der Cisco IOS SSL VPN-Konfiguration verwendet werden kann, oder laden Sie die Software auf den Router, falls erforderlich.

Hinweis Sie benötigen unter Umständen einen CCO-Benutzernamen und ein Kennwort, um Software von den Cisco-Software-Download-Websites herunterzuladen. Diese Anmeldeinformationen erhalten Sie, indem Sie auf **Registrieren** am oberen Rand der Cisco.com-Website klicken und die erforderlichen Informationen eingeben. Ihre Benutzer-ID und das Kennwort wird Ihnen per E-Mail zugeschickt.

Schritt 1 Sehen Sie sich das Feld **Speicherort** an. Befindet sich der Pfad zum Installationspaket in diesem Feld, sind keine weiteren Aktionen erforderlich. Cisco SDM konfiguriert den Router für den Download der Software von diesem Speicherort. Beispiel 19-2 zeigt einen Pfad zum Software-Installationspaket an.

Beispiel 19-2 Full Tunnel-Paket, auf dem Router installiert

```
flash:sslclient-win-1.0.2.127.pkg
```

Schritt 2 Wenn das Feld **Speicherort** leer ist, klicken Sie auf die Schaltfläche **...** rechts vom Feld, um den Speicherort der Software anzugeben.

Schritt 3 Wenn die Software auf dem Router installiert ist, wählen Sie **Router-Dateisystem**, und suchen Sie nach der Datei.

Wenn sich die Software auf Ihrem PC befindet, wählen Sie **Arbeitsplatz**, und suchen Sie nach der Datei.

Cisco SDM trägt das Router-Dateisystem oder den PC-Pfad, das bzw. den Sie angegeben haben, in das Feld **Speicherort** ein.

Schritt 4 Befindet sich die Software weder auf dem Router noch auf Ihrem PC, müssen Sie sie auf Ihren PC herunterladen und dann den Pfad zu der Datei in dieses Feld eingeben.

a. Klicken Sie im Fenster auf den Link für die aktuellsten Downloads. Sie werden mit der Download-Seite für die gewünschte Software verbunden.

b. Möglicherweise sind auf der daraufhin angezeigten Webseite Softwarepakete für andere als Cisco IOS-Plattformen und auch für IOS-Plattformen verfügbar. Doppelklicken Sie auf die aktuellste Version der Software, die Sie für Cisco IOS-Plattformen herunterladen möchten, und geben Sie bei der entsprechenden Aufforderung Ihren CCO-Benutzernamen und das Kennwort ein.

c. Laden Sie das Paket auf den PC herunter.

d. Klicken Sie im Cisco IOS SSL VPN-Assistenten auf die Schaltfläche **...** rechts neben dem Feld **Speicherort**, wählen Sie im daraufhin angezeigten Fenster **Speicherort wählen** die Option **Arbeitsplatz** aus, und navigieren Sie zu dem Verzeichnis, in dem Sie die Datei abgelegt haben.

e. Wählen Sie die Datei mit dem Installationspaket aus, und klicken Sie im Fenster **Speicherort wählen**, auf **OK**. Cisco SDM trägt den Pfad in das Feld **Speicherort** ein. Das Beispiel zeigt ein Installationspaket, das sich auf dem Desktop des PCs befindet.

Beispiel 19-3 Full Tunnel-Paket, auf dem Router installiert

```
C:\Dokumente und
Einstellungen\Benutzername\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco SDM installiert die Software auf dem Router aus dem PC-Verzeichnis, das Sie angegeben haben, als Sie die Konfiguration durch Klicken auf **Fertig stellen** an den Router gesendet haben.

Cisco Secure Desktop aktivieren

Der Router kann Cisco Secure Desktop auf dem Benutzer-PC installieren, wenn sich der Benutzer beim Cisco IOS SSL VPN anmeldet. Web-Transaktionen können Cookies, Browser-Verlaufsdateien, E-Mail-Anhänge und andere Dateien auf dem PC hinterlassen, nachdem sich der Benutzer abgemeldet hat. Cisco Secure Desktop erstellt eine sichere Partition auf dem Desktop und verwendet einen Department of Defense-Algorithmus, um die Dateien nach Beenden der Sitzung zu entfernen.

Cisco Secure Desktop installieren

Clients müssen das Installationspaket der Cisco Secure Desktop-Software vom Router herunterladen. Wenn diese Software zusammen mit Cisco SDM installiert wurde, wird der entsprechende Pfad automatisch im Feld **Speicherort** angezeigt, wie in Beispiel 19-4 dargestellt.

Beispiel 19-4 Cisco Secure Desktop-Paket, auf dem Router installiert

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

In Beispiel 19-4 wird das Cisco Secure Desktop-Installationspaket in den Router-Flash geladen. Wenn das Primärgerät Ihres Routers eine Disk oder ein Steckplatz ist, beginnt der angezeigte Pfad mit `Diskn` oder `Steckplatzn`.

Wenn dieses Feld leer ist, müssen Sie nach dem Installationspaket suchen, damit Cisco SDM es auf das Primärgerät des Routers laden kann, oder Sie laden das Software-Installationspaket von Cisco.com herunter, indem Sie auf den Link für die **aktuellsten Downloads** am unteren Fensterrand klicken. Über diesen Link gelangen Sie zur folgenden Webseite:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Hinweis Sie benötigen unter Umständen einen CCO-Benutzernamen und ein Kennwort, um Software von den Cisco-Software-Download-Websites herunterzuladen. Diese Anmeldeinformationen erhalten Sie, indem Sie auf **Registrieren** am oberen Rand der Cisco.com-Website klicken und die erforderlichen Informationen eingeben. Ihre Benutzer-ID und das Kennwort wird Ihnen per E-Mail zugeschickt.

Klicken Sie auf Suchen nach dem Installationspaket für Cisco SDM, um zu erfahren, wie Sie nach dem Installationspaket für die Cisco Secure Desktop-Software suchen können, und geben Sie einen Pfad für Cisco SDM an.

Common Internet File System

Mit dem Common Internet File System (CIFS) können Clients mithilfe einer Webbrowser-Oberfläche per Remote-Zugriff Dateien auf Microsoft Windows-basierten Dateiservern durchsuchen, darauf zugreifen und erstellen.

WINS-Server

Microsoft Windows Internet Naming Service (WINS)-Server verwalten die Datenbank, die Client-IP-Adressen zu ihren entsprechenden NetBIOS-Namen zuordnet. Geben Sie die IP-Adressen der WINS-Server in Ihrem Netzwerk in dieses Feld ein. Verwenden Sie Semikola (;) zum Trennen der einzelnen Adressen.

Wenn Sie beispielsweise die IP-Adressen 10.0.0.18 und 10.10.10.2 eingeben möchten, geben Sie 10.0.0.18;10.10.10.2 in dieses Feld ein.

Permissions (Berechtigungen)

Geben Sie die Berechtigungen an, die Sie den Benutzern gewähren möchten.

Clientless Citrix aktivieren

Clientless Citrix ermöglicht es Benutzern, Anwendungen wie Microsoft Word oder Excel auf Remote-Servern auszuführen, wie sie auch lokal ausgeführt würden, ohne dass sich eine Client-Software auf dem PC befinden muss. Die Citrix-Software muss auf einem oder mehreren Servern in einem Netzwerk installiert sein, das vom Router erreicht werden kann.

Citrix-Server

Wenn Sie eine neue Liste erstellen möchten, klicken Sie auf **Hinzufügen**, und geben Sie in das daraufhin angezeigte Dialogfeld die erforderlichen Informationen ein. Verwenden Sie die Schaltflächen **Bearbeiten**, **Löschen**, um URL-Listen in dieser Tabelle zu ändern oder zu löschen.

Übersicht

In diesem Fenster wird eine Übersicht über die Cisco IOS SSL VPN-Konfiguration angezeigt, die Sie erstellt haben. Klicken Sie auf **Fertig stellen**, um die Konfiguration an den Router zu senden, oder klicken Sie auf **Zurück**, um zu dem betreffenden Assistentenfenster zurückzukehren, auf dem Sie Änderungen vornehmen müssen.

Wenn Sie die CLI Befehle anzeigen möchten, die Sie an den Router senden, wählen Sie **Bearbeiten > Einstellungen**, und aktivieren Sie die Option **Zeigen Sie die Befehle in der Vorschau an, bevor Sie sie an den Router senden**.

Edit SSL VPN (SSL VPN bearbeiten)

Im Fenster **Edit SSL VPN** (SSL VPN bearbeiten) können Sie Cisco IOS SSL VPN-Konfigurationen ändern oder erstellen. Im oberen Bereich der Registerkarte werden die konfigurierten Cisco IOS SSL VPN-Kontexte aufgeführt. Im unteren Bereich werden Details zu dem betreffenden Kontext angezeigt.

Klicken Sie auf Cisco IOS SSL VPN, um eine Übersicht der Cisco IOS SSL VPN-Funktionen zu erhalten, die Cisco SDM unterstützt.

Klicken Sie auf Cisco IOS SSL VPN-Links unter Cisco.com, um Links zu Cisco IOS SSL VPN-Dokumenten anzuzeigen.

Klicken Sie auf Cisco IOS SSL VPN-Kontexte, Gateways und Richtlinien, um eine Beschreibung dazu zu erhalten, wie die Komponenten einer Cisco IOS SSL VPN-Konfiguration zusammenwirken.

SSL VPN-Kontexte

In diesem Bereich werden die auf dem Router konfigurierten Cisco IOS SSL VPN-Kontexte angezeigt. Klicken Sie in diesem Bereich auf einen Kontext, um die detaillierten Informationen dazu im unteren Bereich des Fensters anzuzeigen. Fügen Sie einen neuen Kontext hinzu, indem Sie auf **Hinzufügen** klicken und in das daraufhin angezeigte Dialogfeld die erforderlichen Informationen eingeben. Bearbeiten Sie einen Kontext, indem Sie ihn auswählen und auf **Bearbeiten** klicken. Entfernen Sie einen Kontext und die dazugehörigen Gruppenrichtlinien, indem sie ihn auswählen und auf **Löschen** klicken.

Sie können einen Kontext aktivieren, der nicht verwendet wird, indem Sie ihn auswählen und auf **Aktivieren** klicken. Sie können einen Kontext deaktivieren, indem Sie ihn auswählen und auf **Deaktivieren** klicken.

Folgende Informationen werden zu den einzelnen Kontexten angezeigt:

Name

Der Name des Cisco IOS SSL VPN-Kontexts. Wenn Sie den Kontext im Cisco IOS SSL VPN-Assistenten erstellt haben, ist der Name die Zeichenfolge, die Sie in das Fenster für die IP-Adresse und den Namen eingegeben haben.

Gateway

Das Gateway, den der Kontext verwendet, enthält die IP-Adresse und das digitale Zertifikat, das der Cisco IOS SSL VPN-Kontext verwendet.

Domäne

Wenn eine Domäne für den Kontext konfiguriert wurde, wird diese in dieser Spalte angezeigt. Wenn eine Domäne konfiguriert ist, müssen die Benutzer diese Domäne in den Webbrowser eingeben, um auf das Portal zuzugreifen.

Status

Enthält Symbole für eine schnelle Identifizierung des Status.

Administrativer Status

Textbeschreibung des Status.

- In Betrieb – Kontext ist in Betrieb. Benutzer, die in den unter dem Kontext konfigurierten Richtlinien angegeben sind, können auf ihr Cisco IOS SSL VPN-Portal zugreifen.
- Nicht in Betrieb – Kontext ist außer Betrieb. Benutzer, die in Richtlinien festgelegt sind, welche unter dem Kontext konfiguriert wurden, können nicht auf ihr Cisco IOS SSL VPN-Portal zugreifen.

Beispiel für eine Anzeige

Die folgende Tabelle stellt ein Beispiel für eine Cisco IOS SSL VPN-Kontextanzeige dar.

Name	Gateway	Domäne	Status	Administrativer Status
WorldTravel	Gateway1	wtravel.net		In Betrieb
A+Insurance	Gateway2	aplus.com		Nicht in Betrieb

Details über SSL VPN-Kontext: *Name*

In diesem Bereich werden Details zu dem Kontext mit der Bezeichnung *Name* angezeigt, die Sie im oberen Fensterbereich ausgewählt haben. Sie können die angezeigten Einstellungen ändern, indem Sie im oberen Fensterbereich auf **Bearbeiten** klicken.

SSL VPN-Kontext

Verwenden Sie dieses Fenster, um einen Cisco IOS SSL VPN-Kontext zu bearbeiten.

Name

Geben Sie den Namen eines neuen Kontexts ein, oder wählen Sie den Namen eines vorhandenen Kontexts, um ihn zu bearbeiten.

Verknüpftes Gateway

Wählen Sie ein vorhandenes Gateway aus, oder klicken Sie auf **Gateway erstellen**, um ein neues Gateway für den Kontext zu konfigurieren. Das Gateway enthält die IP-Adresse und das digitale Zertifikat, das für diesen Kontext verwendet wird. Für jedes Gateway ist eine einmalige öffentliche IP-Adresse erforderlich.

Domäne

Wenn Sie über eine Domäne für diesen Kontext verfügen, geben Sie sie in dieses Feld ein. Cisco IOS SSL VPN-Benutzer können diesen Domänennamen beim Zugriff auf das Portal anstatt einer IP-Adresse verwenden. Beispiel ist **meinunternehmen.com**.

Authentifizierungsliste

Wählen Sie die AAA-Methodenliste, die zur Authentifizierung der Benutzer für diesen Kontext verwendet werden soll.

Authentifizierungsdomäne

Geben Sie den Domänennamen ein, der an den Benutzernamen angehängt werden soll, bevor dieser zur Authentifizierung gesendet wird. Dieser Domänenname muss mit der Domäne übereinstimmen, die auf dem AAA-Server für die für diesen Kontext authentifizierten Benutzer verwendet wird.

Kontrollkästchen „Kontext aktivieren"

Aktivieren Sie dieses Kontrollkästchen, wenn der Kontext nach Abschluss der Konfiguration aktiviert werden soll. Wenn Sie den Kontext hier aktivieren, müssen Sie nicht zu diesem Fenster zurückkehren, um ihn zu deaktivieren. Sie können einzelne Kontexte auf der Registerkarte **Edit SSL VPN** (SSL VPN bearbeiten) aktivieren oder deaktivieren.

Maximale Anzahl von Benutzern

Geben Sie die maximale Anzahl von Benutzern ein, die diesen Kontext gleichzeitig verwenden dürfen.

VRF-Name

Geben Sie den VPN Routing and Forwarding (VRF)-Namen für diesen Kontext ein. Dieser VRF-Name muss bereits auf dem Router konfiguriert sein.

Standardgruppenrichtlinie

Wählen Sie die Richtlinie, die Sie als Standardgruppenrichtlinie verwenden möchten. Die Standardgruppenrichtline wird für Benutzer verwendet, die in keiner der auf dem AAA-Server konfigurierten Richtlinien enthalten sind.

Bestimmen von inneren und äußeren Schnittstellen

Eine ACL, die auf eine Schnittstelle angewendet wird, auf der eine Cisco IOS SSL VPN-Verbindung konfiguriert ist, kann unter Umständen den SSL-Datenverkehr blockieren. Cisco SDM kann die ACL automatisch ändern, damit dieser Datenverkehr die Firewall passieren kann. Sie müssen jedoch angeben, welche Schnittstelle die innere (vertrauenswürdige) und welche die äußere (nicht vertrauenswürdige) Schnittstelle für Cisco SDM darstellt, um den Zugriffssteuerungseintrag (Access Control Entry, ACE) zu erstellen, der über die Firewall geleitet werden kann.

Aktivieren Sie das Kontrollkästchen **Innere**, wenn es sich bei der aufgeführten Schnittstelle um eine innere Schnittstelle handelt, und aktivieren Sie die Option **Äußere**, wenn es sich um eine nicht vertrauenswürdige Schnittstelle handelt.

Gateway auswählen

Wählen Sie in diesem Fenster ein vorhandenes Gateway aus. Dieses Fenster stellt die Informationen bereit, die Sie benötigen, um festzustellen, welches Gateway Sie auswählen müssen. Hier werden die Namen und IP-Adressen aller Gateways und die Anzahl der Kontexte, mit der die einzelnen Gateways verknüpft sind, angezeigt und angegeben ob das Gateway aktiviert ist oder nicht.

Kontext: Gruppenrichtlinien

In diesem Fenster werden die für den gewählten Cisco IOS SSL VPN-Kontext konfigurierten Gruppenrichtlinien angezeigt. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um diese Gruppenrichtlinien zu verwalten.

Dieses Fenster zeigt für jede Richtlinie den Namen an, und ob es sich um die Standardgruppenrichtlinie handelt. Die Standardgruppenrichtline ist die Richtlinie, die einem Benutzer zugeordnet wurde, der in keiner der anderen Richtlinien enthalten ist. Sie können die Gruppenrichtlinie ändern, indem Sie zu dem Kontextfenster zurückkehren und eine andere Richtlinie als Standard wählen.

Klicken Sie auf eine Richtlinie in der Liste, um detaillierte Informationen dazu im unteren Bereich des Fensters anzuzeigen. Klicken Sie auf die Links, um eine Beschreibung dieser Informationen zu erhalten.

Gruppenrichtlinie: Registerkarte Allgemein

Gruppenrichtlinie: Registerkarte Clientless

Gruppenrichtlinie: Registerkarte Thin Client

Gruppenrichtlinie: Registerkarte SSL VPN-Client (Full Tunnel)

Klicken Sie hier, um weitere Informationen zu erhalten

Klicken Sie auf den Link im Fenster, um wichtige Informationen zu erhalten. Klicken Sie auf Weitere Informationen zu Gruppenrichtlinien, um die Informationen dieser Hilfeseite aufzurufen.

Weitere Informationen zu Gruppenrichtlinien

Mit Cisco IOS SSL VPN-Gruppenrichtlinien werden das Portal und die Links für die Benutzer definiert, die von den jeweiligen Richtlinien betroffen sind. Wenn ein Remote-Benutzer die URL für Cisco IOS SSL VPN eingibt, die ihm zugewiesen wurde, muss der Router festlegen, von welcher Richtlinie der Benutzer ein Mitglied ist, um das Portal anzuzeigen, das für diese Richtlinie konfiguriert wurde. Wenn nur eine Cisco IOS SSL VPN-Richtlinie auf dem Router konfiguriert ist, kann der Router die Benutzer lokal authentifizieren oder einen AAA-Server verwenden und anschließend das Portal anzeigen.

Wenn jedoch mehrere Richtlinien konfiguriert sind, muss sich der Router darauf verlassen, dass ein AAA-Server festlegt, welche Richtlinie bei jedem Anmeldeversuch eines Remote-Benutzers verwendet werden soll. Wenn Sie mehrere Cisco IOS SSL VPN-Gruppenrichtlinien konfiguriert haben, müssen Sie mindestens einen AAA-Server für den Router konfigurieren und für jede Benutzergruppe, für die Sie eine Cisco IOS SSL VPN-Richtlinie erstellt haben, eine Richtlinie auf diesem Server konfigurieren. Die Richtliniennamen auf dem AAA-Server müssen den Namen der Gruppenrichtlinien entsprechen, die auf dem Router konfiguriert wurden, und sie müssen mit den Anmeldeinformationen der Benutzer konfiguriert sein, die Mitglieder der Gruppe sind.

Wenn zum Beispiel ein Router mit lokaler Authentifizierung für Bob Smith konfiguriert wurde und nur die Gruppenrichtlinie **Vertrieb** konfiguriert ist, ist nur ein Portal zur Anzeige verfügbar, wenn Bob Smith versucht, sich anzumelden. Wenn jedoch drei Cisco IOS SSL VPN-Gruppenrichtlinien konfiguriert sind, **Vertrieb**, **Feld** und **Produktion**, kann der Router nicht selbst ermitteln, von welcher Richtliniengruppe Bob Smith Mitglied ist. Wenn ein AAA-Server mit den korrekten Informationen für diese Richtlinien konfiguriert ist, kann der Router Kontakt zu dem Server aufnehmen und die Information empfangen, dass Bob Smith ein Mitglied der Gruppe **Vertrieb** ist. Der Router kann dann das korrekte Portal für die Gruppe **Vertrieb** anzeigen.

Informationen zum Konfigurieren des AAA-Servers finden Sie im Abschnitt zum Konfigurieren der RADIUS-Attributunterstützung für SSL VPN im Dokument über *SSL VPN-Erweiterungen* unter folgendem Link:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Gruppenrichtlinie: Registerkarte Allgemein

Wenn Sie eine neue Gruppenrichtlinie erstellen, müssen Sie in jedes Feld der Registerkarte **Allgemein** Informationen eingeben.

Name

Geben Sie einen Namen für diese Gruppenrichtlinie ein, zum Beispiel Entwicklung, Personal oder Marketing.

Timeouts

Geben Sie für das Leerlauf-Timeout die Anzahl der Sekunden ein, die der Client im Leerlauf bleiben kann, bevor die Sitzung beendet wird.

Geben Sie für das Sitzungs-Timeout die maximale Anzahl der Sekunden für eine Sitzung ein, unabhängig von der Aktivität in der Sitzung.

Kontrollkästchen „Als Standardgruppenrichtlinie einstellen“

Aktivieren Sie dieses Kontrollkästchen, wenn Sie diese Gruppenrichtlinie als Standardgruppenrichtlinie verwenden möchten. Die Standardgruppenrichtlinie ist die Richtlinie, die einem Benutzer zugeordnet wurde, der in keiner der anderen Richtlinien enthalten ist. Wenn Sie dieses Kontrollkästchen aktivieren, wird diese Richtlinie als Standardrichtlinie im Gruppenrichtlinienfenster angezeigt.

Gruppenrichtlinie: Registerkarte Clientless

Clientless Citrix ermöglicht es Benutzern, Anwendungen so auf Remote-Servern auszuführen, wie sie auch lokal ausgeführt würden, ohne dass Client-Software auf den Remote-Systemen installiert werden muss, die diese Anwendungen nutzen. Die Citrix-Software muss auf einem oder mehreren Servern in einem Netzwerk installiert sein, das vom Router erreicht werden kann.

Geben Sie Informationen in diese Registerkarte ein, wenn Sie möchten, dass Cisco IOS SSL VPN-Clients in der Lage sind, Clientless Citrix zu verwenden.

Clientless Webbrowsing

Wählen Sie eine oder mehrere URL-Listen aus, die Sie im Portal anzeigen möchten, das die Benutzer in dieser Gruppe anzeigen können. Wenn Sie eine URL-Liste untersuchen möchten, wählen Sie einen Namen aus der Liste aus, und klicken Sie auf **Anzeigen**. Die URLs in der Liste, die Sie festlegen, werden im Portal angezeigt.

Wenn Sie Benutzer auf die URLs in der Liste beschränken und verhindern möchten, dass sie zusätzliche URLs eingeben, klicken Sie auf **URL-Leiste auf der Portalseite ausblenden**.

CIFS aktivieren

Wählen Sie diese Option, wenn Sie zulassen möchten, dass die Gruppenmitglieder Dateien auf MS Windows-Servern im Unternehmensnetzwerk durchsuchen. Sie müssen die Liste der WINS-Server angeben, welche die Anzeige der entsprechenden Dateien für diese Benutzer ermöglicht. Wenn Sie den Inhalt einer WINS-Server-Liste überprüfen möchten, wählen Sie die Liste aus, und klicken Sie auf **Anzeigen**.

Klicken Sie auf **Lesen**, um den Gruppenmitgliedern das Lesen von Dateien zu gestatten. Klicken Sie auf **Schreiben**, um den Gruppenmitgliedern das Ändern von Dateien zu gestatten.

Für die Verfügbarkeit dieser Funktion muss mindestens eine WINS-Server-Liste für diesen Cisco IOS SSL VPN-Kontext konfiguriert sein.

Gruppenrichtlinie: Registerkarte Thin Client

Nehmen Sie Einstellungen auf dieser Registerkarte vor, wenn Sie Thin Client, auch als Portweiterleitung bekannt, für die Mitglieder dieser Gruppe konfigurieren möchten.

Klicken Sie auf **Thin Client aktivieren** (**Port-Weiterleitung**), und geben Sie eine Port-Weiterleitungsliste ein, um diese Funktion zu aktivieren. Es muss mindestens eine Port-Weiterleitungsliste für den Cisco IOS SSL VPN-Kontext konfiguriert sein, unter dem diese Gruppenrichtlinie konfiguriert ist. Klicken Sie auf **Anzeigen**, um die gewählte Port-Weiterleitungsliste zu untersuchen.

Gruppenrichtlinie: Registerkarte SSL VPN-Client (Full Tunnel)

Nehmen Sie Einstellungen auf dieser Registerkarte vor, damit die Gruppenmitglieder die Full Tunnel Client-Software herunterladen und verwenden können.

Hinweis Sie müssen den Speicherort der Full Tunnel Client-Software durch Klicken auf **Pakete** in der SSL VPN-Baumstruktur und Angeben des Speicherorts des Installationspakets festlegen und anschließend auf **Installieren** klicken.

Aktivieren Sie die Full Tunnel-Verbindungen durch Auswählen von **Aktivieren** aus der Liste. Wenn Sie Full Tunnel-Verbindungen anfordern möchten, wählen Sie **Erforderlich**. Wenn Sie **Erforderlich** wählen, funktioniert die Clientless- und Thin Client-Kommunikation nur dann, wenn die Cisco IOS SSL VPN-Client-Software erfolgreich auf dem Client-PC installiert wurde.

IP-Adressenpool, aus dem Clients eine IP-Adresse zugewiesen wird

Clients, die Full Tunnel-Kommunikationen einrichten, werden vom Router IP-Adressen zugewiesen. Geben Sie den Namen des Pools an, oder klicken Sie auf die Schaltfläche **...**, um einen neuen Pool zu erstellen, aus dem der Router Adressen zuweisen kann.

Kontrollkästchen „Keep full-tunnel client software installed on client's PC“ (Installation der Full Tunnel-Client-Software auf Client-PC beibehalten)

Aktivieren Sie dieses Kontrollkästchen, wenn die Full Tunnel-Software nach der Abmeldung auf dem Client-PC verbleiben soll. Wenn Sie dieses Kontrollkästchen nicht aktivieren, laden die Clients die Software bei jedem Verbinden mit dem Gateway herunter.

Feld „Renegotiate Key“ (Schlüssel neu aushandeln)

Geben Sie die Anzahl an Sekunden ein, nach deren Ablauf der Tunnel heruntergefahren werden sollte, damit ein neuer SSL-Schlüssel ausgehandelt werden und der Tunnel neu eingerichtet werden kann.

ACL zur Einschränkung des Zugriffs für Benutzer in dieser Gruppe auf Unternehmensressourcen

Sie können eine Zugriffsliste (ACL) auswählen oder erstellen, welche die Ressourcen im Unternehmensnetzwerk festlegt, auf welche die Mitglieder beschränkt sind.

Die Startseite, die der Client angezeigt bekommen sollte, wenn ein Webbrowser mit installierter Full Tunnel-Software geöffnet wird

Geben Sie den URL für die Startseite ein, die den Full Tunnel-Clients in dieser Gruppe angezeigt werden soll.

Dead Peer Detection-Timeouts

Dead Peer Detection (DPD) ermöglicht es einem System, einen Peer zu erkennen, der nicht mehr reagiert. Sie können separate Timeouts einstellen, mit denen die Router Clients und Server erkennen können, die nicht mehr reagieren. Der Bereich für beide liegt zwischen 0 und 3600 Sekunden.

Schaltfläche „DNS- und WINS-Server konfigurieren“

Klicken Sie auf diese Schaltfläche, um das DNS- und WINS-Server-Dialogfeld zu öffnen, in dem Sie die IP-Adressen der DNS- und WINS-Servers im Unternehmens-Intranet angeben können, die Clients beim Zugriff auf Intranet-Hosts und -Dienste verwenden sollten.

Schaltfläche zum Konfigurieren der erweiterten Tunneloptionen

Klicken Sie auf diese Schaltfläche, um das Dialogfeld **Erweiterte Tunneloptionen** zu öffnen, in dem Sie Tunnel-Einstellungen für Split Tunneling, Split DNS und Proxy-Server-Einstellungen für Clients konfigurieren können, die Microsoft Internet Explorer verwenden.

Erweiterte Tunneloptionen

Die Einstellungen, die Sie in diesem Dialogfeld vornehmen, ermöglichen es Ihnen, den verschlüsselten Datenverkehr zu steuern, die DNS-Server im Unternehmens-Intranet sowie die Proxy Server-Einstellungen festzulegen, die an die Client-Browser gesendet werden sollen.

Split-Tunneling

Das Verschlüsseln des gesamten Tunnel-Datenverkehrs erfordert unter Umständen erhebliche Systemressourcen. Mit Split Tunneling können Sie die Netzwerke festlegen, deren Datenverkehr verschlüsselt werden soll, und den Datenverkehr für andere Netzwerk von der Verschlüsselung ausnehmen. Sie können entweder festlegen, welcher Tunnel-Datenverkehr verschlüsselt werden soll, oder Sie geben den Datenverkehr an, der *nicht* verschlüsselt werden soll, und lassen zu, dass der Router den gesamten verbleibenden Tunnel-Datenverkehr verschlüsselt. Sie können nur eine Liste erstellen, eingeschlossener und ausgeschlossener Datenverkehr schließen sich gegenseitig aus.

Klicken Sie auf **Datenverkehr einschließen**, und verwenden Sie die Tasten **Hinzufügen**, **Bearbeiten** und **Löschen**, um eine Liste der Zielnetzwerke zu erstellen, deren Datenverkehr verschlüsselt werden soll. Oder klicken Sie auf **Datenverkehr ausschließen**, und erstellen Sie eine Liste der Zielnetzwerke, deren Datenverkehr *nicht* verschlüsselt werden soll.

Klicken Sie auf **Lokale LANs ausschließen**, um den Client-Datenverkehr, der an LANs gerichtet ist, an die der Router angeschlossen ist, explizit von der Verschlüsselung auszuschließen. Wenn es Netzwerkdrucker in diesen LANs gibt, müssen Sie diese Option verwenden.

Weitere Informationen zu Split Tunneling.

Split DNS

Wenn die Cisco IOS SSL VPN-Clients den DNS-Server im Unternehmensnetzwerk nur zum Auflösen spezieller Domänen verwenden sollen, können Sie diese Domänen in diesen Bereich eingeben. Es sollte sich um Domänen innerhalb des Unternehmens-Intranets handeln. Trennen Sie die einzelnen Einträge durch Semikola voneinander ab und verwenden Sie keine Wagenrückläufe. Es folgt eine Beispielliste von Einträgen:

IhrUnternehmen.com;dev-lab.net;extranet.net

Die Clients müssen die DNS-Server verwenden, die von ihren ISPs zum Auflösen aller anderen Domänen bereitgestellt werden.

Browser Proxy-Einstellungen

Die Einstellungen in diesem Bereich werden an die Browser der Microsoft Internet Explorer-Clients mit Full Tunnel-Verbindungen gesendet. Diese Einstellungen haben keine Auswirkung, wenn die Clients einen anderen Browser verwenden.

Keinen Proxy-Server verwenden.

Klicken Sie auf diese Option, um Cisco IOS SSL VPN-Client-Browser anzuweisen, keinen Proxy-Server zu verwenden.

Proxy-Einstellungen automatisch erfassen

Klicken Sie auf diese Option, um Cisco IOS SSL VPN-Client-Browser anzuweisen, Proxy-Server-Einstellungen automatisch zu erkennen.

Proxy-Einstellungen für lokale Adressen umgehen

Klicken Sie auf diese Option, wenn Sie möchten, dass Clients, die eine Verbindung zu lokalen Adressen herstellen, normale Proxy-Einstellungen umgehen können.

Proxy-Server

Geben Sie in dieses Feld die IP-Adresse des Proxy-Servers und die Portnummer für den Dienst ein, den er bereitstellt. Wenn der Proxy-Server zum Beispiel FTP-Anforderungen unterstützt, geben Sie die IP-Adresse des Proxy-Servers und Portnummer 21 ein.

Verwenden Sie keine Proxy-Server für Adressen, die folgendermaßen beginnen

Wenn Sie nicht möchten, dass Clients Proxy-Server verwenden, wenn Sie Datenverkehr an bestimmte IP-Adressen oder Netzwerke senden, können Sie diese IP-Adressen oder Netzwerke hier eingeben. Trennen Sie die einzelnen Einträge durch Semikola voneinander ab. Wenn die Clients beispielsweise keinen Proxy-Server verwenden sollen, wenn diese eine Verbindung zu einem beliebigen Server in den Netzwerken 10.10.0.0 oder 10.11.0.0 herstellen, geben Sie 10.10;10.11 ein. Sie können beliebig viele Netzwerke eingeben.

DNS- und WINS-Server

Geben Sie die IP-Adressen für die DNS- und WINS-Servers des Unternehmens ein, die an Cisco IOS SSL VPN-Clients gesendet werden. Cisco IOS SSL VPN-Clients verwenden diese Server für den Zugriff auf Hosts und Dienste im Unternehmens-Intranet.

Geben Sie Adressen für primäre und sekundäre DNS-Server und WINS-Server an.

Weitere Informationen zu Split Tunneling

Wenn eine Cisco IOS SSL VPN-Verbindung mit einem Remote-Client eingerichtet wird, wird unter Umständen der gesamte Datenverkehr, den der Client sendet und empfängt, durch den Cisco IOS SSL VPN-Tunnel geleitet, einschließlich des Datenverkehrs, der sich nicht im Unternehmens-Intranet befindet. Dies kann zu verringerter Netzwerkleistung führen. Mit Split Tunneling können Sie den Datenverkehr festlegen, der durch den Cisco IOS SSL VPN-Tunnel gesendet werden soll, und zulassen, dass der verbleibende Datenverkehr ungeschützt bleibt und von anderen Routern verarbeitet wird.

Im Split Tunneling-Bereich können Sie entweder den Datenverkehr festlegen, der im Cisco IOS SSL VPN *eingeschlossen* werden soll, und den gesamten verbleibenden Datenverkehr standardmäßig ausschließen, oder Sie geben den Datenverkehr ein, der vom Cisco IOS SSL VPN *ausgeschlossen* werden soll, und den gesamten verbleibenden Datenverkehr standardmäßig einschließen.

Beispiel: Ihre Organisation verwendet die Netzwerkadressen 10.11.55.0 und 10.12.55.0. Sie fügen diese Netzwerkadressen zur Liste der Zielnetzwerke hinzu, und klicken dann auf das Optionsfeld **Datenverkehr einschließen**. Der gesamte verbleibende Internet-Datenverkehr, zum Beispiel der Datenverkehr zu Google oder Yahoo, würde direkt in das Internet geleitet.

In einem anderen Beispiel ist es sinnvoller, Datenverkehr zu bestimmten Netzwerken aus dem Cisco IOS SSL VPN-Tunnel auszuschließen. In diesem Fall geben Sie die Adressen für diese Netzwerke zur Liste der Zielnetzwerke ein und klicken dann auf das Optionsfeld **Datenverkehr ausschließen**. Der gesamte Datenverkehr, der an diese Netzwerke gerichtet ist, wird nun über nicht gesicherte Routen und der verbleibende Datenverkehr über den Cisco IOS SSL VPN-Tunnel gesendet.

Wenn Benutzer über Drucker in lokalen LANs verfügen, die sie während der Verbindung zum Cisco IOS SSL VPN verwenden möchten, müssen Sie im Split Tunneling-Bereich auf **Lokale LANs ausschließen** klicken.

Hinweis Die Liste der Zielnetzwerke im Split Tunneling-Bereich enthält unter Umständen bereits Netzwerkadressen. Die Datenverkehrseinstellungen, die Sie im Split Tunneling-Bereich vornehmen, haben Vorrang vor den zuvor aufgeführten Netzwerken.

DNS- und WINS-Server

Geben Sie die IP-Adressen für die DNS- und WINS-Servers des Unternehmens ein, die an Cisco IOS SSL VPN-Clients gesendet werden. Cisco IOS SSL VPN-Clients verwenden diese Server für den Zugriff auf Hosts und Dienste im Unternehmens-Intranet.

Geben Sie Adressen für primäre und sekundäre DNS-Server und WINS-Server an.

Kontext: HTML-Einstellungen

Die in diesem Fenster vorgenommenen Einstellungen steuern das Erscheinungsbild des Portals für den ausgewählten Cisco IOS SSL VPN-Kontext.

Thema auswählen

Sie können das Erscheinungsbild des Portals festlegen, indem Sie ein vordefiniertes Thema auswählen, anstatt jede Farbe einzeln selbst festzulegen. Wenn Sie ein Thema auswählen, werden die Einstellungen für dieses Thema in den Feldern angezeigt, die mit der Schaltfläche **Anpassen** verknüpft sind.

Schaltfläche „Anpassen“

Klicken Sie auf diese Schaltfläche, wenn Sie jede auf dem Portal verwendete Farbe einzeln auswählen sowie eine Meldung beim Anmelden und einen Titel festlegen möchten. Wenn Sie ein vordefiniertes Thema auswählen, werden die Werte für dieses Thema in den Feldern dieses Abschnitts angezeigt. Sie können diese Werte ändern. Die eingegebenen Werte werden auf dem Portal dann für den ausgewählten Kontext verwendet. Änderungen, die Sie in diesem Fenster vornehmen, wirken sich nur auf das erstellte Portal aus. Sie haben keine Auswirkung auf die Standardwerte für das Thema.

Meldung beim Anmelden

Geben Sie die Meldung ein, die für die Clients beim Anmelden angezeigt wird, wenn das Portal über ihre Browser dargestellt wird. Beispiel:

```
Willkommen im Netzwerk von Unternehmensname. Melden Sie sich ab, wenn
Sie kein autorisierter Benutzer sind.
```

Titel

Geben Sie den Titel für das Portal ein. Beispiel:

```
Anmeldeseite für das Netzwerk von Unternehmensname
```

Hintergrundfarbe für Titel

Der Standardwert für die Hintergrundfarbe, die hinter dem Titel erscheint, lautet #9999CC. Ändern Sie diesen Wert, indem Sie auf die Schaltfläche **...** klicken und eine andere Farbe auswählen.

Hintergrundfarbe für sekundäre Titel

Der Standardwert für die Hintergrundfarbe, die hinter dem Titel erscheint, lautet #9729CC. Ändern Sie diesen Wert, indem Sie auf die Schaltfläche **...** klicken und eine andere Farbe auswählen, oder indem Sie den Hexadezimalwert für eine andere Farbe eingeben.

Textfarbe

Der Standardwert für die Textfarbe ist Weiß. Ändern Sie diesen Wert, indem Sie auf den Abwärtspfeil klicken und eine andere Farbe auswählen.

Sekundäre Textfarbe

Der Standardwert für die sekundäre Textfarbe ist Schwarz. Ändern Sie diesen Wert, indem Sie auf den Abwärtspfeil klicken und eine andere Farbe auswählen.

Logo-Datei

Wenn Sie über ein Logo verfügen, das auf dem Portal angezeigt werden soll, klicken Sie auf die Schaltfläche **...**, um auf Ihrem PC danach zu suchen. Das Logo wird im Router-Flash gespeichert, wenn Sie auf **OK** klicken, und erscheint dann in der oberen linken Ecke des Portals.

Schaltfläche „Vorschau“

Klicken Sie auf diese Schaltfläche, um eine Vorschau der Portalansicht mit dem vordefinierten Thema oder den von Ihnen festgelegten benutzerdefinierten Werten anzuzeigen.

Farbe auswählen

Klicken Sie auf **Basis**, um eine vordefinierte Farbe auszuwählen, oder klicken Sie auf **RGB**, um eine benutzerdefinierte Farbe zu erstellen.

Basis

Wählen Sie die gewünschte Farbe aus der Palette an der linken Seite aus. Die ausgewählte Farbe wird in dem großen Quadrat rechts im Dialogfeld angezeigt.

RGB

Verwenden Sie die Schieberegler für Rot, Grün und Blau zusammen, um eine benutzerdefinierte Farbe zu erstellen. Die erstellte Farbe wird in dem großen Quadrat rechts im Dialogfeld angezeigt.

Kontext: NetBIOS-Namensserver-Listen

Zeigen Sie in diesem Fenster alle NetBIOS-Namensserver-Listen an, die für den ausgewählten Cisco IOS SSL VPN-Kontext konfiguriert wurden. CIFS verwendet NetBIOS-Server, um das unternehmenseigene Microsoft Windows-Dateisystem für die Cisco IOS SSL VPN-Benutzer anzuzeigen.

Im Bereich **NetBIOS-Namensserver-Listen** werden alle für den Kontext konfigurierten Namensserver-Listen angezeigt. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um diese Listen zu verwalten. Klicken Sie auf einen Listennamen, um den Inhalt dieser Liste im Bereich der Details zum NetBIOS-Namensserver anzuzeigen.

NetBIOS-Namensserver-Listen hinzufügen oder bearbeiten

In diesem Fenster können Sie eine NetBIOS-Namensserver-Liste erstellen oder verwalten. Sie müssen einen Namen für jede erstellte Liste eingeben und die IP-Adresse, das Timeout und die Anzahl der Versuche für jeden Server in der Liste angeben. Ein Server in jeder Liste muss als Master-Server bestimmt werden.

In diesem Dialogfeld wird jeder Server in der Liste zusammen mit seinem Master-Status, den Timeout- und Neuversuchswerten angezeigt.

NBNS-Server hinzufügen oder bearbeiten

Sie müssen die IP-Adresse jedes einzelnen Servers zusammen mit der Anzahl der Sekunden eingeben, die der Router warten soll, bevor er erneut versucht, eine Verbindung zum Server herzustellen, sowie die Anzahl der Versuche des Routers, Kontakt zum Server herzustellen.

Aktivieren Sie die Option **Als Master-Server einstellen**, wenn Sie möchten, dass dieser Server der erste in der Liste ist, den der Router kontaktiert.

Kontext: Port-Weiterleitungslisten

Konfigurieren Sie in diesem Fenster die Port-Weiterleitungslisten für den ausgewählten Kontext. Die Listen können einer beliebigen Gruppenrichtlinie zugeordnet werden, die unter dem ausgewählten Kontext konfiguriert ist. Port-Weiterleitungslisten zeigen die TCP-Anwendungsdienste für Cisco IOS SSL VPN-Clients an.

Im oberen Bereich des Fensters werden die Port-Weiterleitungslisten angezeigt, die für den ausgewählten Kontext konfiguriert wurden. Klicken Sie auf einen Listennamen, um detaillierte Informationen zur Liste im unteren Bereich des Fensters anzuzeigen.

Das Fenster zeigt die IP-Adresse, die verwendete Portnummer, die entsprechende Portnummer auf dem Client sowie eine Beschreibung an, sofern eine eingegeben wurde.

Port-Weiterleitungsliste hinzufügen oder bearbeiten

In diesem Fenster können Sie Port-Weiterleitungslisten erstellen und verwalten. Für jede Liste muss ein Name eingegeben werden und es muss mindestens ein Servereintrag vorhanden sein. Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um Einträge in der Liste zu erstellen, zu modifizieren und daraus zu entfernen.

Kontext: URL-Listen

URL-Listen geben an, welche Links auf dem Portal für Benutzer einer bestimmten Gruppe angezeigt werden können. Konfigurieren Sie eine oder mehrere URL-Listen für jeden Kontext und verwenden Sie dann die Gruppenrichtlinien-Fenster, um diese Listen mit bestimmten Gruppenrichtlinien zu verknüpfen.

Im oberen Bereich des Fensters werden alle URL-Listen angezeigt, die für den Kontext konfiguriert wurden. Im unteren Bereich des Fensters wird der Inhalt der ausgewählten Liste angezeigt. Für jede Liste wird die Überschrift, die über der URL-Liste erscheint, sowie jeder URL in der Liste angezeigt.

Verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Löschen**, um diese URL-Listen zu erstellen und zu verwalten.

URL-Liste hinzufügen oder bearbeiten

Sie müssen einen Namen für jede URL-Liste sowie Text für die Überschrift eingeben, die über der URL-Liste angezeigt wird.

Der Text in der Überschrift sollte eine allgemeine Beschreibung des Inhalts der Links in der Liste sein. Wenn zum Beispiel eine URL-Liste Zugriff auf die Webseiten *Gesundheitsplan* und *Versicherung* bietet, können Sie die Überschrift `Zuwendungen` verwenden.

Verwenden Sie die Schaltfläche **Hinzufügen**, um einen neuen Eintrag zur Liste hinzuzufügen, und die Schaltflächen **Bearbeiten** und **Löschen**, um die Liste zu verwalten. Jeder hinzugefügte Eintrag wird im Listenbereich angezeigt.

Kontext: Cisco Secure Desktop

Cisco Secure Desktop verschlüsselt Cookies, Browser-Verlaufsdateien, temporäre Dateien und E-Mail-Anhänge, die Sicherheitsprobleme verursachen könnten, wenn sie unverschlüsselt bleiben. Nachdem eine Cisco IOS SSL VPN-Sitzung beendet wurde, entfernt Cisco Secure Desktop die Daten mit einem Department of Defense Sanitation-Algorithmus.

Klicken Sie auf **Cisco Secure Desktop aktivieren**, um allen Benutzern dieses Kontexts zu erlauben, **Cisco Secure Desktop** herunterzuladen und zu verwenden. Wenn das Installationspaket für diese Software nicht auf dem Router gefunden werden kann, wird in diesem Fenster eine Meldung angezeigt.

Um das Installationspaket für Cisco Secure Desktop auf den Router zu laden, klicken Sie im Verzeichnisbaum Cisco IOS SSL VPN auf **Pakete**, und folgen Sie den Anweisungen im Fenster.

SSL VPN-Gateways

In diesem Fenster werden die auf dem Router konfigurierten Cisco IOS SSL VPN-Gateways angezeigt. Hier können Sie vorhandene Gateways ändern und neue konfigurieren. Ein Cisco IOS SSL VPN-Gateway ist das Benutzerportal zum sicheren Netzwerk.

SSL VPN-Gateways

In diesem Bereich des Fensters werden die auf dem Router konfigurierten Cisco IOS SSL VPN-Gateways angezeigt. Zusätzlich werden der Name und die IP-Adresse des Gateways, die Anzahl der für die Verwendung des Gateway konfigurierten Kontexte sowie der Status des Gateway angezeigt.


Das Gateway ist aktiviert und in Betrieb.


Das Gateway ist deaktiviert und außer Betrieb.

Klicken Sie auf ein Gateway, um detaillierte Informationen dazu im unteren Bereich des Fensters anzuzeigen. Aktivieren Sie ein Gateway, das **Deaktiviert** ist, indem Sie es auswählen und auf **Aktivieren** klicken. Sie können ein Gateway deaktivieren, indem Sie es auswählen und auf **Deaktivieren** klicken. Wenn Sie ein Gateway bearbeiten möchten, wählen Sie es aus, und klicken Sie auf die Schaltfläche **Bearbeiten**. Wenn Sie ein Gateway entfernen möchten, wählen Sie es aus, und klicken Sie auf die Schaltfläche **Löschen**.

Details of SSL VPN Gateway (Details zum SSL VPN-Gateway)

In diesem Bereich des Fensters werden Konfigurationsdetails zum Gateway, das im oberen Fensterbereich ausgewählt ist, sowie die Namen der Cisco IOS SSL VPN-Kontexte angezeigt, die für die Verwendung dieses Gateways konfiguriert wurden.

Weitere Informationen zu Gateway-Konfigurationsdetails finden Sie unter Add or Edit a SSL VPN Gateway (SSL VPN Gateway hinzufügen oder bearbeiten). Weitere Informationen zu Kontexten finden Sie unter SSL VPN-Kontext.

Add or Edit a SSL VPN Gateway (SSL VPN Gateway hinzufügen oder bearbeiten)

In diesem Fenster können Sie ein Cisco IOS SSL VPN-Gateway erstellen oder bearbeiten.

Gateway-Name

Der Gateway-Name identifiziert dieses Gateway eindeutig auf dem Router und stellt den Namen dar, mit dem das Gateway beim Konfigurieren von Cisco IOS SSL VPN-Kontexten bezeichnet wird.

IP-Adresse

Wählen Sie die IP-Adresse aus, die der Gateway verwenden soll, oder geben Sie sie ein. Hierbei muss es sich um eine öffentliche IP-Adresse handeln. Es darf keine Adresse sein, die von einem anderen Gateway auf dem Router verwendet wird.

Digitales Zertifikat

Wählen Sie das Zertifikat, das für die SSL-Authentifizierung an Cisco IOS SSL VPN-Clients gesendet wird.

Kontrollkästchen „HTTP-Umleitung“

Deaktivieren Sie dieses Kontrollkästchen, wenn Sie keine HTTP-Umleitung verwenden möchten. Bei der HTTP-Umleitung werden HTTP-Anforderungen automatisch an Port 443 umgeleitet, den Port, der für die sichere Cisco IOS SSL VPN-Kommunikation verwendet wird.

Kontrollkästchen „Gateway aktivieren“

Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das Gateway nicht aktivieren möchten. Sie können das Gateway auch über das Fenster **SSL VPN-Gateways** aktivieren und deaktivieren.

Pakete

In diesem Fenster können Sie Software-Installationspakete abrufen, die auf Cisco IOS SSL VPN-Clients heruntergeladen werden müssen, um Cisco IOS SSL VPN-Funktionen zu unterstützen und diese auf den Router laden. Sie können dieses Fenster auch verwenden, um Installationspakete zu entfernen, die installiert wurden.

Folgen Sie den in dem Fenster beschriebenen Schritten, um die Installationspakete von *Cisco.com* auf Ihren PC zu laden, und kopieren Sie sie dann von Ihrem PC auf den Router. Wenn Sie eines der Installationspakete abrufen möchten, beginnen Sie mit Schritt 1, indem Sie auf den Link zur Download-Website klicken.

Hinweis Für den Zugriff auf diese Download-Websites sind ein CCO-Benutzername und ein Kennwort erforderlich. Wenn Sie nicht über einen CCO-Benutzernamen und ein Kennwort verfügen, können Sie diese Angaben anfordern, indem Sie am oberen Rand einer beliebigen Website unter *Cisco.com* auf **Registrieren** klicken und das daraufhin angezeigte Formular ausfüllen. Ihr Benutzername und das Kennwort wird Ihnen per E-Mail zugeschickt.

Wenn Sie bereits Installationspakete auf Ihren PC oder den Router geladen haben, führen Sie die Schritte 2 und 3 aus, um den aktuellen Speicherort der Installationspakete anzugeben und die Pakete in den Router-Flash zu kopieren.

Klicken Sie in jedem Abschnitt auf die Schaltfläche **...**, um den aktuellen Speicherort des Installationspakets anzugeben.

Wenn Sie den aktuellen Speicherort festgelegt, sowie angegeben haben, ob Sie das Paket in den Router-Flash kopieren möchten, klicken Sie auf **Installieren**.

Nachdem die Pakete in den Router geladen wurden, werden im Fenster der Name, die Version und das Erstellungsdatum des Pakets angezeigt. Wenn ein Administrationstool im Paket enthalten ist, zeigt das Fenster eine Schaltfläche an, mit der Sie dieses Tool ausführen können.

Das Installationspaket für den Cisco IOS SSL VPN-Client ist unter dem folgenden Link verfügbar:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Das Installationspaket für Cisco Secure Desktop ist unter dem folgenden Link verfügbar:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Paket installieren

Geben Sie den aktuellen Speicherort eines Installationspakets an, indem Sie in diesem Fenster danach suchen. Wenn sich das Installationspaket bereits auf dem Router befindet, klicken Sie auf **Router**, und suchen Sie danach. Befindet sich das Installationspaket auf dem PC, klicken Sie auf **Arbeitsplatz**, und suchen Sie danach. Wenn Sie den aktuellen Speicherort des Installationspaket angegeben haben, klicken Sie auf **OK**.

Der Speicherort wird im Fenster **Pakete** angezeigt.

Cisco IOS SSL VPN-Kontexte, Gateways und Richtlinien

Cisco SDM bietet eine einfache Methode zum Konfigurieren von Cisco IOS SSL VPN-Verbindungen für Remote-Benutzer. Die in dieser Technologie verwendete Terminologie kann jedoch verwirrend sein. In diesem Hilfethema werden die Cisco IOS SSL VPN-Begriffe erläutert, die auf den Cisco SDM-Konfigurationsfenstern verwendet werden, und es wird beschrieben, wie die Komponenten von Cisco IOS SSL VPN zusammenarbeiten. Zusätzlich ist ein Beispiel für die Verwendung des Cisco IOS SSL VPN-Assistenten und der Bearbeitungsfenster in Cisco SDM enthalten.

Bevor die einzelnen Komponenten behandelt werden, ist es sinnvoll, folgende Punkte zu beachten:

- Ein Cisco IOS SSL VPN-Kontext kann mehrere Gruppenrichtlinien unterstützen.
- Jeder Kontext muss über ein verknüpftes Gateway verfügen.
- Ein Gateway kann mehrere Kontexte unterstützen.
- Wenn sich mehrere Gruppenrichtlinien auf dem Router befinden, muss ein AAA-Server zur Authentifizierung verwendet werden.

Cisco IOS SSL VPN-Kontexte

Ein Cisco IOS SSL VPN-Kontext identifiziert die Ressourcen, die für die Unterstützung von SSL VPN-Tunneln zwischen Remote-Clients und dem unternehmenseigenen oder privaten Intranet benötigt werden, und unterstützt eine oder mehrere Gruppenrichtlinien. Ein Cisco IOS SSL VPN-Kontext bietet die folgenden Ressourcen:

- Ein verknüpftes Cisco IOS SSL VPN-Gateway, das eine IP-Adresse bereitstellt, die von den Clients erreicht werden kann, und ein Zertifikat, das zum Einrichten einer sicheren Verbindung erforderlich ist.
- Mittel zur Authentifizierung. Sie können Benutzer lokal oder durch Verwendung von AAA-Servern authentifizieren.
- Die HTML-Anzeigeeinstellungen für das Portal, das Links zu Netzwerkressourcen bereitstellt.
- Port-Weiterleitungslisten, welche die Verwendung von Thin Client-Applets auf Remote-Clients ermöglichen. Jede Liste sollte für die Verwendung in einer bestimmten Gruppenrichtlinie konfiguriert werden.
- URL-Listen, die Links zu Ressourcen im Unternehmens-Intranet enthalten. Jede Liste sollte für die Verwendung in einer bestimmten Gruppenrichtlinie konfiguriert werden.
- NetBIOS-Namensserver-Listen. Jede Liste sollte für die Verwendung in einer bestimmten Gruppenrichtlinie konfiguriert werden.

Diese Ressourcen sind beim Konfigurieren von Cisco IOS SSL VPN-Gruppenrichtlinien verfügbar.

Ein Cisco IOS SSL VPN-Kontext kann mehrere Gruppenrichtlinien unterstützen. Ein Cisco IOS SSL VPN-Kontext kann nur mit einem Gateway verknüpft werden.

Cisco IOS SSL VPN-Gateways

Ein Cisco IOS SSL VPN-Gateway stellt einem oder mehreren Cisco IOS SSL VPN-Kontexten eine erreichbare IP-Adresse und ein Zertifikat zur Verfügung. Jeder auf einem Router konfigurierte Gateway muss mit seiner eigenen IP-Adresse konfiguriert werden; IP-Adressen können nicht von mehreren Gateways gemeinsam verwendet werden. Es ist möglich, die IP-Adresse einer Router-Schnittstelle oder eine andere erreichbare IP-Adresse zu verwenden, falls eine verfügbar ist. Es muss entweder ein digitales Zertifikat oder ein selbstsigniertes Zertifikat für die Gateways konfiguriert werden. Alle Gateways auf dem Router können dasselbe Zertifikat verwenden.

Ein Gateway kann zwar von mehreren Cisco IOS SSL VPN-Kontexten verwendet werden, es müssen jedoch Ressourcenbeschränkungen und die Erreichbarkeit von IP-Adressen berücksichtigt werden.

Cisco IOS SSL VPN-Richtlinien

Mit Cisco IOS SSL VPN-Gruppenrichtlinien können Sie die Anforderungen von verschiedenen Benutzergruppen berücksichtigen. Eine Benutzergruppe, die remote arbeitet, benötigt Zugriff auf andere Netzwerkressourcen als Vertriebsmitarbeiter, die im Außendienst arbeiten. Geschäftspartner und externe Lieferanten müssen auf die Informationen zugreifen, mit denen sie in Ihrer Organisation arbeiten müssen. Dabei muss jedoch sichergestellt werden, dass sie über keinen Zugriff auf vertrauliche Informationen oder andere Ressourcen verfügen, die sie nicht benötigen. Wenn Sie eine andere Richtlinie für jede dieser Gruppen erstellen, können Sie Remote-Benutzern die benötigten Ressourcen zur Verfügung stellen und verhindern, dass sie auf andere Ressourcen zugreifen.

Wenn Sie eine Gruppenrichtlinie konfigurieren, stehen die konfigurierten Ressourcen für den Kontext, der mit der Richtlinie verknüpft ist, wie URL-Listen, Port-Weiterleitungslisten und NetBIOS-Namensserver-Listen, zur Auswahl.

Wenn mehrere Gruppenrichtlinien auf dem Router konfiguriert sind, müssen Sie den Router für die Verwendung eines AAA-Servers zur Authentifizierung von Benutzern und zum Ermitteln der Richtliniengruppe konfigurieren, zu der ein bestimmter Benutzer gehört. Weitere Informationen erhalten Sie, wenn Sie auf Weitere Informationen zu Gruppenrichtlinien klicken.

Beispiel

In diesem Beispiel klickt ein Benutzer auf **Create a new SSL VPN** (Neues SSL VPN erstellen) und verwendet den Assistenten, um die erste Cisco IOS SSL VPN-Konfiguration auf dem Router zu verwenden. Wenn dieser Assistent abgeschlossen wird, wird ein neuer Kontext, Gateway und eine neue Gruppenrichtlinie erstellt. Die nachfolgende Tabelle enthält die Informationen, die der Benutzer in die einzelnen Fenster des Assistenten eingibt, sowie die Konfiguration, die Cisco SDM mit diesen Informationen erstellt.

Fenster des Cisco IOS SSL VPN-Assistenten	Konfiguration
Fenster „Create SSL VPN" (SSL VPN erstellen)	
Der Bereich der erforderlichen Aufgaben zeigt an, dass keine digitalen Zertifikate auf dem Router konfiguriert sind. Der Benutzer klickt auf **selbst signiertes Zertifikat** und konfiguriert ein Zertifikat im Dialogfeld **Bleibendes selbst signiertes Zertifikat**. Der Benutzer ändert nicht den von Cisco SDM angegebenen Namen **Router_Zertifikat**. Der Benutzer klickt auf **Create new SSL VPN** (Neues SSL VPN erstellen).	Cisco SDM konfiguriert ein selbst signiertes Zertifikat mit der Bezeichnung **Router_Zertifikat**, das in allen Cisco IOS SSL VPN-Konfigurationen zur Verwendung verfügbar ist.
Fenster „IP-Adresse und Name"	

Fenster des Cisco IOS SSL VPN-Assistenten	Konfiguration
Der Benutzer gibt die folgenden Informationen ein: IP-Adresse: 172.16.5.5 Name: Asien Aktivieren Sie **Sicheren SDM-Zugriff über 192.168.1.1 zulassen**. Zertifikat: **Router_Zertifikat**	Cisco SDM erstellt einen Kontext mit der Bezeichnung **Asien**. Cisco SDM erstellt ein Gateway mit der Bezeichnung **Gateway_1**, das die IP-Adresse 172.16.5.5 und **Router_Zertifikat** verwendet. Dieses Gateway kann mit mehreren Cisco IOS SSL VPN-Kontexten verknüpft werden. Benutzer greifen auf das Cisco IOS SSL VPN-Portal zu, indem sie **http://172.16.5.5/Asien** eingeben. Wenn dieser Gateway mit weiteren Kontexten verknüpft ist, wird dieselbe IP-Adresse im URL für diese Kontexte verwendet. Wenn der Kontext **Europa** zum Beispiel auch für die Verwendung von Gateway_1 konfiguriert ist, geben die Benutzer **https://172.16.5.5/Europa** ein, um auf das Portal zuzugreifen. Nachdem die Konfiguration an den Router geleitet wurde, müssen die Benutzer **http://172.16.5.5:4443** eingeben, um Cisco SDM mit dieser IP-Adresse zu starten: Cisco SDM beginnt auch mit der Konfiguration der ersten Gruppenrichtlinie mit der Bezeichnung **Richtlinie_1**.
Fenster „Benutzerauthentifizierung“	
Der Benutzer wählt die Option **Lokal auf diesem Router**. Der Benutzer fügt ein Benutzerkonto zur vorhandenen Liste hinzu.	Cisco SDM erstellt die Authentifizierungsliste **sdm_vpn_xauth_ml_1**. Diese Liste wird im Cisco IOS SSL VPN-Kontextfenster angezeigt, wenn der Benutzer den Assistenten abschließt. Die Benutzer, die im Fenster **Benutzerauthentifizierung** aufgeführt werden, sind die Mitglieder dieser Authentifizierungsliste und werden durch Richtlinie_1 bestimmt.
Fenster „Intranet-Websites konfigurieren“	

Fenster des Cisco IOS SSL VPN-Assistenten	Konfiguration
Der Benutzer konfiguriert die URL-Liste **Ulist_1**. Die Überschrift lautet **Taiwan**.	Die URL-Liste mit der Überschrift **Taiwan** wird auf dem Portal angezeigt, das für die Benutzer in **sdm_vpn_xauth_ml_1** angezeigt wird, wenn sie sich anmelden. Die URL-Liste steht zur Konfiguration in anderen Gruppenrichtlinien zur Verfügung, die unter dem Kontext **Asien** konfiguriert wurden.
Fenster „Full Tunnel aktivieren“	
Der Benutzer klickt auf **Full Tunnel aktivieren**, und wählt einen vordefinierten Adressenpool aus. Es sind keine erweiterten Optionen konfiguriert.	Client-PCs laden die Full Tunnel-Client-Software herunter, wenn sie sich zum ersten Mal anmelden, und es wird ein Full Tunnel zwischen dem PC und dem Router eingerichtet, wenn sich der Benutzer beim Portal anmeldet.
Fenster „Customize SSL VPN Portal“ (SSL VPN-Portal anpassen)	
Der Benutzer wählt **Seewind**.	Cisco SDM konfiguriert die HTTP-Anzeigeeinstellungen mit diesem Farbschema. Das Portal, das angezeigt wird, wenn sich Benutzer aus **Richtlinie_1** anmelden, verwendet diese Einstellungen. Diese Portaleinstellungen gelten auch für alle Richtlinien, die unter dem Kontext **Asien** konfiguriert sind. Der Benutzer kann die HTTP-Anzeigeeinstellungen in den Fenstern **Edit SSL VPN** (SSL VPN bearbeiten) nach Abschluss des Assistenten anpassen.
Fenster „SSL VPN Passthrough Configuration“ (SSL VPN Passthrough-Konfiguration)	
Der Benutzer aktiviert die Option **Allow SSL VPN to work with NAC and Firewall** (Zusammenarbeit von SSL VPN mit NAC und Firewall zulassen).	Cisco SDM fügt eine ACL mit dem folgenden Eintrag hinzu. `permit tcp any host 172.16.5.5 eq 443`

Fenster des Cisco IOS SSL VPN-Assistenten	Konfiguration
Übersichtsfenster	
Im Übersichtsfenster werden die Informationen angezeigt, die rechts aufgeführt sind. Zusätzliche Informationen können in den SSL VPN-Bearbeitungsfenstern angezeigt werden.	SSL VPN-Richtliniename: Richtlinie_1 SSL VPN-Gatewayname: Gateway_1 Methodenliste für Benutzerauthentifizierung: Lokal Full Tunnel-Konfiguration SVC-Status: Ja IP-Adressenpool: Pool_1 Split Tunneling: Deaktiviert Split DNS: Deaktiviert Full Tunnel-Client installieren: Aktiviert

Wenn diese Konfiguration gesendet wird, verfügt der Router über einen Cisco IOS SSL VPN-Kontext mit der Bezeichnung **Asien**, ein Gateway mit der Bezeichnung **Gateway_1** und eine Gruppenrichtlinie mit der Bezeichnung **Richtlinie_1**. Diese Informationen werden im SSL VPN-Bearbeitungsfenster angezeigt, wie in der nachstehenden Tabelle aufgeführt:

Name	Gateway	Domäne	Status	Administrativer Status
Asien	Gateway_1	Asien		In Betrieb

Details zum SSL VPN-Kontext „Asien“:	
Elementname	**Elementwert**
Gruppenrichtlinien	
Richtlinie_1	
Dienste	URL-Mangling, Full Tunnel
Den Benutzern angezeigte URLs	http://172.16.5.5/Preisliste
	http://172.16.5.5/Katalog
Den Benutzern angezeigte Server	<Keine>
WINS-Server	<Keine>

Richtlinie_1 bietet den grundlegenden Cisco IOS SSL VPN-Dienst URL-Mangling und gibt an, dass ein Full Tunnel zwischen Clients und Router eingerichtet wird. Es sind keine weiteren Funktionen konfiguriert. Sie können Funktionen zu Richtlinie_1 hinzufügen, zum Beispiel Thin Client und Common Internet File System, indem Sie die Option **Configure advanced features for an existing SSL VPN** (Erweiterte Funktionen für ein vorhandenes SSL VPN konfigurieren) wählen und anschließend **Asien** und **Richtlinie_1** im Fenster **Select the Cisco IOS SSL VPN User Group** (Cisco IOS SSL VPN-Benutzergruppe auswählen) und die Funktionen im Fenster **Erweiterte Funktionen** auswählen. In diesem Assistenten können auch zusätzliche URL-Listen konfiguriert werden.

Sie können eine neue Gruppenrichtlinie unter dem Kontext **Asien** erstellen, indem Sie **Add a new policy to an existing SSL VPN for a new group of users** (Fügen Sie für eine neue Benutzergruppe eine neue Richtlinie zu einem vorhandenen SSL VPN hinzu) auswählen.

Sie können Einstellungen für den Kontext **Asien** und die Richtlinien, die unter diesem Kontext konfiguriert sind, anpassen, indem Sie **Asien** in der Kontextliste auswählen und auf **Bearbeiten** klicken. Im Fenster zum Bearbeiten des SSL VPN-Kontexts für Asien wird eine Baumstruktur angezeigt, über die Sie weitere Ressourcen für den Kontext konfigurieren und zusätzliche Richtlinien bearbeiten und konfigurieren können. Sie können die Einstellungen für Gateway_1 bearbeiten, indem Sie auf **SSL VPN Gateways** unter dem SSL VPN-Knoten klicken, **Gateway_1** auswählen und auf **Bearbeiten** klicken.

Wie gehe ich vor?

Diese Themen erläutern häufige Konfigurationsaufgaben, die mit dieser Funktion verknüpft sind.

Wie kann ich überprüfen, ob mein Cisco IOS SSL VPN funktioniert?

Die beste Möglichkeit, festzustellen, dass ein Cisco IOS SSL VPN-Kontext den Zugriff bereitstellt, den Sie für die Benutzer konfiguriert haben, besteht darin, sich selbst als Benutzer zu konfigurieren und zu versuchen, auf alle Websites und Dienste zuzugreifen, für deren Bereitstellung der Kontext konfiguriert ist. Verwenden Sie die folgende Vorgehensweise als Anleitung zum Einrichten dieses Tests.

Schritt 1 Stellen Sie sicher, dass Anmeldeinformationen, die Sie verwenden können, in allen entsprechenden Richtlinien auf dem AAA-Server enthalten sind.

Schritt 2 Wenn das funktioniert, öffnen Sie eine Cisco SDM-Sitzung auf dem Router, damit Sie den Cisco IOS SSL VPN-Datenverkehr überwachen können, den Sie generieren. Dieser Vorgang muss auf einem anderen PC durchgeführt werden, wenn der PC, den Sie zum Testen des Cisco IOS SSL VPN-Kontexts verwenden, sich nicht in einem Netzwerk befindet, von dem Sie auf Cisco SDM zugreifen können. Wechseln Sie zu **Monitor > VPN-Status > SSL VPN**.

Schritt 3 Geben Sie die URL für die einzelnen Web-Portale ein, die für diesen Cisco IOS SSL VPN-Kontext konfiguriert sind. Überprüfen Sie, ob jede Seite das Erscheinungsbild aufweist, das Sie konfiguriert haben, und ob alle in den URL-Links für die Richtlinie festgelegten Links auf der Seite angezeigt werden.

Schritt 4 Prüfen Sie alle Links und Dienste, die den in dieser Richtlinie enthaltenen Benutzern zur Verfügung stehen sollten. Wenn eine der Richtlinien, die Sie testen, ein Download von Cisco Secure Desktop oder der Full Tunnel-Client-Software bereitstellt, geben Sie die URLs zu den Web-Portalen für diese Richtlinien ein, und klicken Sie auf die Links, die das Herunterladen dieser Software erfordern. Überprüfen Sie, ob die Software ordnungsgemäß heruntergeladen wird, und ob Sie auf die Dienste zugreifen können, auf die ein Benutzer über diese Links zugreifen können soll.

Schritt 5 Wenn Sie vor dem Testen eine Cisco SDM-Sitzung herstellen konnten, klicken Sie auf den Zweig für den Kontext, den Sie testen, und sehen Sie sich die Statistiken zum Cisco IOS SSL VPN-Datenverkehr im Cisco IOS SSL VPN-Fenster an.

Schritt 6 Kehren Sie unter Berücksichtigung der Testergebnisse zu Cisco SDM zurück, und beheben Sie alle erkannten Konfigurationsprobleme.

Wie konfiguriere ich ein Cisco IOS SSL VPN nachdem ich eine Firewall konfiguriert habe?

Auch wenn Sie bereits eine Firewall konfiguriert haben, können Sie noch die Cisco IOS SSL VPN-Assistenten in Cisco SDM verwenden, um Cisco IOS SSL VPN-Kontexte und -Richtlinien zu erstellen. Cisco SDM überprüft die generierten Cisco IOS SSL VPN-CLI-Befehle anhand der auf dem Router vorhandenen Konfiguration. Wenn eine vorhandene Firewallkonfiguration ermittelt wird, für die eine Änderung erforderlich ist, um das Passieren von Cisco IOS SSL VPN-Datenverkehr zuzulassen, werden Sie benachrichtigt. Sie können zulassen, dass Cisco SDM die erforderlichen Änderungen an der Firewall vornimmt, oder Sie lassen die Firewall intakt und nehmen die Änderungen manuell vor, indem Sie zu **Konfigurieren > Firewall und ACL > Firewallrichtlinie/ACL bearbeiten** wechseln, und die Zulassungsanweisungen eingeben, die Sie benötigen, um zuzulassen, dass Cisco IOS SSL VPN-Datenverkehr die Firewall passiert.

Wie kann ich eine VRF-Instanz mit einem Cisco IOS SSL VPN-Kontext verknüpfen?

VPN Routing and Forwarding (VFR)-Instanzen verwalten eine Routing-Tabelle und eine Weiterleitungstabelle für ein VPN. Sie können eine VR-Instanz oder einen Namen mit einem Cisco IOS SSL VPN-Kontext verknüpfen, indem Sie zu **Konfigurieren > VPN > SSL VPN > Edit SSL VPN** (SSL VPN bearbeiten) wechseln. Wählen Sie den Kontext aus, mit dem Sie eine VRF-Instanz verknüpfen möchten, und klicken Sie auf **Bearbeiten**. Wählen Sie im daraufhin angezeigten Dialogfeld den Namen der VRF-Instanz aus.

Hinweis Diese VRF-Instanz muss bereits auf dem Router konfiguriert sein.

KAPITEL 20

VPN-Fehlerbehebung

Cisco SDM kann Fehler beheben, die in von Ihnen konfigurierten VPN-Verbindungen auftreten. Cisco SDM meldet, ob Verbindungstests erfolgreich waren. Ist das nicht der Fall, erhalten Sie Empfehlungen für Maßnahmen, mit denen Sie Verbindungsprobleme beheben können.

Über den folgenden Link erhalten Sie Informationen zur VPN-Fehlerbehebung mit der CLI.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/useguide/u13_rtrb.htm

VPN-Fehlerbehebung

Dieses Fenster wird angezeigt, wenn Sie Fehler in einem Site-to-Site-VPN, einem GRE over IPSec-Tunnel, einer Easy VPN-Remote-Verbindung oder einer Easy VPN-Serververbindung beheben.

Hinweis Im Rahmen der VPN-Fehlerbehebung werden für Site-to-Site-VPN-, GRE over IPsec- oder Easy VPN-Clientverbindungen nicht Fehler von mehr als zwei Peers behoben.

Details zum Tunnel

In diesem Feld sind Details zum VPN-Tunnel angegeben.

Schnittstelle

Die Schnittstelle, an der der VPN-Tunnel konfiguriert ist.

Peer

Die IP-Adresse oder der Hostname der Geräte am anderen Ende der VPN-Verbindung.

Übersicht

Klicken Sie auf diese Schaltfläche, wenn Sie eine Übersicht über die Fehlerbehebungsinformationen anzeigen möchten.

Details

Klicken Sie auf diese Schaltfläche, wenn Sie ausführliche Fehlerbehebungsinformationen anzeigen möchten.

Aktivität

In dieser Spalte werden die Aktivitäten zur Fehlerbehebung aufgeführt.

Status

Zeigt den Status der einzelnen Fehlerbehebungsaktivitäten durch die folgenden Symbole und Warntexte an:

 Die Verbindung ist aktiv.

 Die Verbindung ist nicht aktiv.

 Test erfolgreich.

 Test fehlgeschlagen.

Fehlerursache(n)

In diesem Feld werden die möglichen Gründe für den Fehler beim VPN-Tunnel angegeben.

Empfohlene Aktion(en)

In diesem Feld finden Sie eine mögliche Maßnahme/Lösung, um das Problem zu beheben.

Schaltfläche „Schließen“

Klicken Sie auf diese Schaltfläche, um das Fenster zu schließen.

Schaltfläche „Test Specific Client“

Diese Schaltfläche ist aktiviert, wenn Sie Verbindungen für einen Easy VPN-Server testen, der auf dem Router konfiguriert ist. Klicken Sie auf diese Schaltfläche, und geben Sie den Client an, zu dem Sie die Konnektivität testen möchten.

Diese Schaltfläche ist unter den folgenden Umständen deaktiviert:

- Die allgemeinen Tests wurden nicht durchgeführt oder nicht erfolgreich abgeschlossen.
- Das IOS-Abbild unterstützt nicht die erforderlichen Debugging-Befehle.
- Die zum Starten von Cisco SDM verwendete Ansicht verfügt nicht über Root-Berechtigungen.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Beheben von Fehlern in der VPN-Verbindung	Klicken Sie auf die Schaltfläche **Start**. Während der Ausführung des Tests wechselt die Bezeichnung der Schaltfläche **Start** zu **Stopp**. Sie können die Fehlerbehebung während der Durchführung des Tests abbrechen.
Den Testbericht speichern.	Klicken Sie auf die Schaltfläche **Bericht speichern**, um den Testbericht in HTML-Format zu speichern. Diese Schaltfläche ist deaktiviert, während der Test läuft.

VPN-Fehlerbehebung: Easy VPN-Client angeben

In diesem Fenster können Sie den Easy VPN-Client angeben, für den Sie ein Debugging durchführen möchten.

IP-Adresse

Geben Sie die IP-Adresse des Easy VNP-Clients ein, für den Sie ein Debugging durchführen möchten.

Dauer der Abfrage der Anforderung: X Minuten

Geben Sie an, wie lange der Easy VPN-Server Anforderungen vom Easy VPN-Client abfragen muss.

Schaltfläche „Fortfahren“

Klicken Sie nach der Auswahl des gewünschten Typs der Datenverkehrsgenerierung auf diese Schaltfläche, um mit den Tests fortzufahren.

Schaltfläche „Schließen“

Klicken Sie auf diese Schaltfläche, um das Fenster zu schließen.

VPN-Fehlerbehebung: Generate Traffic (Datenverkehr generieren)

Dieses Fenster ermöglicht Ihnen die Erzeugung der Fehlerbereinigung (Debugging) von site-to-site VPN oder Easy VPN-Verkehr. Sie können zulassen, dass Cisco SDM VPN-Datenverkehr generiert, oder VPN-Datenverkehr selbst generieren.

VPN-Datenverkehr in dieser Verbindung ist definiert als

In diesem Bereich ist der aktuelle VPN-Datenverkehr auf der Schnittstelle aufgelistet.

Aktion

Diese Spalte gibt an, ob der Datenverkehrstyp auf der Schnittstelle zulässig ist.

Quelle

Die Quell-IP-Adresse.

Ziel

Die Ziel-IP-Adresse.

Dienst

Diese Spalte listet den Datenverkehrstyp auf der Schnittstelle auf.

Protokoll

Diese Spalte gibt an, ob die Logging-Funktion für diesen Datenverkehr aktiviert wurde.

Attribute

Weitere definierte Attribute.

SDM soll VPN-Datenverkehr generieren

Wählen Sie diese Option aus, wenn Cisco SDM VPN-Datenverkehr für das Debugging auf der Schnittstelle generieren soll.

Hinweis Cisco SDM generiert keinen VPN-Verkehr, wenn der Datenverkehr des VPN-Tunnels von einer nicht IP-basierte Zugriffssteuerungsliste (Access Control List, ACL) stammt oder es sich bei der angewendeten und aktuellen CLI-Ansicht um keine Root-Ansicht handelt.

Geben Sie die IP-Adresse eines Hosts im Quellnetzwerk ein

Geben Sie die Host-IP-Adresse im Quellnetzwerk ein.

Geben Sie die IP-Adresse eines Hosts im Zielnetzwerk ein

Geben Sie die Host-IP-Adresse im Zielnetzwerk ein.

Ich generiere VPN-Datenverkehr vom Quellnetzwerk

Wählen Sie diese Option aus, wenn Sie VPN-Datenverkehr von Quellnetzwerk generieren möchten.

Wartezeit

Geben Sie an, wie viele Sekunden der Easy VPN-Server darauf warten soll, dass Sie Quellverkehr generieren. Achten Sie darauf, dass Sie sich genügend Zeit geben, zum Generieren von Datenverkehr zu anderen Systemen zu wechseln.

Schaltfläche „Fortfahren“

Klicken Sie nach der Auswahl des gewünschten Typs der Datenverkehrsgenerierung auf diese Schaltfläche, um mit den Tests fortzufahren.

Schaltfläche „Schließen“

Klicken Sie auf diese Schaltfläche, um das Fenster zu schließen.

VPN-Fehlerbehebung: GRE-Datenverkehr generieren

Dieser Bildschirm wird angezeigt, wenn Sie GRE over IPSec-Datenverkehr generieren.

SDM soll VPN-Datenverkehr generieren

Wählen Sie diese Option aus, wenn Cisco SDM VPN-Datenverkehr für das Debugging auf der Schnittstelle generieren soll.

Geben Sie die Remote-Tunnel-IP-Adresse ein

Geben Sie die IP-Adresse des Remote-GRE-Tunnels ein. Verwenden Sie nicht die Adresse der Remote-Schnittstelle.

Ich generiere VPN-Datenverkehr vom Quellnetzwerk

Wählen Sie diese Option aus, wenn Sie VPN-Datenverkehr von Quellnetzwerk generieren möchten.

Wartezeit

Geben Sie an, wie viele Sekunden der Easy VPN-Server darauf warten soll, dass Sie Quellverkehr generieren. Achten Sie darauf, dass Sie sich genügend Zeit geben, zum Generieren von Datenverkehr zu anderen Systemen zu wechseln.

Schaltfläche „Fortfahren“

Klicken Sie nach der Auswahl des gewünschten Typs der Datenverkehrsgenerierung auf diese Schaltfläche, um mit den Tests fortzufahren.

Schaltfläche „Schließen“

Klicken Sie auf diese Schaltfläche, um das Fenster zu schließen.

Cisco SDM-Warnung: SDM aktiviert die Router-Debugging-Meldungen...

Dieses Fenster wird angezeigt, wenn Cisco SDM mit der erweiterten Fehlerbehebung beginnen kann. Die erweiterte Fehlerbehebung umfasst das Übermitteln von Debugging-Befehlen an den Router, der auf zu meldende Ergebnisse wartet, und anschließend das Entfernen der Debugging-Befehle, damit die Leistung des Routers nicht weiter beeinträchtigt wird.

Diese Meldung wird angezeigt, weil dieser Prozess mehrere Minuten in Anspruch nehmen und die Routerleistung beeinträchtigen kann.

KAPITEL 21

Sicherheitsprüfung

Die Sicherheitsprüfung ist eine Funktion, mit der die vorhandenen Routerkonfigurationen untersucht werden. Anschließend wird der Router aktualisiert, um Router und Netzwerk sicherer zu machen. Die Sicherheitsprüfung basiert auf der Cisco IOS AutoSecure-Funktion; die Prüfung führt Tests durch und hilft bei der Konfiguration fast aller AutoSecure-Funktionen. Eine vollständige Liste der Funktionen, die während der Sicherheitsüberprüfung geprüft werden, sowie eine Liste der wenigen AutoSecure-Funktionen, die von der Sicherheitsprüfung nicht unterstützt werden, finden Sie unter Cisco SDM und Cisco IOS AutoSecure.

Das Sicherheitsaudit wird in einem von zwei Modi durchgeführt – dem Sicherheitsaudit-Assistenten, mit dem Sie potenziell sicherheitsbezogene Konfigurationsänderungen auswählen und auf Ihrem Router implementieren können, und One-Step Lockdown, das automatisch alle empfohlenen sicherheitsbezogenen Konfigurationsänderungen vornimmt.

Sicherheitsaudit durchführen

Wenn Sie diese Option auswählen, wird der Sicherheitsaudit-Assistent gestartet. Der Sicherheitsaudit-Assistent testet die Konfiguration Ihres Routers, um festzustellen, ob potenzielle Sicherheitsprobleme in der Konfiguration vorhanden sind. Anschließend wird ein Bildschirm angezeigt, in dem Sie entscheiden können, welches dieser Sicherheitsprobleme Sie beheben möchten. Wenn Sie Ihre Entscheidung getroffen haben, nimmt der Sicherheitsprüfungs-Assistent die erforderlichen Änderungen an der Routerkonfiguration vor, um diese Probleme zu beheben.

So führt Cisco SDM eine Sicherheitsprüfung durch und behebt anschließend die gefundenen Probleme:

Schritt 1 Wählen Sie im linken Bereich die Option **Sicherheitsprüfung** aus.

Schritt 2 Klicken Sie auf **Sicherheitsaudit durchführen**.

Die Seite **Willkommen beim Sicherheitsprüfungs-Assistenten!** wird angezeigt.

Schritt 3 Klicken Sie auf **Weiter >**.

Die Seite **Sicherheitsaudit-Schnittstellenkonfiguration** wird angezeigt.

Schritt 4 Der Sicherheitsprüfungs-Assistent muss wissen, welche Ihrer Routerschnittstellen mit Ihrem inneren Netzwerk und welche Schnittstelle mit Ihrem äußeren Netzwerk verbunden ist. Aktivieren Sie für jede aufgeführte Schnittstelle entweder das Kontrollkästchen **Innen** oder **Außen**, um anzugeben, wo die Schnittstelle angeschlossen ist.

Schritt 5 Klicken Sie auf **Weiter >**.

Der Sicherheitsaudit-Assistent testet Ihre Routerkonfiguration, um zu ermitteln, welche potenziellen Sicherheitsprobleme möglicherweise vorhanden sind. Daraufhin wird ein Bildschirm angezeigt, auf dem der Fortschritt dieser Aktion dargestellt und alle geprüften Konfigurationsoptionen aufgeführt sind. Zusätzlich wird angezeigt, ob die aktuelle Routerkonfiguration diese Tests bestanden hat.

Wenn Sie diesen Bericht in einer Datei speichern möchten, klicken Sie auf **Bericht speichern**.

Schritt 6 Klicken Sie auf **Schließen**.

Daraufhin wird der Bildschirm **Sicherheitsprüfung – Berichtskarte** mit einer Liste möglicher Sicherheitsprobleme angezeigt.

Schritt 7 Aktivieren Sie neben den Problemen, die Cisco Router and Security Device Manager (Cisco SDM) beheben soll, das Kontrollkästchen **Beheben**. Klicken Sie auf die Problembeschreibung, um eine Hilfeseite zu dem Problem mit einer Beschreibung des Problems und einer Liste der Cisco IOS-Befehle, die zu Ihrer Konfiguration hinzugefügt werden, anzuzeigen.

Schritt 8 Klicken Sie auf **Weiter >**.

Schritt 9 Der Sicherheitsaudit-Assistent kann einen oder mehrere Bildschirme anzeigen, in die Sie Informationen eingeben müssen, um bestimmte Probleme zu beheben. Geben Sie die erforderlichen Informationen ein, und klicken Sie auf jedem dieser Bildschirme auf **Weiter >**.

Schritt 10 In der Zusammenfassung des Assistenten wird eine Liste aller Konfigurationsänderungen angezeigt, die während der Sicherheitsprüfung durchgeführt werden. Klicken Sie auf **Fertig stellen**, um diese Änderungen an Ihren Router zu senden.

One-Step Lockdown

Diese Option testet Ihre Routerkonfiguration auf potenzielle Sicherheitsprobleme und nimmt automatisch alle erforderlichen Konfigurationsänderungen vor, um alle gefundenen Probleme zu beheben. Die Bedingungen werden überprüft und gegebenenfalls folgendermaßen korrigiert:

- Deaktivieren des Finger-Dienstes
- Deaktivieren des PAD-Dienstes
- Deaktivieren des TCP Small Servers-Dienstes
- Deaktivieren des UDP Small Servers-Dienstes
- Deaktivieren des IP BOOTP Server-Dienstes
- Deaktivieren des IP-Identifizierungsdienstes
- Deaktivieren von CDP
- Deaktivieren von IP Source Routing
- Aktivieren des Dienstes für Kennwortverschlüsselung
- Aktivieren von TCP Keepalives für eingehende Telnet-Sitzungen
- Aktivieren von TCP Keepalives für ausgehende Telnet-Sitzungen
- Aktivieren von Sequenznummern und Zeitstempeln für Debugging-Meldungen
- Aktivieren von IP CEF
- Deaktivieren von Gratuitous ARP-Anfragen
- Einstellen der Mindestlänge für Kennwörter auf weniger als 6 Zeichen

- Einstellen der Authentifizierungsfehlerrate auf weniger als 3 Wiederholungen
- Einstellen der TCP Synwait-Zeit
- Festlegen eines Banners
- Logging aktivieren
- Einstellen von „Geheimes Kennwort aktivieren“
- Deaktivieren von SNMP
- Einstellen des Scheduler-Intervalls
- Einstellen von Scheduler Allocate
- Einstellen von Benutzern
- Aktivieren von Telnet-Einstellungen
- Aktivieren von NetFlow Switching
- IP Redirects deaktivieren
- Deaktivieren von IP Proxy Arp
- Deaktivieren von IP Directed Broadcast
- Deaktivieren des MOP-Dienstes
- Deaktivieren von IP Unreachables
- Deaktivieren von IP Mask Reply
- Deaktivieren von IP Unreachables für NULL-Schnittstelle
- Aktivieren von Unicast RPF für alle äußeren Schnittstellen
- Aktivieren der Firewall für alle äußeren Schnittstellen
- Festlegen der Zugriffsklasse für den HTTP-Server-Dienst
- Festlegen der Zugriffsklasse für VTY-Leitungen
- Aktivieren von SSH für Zugriff auf den Router

Willkommensseite

Auf diesem Bildschirm werden der Sicherheitsprüfungs-Assistent und die Änderungen angezeigt, die der Assistent versucht, an Ihrer Routerkonfiguration vorzunehmen.

Seite zur Schnittstellenauswahl

Auf diesem Bildschirm wird eine Liste aller Schnittstellen angezeigt. Hier müssen Sie angeben, welche Routerschnittstellen äußere Schnittstellen sind, also Schnittstellen, die mit unsicheren Netzwerken wie dem Internet verbunden sind. Durch Identifizieren der äußeren Schnittstellen kann die Sicherheitskonfiguration feststellen, für welche Schnittstellen Firewall-Sicherheitsfunktionen konfiguriert werden müssen.

Spalte Schnittstelle

In dieser Spalte werden alle Routerschnittstellen aufgeführt.

Spalte Außen

In dieser Spalte wird ein Kontrollkästchen für jede Schnittstelle angezeigt, die in der Spalte **Schnittstelle** aufgeführt ist. Aktivieren Sie das Kontrollkästchen für jede Schnittstelle, die mit einem Netzwerk außerhalb Ihres Netzwerks, zum Beispiel dem Internet, verbunden ist.

Spalte Innen

In dieser Spalte wird ein Kontrollkästchen für jede Schnittstelle angezeigt, die in der Spalte **Schnittstelle** aufgeführt ist. Aktivieren Sie das Kontrollkästchen für jede Schnittstelle, die direkt mit Ihrem lokalen Netzwerk verbunden und somit durch Ihre Firewall vor dem Internet geschützt ist.

Seite Berichtskarte

Auf der Popup-Seite **Berichtskarte** wird eine Liste mit empfohlenen Konfigurationsänderungen angezeigt, nach deren Durchführung das Netzwerk sicherer würde. Mit der Schaltfläche **Speichern**, die nach der Durchführung aller Prüfungen aktiviert wird, können Sie die Berichtskarte in einer Datei speichern, die Sie dann drucken oder per E-Mail versenden können. Wenn Sie auf **Schließen** klicken, wird ein Dialogfeld mit den gemeldeten Sicherheitsproblemen angezeigt, in dem auch solche Sicherheitskonfigurationen aufgeführt sein können, die Cisco SDM rückgängig machen kann.

Seite Beheben

Auf dieser Seite werden die Konfigurationsänderungen angezeigt, die auf der Seite **Berichtskarte** empfohlen werden. In der Liste **Option auswählen** können Sie die Sicherheitsprobleme anzeigen, die Cisco SDM beheben kann, oder die Sicherheitskonfigurationen anzeigen, die Cisco SDM rückgängig machen kann.

Option auswählen: Sicherheitsprobleme beheben

Auf der Seite **Berichtskarte** wird eine Liste mit empfohlenen Konfigurationsänderungen angezeigt, nach deren Durchführung der Router und das Netzwerk sicherer wird. Die potenziellen Sicherheitsprobleme in Ihrer Routerkonfiguration werden in der linken Spalte aufgeführt. Klicken Sie auf ein potenzielles Problem, um weitere Informationen zu diesem Problem zu erhalten. In der Online-Hilfe wird eine ausführlichere Beschreibung des Problems mit den empfohlenen Konfigurationsänderungen angezeigt. Wenn Sie alle potenziellen Probleme beheben möchten, klicken Sie auf **Alle beheben**, und klicken Sie dann auf **Weiter >**, um fortzufahren. Zur Behebung einzelner Sicherheitsprobleme aktivieren Sie das Kontrollkästchen **Beheben** neben dem Problem bzw. den Problemen, das bzw. die behoben werden sollen, und klicken Sie dann auf **Weiter >**, um den Sicherheitsprüfungs-Assistenten fortzusetzen. Während der Sicherheitsprüfung werden die ausgewählten Probleme behoben und dabei gegebenenfalls weitere Informationen von Ihnen abgefragt. Anschließend wird eine Liste der neuen Konfigurationsbefehle angezeigt, die zur Routerkonfiguration hinzugefügt werden.

Alle beheben

Klicken Sie auf diese Schaltfläche, um ein Häkchen neben allen potenziellen Sicherheitsproblemen zu setzen, die auf dem Bildschirm **Berichtskarte** aufgeführt sind.

Option auswählen: Sicherheitskonfigurationen rückgängig machen

Wenn diese Option aktiviert ist, zeigt Cisco SDM die Sicherheitskonfigurationen an, die rückgängig gemacht werden können. Wenn Cisco SDM alle Sicherheitskonfigurationen rückgängig machen soll, klicken Sie auf **Alle rückgängig**. Wenn Sie eine Sicherheitskonfiguration angeben möchten, die rückgängig gemacht werden soll, aktivieren Sie das Kontrollkästchen **Rückgängig** neben dieser Konfiguration. Nachdem Sie festgelegt haben, welche Sicherheitskonfigurationen rückgängig gemacht werden sollen, klicken Sie auf **Weiter >**. Sie müssen mindestens eine Sicherheitskonfiguration auswählen, die rückgängig gemacht werden soll.

Alle rückgängig

Klicken Sie auf diese Schaltfläche, um ein Häkchen neben alle Sicherheitskonfigurationen zu setzen, die Cisco SDM rückgängig machen kann.

Sie können anzeigen, welche Sicherheitskonfigurationen Cisco SDM rückgängig machen kann, indem Sie auf folgende Option klicken:

Sicherheitskonfigurationen, die Cisco SDM rückgängig machen kann

Ich möchte, dass Cisco SDM einige Probleme behebt, jedoch andere Sicherheitskonfigurationen rückgängig macht.

Wenn Sie möchten, dass Cisco SDM einige Sicherheitsprobleme behebt, jedoch andere nicht benötigte Sicherheitskonfigurationen rückgängig macht, können Sie den Sicherheitsprüfungs-Assistenten einmal ausführen, um die zu behebenden Probleme festzulegen, und den Assistenten dann erneut ausführen, um die Sicherheitskonfigurationen auszuwählen, die Sie rückgängig machen möchten.

Deaktivieren des Finger-Dienstes

Die Sicherheitsprüfung deaktiviert möglichst immer den Finger-Dienst. Der Finger-Dienst wird verwendet, um festzustellen, welche Benutzer bei einem Netzwerkgerät angemeldet sind. Diese Informationen sind zwar nicht extrem vertraulich, können jedoch manchmal für Hacker nützlich sein.

Der Finger-Dienst kann zusätzlich für einen bestimmten Typ des Denial-of-Service (DoS)-Angriffs namens „Finger of death“ verwendet werden, bei dem jede Minute eine Finger-Anfrage an einen bestimmten Computer gesendet, die Verbindung jedoch niemals getrennt wird.

Folgende Konfiguration wird an den Router gesendet, um den Finger-Dienst zu deaktivieren:

```
no service finger
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren des PAD-Dienstes

Bei der Sicherheitsprüfung werden alle Befehle zum Zusammensetzen und Auflösen von Paketen (PAD) sowie Verbindungen zwischen PAD-Geräten und Zugriffsservern möglichst immer deaktiviert.

Folgende Konfiguration wird an den Router gesendet, um PAD zu deaktivieren:

```
no service pad
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren des TCP Small Servers-Dienstes

Die Sicherheitsprüfung deaktiviert Small Server-Dienste, wann immer möglich. Standardmäßig bieten Cisco-Geräte, auf denen Cisco IOS Version 11.3 oder früher ausgeführt wird, die Small Server-Dienste: echo, chargen, and discard. (In der Cisco IOS Software-Version 12.0 und später sind Small Servers-Dienste standardmäßig deaktiviert.) Diese Dienste, insbesondere die User Datagram Protocol-(UDP)-Versionen, werden ab und zu für berechtigte Zwecke verwendet, sie können jedoch zum Starten von DoS-Angriffen und anderen Angriffen verwendet werden, die andernfalls durch die Paketfilterung verhindert werden könnten.

So kann ein Hacker zum Beispiel ein Domänennamensystem (DNS)-Paket senden, die Quelladresse zu einem DNS-Server fälschen, der andernfalls nicht erreichbar wäre, und den Quellport zu einem DNS-Dienstport (Port 53) fälschen. Wenn ein solches Paket an den UDP Echo-Port des Routers gesendet würde, würde der Router ein DNS-Paket an den betreffenden Server senden. Es würden keine Prüfungen für ausgehende Zugriffslisten für dieses Paket durchgeführt, da davon ausgegangen würde, dass das Paket lokal vom Router selbst generiert wurde.

Auch wenn die meisten Missbrauchsfälle der Small Servers-Dienste durch Anti-Spoofing-Zugriffslisten vermieden oder entschärft werden können, sollten die Dienste in jedem Router, der Teil der Firewall ist oder sich in einem sicherheitsrelevanten Teil des Netzwerks befindet, möglichst immer deaktiviert sein. Da die Dienste selten verwendet werden, ist es meist die beste Vorgehensweise, diese Dienste auf allen Routern jeglicher Art zu deaktivieren.

Folgende Konfiguration wird an den Router gesendet, um den TCP Small Servers-Dienst zu deaktivieren:

```
no service tcp-small-servers
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren des UDP Small Servers-Dienstes

Die Sicherheitsprüfung deaktiviert Small Server-Dienste, wann immer möglich. Standardmäßig bieten Cisco-Geräte, auf denen Cisco IOS Version 11.3 oder früher ausgeführt wird, die Small Server-Dienste: echo, chargen, and discard. (In der Cisco IOS Software-Version 12.0 und später sind Small Servers-Dienste standardmäßig deaktiviert.) Diese Dienste, insbesondere die UDP-Versionen, werden ab und zu für berechtigte Zwecke verwendet, sie können jedoch zum Starten von DoS-Angriffen und anderen Angriffen verwendet werden, die andernfalls durch die Paketfilterung verhindert werden könnten.

So kann ein Hacker zum Beispiel ein DNS-Paket senden, die Quelladresse zu einem DNS-Server fälschen, der andernfalls nicht erreichbar wäre, und den Quellport zu einem DNS-Dienstport (Port 53) fälschen. Wenn ein solches Paket an den UDP Echo-Port des Routers gesendet würde, würde der Router ein DNS-Paket an den betreffenden Server senden. Es würden keine Prüfungen für ausgehende Zugriffslisten für dieses Paket durchgeführt, da davon ausgegangen würde, dass das Paket lokal vom Router selbst generiert wurde.

Auch wenn die meisten Missbrauchsfälle der Small Servers-Dienste durch Anti-Spoofing-Zugriffslisten vermieden oder entschärft werden können, sollten die Dienste in jedem Router, der Teil der Firewall ist oder sich in einem sicherheitsrelevanten Teil des Netzwerks befindet, möglichst immer deaktiviert sein. Da die Dienste selten verwendet werden, ist es meist die beste Vorgehensweise, diese Dienste auf allen Routern jeglicher Art zu deaktivieren.

Folgende Konfiguration wird an den Router gesendet, um den UDP Small Servers-Dienst zu deaktivieren:

```
no service udp-small-servers
```

Deaktivieren des IP BOOTP Server-Dienstes

Die Sicherheitsprüfung deaktiviert den Bootstrap Protocol (BOOTP)-Dienst, wann immer möglich. Mit BOOTP können sowohl Router als auch Computer erforderliche Internet-Informationen beim Starten automatisch über einen zentral verwalteten Server konfigurieren. Dies umfasst auch das Herunterladen der Cisco IOS-Software. Dies kann dazu führen, dass BOOTP potenziell von einem Hacker zum Herunterladen einer Kopie der Cisco IOS-Software des Routers verwendet wird.

Darüber hinaus ist der BOOTP-Dienst anfällig für DoS-Angriffe; aus diesem Grund sollte er auch deshalb deaktiviert oder über eine Firewall gefiltert werden.

Folgende Konfiguration wird an den Router gesendet, um BOOTP zu deaktivieren:

```
no ip bootp server
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren des IP-Identifizierungsdienstes

Die Sicherheitsprüfung deaktiviert die Identifizierungsunterstützung, wann immer möglich. Mit der Identifizierungsunterstützung können Sie einen TCP-Port zur Identifikation abfragen. Mit dieser Funktion kann ein nichtsicheres Protokoll die Identität eines Clients, der eine TCP-Verbindung startet, und eines Hosts melden, der auf die Verbindung antwortet. Mit der Identifikationsunterstützung können Sie einen TCP-Port auf einem Host verbinden, eine einfache Textzeichenfolge zum Anfordern von Informationen ausgeben und eine Antwort in Form einer einfachen Textzeichenfolge empfangen.

Es ist gefährlich, wenn ein System auf einem direkt verbundenen Segment ermitteln kann, dass es sich bei dem Router um ein Cisco-Gerät handelt, welche Modellnummer dieses Gerät hat und welche Cisco IOS-Softwareversion ausgeführt wird. Diese Informationen können zum Durchführen von Angriffen auf den Router verwendet werden.

Folgende Konfiguration wird an den Router gesendet, um den IP-Identifizierungsdienst zu deaktivieren:

```
no ip identd
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von CDP

Die Sicherheitsprüfung deaktiviert das Cisco Discovery Protocol (CDP), wann immer möglich. CDP ist ein systemeigenes Protokoll, das Cisco-Router zum gegenseitigen Identifizieren auf einem LAN-Segment verwenden. Es ist deswegen gefährlich, weil dieses Protokoll es einem System auf einem direkt verbundenen Segment ermöglicht zu ermitteln, dass es sich bei dem Router um ein Cisco-Gerät handelt, welche Modellnummer dieses Gerät hat und welche Cisco IOS-Softwareversion ausgeführt wird. Diese Informationen können zum Durchführen von Angriffen auf den Router verwendet werden.

Folgende Konfiguration wird an den Router gesendet, um CDP zu deaktivieren:

```
no cdp run
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von IP Source Routing

Die Sicherheitsprüfung deaktiviert IP Source Routing, wann immer möglich. Das IP-Protokoll unterstützt Source Routing-Optionen, mit denen der Absender eines IP-Datagramms die Route steuern kann, die das Datagramm zu seinem endgültigen Ziel nimmt, und meist auch die Route, die eine Antwort nimmt. Diese Optionen werden nur selten für legale Zwecke in Netzwerken eingesetzt. Einige ältere IP-Implementierungen können Source Routing-Pakete nicht ordnungsgemäß verarbeiten. Aus diesem Grund kann es passieren, dass Systeme, die diese Implementierungen ausführen, ausfallen, wenn sie Datagramme mit Source Routing-Optionen erhalten.

Wenn IP Source Routing deaktiviert ist, kann ein Cisco-Router ein IP-Paket, das eine Source Routing-Option transportiert, niemals weiterleiten.

Folgende Konfiguration wird an den Router gesendet, um IP Source Routing zu deaktivieren:

```
no ip source-route
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Aktivieren des Dienstes für Kennwortverschlüsselung

Die Sicherheitsprüfung aktiviert die Kennwortverschlüsselung möglichst immer. Bei der Kennwortverschlüsselung wird die Cisco IOS-Software umgeleitet, um die Kennwörter, geheime Informationen des Challenge Handshake Authentication Protocol (CHAP) und ähnliche Daten, die in der Konfigurationsdatei gespeichert sind, zu verschlüsseln. Dieser Vorgang ist nützlich, um zu verhindern, dass zufällige Beobachter Kennwörter lesen können, wenn sie beispielsweise über die Schulter des Administrators auf den Bildschirm sehen.

Folgende Konfiguration wird an den Router gesendet, um die Kennwortverschüsselung zu aktivieren:

```
Kennwortverschlüsselungsdienst
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Aktivieren von TCP Keepalives für eingehende Telnet-Sitzungen

Das Sicherheitsaudit aktiviert TCP Keepalive-Meldungen möglichst immer sowohl für eingehende als auch für ausgehende Telnet-Sitzungen. Wenn TCP Keepalive-Meldungen aktiviert sind, generiert der Router regelmäßige Keepalive-Meldungen, damit er beschädigte Telnet-Verbindungen erkennen und entfernen kann.

Folgende Konfiguration wird an den Router gesendet, um die TCP-Keepalives für eingehende Telnet-Sitzungen zu aktivieren:

```
service tcp-keepalives-in
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Aktivieren von TCP Keepalives für ausgehende Telnet-Sitzungen

Die Sicherheitsprüfung aktiviert TCP Keepalive-Meldungen möglichst immer sowohl für eingehende als auch für ausgehende Telnet-Sitzungen. Wenn TCP Keepalive-Meldungen aktiviert sind, generiert der Router regelmäßige Keepalive-Meldungen, damit er beschädigte Telnet-Verbindungen erkennen und entfernen kann.

Folgende Konfiguration wird an den Router gesendet, um die TCP-Keepalives für ausgehende Telnet-Sitzungen zu aktivieren:

```
service tcp-keepalives-out
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Aktivieren von Sequenznummern und Zeitstempeln für Debugging-Meldungen

Das Sicherheitsaudit aktiviert bei allen Debugging- und Protokollmeldungen möglichst immer Sequenznummern und Zeitstempel. Zeitstempel auf Debugging- und Protokollmeldungen geben die Uhrzeit und das Datum der Meldungserstellung an. Sequenznummern geben die Reihenfolge an, in der Meldungen mit identischen Zeitstempeln generiert wurden. Die Kenntnis des Zeitpunkts und der Reihenfolge der Meldungsgenerierung ist wichtig bei der Diagnose potenzieller Angriffe.

Folgende Konfiguration wird an den Router gesendet, um Zeitstempel und Sequenznummern zu aktivieren:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

Aktivieren von IP CEF

Das Sicherheitsaudit aktiviert möglichst immer CEF (Cisco Express Forwarding) oder DCEF (Distributed Cisco Express Forwarding). Da es nicht erforderlich ist, Cache-Einträge zu erstellen, wenn Datenverkehr an neuen Zielen eintrifft, verhält sich CEF bei großen Datenverkehrsmengen, die an viele Ziele adressiert sind, vorhersehbarer als andere Modi. Für CEF konfigurierte Routen zeigen bei SYN-Angriffen eine bessere Leistung als Router, die den traditionellen Cache verwenden.

Folgende Konfiguration wird an den Router gesendet, um CEF zu aktivieren:

```
ip cef
```

Deaktivieren von Gratuitous ARP-Anfragen

Die Sicherheitsprüfung deaktiviert möglichst immer Anfragen des ARP (IP Gratuitous Address Resolution Protocol). Ein Gratuitous ARP ist ein ARP-Broadcast, bei dem die Quell- und Ziel-MAC-Adressen identisch sind. Es wird hauptsächlich von einem Host verwendet, um das Netzwerk über seine IP-Adresse zu informieren. Eine Spoofed Gratuitous ARP-Meldung kann zur Folge haben, dass Netzwerkzuordnungsinformationen fehlerhaft gespeichert werden und zu einer Fehlfunktion des Netzwerks führen.

Folgende Konfiguration wird an den Router gesendet, um Gratuitous ARPs zu deaktivieren:

```
no ip gratuitous-arps
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Einstellen der Mindestlänge für Kennwörter auf weniger als 6 Zeichen

Die Sicherheitsprüfung konfiguriert Ihren Router möglichst immer für die Abfrage einer Kennwortlänge von mindestens sechs Zeichen. Eine Methode, die Hacker verwenden, um Kennwörter herauszufinden, ist das Ausprobieren aller möglichen Kombinationen von Zeichen, bis das Kennwort ermittelt wird. Längere Kennwörter haben exponenziell mehr mögliche Kombinationen von Zeichen, sodass diese Angriffsmethode erheblich schwerer wird.

Bei dieser Konfigurationsänderung müssen alle Kennwörter auf dem Router, einschließlich des Benutzerkennworts, des Aktivierungskennworts, des geheimen Kennworts, des Konsolenkennworts und der AUX-, tty- und vty-Kennwörter mindestens sechs Zeichen lang sein. Diese Konfigurationsänderung wird nur durchgeführt, wenn die Cisco IOS-Version, die auf Ihrem Router ausgeführt wird, die Funktion für die Mindestlänge von Kennwörtern unterstützt.

Folgende Konfiguration wird an den Router gesendet:

```
security passwords min-length <6>
```

Einstellen der Authentifizierungsfehlerrate auf weniger als 3 Wiederholungen

Das Sicherheitsaudit konfiguriert Ihren Router möglichst immer so, dass der Zugriff nach drei erfolglosen Anmeldeversuchen blockiert wird. Eine Methode, Kennwörter herauszufinden, ist der „Wörterbuchangriff“, bei dem Software verwendet wird, die versucht, sich mit jedem Wort aus einem Wörterbuch anzumelden. Mit dieser Konfiguration wird der Zugriff auf den Router nach drei erfolglosen Anmeldeversuchen für eine Zeitspanne von 15 Sekunden gesperrt und Wörterbuchangriffe somit deaktiviert. Diese Konfiguration blockiert nicht nur den Zugriff auf den Router, sondern generiert zusätzlich nach drei erfolglosen Anmeldeversuchen eine Protokollmeldung, die dem Administrator die erfolglosen Anmeldeversuche meldet.

Folgende Konfiguration wird an den Router gesendet, um den Routerzugriff nach drei erfolglosen Anmeldeversuchen zu blockieren:

```
security authentication failure rate <3>
```

Einstellen der TCP Synwait-Zeit

Das Sicherheitsaudit stellt die TCP synwait-Zeit möglichst immer auf 10 Sekunden ein. Die TCP synwait-Zeit ist ein Wert, der zur Abwehr von SYN Flooding Attacks, einer Form des Denial-of-Service (DoS)-Angriffs, nützlich ist. Eine TCP-Verbindung erfordert einen Dreiphasen-Handshake, um die Verbindung erstmalig herzustellen. Der Absender sendet eine Verbindungsanfrage, der Empfänger sendet eine Bestätigung und der Absender sendet dann eine Empfangsbestätigung dieser Bestätigung. Wenn dieser Dreiphasen-Handshake abgeschlossen ist, ist die Verbindung hergestellt und die Datenübertragung kann beginnen. Eine SYN Flooding Attack sendet wiederholte Verbindungsanfragen an einen Host, sendet jedoch keine Empfangsbestätigung der Bestätigungen, mit der die Verbindungen vervollständigt werden. Auf diese Weise werden immer mehr unvollständige Verbindungen auf der Hostseite aufgebaut. Da der Puffer für unvollständige Verbindungen im Allgemeinen kleiner ist als der Puffer für vollständige Verbindungen, kann der Host durch diesen Vorgang überlastet und deaktiviert werden. Wenn Sie die TCP synwait-Zeit auf 10 Sekunden einstellen, kann der Router eine unvollständige Verbindung nach 10 Sekunden trennen und somit die Ansammlung unvollständiger Verbindungen beim Host vermeiden.

Folgende Konfiguration wird an den Router gesendet, um die TCP synwait-Zeit auf 10 Sekunden einzustellen:

```
ip tcp synwait-time <10>
```

Festlegen eines Banners

Die Sicherheitsprüfung konfiguriert möglichst immer ein Textbanner. In einigen Gerichtsbarkeiten wird die zivile und/oder kriminalrechtliche Verfolgung von Hackern, die in Ihr System einbrechen, vereinfacht, wenn Sie ein Banner präsentieren, das unberechtigte Benutzer darüber informiert, dass ihr Zugriff in der Tat nicht zulässig ist. In anderen Gerichtsbarkeiten ist es möglicherweise untersagt, die Aktivitäten sogar unberechtigter Benutzer zu überwachen, wenn Sie keine Schritte unternommen haben, diesen Benutzern Ihre Absicht der Überwachung mitzuteilen. Das Textbanner ist eine Methode einer solchen Benachrichtigung.

Folgende Konfiguration wird an den Router gesendet, um ein Textbanner zu erstellen, dabei wird <*Firmenname*>, <*E-Mail-Adresse des Administrators*> und <*Telefonnummer des Administrators*> durch die entsprechenden Werte ersetzt, die Sie in die Sicherheitsprüfung eingegeben haben:

```
banner ~
Authorized access only
This system is the property of <Firmenname> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <E-Mail-Adresse des Administrators> <Telefonnummer des
Administrators>.
~
```

Logging aktivieren

Die Sicherheitsprüfung aktiviert möglichst immer das Logging mit Zeitstempeln und Sequenznummern. Das Logging ist bei der Ermittlung und Reaktion auf Ereignisse bezüglich der Sicherheit sehr wichtig, da es ausführliche Informationen zu Ereignissen im Netzwerk liefert. Zeitstempel und Sequenznummern bieten Informationen zu dem Datum, der Uhrzeit und der Reihenfolge von Netzwerkereignissen.

Folgende Konfiguration wird an den Router gesendet, um Logging zu aktivieren und zu konfigurieren; dabei wird <*Größe des Logging-Puffers*> und <*IP-Adresse des Logging-Servers*> durch die entsprechenden Werte ersetzt, die Sie in die Sicherheitsprüfung eingegeben haben:

```
logging console critical
logging trap debugging
logging buffered <Größe des Logging-Puffers>
logging <IP-Adresse des Logging-Servers>
```

Einstellen von „Geheimes Kennwort aktivieren“

Die Sicherheitsprüfung konfiguriert für einen besseren Kennwortschutz möglichst immer den Cisco IOS-Befehl **enable secret**. Mit dem Befehl **enable secret** können Sie das Kennwort einstellen, das den privilegierten Administratorzugriff auf das Cisco IOS-System gewährt. Der Befehl **enable secret** verwendet einen viel sichereren Verschlüsselungsalgorithmus (MD5) zum Schutz dieses Kennworts als der ältere Befehl **enable password**. Die stärkere Verschlüsselung ist eine sehr wichtige Methode, das Routerkennwort und somit den Netzwerkzugriff zu schützen.

Folgende Konfiguration wird an den Router gesendet, um den Befehl zu konfigurieren:

```
enable secret <>
```

Deaktivieren von SNMP

Die Sicherheitsprüfung deaktiviert möglichst immer das Simple Network Management Protocol (SNMP). SNMP ist ein Netzwerkprotokoll, das eine Möglichkeit zum Abrufen und Platzieren von Daten zu Netzwerkleistung und Vorgängen im Netzwerk bietet. Es wird häufig zur Routerüberwachung und auch oft für Änderungen an der Routerkonfiguration verwendet. Version 1 des SNMP-Protokolls, die am häufigsten verwendet wird, ist jedoch häufig aus folgenden Gründen ein Sicherheitsrisiko:

- Es verwendet Authentifizierungszeichenfolgen (Kennwörter), sogenannte *Community-Zeichenfolgen*, die gespeichert und als reiner Text im Netzwerk versendet werden.
- Die meisten SNMP-Implementierungen versenden diese Zeichenfolgen wiederholt als Teil der periodischen Abfrage.
- Es ist ein Datagramm-basiertes Transaktionsprotokoll, das leicht gefälscht werden kann.

Da SNMP zum Abrufen einer Kopie der Netzwerk-Routingtabelle und weiterer kritischer Netzwerkinformationen verwendet werden kann, empfiehlt Cisco, SNMP zu deaktivieren, wenn es in Ihrem Netzwerk nicht benötigt wird. Die Sicherheitsprüfung fordert zu Beginn dazu auf, SNMP zu deaktivieren.

Folgende Konfiguration wird an den Router gesendet, um SNMP zu deaktivieren:

```
no snmp-server
```

Einstellen des Scheduler-Intervalls

Die Sicherheitsprüfung konfiguriert möglichst immer das Scheduler-Intervall auf dem Router. Wenn ein Router schnell eine große Anzahl von Paketen wechselt, ist es möglich, dass er so viel Zeit für die Antwort auf Interrupts von den Netzwerkschnittstellen benötigt, dass keine anderen Aufgaben erledigt werden können. Dieser Zustand kann durch einige sehr schnelle Paketströme verursacht werden. Dieser Zustand kann den Verwaltungszugriff auf den Router unterbrechen. Dies kann sehr gefährlich sein, wenn das Gerät angegriffen wird. Das Einstellen des Scheduler-Intervalls stellt sicher, dass der Verwaltungszugriff auf den Router immer möglich ist, da der Router nach dem angegebenen Zeitintervall Systemvorgänge durchführt, auch wenn die CPU-Auslastung bei 100 % liegt.

Folgende Konfiguration wird an den Router gesendet, um das Scheduler-Intervall einzustellen:

```
scheduler interval 500
```

Einstellen von Scheduler Allocate

Auf Routern, die den Befehl **scheduler interval** nicht unterstützen, konfiguriert die Sicherheitsprüfung möglichst immer den Befehl **scheduler allocate**. Wenn ein Router schnell eine große Anzahl von Paketen wechselt, ist es möglich, dass er so viel Zeit für die Antwort auf Interrupts von den Netzwerkschnittstellen benötigt, dass keine anderen Aufgaben erledigt werden können. Dieser Zustand kann durch einige sehr schnelle Paketströme verursacht werden. Dieser Zustand kann den Verwaltungszugriff auf den Router unterbrechen. Dies kann sehr gefährlich sein, wenn das Gerät angegriffen wird. Der Befehl **scheduler allocate** reserviert einen bestimmten Prozentsatz der CPU-Prozesse für andere Aktivitäten als Netzwerk-Switching, beispielsweise Verwaltungsvorgänge.

Folgende Konfiguration wird an den Router gesendet, um den Prozentanteil für Scheduler Allocate einzustellen:

```
scheduler allocate 4000 1000
```

Einstellen von Benutzern

Die Sicherheitsprüfung sichert die Konsolen-, AUX-, VTY- und tty-Leitungen durch Konfigurieren von Telnet-Benutzerkonten, um den Zugriff auf diese Leitungen möglichst immer zu authentifizieren. Security Audit zeigt ein Dialogfeld an, in dem Sie Benutzerkonten und Passwörter für diese Anschlüsse definieren können.

Aktivieren von Telnet-Einstellungen

Das Sicherheitsaudit sichert die Konsolen-, AUX-, VTY- und tty-Leitungen durch Implementieren der folgenden Konfigurationen, wann immer es möglich ist:

- Konfiguriert die Befehle **transport input** und **transport output**, um festzulegen, welche Protokolle zum Verbinden mit diesen Leitungen verwendet werden können.
- Stellt den Wert für exec-timeout auf der Konsolen- und AUX-Leitung auf 10 Minuten ein, was dazu führt, dass ein Administrator-Benutzer nach 10 Minuten ohne Aktivität bei diesen Leitungen abgemeldet wird.

Folgende Konfiguration wird an den Router gesendet, um die Konsolen-, AUX-, vty- und tty-Leitungen zu sichern:

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Aktivieren von NetFlow Switching

Die Sicherheitsprüfung aktiviert das NetFlow Switching möglichst immer. NetFlow Switching ist eine Cisco IOS-Funktion, mit der die Routing-Leistung bei der Verwendung von Zugriffssteuerungslisten (ACLs) und anderen Funktionen, die Netzwerksicherheit herstellen und erhöhen, verbessert wird. NetFlow identifiziert Ströme von Netzwerkpaketen auf der Grundlage der IP-Adressen von Quelle und Ziel sowie TCP-Portnummern. NetFlow kann dann einfach das ursprüngliche Paket eines Stroms zum Vergleich mit ACLs und für andere Sicherheitsprüfungen verwenden, anstatt jedes Paket im Netzwerkstrom verwenden zu müssen. Auf diese Weise wird die Leistung verbessert, und Sie können alle Sicherheitsfunktionen des Routers verwenden.

Folgende Konfiguration wird an den Router gesendet, um NetFlow zu aktivieren:

```
ip route-cache flow
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

IP Redirects deaktivieren

Die Sicherheitsprüfung deaktiviert möglichst immer die Weiterleitungsmeldungen des Internet Message Control Protocol (ICMP). ICMP unterstützt IP-Datenverkehr durch Weiterleiten von Informationen zu Pfaden, Routen und Netzwerkbedingungen. ICMP-Weiterleitungsmeldungen weisen einen Endknoten an, einen speziellen Router als Pfad zu einem bestimmten Ziel zu verwenden. In einem ordnungsgemäß funktionierenden IP-Netzwerk sendet ein Router Weiterleitungen nur an Hosts innerhalb seiner eigenen lokalen Subnetze, kein Endknoten sendet jemals eine Weiterleitung und keine Weiterleitung wird jemals um mehr als einen Netzwerk-Hop geleitet. Ein Hacker könnte diese Regeln jedoch verletzen; einige Angriffe basieren auf diesem Prinzip. Das Deaktivieren von ICMP-Weiterleitungen hat keine Auswirkungen auf den Netzwerkbetrieb und verhindert diese mögliche Angriffsmethode.

Folgende Konfiguration wird an den Router gesendet, um ICMP-Weiterleitungsmeldungen zu deaktivieren:

```
no ip redirects
```

Deaktivieren von IP Proxy Arp

Die Sicherheitsprüfung deaktiviert möglichst immer das Proxy Address Resolution Protocol (ARP). ARP wird vom Netzwerk verwendet, um IP-Adressen in MAC-Adressen zu konvertieren. Normalerweise ist ARP auf ein einzelnes LAN beschränkt, ein Router kann jedoch als Proxy für ARP-Anfragen dienen, sodass ARP-Anfragen über mehrere LAN-Segmente hinweg verfügbar sind. Da Proxy ARP die LAN-Sicherheitsbarriere durchbricht, sollte es nur zwischen zwei LANs mit gleicher Sicherheitsstufe und nur wenn nötig verwendet werden.

Folgende Konfiguration wird an den Router gesendet, um Proxy ARP zu deaktivieren:

```
no ip proxy-arp
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von IP Directed Broadcast

Die Sicherheitsprüfung deaktiviert IP Directed Broadcasts möglichst immer. Ein IP Directed Broadcast ist ein Datagramm, das an die Broadcast-Adresse eines Subnetzes gesendet wird, an welches das Absendergerät nicht direkt angeschlossen ist. Das Directed Broadcast wird als Unicast-Paket durch das Netzwerk geleitet, bis es am Ziel-Subnetz eintrifft. Dort wird es in ein Link-Layer Broadcast konvertiert. Aufgrund der Eigenschaften der IP-Adressierungsarchitektur kann nur der letzte Router in der Kette, derjenige, der direkt an das Ziel-Subnetz angeschlossen ist, ein Directed Broadcast endgültig identifizieren. Directed Broadcasts werden ab und zu für legale Zwecke verwendet; diese Verwendung ist außerhalb der Finanzdienstleistungsbranche jedoch nicht üblich.

IP Directed Broadcasts werden im extrem häufigen und beliebten Denial-of-Service-Angriff „Smurf“ verwendet und können auch für ähnliche Angriffe eingesetzt werden. Bei einem Smurf-Angriff sendet der Hacker eine ICMP-Echoanforderung von einer gefälschten Quelladresse an eine Directed Broadcast-Adresse. Daraufhin senden alle Hosts im Ziel-Subnetz Antworten an die gefälschte Quelle. Durch das Senden eines fortlaufenden Stroms solcher Anforderungen ist der Hacker in der Lage, einen viel größeren Antwortstrom zu erzeugen, der den Host, dessen Adresse gefälscht wird, vollständig überschwemmen kann.

Wenn IP Directed Broadcasts deaktiviert werden, werden Directed Broadcasts, die anderenfalls an dieser Schnittstelle explosionsartig in Link-Layer Broadcasts konvertiert würden, stattdessen entfernt.

Folgende Konfiguration wird an den Router gesendet, um den IP Directed Braodcasts zu deaktivieren:

```
no ip directed-broadcast
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren des MOP-Dienstes

Die Sicherheitsprüfung deaktiviert das Maintenance Operations Protocol (MOP) möglichst immer auf allen Ethernet-Schnittstellen. MOP liefert dem Router Konfigurationsinformationen bei der Kommunikation mit DECNet-Netzwerken. MOP ist anfällig für verschiedene Angriffe.

Folgende Konfiguration wird an den Router gesendet, um den MOP-Dienst auf Ethernet-Schnittstellen zu deaktivieren:

```
no mop enabled
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von IP Unreachables

Die Sicherheitsprüfung deaktiviert möglichst immer „Host unerreichbar“-Meldungen des Internet Message Control Protocol (ICMP). ICMP unterstützt IP-Datenverkehr durch Weiterleiten von Informationen zu Pfaden, Routen und Netzwerkbedingungen. „Host unerreichbar“-Meldungen von ICMP werden gesendet, wenn ein Router ein Nonbroadcast-Paket erhält, das ein unbekanntes Protokoll verwendet, oder wenn der Router ein Paket empfängt, das er nicht an das Endziel ausliefern kann, da ihm keine Route zur Zieladresse bekannt ist. Diese Meldungen können von einem Hacker verwendet werden, um in den Besitz von Netzwerkzuordnungsinformationen zu gelangen.

Folgende Konfiguration wird an den Router gesendet, um ICMP „Host unerreichbar“-Meldungen zu deaktivieren:

```
int <all-interfaces>
no ip unreachables
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von IP Mask Reply

Die Sicherheitsprüfung deaktiviert möglichst immer die Maskenanforderungsmeldungen des Internet Message Control Protocol (ICMP). ICMP unterstützt IP-Datenverkehr durch Weiterleiten von Informationen zu Pfaden, Routen und Netzwerkbedingungen.
ICMP-Maskenanforderungsmeldungen werden gesendet, wenn ein Netzwerkgerät die Subnetzmaske für ein bestimmtes Subnetzwerk im Verbundnetzwerk kennen muss. ICMP-Maskenanforderungsmeldungen werden von den Geräten, die über die gewünschten Informationen verfügen, an das Gerät gesendet, das die Informationen anfordert. Diese Meldungen können von einem Hacker verwendet werden, um in den Besitz von Netzwerkzuordnungsinformationen zu gelangen.

Folgende Konfiguration wird an den Router gesendet, um ICMP-Maskenanforderungsmeldungen zu deaktivieren:

```
no ip mask-reply
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Deaktivieren von IP Unreachables für NULL-Schnittstelle

Die Sicherheitsprüfung deaktiviert möglichst immer „Host unerreichbar“-Meldungen des Internet Message Control Protocol (ICMP). ICMP unterstützt IP-Datenverkehr durch Weiterleiten von Informationen zu Pfaden, Routen und Netzwerkbedingungen. „Host unerreichbar“-Meldungen von ICMP werden gesendet, wenn ein Router ein Nonbroadcast-Paket erhält, das ein unbekanntes Protokoll verwendet, oder wenn der Router ein Paket empfängt, das er nicht an das Endziel ausliefern kann, da ihm keine Route zur Zieladresse bekannt ist. Da die NULL-Schnittstelle eine Paketsenke ist, werden Pakete, die dorthin weitergeleitet werden, immer verworfen und generieren „Host unerreichbar“-Meldungen, wenn sie nicht deaktiviert werden. Wenn die Null-Schnittstelle zum Blockieren eines Denial-of-Service-Angriffs verwendet wird, überfluten die Meldungen in diesem Fall das lokale Netzwerk. Durch das Deaktivieren dieser Meldungen wird eine solche Situation vermieden. Da alle blockierten Pakete an die NULL-Schnittstelle weitergeleitet werden, könnte ein Hacker, der „Host unerreichbar“-Meldungen erhält, die Meldungen in diesem Fall verwenden, um die Konfiguration von Zugriffssteuerungslisten (ACL) zu ermitteln.

Wenn die „NULL 0“-Schnittstelle auf Ihrem Router konfiguriert ist, sendet die Sicherheitsprüfung die folgende Konfiguration an den Router, um ICMP „Host unerreichbar“-Meldungen für verworfene Pakete oder Pakete, die an die NULL-Schnittstelle geleitet wurden, zu deaktivieren:

```
int null 0
no ip unreachables
```

Dieser Vorgang kann rückgängig gemacht werden. Klicken Sie auf Rückgängig machen von Problembehebungen in der Sicherheitsprüfung, um zu erfahren, wie.

Aktivieren von Unicast RPF für alle äußeren Schnittstellen

Die Sicherheitsprüfung aktiviert Unicast Reverse Path Forwarding (RPF) möglichst immer auf allen Schnittstellen, die mit dem Internet verbunden sind. RPF ist eine Funktion, mit der der Router die Quelladresse eines beliebigen Pakets auf die Schnittstelle überprüft, über die das Paket auf den Router gelangt ist. Wenn die Eingangsschnittstelle laut Routingtabelle kein möglicher Pfad zur Quelladresse ist, wird das Paket entfernt. Diese Überprüfung der Quelladresse wird verwendet, um IP-spoofening zu verhindern.

Dieser Vorgang funktioniert nur, wenn das Routing symmetrisch ist. Wenn das Netzwerk so aufgebaut ist, dass Datenverkehr von Host A zu Host B normalerweise einen anderen Pfad nehmen würde, als Datenverkehr von Host B zu Host A, schlägt die Prüfung immer fehl, und es ist keine Kommunikation zwischen den beiden Hosts möglich. Diese Art von asymmetrischem Routing kommt häufig im Kern des Internet vor. Stellen Sie vor dem Aktivieren dieser Funktion sicher, dass in Ihrem Netzwerk kein asymmetrisches Routing verwendet wird.

Zusätzlich kann Unicast RPF nur aktiviert werden, wenn IP Cisco Express Forwarding (CEF) aktiviert ist. Die Sicherheitsprüfung prüft die Routerkonfiguration, um festzustellen, ob IP CEF aktiviert ist. Wenn IP CEF nicht aktiviert ist, empfiehlt die Sicherheitsprüfung, dass IP CEF aktiviert wird, und aktiviert es, wenn diese Empfehlung bestätigt wird. Wenn IP CEF weder von der Sicherheitsprüfung noch auf andere Weise aktiviert ist, kann Unicast RPF nicht aktiviert werden.

Die folgenden Konfiguration wird für jede Schnittstelle, die eine Verbindung nach außerhalb des privaten Netzwerks hat, an den Router gesendet, um Unicast RPF zu aktivieren. Dabei wird <*äußere Schnittstelle*> durch die Kennung der Schnittstelle ersetzt:

```
Schnittstelle <äußere Schnittstelle>
ip verify unicast reverse-path
```

Aktivieren der Firewall für alle äußeren Schnittstellen

Wenn das Cisco IOS-Abbild, das auf dem Router ausgeführt wird, den Firewall-Funktionssatz enthält, aktiviert die Sicherheitsprüfung möglichst immer Context-Based Access Control (CBAC) auf dem Router. CBAC ist eine Komponente des Cisco IOS Firewall-Funktionssatzes und filtert Pakete auf der Grundlage von Application-Layer-Informationen, beispielsweise danach, welche Arten von Befehlen innerhalb der Sitzung ausgeführt werden. Wenn beispielsweise ein nicht unterstützter Befehl in einer Sitzung entdeckt wird, kann dem Paket der Zugriff verweigert werden.

CBAC erhöht die Sicherheit für TCP- und User Datagram Protocol (UDP)-Anwendungen, die gut bekannte Ports verwenden, zum Beispiel Port 80 für HTTP oder Port 443 für Secure Sockets Layer (SSL). Dies geschieht durch Überwachen der Quell- und Zieladressen. Ohne CBAC ist erweiterter Anwendungsdatenverkehr nur durch Schreiben von Zugriffssteuerungslisten (ACLs) zulässig. Dieser Ansatz macht die Firewall durchlässig. Aus diesem Grund weisen die meisten Administratoren diese Art von Anwendungsdatenverkehr möglichst ab. Wenn CBAC aktiviert ist, können Sie Mulitmedia- und anderen Anwendungsdatenverkehr jedoch problemlos zulassen, indem Sie die Firewall bei Bedarf öffnen und ansonsten geschlossen halten.

Bei Aktivierung von CBAC verwendet das Sicherheitsaudit die Cisco SDM-Bildschirme **Firewall erstellen**, um eine Firewallkonfiguration zu erzeugen.

Festlegen der Zugriffsklasse für den HTTP-Server-Dienst

Die Sicherheitsprüfung aktiviert möglichst immer den HTTP-Dienst auf dem Router mit einer Zugriffsklasse. Der HTTP-Dienst erlaubt die Remote-Konfiguration und die Überwachung über einen Webbrowser, ist jedoch nicht allzu sicher, da während des Authentifizierungsvorgangs unverschlüsselte Kennwörter über das Netzwerk gesendet werden. Aus diesem Grund beschränkt die Sicherheitsprüfung den Zugriff auf den HTTP-Dienst durch Konfigurieren einer Zugriffsklasse, die den Zugriff nur über direkt verbundene Netzwerkknoten zulässt.

Folgende Konfiguration wird an den Router gesendet, um den HTTP-Dienst mit einer Zugriffsklasse zu aktivieren:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Festlegen der Zugriffsklasse für VTY-Leitungen

Das Sicherheitsaudit konfiguriert möglichst immer eine Zugriffsklasse für VTY-Leitungen. Da vty-Verbindungen den Remote-Zugriff auf Ihren Router zulassen, sollten sie nur auf bekannte Netzwerkknoten beschränkt sein.

Folgende Konfiguration wird an den Router gesendet, um eine Zugriffsklasse für vty-Leitungen zu konfigurieren:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Darüber hinaus wird die folgende Konfiguration auf jede vty-Leitung angewendet:

```
access-class <std-acl-num>
```

Aktivieren von SSH für Zugriff auf den Router

Wenn es sich bei dem Cisco IOS-Abbild, das auf dem Router ausgeführt wird, um ein Crypto-Abbild handelt (ein Abbild, das die 56-Bit Data Encryption Standard (DES)-Verschlüsselung verwendet und Exportbeschränkungen unterliegt), dann implementiert die Sicherheitsprüfung möglichst immer die folgenden Konfigurationen, um den Telnet-Zugriff zu sichern:

- Aktivieren der Secure Shell (SSH) für den Telnet-Zugriff. SSH macht den Telnet-Zugriff sehr viel sicherer.
- Einstellen des SSH-Timeout-Werts auf 60 Sekunden, sodass unvollständige SSH-Verbindungen nach 60 Sekunden heruntergefahren werden.
- Einstellen der maximalen Anzahl erfolgloser SSH-Anmeldeversuche auf zwei, bevor der Zugriff auf den Router gesperrt wird.

Folgende Konfiguration wird an den Router gesendet, um die Zugriffs- und Dateiübertragungsfunktionen zu sichern:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Hinweis Wenn Sie die oben angegebenen Konfigurationsänderungen vorgenommen haben, müssen Sie die Größe des SSH-Schlüsselmoduls festlegen und einen Schlüssel generieren. Verwenden Sie dazu die Seite SSH.

AAA aktivieren

Cisco IOS-Authentifizierung, Autorisation und Accounting (AAA) ist ein architektonisches Rahmenwerk zur Konfiguration von drei voneinander unabhängigen Sicherheitsfunktionen. Dies geschieht auf eine konsistente Art und Weise. AAA bietet eine modulare Möglichkeit zur Anwendung von Authentifizierung, Autorisierung und Accounting-Diensten.

Cisco SDM führt die folgenden Vorsichtsmaßnahmen während der Aktivierung von AAA aus, damit der Zugriff auf den Router nicht verloren geht.

- Authentifizierung und Autorisierung für VTY Anschlüsse konfigurieren

  …Die lokale Datenbank wird sowohl für die Authentifizierung als auch für die Autorisierung benutzt.

- Authentifizierung für Konsolenanschlüsse konfigurieren

  …Die lokale Datenbank wird für die Authentifizierung benutzt.

- http-Authentifizierung für die Benutzung der lokalen Datenbank anpassen

Konfigurationsübersichtsbildschirm

Auf diesem Bildschirm wird, ausgehend von den Sicherheitsproblemen, die Sie zur Behebung auf dem Bildschirm **Berichtskarte** ausgewählt haben, eine Liste aller Konfigurationsänderungen angezeigt, die an die Routerkonfiguration gesendet werden.

Cisco SDM und Cisco IOS AutoSecure

AutoSecure ist eine Funktion von Cisco IOS, mit der Sie, wie bei Cisco SDM, Sicherheitsfunktionen einfacher auf Ihrem Router konfigurieren können, sodass Ihr Netzwerk besser geschützt ist. Cisco SDM implementiert fast alle Konfigurationen, die AutoSecure anbietet.

In Cisco SDM implementierte AutoSecure-Funktionen

Die folgenden AutoSecure-Funktionen werden in diese Version von Cisco SDM implementiert. Eine Erläuterung dieser Dienste und Funktionen finden Sie unter den nachfolgenden Links:

- Deaktivieren von SNMP
- Deaktivieren des Finger-Dienstes
- Deaktivieren des PAD-Dienstes
- Deaktivieren des TCP Small Servers-Dienstes
- Deaktivieren des IP BOOTP Server-Dienstes
- Deaktivieren des IP-Identifizierungsdienstes
- Deaktivieren von CDP
- Deaktivieren von IP Source Routing
- IP Redirects deaktivieren
- Deaktivieren von IP Proxy Arp
- Deaktivieren von IP Directed Broadcast
- Deaktivieren des MOP-Dienstes
- Deaktivieren von IP Unreachables
- Deaktivieren von IP Unreachables für NULL-Schnittstelle
- Deaktivieren von IP Mask Reply
- Aktivieren des Dienstes für Kennwortverschlüsselung
- Deaktivieren von IP Unreachables für NULL-Schnittstelle
- Deaktivieren von IP Unreachables für NULL-Schnittstelle
- Einstellen der Mindestlänge für Kennwörter auf weniger als 6 Zeichen
- Aktivieren von IP CEF

- Aktivieren der Firewall für alle äußeren Schnittstellen
- Einstellen von Benutzern
- Logging aktivieren
- Aktivieren der Firewall für alle äußeren Schnittstellen
- Einstellen der Mindestlänge für Kennwörter auf weniger als 6 Zeichen
- Aktivieren der Firewall für alle äußeren Schnittstellen
- Einstellen von Benutzern
- Einstellen von Benutzern
- Einstellen von Benutzern
- Aktivieren von Unicast RPF für alle äußeren Schnittstellen
- Aktivieren der Firewall für alle äußeren Schnittstellen

Nicht in Cisco SDM implementierte AutoSecure-Funktionen

Die folgenden AutoSecure-Funktionen sind nicht in dieser Version von Cisco SDM implementiert:

- Deaktivieren von NTP – Basierend auf der Eingabe deaktiviert AutoSecure das Network Time Protocol (NTP), falls es nicht benötigt wird. Andernfalls wird NTP mit der MD5-Authentifizierung konfiguriert. Bei Cisco SDM wird das Deaktivieren von NTP nicht unterstützt.
- Konfigurieren von AAA – Wenn der AAA-Dienst (Authentication, Authorization, and Accounting = Authentifizierung, Autorisierung und Kontozuordnung) nicht konfiguriert ist, richtet AutoSecure AAA-Dienste lokal ein und fordert zur Konfiguration einer lokalen Datenbank für Benutzernamen und Kennwörter auf dem Router auf. Cisco SDM unterstützt keine AAA-Konfiguration.
- Festlegen von SPD-Werten – Cisco SDM legt keine Selective Packet Discard-(SPD-)Werte fest.
- Aktivieren von TCP Intercepts – Cisco SDM aktiviert keine TCP Intercepts.
- Konfigurieren von Anti-Spoofing ACLs auf äußeren Schnittstellen – AutoSecure erstellt drei benannte Zugriffslisten zur Vermeidung von Anti-Spoofing-Quelladressen. Cisco SDM konfiguriert diese ACLs nicht.

Auf andere Weise in Cisco SDM implementierte AutoSecure-Funktionen

- Deaktivieren von SNMP – Cisco SDM deaktiviert SNMP, bietet jedoch anders als AutoSecure keine Option zum Konfigurieren von SNMP Version 3.
- Aktivieren von SSH für Zugriff auf den Router – Cisco SDM aktiviert und konfiguriert SSH auf Cisco IOS Crypto-Abbildern, aktiviert jedoch im Gegensatz zu AutoSecure keinen Service Control Point (SCP) und deaktiviert auch nicht den weiteren Zugriff und Dateiübertragungsdienste wie FTP.

Sicherheitskonfigurationen, die Cisco SDM rückgängig machen kann

In dieser Tabelle werden die Sicherheitskonfigurationen aufgeführt, die Cisco SDM rückgängig machen kann.

Sicherheitskonfiguration	Entsprechende CLI
Deaktivieren des Finger-Dienstes	No service finger
Deaktivieren des PAD-Dienstes	No service pad
Deaktivieren des TCP Small Servers-Dienstes	No service tcp-small-servers no service udp-small-servers
Deaktivieren des IP BOOTP Server-Dienstes	No ip bootp server
Deaktivieren des IP-Identifizierungsdienstes	No ip identd
Deaktivieren von CDP	No cdp run
Deaktivieren von IP Source Routing	No ip source-route
Aktivieren von NetFlow Switching	ip route-cache flow
IP Redirects deaktivieren	no ip redirects
Deaktivieren von IP Proxy Arp	no ip proxy-arp
Deaktivieren von IP Directed Broadcast	no ip directed-broadcast

Sicherheitskonfiguration	Entsprechende CLI
Deaktivieren des MOP-Dienstes	No mop enabled
Deaktivieren von IP Unreachables	int <all-interfaces> no ip unreachables
Deaktivieren von IP Mask Reply	no ip mask-reply
Deaktivieren von IP Unreachables für NULL-Schnittstelle	int null 0 no ip unreachables
Aktivieren des Dienstes für Kennwortverschlüsselung	Kennwortverschlüsselungsdienst
Aktivieren von TCP Keepalives für eingehende Telnet-Sitzungen	service tcp-keepalives-in
Aktivieren von TCP Keepalives für ausgehende Telnet-Sitzungen	service tcp-keepalives-out
Deaktivieren von Gratuitous ARP-Anfragen	no ip gratuitous-arps

Rückgängig machen von Problembehebungen in der Sicherheitsprüfung

Cisco SDM kann diese Problembehebung rückgängig machen. Wenn Sie möchten, dass Cisco SDM diese Sicherheitskonfiguration entfernt, führen Sie den Sicherheitsprüfungs-Assistenten aus. Wählen Sie im Fenster **Berichtskarte** die Option **Sicherheitskonfigurationen rückgängig machen** aus, setzen Sie neben diese Konfiguration und neben andere Konfigurationen, die Sie rückgängig machen möchten, ein Fragezeichen, und klicken Sie auf **Weiter >**.

Bildschirm Telnet-/SSH-Konto hinzufügen/bearbeiten

Auf diesem Bildschirm können Sie ein neues Benutzerkonto hinzufügen oder ein vorhandenes Benutzerkonto für den Telnet- und SSH-Zugriff auf Ihren Router bearbeiten.

Benutzername

Geben Sie in dieses Feld den Benutzernamen für das neue Konto ein.

Kennwort

Geben Sie in dieses Feld das Kennwort für das neue Konto ein.

Kennwort bestätigen

Geben Sie in dieses Feld das Kennwort für das neue Konto zur Bestätigung erneut ein. Der Eintrag in diesem Feld muss mit dem Eintrag im Feld **Kennwort** übereinstimmen.

Seite Benutzerkonten für Telnet/SSH konfigurieren

Auf diesem Bildschirm können Sie die Benutzerkonten verwalten, die Telnet- oder Secure Shell (SSH)-Zugriff auf Ihren Router haben. Die Tabelle auf diesem Bildschirm enthält alle Telnet-Benutzerkonten mit dem Benutzernamen des Kontos und Sternchen, die das Kennwort für das Konto darstellen. Beachten Sie, dass dieser Bildschirm nur dann angezeigt wird, wenn Sie noch keine Benutzerkonten konfiguriert haben; aus diesem Grund ist die Tabelle immer leer, wenn sie zum ersten Mal angezeigt wird.

Kontrollkästchen „Autorisierung für Telnet aktivieren“

Aktivieren Sie dieses Kontrollkästchen, um den Telnet- und SSH-Zugriff auf Ihren Router zu aktivieren. Deaktivieren Sie dieses Kontrollkästchen, um den Telnet- und SSH-Zugriff auf Ihren Router zu deaktivieren.

Schaltfläche (Schaltfläche)

Klicken Sie auf diese Schaltfläche, um den Bildschirm **Benutzerkonto hinzufügen** anzuzeigen, auf dem Sie ein Konto hinzufügen können, indem Sie dem Konto einen Benutzernamen und ein Kennwort zuweisen.

Schaltfläche (Schaltfläche)

Klicken Sie in der Tabelle auf ein Benutzerkonto, um es auszuwählen, und klicken Sie auf diese Schaltfläche, um den Bildschirm **Benutzerkonto hinzufügen** anzuzeigen, auf dem Sie den Benutzernamen und das Kennwort des ausgewählten Kontos bearbeiten können.

Schaltfläche „Löschen“

Klicken Sie in der Tabelle auf ein Benutzerkonto, um es auszuwählen, und klicken Sie dann auf diese Schaltfläche, um das ausgewählte Konto zu löschen.

Aktivieren der Seite für geheime Kennwörter und Textbanner

Auf diesem Bildschirm können Sie ein neues geheimes Kennwort und ein Textbanner für den Router eingeben.

Das geheime Kennwort ist ein verschlüsseltes Kennwort, das den Administratorzugriff auf alle Funktionen des Routers ermöglicht. Es ist sehr wichtig, dass das geheime Kennwort sicher und schwer zu ermitteln ist. Ihr geheimes Kennwort muss mindestens sechs Zeichen lang sein, und es wird empfohlen, sowohl Buchstaben als auch Ziffern zu verwenden, kein Wort aus einem Wörterbuch zu verwenden oder persönliche Daten von Ihnen zu verwenden, die erraten werden könnten.

Das Textbanner wird immer dann angezeigt, wenn jemand über Telnet oder SSH eine Verbindung zu Ihrem Router herstellt. Das Textbanner ist eine wichtige Sicherheitsmaßnahme, da es eine Methode ist, unberechtigte Personen darüber zu informieren, dass der Zugriff auf Ihren Router verboten ist. In einigen Gesetzgebungen ist dies eine Voraussetzung für zivile und/oder kriminalrechtliche Verfolgung.

Neues Kennwort

Geben Sie in dieses Feld das neue geheime Kennwort ein.

Neues Kennwort erneut eingeben

Geben Sie in dieses Feld das neue geheime Kennwort zur Bestätigung erneut ein.

Login-Banner

Geben Sie das Textbanner ein, das auf Ihrem Router konfiguriert werden soll.

Seite „Logging“

Auf diesem Bildschirm können Sie das Logging auf dem Router konfigurieren, indem Sie eine Liste der Syslog-Server erstellen, an die Protokollmeldungen weitergeleitet werden, und die Logging-Ebene festlegen, die den Mindest-Schweregrad angibt, den eine Protokollmeldung haben muss, um erfasst zu werden.

Tabelle IP-Adresse/Hostname

In dieser Tabelle wird eine Liste der Hosts aufgeführt, an die die Protokollmeldungen des Routers weitergeleitet werden. Bei diesen Hosts sollte es sich um Syslog-Server handeln, die die Protokollmeldungen des Routers erfassen und verwalten können.

Schaltfläche (Schaltfläche)

Klicken Sie auf diese Schaltfläche, um den Bildschirm **IP-Adresse/Hostname** anzuzeigen, auf dem Sie einen Syslog-Server zur Liste hinzufügen können, indem Sie entweder die betreffende IP-Adresse oder den Hostnamen eingeben.

Schaltfläche (Schaltfläche)

Klicken Sie auf einen Syslog-Server in der Tabelle, um ihn auszuwählen, und klicken Sie dann auf diese Schaltfläche, um den Bildschirm **IP-Adresse/Hostname** anzuzeigen, auf dem Sie die IP-Adresse oder den Hostnamen des ausgewählten Syslog-Servers bearbeiten können.

Schaltfläche „Löschen“

Klicken Sie in der Tabelle auf einen Syslog-Server, um ihn auszuwählen, und klicken Sie dann auf diese Schaltfläche, um den ausgewählten Syslog-Server aus der Tabelle zu löschen.

Feld Logging-Ebene einstellen

Wählen Sie in diesem Feld den Mindest-Schweregrad aus, den eine Router-Protokollmeldung aufweisen muss, damit sie erfasst und an die Syslog-Server in der Tabelle auf diesem Bildschirm weitergeleitet werden kann. Der Schweregrad einer Protokollmeldung wird in Form einer Zahl zwischen 1 und 7 angezeigt, wobei niedrigere Zahlen schwerwiegendere Ereignisse kennzeichnen. Die Schweregrade können folgendermaßen beschrieben werden:

- 0 - Notfälle

  Das System kann nicht verwendet werden
- 1 - Alarme

  Sofortiger Benutzereingriff erforderlich
- 2 - Kritisch

  Es liegt ein kritischer Zustand vor
- 3 - Fehler

  Es liegt ein Fehler vor
- 4 - Warnungen

  Es liegt eine Warnung vor
- 5 - Benachrichtigungen

  Normaler, jedoch außergewöhnlicher Zustand
- 6 - Informationen

  Nur Informationsmeldungen
- 7- Debugging

  Debugging-Meldungen

KAPITEL 22

Routing

Das Fenster **Routing** zeigt die konfigurierten statischen Routen und die konfigurierten Routen für das Routing Internet-Protokoll, (RIP), Open Shortest Path First (OSPF) und Extended Interior Gateway Routing Protocol (EIGRP) an. Über dieses Fenster können Sie die Routen überprüfen, neue Routen hinzufügen, bestehende Routen bearbeiten und Routen löschen.

Hinweis Statische und dynamische Routen, die für GRE over IPSec-Tunnel konfiguriert sind, werden in diesem Fenster angezeigt. Wenn Sie einen Routingeintrag in diesem Fenster löschen, der für GRE over IPSec-Tunnel verwendet wird, ist diese Route nicht mehr für den Tunnel verfügbar.

Statisches Routing

Zielnetzwerk

Dies ist das Netzwerk, für das die statische Route einen Pfad bereitstellt.

Weiterleitung

Dies ist die Schnittstelle oder IP-Adresse, über die Pakete gesendet werden müssen, um das Zielnetzwerk zu erreichen.

Optional

Dieser Bereich zeigt an, ob eine Distanzmetrik eingegeben wurde und ob die Route als permanente Route bestimmt wurde oder nicht.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen einer statischen Route	Klicken Sie auf **Hinzufügen**, und erstellen Sie die statische Route im Fenster **Statische IP-Route hinzufügen**.
Bearbeiten einer statischen Route	Wählen Sie die statische Route aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie die Routeninformationen im Fenster **Statische IP-Route bearbeiten**. Wenn eine Route konfiguriert wurde, die nicht von SDM unterstützt wird, ist die Schaltfläche **Bearbeiten** deaktiviert.
Löschen einer statischen Route	Wählen Sie die statische Route aus, und klicken Sie auf **Löschen**. Bestätigen Sie dann den Löschvorgang im Fenster **Warnung**.
Löschen aller statischen Routen	Klicken Sie auf **Alle löschen**. Bestätigen Sie dann den Löschvorgang im Fenster **Warnung**.

Hinweis

- Wenn SDM einen vorherig konfigurierten Eintrag für eine statische Route ermittelt, für den die Next Hop-Schnittstelle als **Null**-Schnittstelle konfiguriert ist, ist der Eintrag für die statische Route schreibgeschützt.
- Wenn SDM einen vorherig konfigurierten Eintrag für eine statische Route mit den Optionen **tag** oder **name** ermittelt, ist Eintrag schreibgeschützt.
- Wenn Sie einen Cisco 7000-Router konfigurieren und die für ein Next Hop verwendete Schnittstelle nicht unterstützt wird, wird diese Route als schreibgeschützt markiert.
- Schreibgeschützte Einträge können nicht unter Verwendung von SDM bearbeitet oder gelöscht werden.

Dynamisches Routing

Über diesen Bereich des Fensters können Sie dynamische Routen für RIP, OSPF und EIGRP konfigurieren.

Elementname

Wenn keine dynamischen Routen konfiguriert wurden, enthält diese Spalte den Text RIP, OSPF und EIGRP. Wenn eine oder mehrere Routen konfiguriert wurden, enthält diese Spalte die Parameternamen für den konfigurierten Routingtyp.

Routing-Protokoll	Konfigurationsparameter
RIP	RIP-Version, Netzwerk, Passive Schnittstelle
OSPF	Prozess-ID
EIGRP	Autonomes System Nummer

Elementwert

Diese Spalte enthält den Text **Aktiviert** und Konfigurationswerte, wenn ein Routingtyp konfiguriert wurde. Sie enthält den Text **Deaktiviert**, wenn kein Routing-Protokoll konfiguriert wurde.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Konfigurieren einer RIP-Route	Wählen Sie die RIP-Registerkarte aus, und klicken Sie auf **Bearbeiten**. Konfigurieren Sie anschließend die Route im Fenster **RIP Dynamic Route**.

Aufgabe	Vorgehensweise
Konfigurieren einer OSPF-Route	Wählen Sie die OSPF-Registerkarte aus, und klicken Sie auf **Bearbeiten**. Konfigurieren Sie anschließend die Route im angezeigten Fenster.
Konfigurieren einer EIGRP-Route	Wählen Sie die EIGRP-Registerkarte aus, und klicken Sie auf **Bearbeiten**. Konfigurieren Sie anschließend die Route im angezeigten Fenster.

Statische IP-Route hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um eine statische Route hinzuzufügen oder zu bearbeiten.

Zielnetzwerk

Geben Sie die Informationen zur Zielnetzwerkadresse in diese Felder ein.

Präfix

Geben Sie die IP-Adresse des Zielnetzwerks ein. Weitere Informationen finden Sie unter Verfügbare Schnittstellenkonfigurationen.

Präfixmaske

Geben Sie die Subnetzmaske der Zieladresse ein.

Zur Standardroute machen

Aktivieren Sie dieses Feld, um diese Route als Standardroute für diesen Router zu definieren. Eine Standardroute leitet alle unbekannten ausgehenden Datenpakete über diese Route weiter.

Weiterleitung

Geben Sie an, wie Daten ans Zielnetzwerk weitergeleitet werden sollen.

Schnittstelle

Klicken Sie auf **Schnittstelle**, wenn Sie die Schnittstelle des Routers auswählen möchten, der das Paket an das Remote-Netzwerk weiterleitet.

IP-Adresse

Klicken Sie auf **IP-Adresse**, wenn Sie IP-Adresse des Next Hop-Routers eingeben möchten, der das Paket vom Remote-Netzwerk empfängt und an dieses weiterleitet.

Optional

Sie können optional eine Distanzmetrik für diese Route angeben und diese als permanente Route definieren.

Distanzmetrik für diese Route

Geben Sie den Metrikwert ein, der in die Routingtabelle eingegeben werden muss. Gültige Werte liegen im Bereich von 1 bis 255.

Permanente Route

Aktivieren Sie dieses Feld, um diesen Eintrag der statischen Route als permanente Route zu definieren. Permanente Routen werden nicht gelöscht, auch wenn die Schnittstelle inaktiv ist oder der Router nicht mit dem nächsten Router kommunizieren kann.

RIP-Route hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um eine Routing Internet Protokoll-((RIP)-Route hinzuzufügen oder zu bearbeiten.

RIP-Version

Die Werte sind **RIP-Version 1**, **RIP-Version 2** und **Standard**. Wählen Sie die vom Cisco IOS-Abbild unterstützte Version aus, die auf dem Router ausgeführt wird. Wenn Sie **Version 1** wählen, sendet der Router RIP-Pakete der Version 1 und kann Pakete der Version 1 empfangen. Wenn Sie **Version 2** wählen, sendet der Router RIP-Pakete der Version 2 und kann Pakete der Version 2 empfangen. Wenn Sie **Standard** wählen, sendet der Router Pakete der Version 1 und kann RIP-Pakete der Version 1 und 2 empfangen.

IP-Netzwerkliste

Geben Sie die Netzwerke ein, in denen RIP aktiviert werden soll. Klicken Sie auf **Hinzufügen**, um ein Netzwerk hinzuzufügen. Klicken Sie auf **Löschen**, um ein Netzwerk aus der Liste zu löschen.

Liste verfügbarer Schnittstellen

Die verfügbaren Schnittstellen werden in dieser Liste angezeigt.

Schnittstelle passiv machen

Aktivieren Sie das Feld neben der Schnittstelle, wenn diese keine Aktualisierungen an die benachbarte Schnittstelle senden soll. Die Schnittstelle erhält jedoch weiterhin Aktualisierungen.

OSPF-Route hinzufügen oder bearbeiten

Verwenden Sie dieses Fenster, um eine Open Shortest Path First-((OSPF)-Route hinzuzufügen oder zu bearbeiten.

OSPF-Prozess-ID

Dieses Feld kann bearbeitet werden, wenn OSPF erstmalig aktiviert wurde; es ist deaktiviert, sobald OSPF-Routing aktiviert wird. Die Prozess-ID identifiziert den OSPF-Routingprozess des Routers, der an andere Router ausgeführt wird.

IP-Netzwerkliste

Geben Sie die Netzwerke ein, für die Routen erstellt werden sollen. Klicken Sie auf **Hinzufügen**, um ein Netzwerk hinzuzufügen. Klicken Sie auf **Löschen**, um ein Netzwerk aus der Liste zu löschen.

Netzwerk

Die Adresse des Zielnetzwerks für diese Route. Weitere Informationen finden Sie unter Verfügbare Schnittstellenkonfigurationen.

Maske

Die Subnetzmaske, die in diesem Netzwerk verwendet wird.

Bereich

Die OSPF-Bereichsnummer für dieses Netzwerk. Jeder Router in einem bestimmten OSPF-Bereich verwaltet eine topologische Datenbank für diesen Bereich.

Hinweis Wenn SDM ein vorherig konfiguriertes OSPF-Routing ermittelt, das **area**-Befehle enthält, ist die Tabelle **IP-Netzwerkliste** schreibgeschützt und kann nicht bearbeitet werden.

Liste verfügbarer Schnittstellen

Die verfügbaren Schnittstellen werden in dieser Liste angezeigt.

Schnittstelle passiv machen

Aktivieren Sie das Feld neben der Schnittstelle, wenn diese keine Aktualisierungen an die benachbarte Schnittstelle senden soll. Die Schnittstelle erhält jedoch weiterhin Aktualisierungen.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um im Fenster **IP-Adresse** eine IP-Adresse, eine Netzwerknummer und eine Bereichsnummer anzugeben.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um die IP-Adresse, Netzwerknummer oder Bereichsnummer im Fenster **IP-Adresse** zu bearbeiten.

EIGRP-Route hinzufügen oder bearbeiten

Verwenden Sie dieses Fenster, um eine Extended IGRP-(EIGRP)-Route hinzuzufügen oder zu bearbeiten.

Autonomes System Nummer

Die Nummer für das autonome System wird verwendet, um die EIGRP-Routingprozesse des Routers an andere Router zu identifizieren.

IP-Netzwerkliste

Geben Sie die Netzwerke ein, für die Routen erstellt werden sollen. Klicken Sie auf **Hinzufügen**, um ein Netzwerk hinzuzufügen. Klicken Sie auf **Löschen**, um ein Netzwerk aus der Liste zu löschen.

Liste verfügbarer Schnittstellen

Die verfügbaren Schnittstellen werden in dieser Liste angezeigt.

Schnittstelle passiv machen

Aktivieren Sie das Feld neben der Schnittstelle, wenn diese keine Aktualisierungen an die benachbarte Schnittstelle senden soll. Die Schnittstelle kann weder Routing-Aktualisierungen weder senden noch empfangen.

Vorsicht Wenn Sie die Schnittstelle als passive Schnittstelle konfiguriert ist, unterdrückt EIGRP den Austausch von Hello-Paketen zwischen Routern, wodurch die Beziehung zu den benachbarten Routern verloren geht. Damit werden nicht nur die Ankündigungen von Routing-Aktualisierungen verhindert, sondern auch eingehende Routing-Aktualisierungen unterdrückt.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um eine IP-Adresse für das Zielnetzwerk zur Netzwerkliste hinzuzufügen.

Löschen

Wählen Sie eine IP-Adresse aus, und klicken Sie auf **Löschen**, um die IP-Adresse aus der Netzwerkliste zu löschen.

KAPITEL 23

Network Address Translation

Die Netzwerkadressenübersetzung (Network Address Translation, NAT) ist eine stabile Form der Adressenübersetzung, die die Adressierungsfähigkeiten erweitert, indem sowohl eine statische Adressenübersetzung als auch eine dynamische Adressenübersetzung ermöglicht wird. NAT ermöglicht einem Host, der nicht über eine gültige registrierte IP-Adresse verfügt, mit anderen Hosts über das Internet zu kommunizieren. Die Hosts können private Adressen oder Adressen, die einer anderen Organisationen zugewiesen sind, verwenden. In jedem Fall lässt NAT die weitere Verwendung dieser Adressen, die nicht internetfähig sind, zu, und ermöglicht dennoch die Kommunikation mit Hosts im Internet.

Network Address Translation Assistenten

Sie können einen Assistenten benutzen, der Sie durch die Erstellung einer Netzwerkübersetzungsregel (NAT) führt. Wählen Sie einen der nachfolgend aufgeführten Assistenten aus:

- Basic NAT

  Wählen Sie den Basis NAT Assistent aus, wenn Sie Ihr Netzwerk mit dem Internet (oder der Außenwelt) verbinden wollen und Ihr Netzwerk über Hosts, aber keine Server verfügt. Schauen Sie das Schaubild auf der rechten Seite an, wenn Sie **Basic NAT** auswählen. Wenn Ihr Netzwerk ausschließlich aus PCs besteht, die Zugang zum Internet benötigen, wählen Sie **Basic NAT** aus, und klicken Sie auf die Schaltfläche **Starten**.

- Erweitertes NAT

  Wählen Sie den Advanced NAT-Assistenten aus, wenn Sie Ihr Netzwerk mit dem Internet (oder der Außenwelt) verbinden wollen, Ihr Netzwerk aus Hosts und Servern besteht *und* die Server für Hosts von der Außenseite (Hosts aus dem Internet) zugänglich sein müssen. Schauen Sie das Schaubild auf der rechten Seite an, wenn Sie **Advanced NAT** auswählen. Wenn Ihr Netzwerk über E-Mail-Server, Web-Server oder andere Servertypen verfügt und Sie wollen Verbindungen von der Internetseite erlauben, wählen Sie **Advanced NAT** aus, und klicken Sie anschließend auf die Schaltfläche **Starten**.

Hinweis Wenn Sie nicht wollen, dass Ihre Server Verbindungen aus dem Internet zulassen, können Sie den Basic NAT Assistenten benutzen.

Basic NAT-Assistent: Willkommen

Das Basic NAT Willkommensfenster zeigt Ihnen, wie Sie der Assistent durch die Konfiguration der NAT zur Verbindung mit einem oder mehreren LANs, jedoch keine Server, in das Internet führt.

Basic NAT-Assistent: Verbindung

Wählen Sie eine Schnittstelle aus

Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, die mit dem Internet verbunden werden soll. Das ist die Router WAN-Schnittstelle.

Netzwerke auswählen

Die Liste der verfügbaren Netzwerke zeigt die Netzwerke an, die mit Ihrem Router verbunden sind. Wählen Sie aus, welche Netzwerke die WAN-Schnittstelle in der NAT-Konfiguration teilen sollen, die Sie einrichten. Um ein Netzwerk auszuwählen, aktivieren Sie das Kästchen in der Liste der verfügbaren Netzwerke.

Hinweis Wählen Sie kein Netzwerk aus, das mit der WAN-Schnittstelle verbunden ist, die in dieser NAT Konfiguration eingerichtet ist. Löschen Sie dieses Netzwerk von der NAT-Konfiguration, indem Sie das Kästchen deaktivieren.

Die Liste zeigt zu jedem Netzwerk die folgenden Informationen an:

- IP-Adressenbereich, der durch das Netzwerk belegt ist
- Netzwerk LAN-Schnittstelle
- Über das Netzwerk eingegebene Kommentare

Um ein Netzwerk von der NAT-Konfiguration zu löschen, deaktivieren Sie das Kästchen.

Hinweis Wenn Cisco SDM einen Konflikt zwischen der NAT-Konfiguration und einer vorhandenen VPN-Konfiguration für die WAN-Schnittstelle entdeckt, wird dies nach Klicken auf **Weiter** in einem Dialogfeld gemeldet.

Übersicht

Dieses Fenster zeigt Ihnen die von Ihnen erstellte NAT-Konfiguration und ermöglicht Ihnen, die Konfiguration zu speichern. Die Zusammenfassung wird ähnlich dem Nachfolgenden angezeigt:

```
Die Schnittstelle, die an das Internet oder Ihren
Internet-Dienstanbieter verbindet.
    FastEthernet0/0

IP-Adressenbereiche, die sich den Internetanschluss teilen:
    108.1.1.0 bis 108.1.1.255
    87.1.1.0 bis 87.1.1.255
    12.1.1.0 bis 12.1.1.255
    10.20.20.0 bis 10.20.20.255
```

Wenn Sie den Advanced NAT-Assistenten benutzt haben, werden Ihnen zusätzliche Informationen ähnlich dem Nachfolgenden angezeigt:

```
NAT-Regeln für Server:
    Übersetzen 10.10.10.19 TCP Port 6080 in die IP-Adresse der
Schnittstelle FastEthernet0/0 TCP Port 80
    Übersetzen 10.10.10.20 TCP Port 25 in den 194.23.8.1 TCP Port 25
```

Advanced NAT-Assistent: Willkommen

Das Advanced NAT-Willkommensfenster zeigt Ihnen, wie Sie der Assistent durch die Konfiguration der NAT zur Verbindung Ihrer LANs und Servers in das Internet führt.

Advanced NAT-Assistent: Verbindung

Wählen Sie eine Schnittstelle aus

Wählen Sie aus dem Dropdown-Menü die Schnittstelle aus, die mit dem Internet verbunden werden soll. Das ist die Router WAN-Schnittstelle.

Zusätzliche öffentliche IP-Adressen

Klicken Sie auf **Hinzufügen**, um eine Ihrer öffentlichen IP-Adressen einzugeben. Sie können diese IP-Adresse an Server in Ihrem Netzwerk zuweisen, die Sie für das Internet zugänglich machen wollen.

Um eine IP-Adresse aus der Liste zu löschen, wählen Sie die IP-Adresse aus und klicken Sie anschließend auf **Löschen**.

IP-Adresse hinzufügen

Geben Sie eine Ihrer öffentlichen IP-Adressen ein. Sie können diese IP-Adresse an Server in Ihrem Netzwerk zuweisen, die Sie für das Internet zugänglich machen wollen.

Advanced NAT-Assistent: Netzwerke

Netzwerke auswählen

Die Liste der verfügbaren Netzwerke zeigt die Netzwerke an, die mit Ihrem Router verbunden sind. Wählen Sie aus, welche Netzwerke die WAN-Schnittstelle in der NAT-Konfiguration teilen sollen, die Sie einrichten. Um ein Netzwerk auszuwählen, aktivieren Sie das Kästchen in der Liste der verfügbaren Netzwerke.

Hinweis Wählen Sie kein Netzwerk aus, das mit der WAN-Schnittstelle verbunden ist, die in dieser NAT Konfiguration eingerichtet ist. Löschen Sie dieses Netzwerk von der NAT-Konfiguration, indem Sie das Kästchen deaktivieren.

Die Liste zeigt zu jedem Netzwerk die folgenden Informationen an:

- IP-Adressenbereich, der durch das Netzwerk belegt ist
- Netzwerk LAN-Schnittstelle
- Über das Netzwerk eingegebene Kommentare

Um ein Netzwerk von der NAT-Konfiguration zu löschen, deaktivieren Sie das Kästchen.

Um ein Netzwerk hinzuzufügen, das nicht direkt mit Ihrem Router in der Liste verbunden ist, klicken Sie auf **Netzwerke hinzufügen**.

Hinweis Wenn Cisco SDM das Setzen eines Häkchens neben einem Netzwerk nicht zulässt, für das Sie eine NAT-Regel konfigurieren möchten, wurde die mit dem Netzwerk verbundene Schnittstelle bereits als NAT-Schnittstelle festgelegt. Dieser Status wird durch das Wort *Designated* in der Kommentarspalte angezeigt. Wenn Sie für diese Schnittstelle eine NAT-Regel konfigurieren wollen, verlassen Sie den Assistenten, klicken Sie auf die Registerkarte **NAT bearbeiten**, und klicken anschließend auf **NAT-Schnittstellen bestimmen**. Deaktivieren Sie die Schnittstelle. Kehren Sie danach zum Assistenten zurück und konfigurieren Sie die NAT-Regel.

Netzwerk hinzufügen

Sie können der Liste mit den Netzwerken ein Netzwerk hinzufügen, das über den Advanced NAT-Assistenten zur Verfügung gestellt wurde. Sie müssen im Besitz der Netzwerk-IP-Adresse und der Netzwerkmaske sein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

IP-Adresse

Geben Sie eine Netzwerk-IP-Adresse ein.

Subnetzmaske

Geben Sie in dieses Feld die Netzwerk-Subnetzmaske ein oder wählen Sie die Anzahl der Subnetz-Bits im Rollfeld auf der rechten Seite aus. Die Subnetzmaske zeigt dem Router welche Bits der IP-Adresse für die Netzwerkadresse und welche Bits für die Hostadresse bestimmt sind.

Advanced NAT-Assistent: Öffentliche Server-IP-Adressen

Dieses Fenster ermöglicht Ihnen, die öffentlichen IP-Adressen in private IP-Adressen für interne Server zu übersetzen, die Sie für das Internet zugänglich machen wollen.

In der Liste werden die privaten IP-Adressen und Ports (falls benutzt), sowie die öffentlichen IP-Adressen und Ports (falls benutzt), in die sie übersetzt wurden, angezeigt.

Um die Liste der privaten IP-Adressen neu zu ordnen, klicken Sie auf die Spaltenüberschrift **Private IP-Adresse**. Um die Liste der öffentlichen IP-Adressen umzustellen, klicken Sie auf die Spaltenüberschrift **Öffentliche IP-Adresse**.

Schaltfläche „Hinzufügen“

Um eine Übersetzungsregel für einen Server hinzuzufügen, klicken Sie auf **Hinzufügen**.

Schaltfläche „Bearbeiten“

Um eine Übersetzungsregel für einen Server zu bearbeiten, wählen Sie diese in der Liste aus und klicken Sie auf **Bearbeiten**.

Schaltfläche „Löschen“

Um eine Übersetzungsregel zu löschen, wählen Sie diese in der Liste aus und klicken Sie auf **Löschen**.

Adressenübersetzungsregel hinzufügen oder bearbeiten

In diesem Fenster können Sie die IP-Adressenübersetzungsinformationen für einen Server eingeben oder bearbeiten.

Private IP-Adresse

Geben Sie die IP-Adresse ein, die der Server in Ihrem internen Netzwerk benutzt. Dies ist eine IP-Adresse, die extern im Internet nicht mehr benutzt werden kann.

Öffentliche IP-Adresse

Wählen Sie aus dem Dropdown-Menü die öffentliche IP-Adresse aus, in welche die private IP-Adresse des Servers übersetzt werden soll. Die IP-Adressen, die im Dropdown-Menü erscheinen, beinhalten die IP-Adresse der WAN-Schnittstelle des Routers und sämtliche in Ihrem Besitz befindlichen öffentlichen IP-Adressen, die im Verbindungsfenster eingetragen sind (siehe Advanced NAT-Assistent: Verbindung).

Servertyp

Wählen Sie aus dem Dropdown-Menü einen der folgenden Servertypen aus.

- Webserver

  Ein HTTP-Host der HTML und andere WWW orientierte Seiten bedient

- E-Mail-Server

  Ein SMTP-Server zum Versenden von Internet-Mails

- Sonstige

  Ein Server, der kein Web- oder E-Mail-Server ist, aber Portübersetzung voraussetzt, um seinen Service anzubieten. Diese Auswahl aktiviert das Feld Translated Port und das Dropdown-Menü Protokoll.

Wenn Sie keinen Servertyp auswählen, wird sämtlicher Verkehr, der für Ihre für den Server ausgewählte öffentliche IP-Adresse bestimmt ist, zu dieser Adresse geroutet. Die Port-Übersetzung wird nicht ausgeführt.

Original Port

Geben Sie die Portnummer ein, die vom Server benutzt wird, um die Serviceanfragen vom internen Netzwerk anzunehmen.

Translated Port

Geben Sie die Portnummer ein, die vom Server benutzt wird, um die Serviceanfragen vom Internet anzunehmen.

Protokoll

Wählen Sie **TCP** oder **UDP** als Protokoll aus, das vom Server mit den ursprünglichen und übersetzten Ports benutzt wird.

Advanced NAT-Assistent: ACL-Konflikt

Wenn dieses Fenster angezeigt wird, hat Cisco SDM einen Konflikt zwischen der NAT-Konfiguration und einer vorhandenen ACL an der WAN-Schnittstelle ermittelt. Diese ACL kann Bestandteil der Firewall-Konfiguration, einer VPN-Konfiguration oder einer anderen Konfiguration sein.

Um den Konflikt zu lösen, wählen Sie NAT-Konfiguration modifizieren aus oder wählen Sie NAT-Konfiguration *nicht* modifizieren aus. Wenn Sie die NAT-Konfiguration *nicht* modifizieren wollen, kann der Konflikt dazu führen, dass andere Funktionen, die Sie konfiguriert haben, fehlschlagen.

Details anzeigen

Klicken Sie auf die Schaltfläche **Details anschauen**, um die vorgeschlagenen Lösungsmöglichkeiten zur Beseitigung des Konflikts in der NAT-Konfiguration anzuschauen. Diese Schaltfläche wird nicht bei allen Funktionskonflikten angezeigt.

Details

Dieses Fenster listet die Änderungen auf, die Cisco SDM an der NAT-Konfiguration durchführt, um die Konflikte zwischen NAT und anderen konfigurierten Funktionen auf derselben Schnittstelle zu lösen.

Regeln für Network Address Translation

Im Fenster **Regel für Network Address Translation bearbeiten** können Sie NAT-Regeln anzeigen, Adressen-Pools anzeigen und Übersetzungs-Timeouts festlegen. Über dieses Fenster können Sie darüber hinaus Schnittstellen als innere oder äußere Schnittstellen definieren.

Weitere Informationen zu NAT erhalten Sie unter Weitere Informationen zu NAT.

NAT-Schnittstellen bestimmen

Klicken Sie auf diese Option, um zu bestimmen, ob die Schnittstelle als innere oder äußere Schnittstelle verwendet werden soll. NAT verwendet die Zuordnungen Innen/Außen als Referenzpunkte beim Interpretieren von Übersetzungsregeln. Innere Schnittstellen sind die Schnittstellen, die mit privaten Netzwerken verbunden sind, welche der Router bedient. Äußere Schnittstellen sind mit dem WAN oder mit dem Internet verbunden. Die für die Innen- oder Außenseite festgelegten Schnittstellen sind oberhalb in der NAT-Regelliste aufgeführt.

Adressen-Pools

Klicken Sie auf diese Schaltfläche, um Adressen-Pools zu konfigurieren oder zu bearbeiten. Adressen-Pools werden für die dynamische Adressenübersetzung verwendet. Der Router kann bei Bedarf eine dynamische Zuweisung von Adressen aus dem Pool vornehmen. Wenn eine Adresse nicht mehr benötigt wird, wird sie zurück in den Pool gegeben.

Übersetzungs-Timeouts

Wenn die dynamische NAT-Übersetzung konfiguriert ist, wird Übersetzungseinträgen ein Timeout-Zeitwert zugewiesen, nach dem diese ihre Gültigkeit verlieren und aus der Übersetzungstabelle entfernt werden. Klicken Sie auf diese Schaltfläche, um die Timeout-Werte für die NAT-Übersetzungseinträge und andere Werte zu konfigurieren.

Regeln für Network Address Translation

Dieser Bereich zeigt die Schnittstellen, die als innere und äußere Schnittstellen bestimmt sind, und die konfigurierten NAT-Regeln an.

Innere Schnittstellen

Die inneren Schnittstellen sind die Schnittstellen, die mit privaten Netzwerken verbunden sind, die den Router bedienen. NAT greift auf die Bezeichnung **innen** zurück, um eine NAT-Übersetzungsregel zu interpretieren. Sie können Schnittstellen als innere Schnittstellen definieren, indem Sie auf **NAT-Schnittstellen bestimmen** klicken.

Äußere Schnittstellen

Die äußeren Schnittstellen sind die Routerschnittstellen, die mit dem WAN oder dem Internet verbunden sind. NAT greift auf die Bezeichnung **außen** zurück, um eine NAT-Übersetzungsregel zu interpretieren. Sie können Schnittstellen als äußere Schnittstellen definieren, indem Sie auf **NAT-Schnittstellen bestimmen** klicken.

Ursprüngliche Adresse

Dies ist die private Adresse oder der Adressensatz, der im LAN verwendet wird.

Übersetzte Adresse

Dies ist die legale Adresse oder Adressenbereich, die bzw. der im Internet oder im externen Netzwerk verwendet wird.

Regeltyp

Regeln sind entweder Regeln für statische Adressenübersetzungen oder Regeln für dynamische Adressenübersetzungen.

Statische Adressenübersetzung (Static Address Translation) ermöglicht Hosts mit privaten Adressen auf das Internet zuzugreifen. Darüber hinaus ist mit dieser Übersetzung der öffentliche Zugriff vom Internet aus auf diesen Host möglich. Dabei wird eine private IP-Adresse einer öffentlichen oder globalen Adresse statisch zugeordnet. Wenn die statische Übersetzung auf zehn private Adressen angewendet werden soll, müssen Sie für jede Adresse eine gesonderte statische Regel erstellen.

Dynamische Adressenübersetzung (Dynamic Address Translation). Es bestehen zwei Methoden der dynamischen Adressierung unter Verwendung von NAT. Eine Methode ordnet mehrere private Adressen einer einzelnen öffentlichen Adresse und den Portnummern von Hostsitzungen zu, um zu ermitteln, an welchen Host zurücklaufender Datenverkehr geleitet werden soll. Die zweite Methode verwendet benannte Adressen-Pools. Diese Adressen-Pools enthalten öffentliche Adressen. Wenn ein Host mit einer privaten Adresse eine Kommunikation außerhalb des LANs durchführen muss, wird diesem eine öffentliche Adresse aus diesem Pool zugewiesen. Wenn der Host die Adresse nicht mehr benötigt, wird sie zurück in den Pool gegeben.

Ausgewählten Eintrag beim Hinzufügen duplizieren

Wenn Sie eine bestehende Regel als Grundlage für eine neue zu erstellende Regel verwenden möchten, wählen Sie die Regel aus, und klicken Sie auf dieses Kontrollkästchen. Wenn Sie auf **Hinzufügen** klicken, werden die von Ihnen ausgewählten Adressen im Fenster **Adressenübersetzungsregel hinzufügen** angezeigt. Sie können diese Adressen bearbeiten, um die Adressen zu erhalten, die Sie für die neue Regel benötigen, statt die gesamte Adresse in jedes Feld einzugeben.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Bestimmen von inneren und äußeren Schnittstellen Sie müssen mindestens eine innere Schnittstelle und eine äußere Schnittstelle bestimmen, damit der Router NAT ausführen kann.	Klicken Sie auf **NAT-Schnittstellen bestimmen**, und definieren Sie die Schnittstellen als innere oder äußere Schnittstellen im Fenster **Einstellung der NAT-Schnittstelle**. Schnittstellen können auch als innere oder äußere Schnittstellen über das Fenster **Schnittstellen und Verbindungen** bestimmt werden.
Hinzufügen, Bearbeiten oder Löschen eines Adressen-Pools Dynamische Regeln können Adressen-Pools verwenden, um Adressen bei Bedarf Geräten zuzuweisen.	Klicken Sie auf **Adressen-Pools**, und konfigurieren Sie im Dialogfeld die Informationen des Adressen-Pools.

Aufgabe	Vorgehensweise
Das Übersetzungs-Timeout einstellen	Klicken Sie auf **Übersetzungs-Timeouts**,und legen Sie den Timeout-Wert im Fenster **Übersetzungs-Timeouts** fest.
Hinzufügen einer NAT-Regel	Klicken Sie auf **Hinzufügen**, und erstellen Sie die NAT-Regel im Fenster **Regel für Port Address Translation hinzufügen**. Wenn Sie eine bestehende NAT-Regel als Muster für die neue Regel verwenden möchten, wählen Sie die Regel aus, klicken Sie auf **Ausgewählten Eintrag beim Hinzufügen duplizieren**, und klicken Sie anschließend auf **Hinzufügen**.
Bearbeiten einer NAT-Regel	Wählen Sie die NAT-Regel aus, die Sie bearbeiten möchten, klicken Sie auf **Bearbeiten**, und bearbeiten Sie die Regel im Fenster **Adressenübersetzungsregel bearbeiten**.
Löschen einer NAT-Regel	Wählen Sie die NAT-Regel aus, die Sie löschen möchten, und klicken Sie auf **Löschen**. Bestätigen Sie dann das Löschen der Regel im angezeigten Fenster **Warnung**.

Aufgabe	Vorgehensweise
Anzeigen oder Bearbeiten von Routenzuordnungen Wenn virtuelle private Netzwerkverbindungen (Virtual Private Network, VPN) im Router konfiguriert sind, müssen die lokalen IP-Adressen im VPN vor NAT-Übersetzungen geschützt werden. Wenn sowohl ein VPN als auch NAT konfiguriert sind, erstellt Cisco Router and Security Device Manager (Cisco SDM) Routenzuordnungen, um IP-Adressen in einem VPN vor einer Übersetzung zu schützen. Routenzuordnungen können auch unter Verwendung der Befehlszeilenschnittstelle (Command Line Interface, CLI) konfiguriert werden. Sie können die konfigurierten Routenzuordnungen anzeigen und die von diesen Zuordnungen verwendeten Zugriffsregeln bearbeiten.	Klicken Sie auf **Routenzuordnung anzeigen**.
Informationen zum Ausführen verwandter Konfigurationsaufgaben	Lesen Sie eine der folgenden Vorgehensweisen: • Wie konfiguriere ich NAT Passthrough für ein VPN? • Wie konfiguriere ich NAT auf einer nicht unterstützten Schnittstelle? • Wie konfiguriere ich NAT Passthrough für eine Firewall?

Hinweis Wenn eine zuvor konfigurierte NAT-Regel als schreibgeschützt in der Liste mit den Regeln für die Netzwerkadressenübersetzung angezeigt wird, und die Regel nicht bearbeitet kann, kann das verschiedene Ursachen haben. Schreibgeschützte NAT-Regeln lassen sich nicht überarbeiten. Weitere Informationen finden Sie unter dem Hilfethema Ursachen, warum Cisco SDM keine NAT-Regel bearbeiten kann.

NAT-Schnittstellen bestimmen

Verwenden Sie dieses Fenster, um zu bestimmen, ob die in NAT-Übersetzungen verwendeten Schnittstellen als innere oder äußere Schnittstellen definiert werden sollen. NAT verwendet die Begriffe **Innen** und **Außen** beim Interpretieren von Übersetzungsregeln, da Übersetzungen von innen nach außen oder von außen nach innen durchgeführt werden.

Sobald die Schnittstellen bestimmt sind, werden diese Schnittstellen in allen NAT-Übersetzungsregeln verwendet. Die bestimmten Schnittstellen werden oberhalb der Liste mit den Übersetzungsregeln im NAT-Hauptfenster angezeigt.

Schnittstelle

Sämtliche Routerschnittstellen werden in dieser Spalte aufgelistet.

Innere (vertrauenswürdig)

Aktivieren Sie diese Option, um festzulegen, dass die Schnittstelle als innere Schnittstelle verwendet werden soll. Innere Schnittstellen sind im Allgemeinen mit einem LAN verbunden, das den Router bedient.

Äußere (nicht vertrauenswürdig)

Aktivieren Sie diese Option, um festzulegen, dass die Schnittstelle als äußere Schnittstelle verwendet werden soll. Äußere Schnittstellen sind im Allgemeinen mit dem WAN Ihrer Organisation oder mit dem Internet verbunden.

Einstellungen für Übersetzungs-Timeout

Wenn Sie dynamische NAT-Übersetzungsregeln konfigurieren, wird Übersetzungseinträgen ein Timeout-Zeitwert zugewiesen, nach dem diese ihre Gültigkeit verlieren und aus der Übersetzungstabelle entfernt werden. Nehmen Sie die Einstellungen für die Timeout-Werte für verschiedene Übersetzungen in diesem Fenster vor.

DNS-Timeout

Geben Sie die Zeit in Sekunden ein, nach der die Verbindung mit DNS-Servern ablaufen soll.

ICMP-Timeout

Geben Sie die Anzahl der Sekunden ein, die als Zeitlimit für den Datenaustausch über das ICMP-Protokoll (Internet Control Message Protocol) gelten soll. Der Standardwert ist 60 Sekunden.

PPTP-Timeout

Geben Sie die Anzahl der Sekunden ein, die als Zeitlimit für den Datenaustausch über das NAT PPTP-Protokoll (Point-to-Point Tunneling Protocol) gelten soll. Der Standardwert ist 86400 Sekunden (24 Stunden).

Dynamisches NAT-Timeout

Geben Sie die maximale Zeitdauer in Sekunden ein, während der dynamische NAT-Übersetzungen gültig sein sollen.

Max. Anzahl an NAT-Einträgen

Geben Sie die maximale Anzahl an NAT-Einträgen für die Übersetzungstabelle ein.

UDP-Flow-Timeouts

Geben Sie die Zeitdauer in Sekunden ein, während der Übersetzungen für Datenübertragungen mit User Datagram Protocol (UDP) gültig sein sollen. Der Standardwert ist 300 Sekunden (5 Minuten).

TCP-Flow-Timeouts

Geben Sie die Zeitdauer in Sekunden ein, während der Übersetzungen für Datenübertragungen mit Transmission Control Protocol (TCP) gültig sein sollen. Der Standardwert ist 86400 Sekunden (24 Stunden).

Taste Zurücksetzen

Wenn Sie auf diese Taste klicken, werden die Übersetzungs- und Timeout-Parameter auf ihre Standardwerte zurückgesetzt.

Routenzuordnung bearbeiten

Wenn VPNs zusammen mit NAT in einem Router konfiguriert ist, liegt für Pakete, die üblicherweise mit den Kriterien einer IPSec-Regel übereinstimmen, keine Übereinstimmung vor, wenn NAT die IP-Adressen der Datenpakete übersetzt. In diesem Fall bedingt die NAT-Übersetzung, dass Pakete ohne Verschlüsselung gesendet werden. Cisco SDM kann Routenzuordnungen erstellen, um zu verhindern, dass NAT IP-Adressen, die beibehalten werden sollen, übersetzt werden.

Auch wenn Cisco SDM nur Routenzuordnungen erstellt, um die NAT-Aktivitäten zu beschränken, können Routenzuordnungen auch für andere Zwecke verwendet werden. Wenn Routenzuordnungen unter Verwendung der CLI erstellt wurden, werden sie ebenfalls in diesem Fenster angezeigt.

Name

Der Name dieser Routenzuordnung.

Routenzuordnungseinträge

Dieses Feld listet die Routenzuordnungseinträge auf.

Name

Der Name des Routenzuordnungseintrags.

Seq.-Nr.

Die Sequenznummer der Routenzuordnung.

Aktion

Von Cisco SDM erstellte Routenzuordnungen werden mit dem Schlüsselwort **permit** (zulassen) konfiguriert. Wenn dieses Feld den Wert **deny** (verweigern) enthält, wurde die Routenzuordnung unter Verwendung der CLI erstellt.

Zugriffslisten

Die Zugriffslisten, die den Datenverkehr angeben, auf den diese Routenzuordnung angewendet wird.

So bearbeiten Sie einen Routenzuordnungseintrag

Wählen Sie den Eintrag aus, klicken Sie auf **Bearbeiten**, und bearbeiten Sie den Eintrag im Fenster **Routenzuordnungseintrag bearbeiten**.

Routenzuordnungseintrag bearbeiten

Verwenden Sie dieses Fenster, um die in einem Routenzuordnungseintrag angegebene Zugriffsliste zu bearbeiten.

Name

Ein schreibgeschütztes Feld, das den Namen des Routenzuordnungseintrags enthält.

Seq.-Nr.

Ein schreibgeschütztes Feld, die Sequenznummer des Routenzuordnungseintrags enthält. Wenn Cisco SDM eine Routenzuordnung erstellt, wird dieser automatisch eine Sequenznummer zugewiesen.

Aktion

Entweder **permit** (zulassen) oder **deny** (verweigern). Von Cisco SDM erstellte Routenzuordnungen werden mit dem Schlüsselwort **permit** (zulassen) konfiguriert. Wenn dieses Feld den Wert **deny** (verweigern) enthält, wurde die Routenzuordnung unter Verwendung der CLI erstellt.

Zugriffslisten

Dieser Bereich zeigt die Zugriffslisten an, die mit diesem Eintrag verknüpft sind. Routenzuordnungen verwenden diese Zugriffslisten, um zu ermitteln, welcher Datenverkehr vor NAT-Übersetzung geschützt werden soll.

So bearbeiten Sie eine Zugriffsliste in einem Routenzuordnungseintrag

Wählen Sie die Zugriffsliste aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie dann die Zugriffsliste im angezeigten Fenster.

Adressen-Pools

Das Fenster **Adressen-Pools** zeigt die konfigurierten Adressen-Pools an, die in dynamischer NAT-Übersetzung verwendet werden können.

Pool-Name

Dieses Feld enthält den Namen des Adressen-Pools. Verwenden Sie diesen Namen, um den Pool beim Konfigurieren einer dynamischen NAT-Regel anzugeben.

Adresse

Dieses Feld enthält den IP-Adressenbereich im Pool. Geräten, deren IP-Adressen mit der Zugriffsregel im Fenster **Adressenübersetzungsregel hinzufügen** übereinstimmen, werden private IP-Adressen aus diesem Pool zugewiesen.

Welche Aufgabe möchten Sie ausführen?

Aufgabe	Vorgehensweise
Hinzufügen eines Adressen-Pools zur Routerkonfiguration	Klicken Sie auf **Hinzufügen**, und konfigurieren Sie den Pool im Fenster **Adressen-Pool hinzufügen**. Wenn Sie einen bestehenden Pool als Vorlage für den neuen Pool verwenden möchten, wählen Sie den bestehenden Pool aus, klicken Sie auf **Ausgewählten Eintrag beim Hinzufügen duplizieren**, und klicken Sie anschließend auf **Hinzufügen**.
Bearbeiten eines vorhandenen Adressen-Pools	Wählen Sie den Pool aus, klicken Sie auf **Bearbeiten**, und bearbeiten Sie die Pool-Konfiguration im Fenster **Adressen-Pool bearbeiten**.
Löschen eines Adressen-Pools	Wählen Sie den Pool aus, klicken Sie auf **Löschen**, und bestätigen Sie den Löschvorgang im angezeigten Fenster **Warnung**.

Hinweis Wenn Cisco SDM einen vorher konfigurierten NAT-Adressenpool ermittelt, der das Schlüsselwort **type** (Typ) verwendet, ist dieser Adressenpool schreibgeschützt und kann nicht bearbeitet werden.

Adressen-Pool hinzufügen/bearbeiten

Verwenden Sie dieses Fenster, um einen Adressen-Pool für die dynamische Adressenübersetzung, eine Adresse für Port Address Translation (PAT) oder einen TCP-Lastausgleichs-Rotary-Pool anzugeben.

Pool-Name

Geben Sie den Namen des Adressen-Pools ein.

Port Address Translation (PAT)

Es kann vorkommen, dass eine Zuweisung für einen Großteil der Adressen im Pool vorgenommen wurde und die IP-Adressen im Pool nahezu aufgebraucht sind. Wenn das der Fall ist, kann PAT mit einer einzelnen IP-Adresse verwendet werden, um auf weitere Anforderungen für IP-Adressen reagieren zu können. Aktivieren Sie dieses Kontrollkästchen, wenn der Router PAT verwenden soll, wenn die Adressen im Pool nahezu aufgebraucht sind.

IP-Adresse

Geben Sie die IP-Adresse mit dem niedrigsten Zahlenwert des Bereich in das linke Feld ein, und geben Sie die IP-Adresse mit dem höchsten Zahlenwert des Bereichs in das rechte Feld ein. Weitere Informationen finden Sie unter Verfügbare Schnittstellenkonfigurationen.

Netzwerkmaske

Geben Sie Subnetzmaske oder die Anzahl an Netzwerkbits ein, die angeben, wie viele Bits in der IP-Adresse Netzwerkbits darstellen.

Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen

Verwenden Sie dieses Hilfethema, wenn Sie die Richtung ***Von innen nach außen*** im Fenster **„Add or Edit Static Address Translation Rule“** (Regel für statische Adressenübersetzung hinzufügen oder bearbeiten) ausgewählt haben.

Verwenden Sie dieses Fenster, um eine Regel für eine statische Adressenübersetzung hinzuzufügen oder zu bearbeiten. Wenn Sie eine Regel bearbeiten, wird der Regeltyp (statisch oder dynamisch) und die Richtung deaktiviert. Wenn Sie diese Einstellungen ändern müssen, löschen Sie die Regel, und stellen Sie sie unter Verwendung der erforderlichen Einstellungen wieder her.

NAT wird für zwei verschiedene statische Adressübersetzungen eingesetzt: einfach statisch und erweitert statisch.

Hinweis Wenn Sie eine NAT-Regel erstellen, die Adressen von Geräten übersetzen würde, die Teil eines VPN sind, bietet Cisco SDM an, die Erstellung mit einer Routenzuordnung zuzulassen, die diese Adressen vor einer NAT-Übersetzung schützt. Wenn für NAT die Adressenübersetzung von Geräten in einem VPN zugelassen wird, stimmen deren übersetzten Adressen nicht mit der IPSec-Regel, die in der IPSec-Richtlinie verwendet wird, überein, und der Datenverkehr wird unverschlüsselt gesendet. Sie können die von Cisco SDM oder per CLI erstellten Routenzuordnungen anzeigen, indem Sie auf die Schaltfläche **Routenzuordnung anzeigen** im Fenster **NAT** klicken.

Richtung

Dieses Hilfethema erläutert, wie die Felder **Adressenübersetzungsregel hinzufügen** verwendet werden, wenn **Von innen nach außen** ausgewählt wurde.

Von innen nach außen

Wählen Sie diese Option, wenn private Adressen im LAN in Adressen übersetzt werden sollen, die im Internet oder im Intranet Ihrer Organisation zulässig sind. Sie sollten diese Option auswählen, wenn Sie private Adressen in Ihrem LAN verwenden, die im Internet nicht global eindeutig sind.

Von Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete, für die eine Adressenübersetzung erforderlich ist, in den Router kommen können. Sie können hier auf Felder zugreifen, um die IP-Adresse eines einzelnen Hosts oder eine Netzwerkadresse und Subnetzmaske anzugeben, die für die Hosts in einem Netzwerk stehen.

Innere Schnittstelle(n)

Wenn Sie als Richtung **Von innen nach außen** wählen, listet dieser Bereich die Schnittstellen auf, die als innere Schnittstellen bestimmt wurden.

Hinweis Wenn dieser Bereich keine Schnittstellennamen enthält, schließen Sie das Fenster **Regel für Port Address Translation hinzufügen**, klicken Sie im NAT-Fenster auf **NAT-Schnittstellen bestimmen**, und bestimmen Sie, ob Routerschnittstellen als innere oder äußere Schnittstellen verwendet werden sollen. Kehren Sie dann zu diesem Fenster zurück, und konfigurieren Sie die NAT-Regel.

IP-Adresse

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine statische Eins-zu-Eins-Zuordnung zwischen der Adresse eines einzelnen Hosts und einer übersetzten Adresse, die als *innere globale* bezeichnet wird, erstellen möchten, geben Sie die IP-Adresse für diesen Host ein. Geben Sie keine Subnetzmaske in das Feld **Netzwerkmaske** ein.
- Wenn Sie *n*-zu-*n*-Zuordnungen zwischen den privaten Adressen in einem Subnetz und den entsprechenden inneren globalen Adressen vornehmen möchten, geben Sie eine beliebige gültige Adresse aus dem Subnetz ein, dessen Adressen übersetzt werden sollen, und geben Sie in das nächste Feld eine Netzwerkmaske ein.

Netzwerkmaske

Wenn Cisco SDM die Adressen eines Subnetzes übersetzen soll, geben Sie die Maske für dieses Subnetz an. Cisco SDM ermittelt die Netzwerk- und Subnetznummer und den Adressensatz, der für die Übersetzung erforderlich ist, anhand der von Ihnen angegebenen IP-Adresse und Maske.

In Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete mit übersetzten Adressen den Router verlassen. Sie können hier auch auf Felder zugreifen, über die Sie die übersetzte Adresse und andere Informationen angeben können.

Äußere Schnittstelle(n)

Wenn Sie als Richtung **Von innen nach außen** wählen, enthält dieser Bereich die Schnittstellen, die als äußere Schnittstellen bestimmt wurden.

Typ

- Wählen Sie **IP-Adresse**, wenn die Adresse in die im IP-Adressfeld definierte Adresse übersetzt werden soll.
- Wählen Sie **Schnittstelle**, wenn die *Übersetzen von...*-Adresse die Adresse einer Schnittstelle des Routers verwenden sollen. Die *Übersetzen von...*-Adresse wird in die IP-Adresse übersetzt, die der von Ihnen im Feld **Schnittstelle** angegebenen Schnittstelle zugewiesen ist.

Schnittstelle

Dieses Feld ist aktiviert, wenn im Feld **Typ** die Option **Schnittstelle** gewählt wurde. In diesem Feld werden die Schnittstellen des Routers aufgeführt. Wählen Sie die Schnittstelle aus, in deren IP-Adresse die lokalen inneren Adressen übersetzt werden sollen.

Hinweis Wenn im Feld **Typ** die Option **Schnittstelle** ausgewählt wurde, werden nur Übersetzungen unterstützt, bei denen TCP/IP-Ports umgeleitet werden. Das Kontrollkästchen **Weiterleitungs-Port** ist automatisch aktiviert und lässt sich auch nicht deaktivieren.

IP-Adresse

Dieses Feld ist aktiviert, wenn im Feld **Typ** die Option **IP-Adresse** gewählt wurde. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine statische Eins-zu-Eins-Zuordnung zwischen den Adressen einer einzelnen Adresse (innere lokale) und einer einzelnen Adresse (innere globale) erstellen möchten, geben Sie die globale Adresse in dieses Feld ein.

- Wenn Sie die inneren lokalen Adressen eines Subnetzes entsprechenden inneren globalen Adressen zuordnen, geben Sie eine beliebige Adresse, die in der Übersetzung verwendet werden soll, in dieses Feld ein. Die Netzwerkmaske, die im Bereich *Von Schnittstelle übersetzen* eingegeben wurde, wird verwendet, um die verbleibenden inneren globalen Adressen zu berechnen.

Hinweis Wenn Sie keine Netzwerkmaske im Bereich **Von Schnittstelle übersetzen** eingeben, nimmt Cisco SDM nur eine Übersetzung vor.

Weiterleitungs-Port

Aktivieren Sie dieses Kontrollkästchen, wenn Sie Portinformationen für das innere Gerät bei der Übersetzung mit einschließen möchten. So können Sie dieselbe öffentliche IP-Adresse für mehrere Geräte verwenden, solange die für jedes Gerät angegebenen Ports unterschiedlich sind. Sie müssen einen Eintrag für jede Portzuordnung erstellen, die Sie für diese **Übersetzen in**-Adresse vornehmen.

Klicken Sie auf **TCP**, wenn es sich um eine TCP-Portnummer handelt, und klicken Sie auf **UDP**, wenn es sich um eine UDP-Portnummer handelt.

Geben Sie in das Feld **Ursprünglicher Port** die Portnummer für das innere Gerät ein.

Geben Sie in das Feld **Übersetzter Port** die Portnummer ein, die der Router für diese Übersetzung verwenden soll.

Konfigurations-Beispielszenarios

Klicken Sie auf Beispielszenarios für die statische Adressenübersetzung, um Beispiele anzuzeigen, die erläutern, wie die Felder in diesem Fenster verwendet werden.

Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen

Verwenden Sie dieses Hilfethema, wenn Sie die Richtung ***Von außen nach innen*** im Fenster **„Add or Edit Static Address Translation Rule“** (Regel für statische Adressenübersetzung hinzufügen oder bearbeiten) ausgewählt haben.

Verwenden Sie dieses Fenster, um eine Regel für eine statische Adressenübersetzung hinzuzufügen oder zu bearbeiten. Wenn Sie eine Regel bearbeiten, wird der Regeltyp (statisch oder dynamisch) und die Richtung deaktiviert. Wenn Sie diese Einstellungen ändern müssen, löschen Sie die Regel, und stellen Sie sie unter Verwendung der erforderlichen Einstellungen wieder her.

NAT wird für zwei verschiedene statische Adressübersetzungen eingesetzt: einfach statisch und erweitert statisch.

Hinweis Wenn Sie eine NAT-Regel erstellen, die Adressen von Geräten übersetzen würde, die Teil eines VPN sind, bietet Cisco SDM an, die Erstellung mit einer Routenzuordnung zuzulassen, die diese Adressen vor einer NAT-Übersetzung schützt. Wenn für NAT die Adressenübersetzung von Geräten in einem VPN zugelassen wird, stimmen deren übersetzten Adressen nicht mit der IPSec-Regel, die in der IPSec-Richtlinie verwendet wird, überein, und der Datenverkehr wird unverschlüsselt gesendet. Sie können die von Cisco SDM oder per CLI erstellten Routenzuordnungen anzeigen, indem Sie auf die Schaltfläche **Routenzuordnung anzeigen** im Fenster **NAT** klicken.

Richtung

Wählen Sie die Datenverkehrsrichtung für diese Regel aus.

Von außen nach innen

Wählen Sie diese Option, wenn eingehende Adressen in Adressen übersetzt werden sollen, in Ihrem LAN gültig sind. Sie können diese Option bei der Zusammenführung von Netzwerken wählen, wenn die Kompatibilität eines Satzes von eingehenden Adressen mit einem bestehenden Satz im LAN, das den Router bedient, hergestellt werden soll.

Dieses Hilfethema erläutert, wie die verbleibenden Felder verwendet werden, wenn **Von außen nach innen** ausgewählt wurde.

Von Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete, für die eine Adressenübersetzung erforderlich ist, in den Router kommen können. Sie können hier auf Felder zugreifen, um die IP-Adresse eines einzelnen Hosts oder eine Netzwerkadresse und Subnetzmaske anzugeben, die für die Hosts in einem Netzwerk stehen.

Äußere Schnittstellen

Wenn Sie **Von außen nach innen** wählen, enthält dieser Bereich die Schnittstellen, die als äußere Schnittstellen bestimmt wurden.

Hinweis Wenn dieser Bereich keine Schnittstellennamen enthält, schließen Sie das Fenster **Regel für Port Address Translation hinzufügen**, klicken Sie im NAT-Fenster auf **NAT-Schnittstellen bestimmen**, und bestimmen Sie, ob Routerschnittstellen als innere oder äußere Schnittstellen verwendet werden sollen. Kehren Sie dann zu diesem Fenster zurück, und konfigurieren Sie die NAT-Regel.

IP-Adresse

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine statische Eins-zu-Eins-Zuordnung zwischen der Adresse (äußere globale) eines einzelnen Remote-Hosts und einer übersetzten Adresse, die als *äußere lokale* bezeichnet wird, erstellen möchten, geben Sie die IP-Adresse für den Remote-Host ein.
- Wenn Sie *n*-zu-*n*-Zuordnungen zwischen den Adressen in einem Remote-Subnetz und den entsprechenden Adressen (äußere lokale) vornehmen möchten, geben Sie eine beliebige gültige Adresse aus dem Subnetz ein, dessen Adressen übersetzt werden sollen, und geben Sie in das nächste Feld eine Netzwerkmaske ein.

Netzwerkmaske

Wenn Cisco SDM die Adressen in einem Remote-Subnetz übersetzen soll, geben Sie die Maske für dieses Subnetz an. Cisco SDM ermittelt die Netzwerk- und Subnetznummer und den Adressensatz, der für die Übersetzung erforderlich ist, anhand der von Ihnen angegebenen IP-Adresse und Maske.

In Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete mit übersetzten Adressen den Router verlassen. Sie können hier auch auf Felder zugreifen, über die Sie die übersetzte Adresse und andere Informationen angeben können.

Innere Schnittstelle(n)

Wenn Sie **Von außen nach innen** wählen, enthält dieser Bereich die Schnittstellen, die als innere Schnittstellen bestimmt wurden.

IP-Adresse

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine statische Eins-zu-Eins-Zuordnung zwischen den Adressen einer einzelnen Adresse (äußere globale) und einer einzelnen Adresse (äußere lokale) erstellen möchten, geben Sie die Adresse (äußere lokale) in dieses Feld ein.
- Wenn Sie die Adressen (äußere globale) eines Remote-Subnetzes entsprechenden Adressen (äußere lokale) zuordnen, geben Sie eine beliebige Adresse, die in der Übersetzung verwendet werden soll, in dieses Feld ein. Die Netzwerkmaske, die im Bereich **Von Schnittstelle übersetzen** eingegeben wurde, wird verwendet, um die verbleibenden (äußere lokale) Adressen zu berechnen.

Hinweis Wenn Sie keine Netzwerkmaske im Bereich **Von Schnittstelle übersetzen** eingeben, nimmt Cisco SDM nur eine Übersetzung vor.

Weiterleitungs-Port

Aktivieren Sie dieses Kontrollkästchen, wenn Sie Portinformationen für das Gerät auf der Außenseite bei der Übersetzung mit einschließen möchten. So können Sie die erweiterte statische Übersetzung und dieselbe öffentliche IP-Adresse für mehrere Geräte verwenden, solange die für jedes Gerät angegebenen Ports unterschiedlich sind.

Klicken Sie auf **TCP**, wenn es sich um eine TCP-Portnummer handelt, und klicken Sie auf **UDP**, wenn es sich um eine UDP-Portnummer handelt.

Geben Sie in das Feld **Ursprünglicher Port** die Portnummer für das äußere Gerät ein.

Geben Sie in das Feld **Übersetzter Port** die Portnummer ein, die der Router für diese Übersetzung verwenden soll.

Konfigurations-Beispielszenarios

Klicken Sie auf Beispielszenarios für die statische Adressenübersetzung, um Beispiele anzuzeigen, die erläutern, wie die Felder in diesem Fenster verwendet werden.

Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen

Verwenden Sie dieses Hilfethema, wenn Sie die Richtung ***Von innen nach außen*** im Fenster **„Add or Edit Dynamic Address Translation Rule“** (Dynamische NAT-Regel hinzufügen oder bearbeiten) ausgewählt haben.

Verwenden Sie dieses Fenster, um eine Regel für die Adressenübersetzung hinzuzufügen oder zu bearbeiten. Wenn Sie eine Regel bearbeiten, wird der Regeltyp (statisch oder dynamisch) und die Richtung deaktiviert. Wenn Sie diese Einstellungen ändern müssen, löschen Sie die Regel, und stellen Sie sie unter Verwendung der erforderlichen Einstellungen wieder her.

Eine Regel für die dynamische Adressenübersetzung ordnet Hosts Adressen zu, indem Adressen verwendet werden, die in einem Adressen-Pool enthalten sind, die im Zielnetzwerk global eindeutig sind. Der Pool wird definiert, indem ein Adressenbereich angegeben und dem Bereich ein eindeutiger Name zugeteilt wird. Der konfigurierte Router verwendet die verfügbaren Adressen aus dem Pool (die, die nicht für statische Übersetzungen oder für seine eigene WAN-IP-Adresse verwendet werden) für Verbindungen mit dem Internet oder außerhalb des Netzwerks. Wenn eine Adresse nicht mehr verwendet wird, wird sie in den Adressen-Pool zurückgegeben und kann später einem anderen Gerät dynamisch zugewiesen werden.

Hinweis Wenn Sie eine NAT-Regel erstellen, die Adressen von Geräten übersetzen würde, die Teil eines VPN sind, bietet Cisco SDM an, die Erstellung mit einer Routenzuordnung zuzulassen, die diese Adressen vor einer NAT-Übersetzung schützt. Wenn für NAT die Adressenübersetzung von Geräten in einem VPN zugelassen wird, stimmen deren übersetzten Adressen nicht mit der IPSec-Regel, die in der IPSec-Richtlinie verwendet wird, überein, und der Datenverkehr wird unverschlüsselt gesendet.

Richtung

Wählen Sie die Datenverkehrsrichtung für diese Regel aus.

Von innen nach außen

Wählen Sie diese Option aus, wenn private Adressen im LAN in Adressen übersetzt werden sollen, die im Internet oder im Intranet Ihrer Organisation zulässig sind.

Dieses Hilfethema erläutert, wie die verbleibenden Felder verwendet werden, wenn **Von innen nach außen** ausgewählt wurde.

Von Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete, für die eine Adressenübersetzung erforderlich ist, in den Router kommen können. Sie können hier auf Felder zugreifen, um die IP-Adresse eines einzelnen Hosts oder eine Netzwerkadresse und Subnetzmaske anzugeben, die für die Hosts in einem Netzwerk stehen.

Innere Schnittstelle(n)

Wenn Sie als Richtung **Von innen nach außen** wählen, enthält dieser Bereich die Schnittstellen, die als innere Schnittstellen bestimmt wurden.

Hinweis Wenn dieser Bereich keine Schnittstellennamen enthält, schließen Sie das Fenster **Regel für Port Address Translation hinzufügen**, klicken Sie im NAT-Fenster auf **NAT-Schnittstellen bestimmen**, und bestimmen Sie, ob Routerschnittstellen als innere oder äußere Schnittstellen verwendet werden sollen. Kehren Sie dann zu diesem Fenster zurück, und konfigurieren Sie die NAT-Regel.

Zugriffsregel

Dynamische NAT-Übersetzungsregeln verwenden Zugriffsregeln, um die Adressen anzugeben, die übersetzt werden müssen. Wenn Sie **Von innen nach außen** wählen, handelt es sich um innere lokale Adressen. Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die die zu übersetzenden Adressen definiert. Wenn Sie weder den Namen noch die Nummer kennen, können Sie auf die Schaltfläche **...** klicken und eine bestehende Zugriffsregel auswählen. Sie können aber auch eine neue Zugriffsregel erstellen und sie benutzen.

In Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete mit übersetzten Adressen den Router verlassen. Sie können hier auch auf Felder zugreifen, über die Sie die übersetzte Adresse angeben können.

Äußere Schnittstelle(n)

Wenn Sie als Richtung **Von innen nach außen** wählen, enthält dieser Bereich die Schnittstellen, die als äußere Schnittstellen bestimmt wurden.

Typ

Wählen Sie **Schnittstelle**, wenn die *Übersetzen von...*-Adressen die Adresse einer Schnittstelle am Router verwenden sollen. Diese werden in die Adresse, die Sie im Feld **Schnittstelle** angegeben haben, übersetzt, und PAT wird für die Unterscheidung aller Hosts im Netzwerk verwendet. Wählen Sie **Adressen-Pool**, wenn die Adressen in Adressen übersetzt werden sollen, die in einem konfigurierten Adressen-Pool definiert sind.

Schnittstelle

Wenn Sie **Schnittstelle** im Feld **Typ** ausgewählt haben, listet dieses Feld die Schnittstellen im Router auf. Wählen Sie die Schnittstelle aus, in deren IP-Adresse die lokalen inneren Adressen übersetzt werden sollen. PAT wird für die Unterscheidung aller Hosts im Netzwerk verwendet.

Adressen-Pool

Wenn Sie im Feld **Typ** die Option **Adressen-Pool** ausgewählt haben, können Sie den Namen eines konfigurierten Adressen-Pools in dieses Feld eingeben, oder Sie können auf **Adressen-Pool** klicken, um einen Adressen-Pool zu erstellen.

Konfigurations-Beispielszenarios

Klicken Sie auf Beispielszenarios für die dynamische Adressenübersetzung, um Beispiele anzuzeigen, die erläutern, wie die Felder in diesem Fenster verwendet werden.

Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen

Verwenden Sie dieses Hilfethema, wenn Sie die Richtung ***Von außen nach innen*** im Fenster **„Add or Edit Dynamic Address Translation Rule“** (Dynamische NAT-Regel hinzufügen oder bearbeiten) ausgewählt haben.

Verwenden Sie dieses Fenster, um eine Regel für die Adressenübersetzung hinzuzufügen oder zu bearbeiten. Wenn Sie eine Regel bearbeiten, wird der Regeltyp (statisch oder dynamisch) und die Richtung deaktiviert. Wenn Sie diese Einstellungen ändern müssen, löschen Sie die Regel, und stellen Sie sie unter Verwendung der erforderlichen Einstellungen wieder her.

Eine Regel für die dynamische Adressenübersetzung ordnet Hosts Adressen zu, indem Adressen verwendet werden, die in einem Adressen-Pool enthalten sind, die im Zielnetzwerk global eindeutig sind. Der Pool wird definiert, indem ein Adressenbereich angegeben und dem Bereich ein eindeutiger Name zugeteilt wird. Der konfigurierte Router verwendet die verfügbaren Adressen aus dem Pool (die, die nicht für statische Übersetzungen oder für seine eigene WAN-IP-Adresse verwendet werden) für Verbindungen mit dem Internet oder außerhalb des Netzwerks. Wenn eine Adresse nicht mehr verwendet wird, wird sie in den Adressen-Pool zurückgegeben und kann später einem anderen Gerät dynamisch zugewiesen werden.

Hinweis Wenn Sie eine NAT-Regel erstellen, die Adressen von Geräten übersetzen würde, die Teil eines VPN sind, bietet Cisco SDM an, die Erstellung mit einer Routenzuordnung zuzulassen, die diese Adressen vor einer NAT-Übersetzung schützt. Wenn für NAT die Adressenübersetzung von Geräten in einem VPN zugelassen wird, stimmen deren übersetzten Adressen nicht mit der IPSec-Regel, die in der IPSec-Richtlinie verwendet wird, überein, und der Datenverkehr wird unverschlüsselt gesendet.

Richtung

Wählen Sie die Datenverkehrsrichtung für diese Regel aus.

Von außen nach innen

Wählen Sie diese Option, wenn eingehende Adressen in Adressen übersetzt werden sollen, in Ihrem LAN gültig sind. Sie können diese Option bei der Zusammenführung von Netzwerken wählen, wenn die Kompatibilität eines Satzes von eingehenden Adressen mit einem bestehenden Satz im LAN, das den Router bedient, hergestellt werden soll.

Dieses Hilfethema erläutert, wie die verbleibenden Felder verwendet werden, wenn **Von außen nach innen** ausgewählt wurde.

Von Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete, für die eine Adressenübersetzung erforderlich ist, in den Router kommen können. Sie können hier auf Felder zugreifen, um die IP-Adresse eines einzelnen Hosts oder eine Netzwerkadresse und Subnetzmaske anzugeben, die für die Hosts in einem Netzwerk stehen.

Äußere Schnittstellen

Wenn Sie **Von außen nach innen** wählen, enthält dieser Bereich die Schnittstellen, die als äußere Schnittstellen bestimmt wurden.

Hinweis Wenn dieser Bereich keine Schnittstellennamen enthält, schließen Sie das Fenster **Regel für Port Address Translation hinzufügen**, klicken Sie im NAT-Fenster auf **NAT-Schnittstellen bestimmen**, und bestimmen Sie, ob Routerschnittstellen als innere oder äußere Schnittstellen verwendet werden sollen. Kehren Sie dann zu diesem Fenster zurück, und konfigurieren Sie die NAT-Regel.

Zugriffsregel

Dynamische NAT-Übersetzungsregeln verwenden Zugriffsregeln, um die Adressen anzugeben, die übersetzt werden müssen. Wenn Sie **Von außen nach innen** wählen, handelt es sich um äußere globale Adressen. Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die die zu übersetzenden Adressen definiert. Wenn Sie weder den Namen noch die Nummer kennen, können Sie auf die Schaltfläche **...** klicken und eine bestehende Zugriffsregel auswählen. Sie können aber auch eine neue Zugriffsregel erstellen und sie benutzen.

In Schnittstelle übersetzen

Dieser Bereich zeigt die Schnittstellen an, von denen aus Pakete mit übersetzten Adressen den Router verlassen. Sie können hier auch auf Felder zugreifen, über die Sie die übersetzte Adresse angeben können.

Innere Schnittstelle(n)

Wenn Sie **Von außen nach innen** wählen, enthält dieser Bereich die Schnittstellen, die als innere Schnittstellen bestimmt wurden.

Typ

Wählen Sie **Schnittstelle**, wenn die *Übersetzen von...*-Adressen die Adresse einer Schnittstelle am Router verwenden sollen. Diese werden in die Adresse, die Sie im Feld **Schnittstelle** angegeben haben, übersetzt, und PAT wird für die Unterscheidung aller Hosts im Netzwerk verwendet. Wählen Sie **Adressen-Pool**, wenn die Adressen in Adressen übersetzt werden sollen, die in einem konfigurierten Adressen-Pool definiert sind.

Schnittstelle

Wenn Sie **Schnittstelle** im Feld **Typ** ausgewählt haben, listet dieses Feld die Schnittstellen im Router auf. Wählen Sie die Schnittstelle aus, in deren IP-Adresse die lokalen inneren Adressen übersetzt werden sollen. PAT wird für die Unterscheidung aller Hosts im Netzwerk verwendet.

Adressen-Pool

Wenn Sie im Feld **Typ** die Option **Adressen-Pool** ausgewählt haben, können Sie den Namen eines konfigurierten Adressen-Pools in dieses Feld eingeben, oder Sie können auf **Adressen-Pool** klicken, um einen Adressen-Pool zu erstellen.

Konfigurations-Beispielszenarios

Klicken Sie auf Beispielszenarios für die dynamische Adressenübersetzung, um Beispiele anzuzeigen, die erläutern, wie die Felder in diesem Fenster verwendet werden.

Wie macht man … . .

Dieser Abschnitt enthält Verfahren für Aufgaben, die Sie nicht mit dem Assistenten ausführen können.

Wie konfiguriert man die Adressenübersetzung von innen nach außen

Der NAT-Assistent ermöglicht Ihnen die Konfigurierung einer Network Address Translation (NAT)-Regel, damit Sie Adressen von innen nach außen übersetzen können. Um eine NAT-Regel zu konfigurieren, mit der Sie Adressen von außen nach innen übersetzen können, befolgen Sie die Anweisungen in einem der folgenden Abschnitte.

- Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen
- Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von außen nach innen

Wie konfiguriert man NAT mit einem LAN und mehreren WANs?

Der NAT-Assistent ermöglicht Ihnen die Konfigurierung einer NAT-Regel (Network Address Translation) zwischen einer LAN-Schnittstelle Ihres Routers und einer WAN-Schnittstelle. Wenn Sie NAT zwischen einer LAN-Schnittstelle an Ihrem Router und mehreren WAN-Schnittstellen konfigurieren möchten, konfigurieren Sie zunächst mithilfe des NAT-Assistenten eine NAT-Regel (Network Address Translation) zwischen der betreffenden LAN-Schnittstelle Ihres Routers und einer WAN-Schnittstelle. Folgen Sie anschließend den Anweisungen in einer der folgenden Abschnitte:

- Regel für statische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen
- Regel für dynamische Adressenübersetzung hinzufügen oder bearbeiten: Von innen nach außen

Jedes Mal, wenn Sie eine neue Adressenübersetzungsregel hinzufügen, die eine der Richtungen in diesem Abschnitt benutzt, wählen Sie die gleiche LAN-Schnittstelle und eine neue WAN-Schnittstelle aus. Wiederholen Sie diesen Vorgang bei allen WAN-Schnittstellen, die Sie mit einer Adressenübersetzungsregel konfigurieren wollen.

KAPITEL 24

Cisco IOS IPS

Mithilfe des Cisco IOS Intrusion Prevention System (Cisco IOS IPS) können Sie sich vor Eindringlingen auf Routern schützen. Auf dem Router muss dafür die Version Cisco IOS 12.3(8)T4 oder höher laufen. Mit Cisco IOS IPS können Sie den Router überwachen und vor Eindringlingen schützen, indem der Verkehr mit den Signaturen bekannter Bedrohungen verglichen und bei Erkennung einer Bedrohung blockiert wird.

Mit Cisco SDM können Sie den Einsatz von Cisco IOS IPS auf den Schnittstellen festlegen, SDF-Dateien (Signature Definition Files) von Cisco.com importieren und bearbeiten und bestimmen, welche Maßnahme Cisco IOS IPS bei Erkennung einer Bedrohung ergreifen soll.

IPS-Register

Verwenden Sie die Registerkarten an der oberen Seite des IPS-Fensters, um zu dem Bereich zu gelangen, mit dem Sie arbeiten wollen.

- IPS erstellen – Klicken Sie darauf, um zum IPS-Regelassistenten zu gelangen und eine neue Cisco IOS IPS-Regel zu erstellen.
- IPS bearbeiten – Klicken Sie darauf, um Cisco IOS IPS-Regeln zu bearbeiten und Schnittstellenzuweisungen festzulegen oder aufzuheben.
- Security Dashboard - Klicken Sie darauf, um die Tabelle mit den häufigsten Bedrohungen anzuzeigen und Signaturen zu diesen Bedrohungen zu übernehmen.
- IPS-Migration – Wenn der Router ein Cisco IOS-Abbild der Version 12.4(11)T oder höher ausführt, können mit früheren Cisco IOS-Versionen erstellte Cisco IOS IPS-Konfigurationen migriert werden.

IPS-Regeln

Eine Cisco IOS IPS-Regel gibt eine Schnittstelle, den Typ und die Verkehrsrichtung, die Cisco IPS überprüfen soll, sowie den Ort der SDF-Datei (Signature Definition File) an, die der Router verwendet.

IPS erstellen

Von diesem Fenster aus können Sie den IPS-Regelassistenten starten.

Der IPS-Regelassistent fordert Sie zur Eingabe folgender Informationen auf:

- Die Schnittstelle, auf welche die Regel angesetzt werden soll
- Der Datenverkehr, auf den die Cisco IOS IPS angesetzt werden soll (eingehend und/oder ausgehend)
- Der Ort der SDF-Datei (Signature Definition File)

Bei Cisco IOS-Abbildern der Version 12.4(11) oder höher werden Sie außerdem zur Eingabe folgender Informationen aufgefordert:

- Gewünschter Speicherort für Dateien, die Änderungen an der IOS-IPS-Konfiguration enthalten. Eine Datei, in der derartige Informationen gespeichert werden, wird als Delta-Datei bezeichnet.
- Der öffentliche Schlüssel für den Zugriff auf die Informationen in den Delta-Dateien.
- Die Signaturkategorie. Die grundlegende Signaturkategorie ist für Router mit weniger als 128 MB Flash-Speicher geeignet. Die erweiterte Signaturkategorie ist für Router mit mehr als 128 MB Flash-Speicher geeignet.

Das Beispielszenario schildert eine Konfiguration, bei der eine Cisco IOS IPS-Regel verwendet wird. Nach dem Erstellen der Cisco IOS IPS-Regel und der Übergabe der Konfiguration an den Router können Sie auf die Registerkarte **IPS-Regel bearbeiten** klicken, um die Regel abzuändern.

Weitere Informationen über Cisco IOS IPS finden Sie in den Dokumenten unter dem folgenden Link:

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Klicken Sie auf die Schaltfläche **IPS-Regelassistent starten**, um den Vorgang zu starten.

IPS erstellen: Willkommen

Dieses Fenster zeigt eine Zusammenfassung der Aufgaben an, die nach Abschluss des IPS-Regelassistenten ausgeführt werden.

Klicken Sie auf **Weiter**, um mit dem Definieren einer Cisco IOS IPS-Regel zu beginnen.

IPS erstellen: Schnittstellen auswählen

Wählen Sie die Schnittstellen aus, auf welche die Cisco IOS IPS-Regel angesetzt werden soll, und legen Sie fest, ob die Regel auf den eingehenden oder den ausgehenden Verkehr angewendet werden soll. Wenn Sie beide Kästchen aktivieren (eingehend und ausgehend), wird die Regel auf den Verkehr angewendet, der in beide Richtungen fließt.

Beispiel: Anhand der folgenden Einstellungen wird die Cisco IOS IPS-Regel auf den eingehenden Datenverkehr der BRI 0 Schnittstelle sowie auf die ein- und ausgehenden Daten der Schnittstelle FastEthernet 0 angesetzt.

Schnittstellen-name	Eingehend	Ausgehend
BRI 0	Aktivieren	—
FastEthernet 0	Aktivieren	Aktivieren

IPS erstellen: SDF Standort

Cisco IOS IPS untersucht den Datenverkehr anhand eines Vergleichs mit den Signaturen, die in der SDF-Datei (Signature Definition File) enthalten sind. Die SDF kann in einem Router-Flash-Memory oder einem Remote-System, auf das der Router zugreifen kann, untergebracht sein. Sie können mehrere SDF Standorte festlegen, sodass der Router die Möglichkeit hat, wenn er den ersten Standort nicht erreicht, die anderen Standorte zu kontaktieren, bis er eine SDF findet.

Klicken Sie auf **Hinzufügen**, **Löschen**, **Nach Oben** und **Nach Unten**, um eine Liste mit SDF-Verzeichnisangaben zu ergänzen, zu löschen bzw. zu sortieren, auf die der Router anschließend zum Abruf einer SDF zugreifen kann. Der Router beginnt beim ersten Eintrag und arbeitet sich in der Liste nach unten, bis er eine SDF findet.

Cisco IOS-Abbilder, die Cisco IOS IPS unterstützen, besitzen integrierte Signaturen. Wenn Sie das Kästchen an der Unterseite des Fensters aktivieren, verwendet der Router die eingebauten Signaturen nur dann, wenn er keine SDF aus der Liste finden kann.

IPS erstellen: Signaturdatei

Die Cisco IOS IPS-Signaturdatei enthält die Standardsignaturdaten, die in jeder Aktualisierung der Datei auf Cisco.com vorhanden sind. Alle Änderungen an dieser Konfiguration werden in einer Delta-Datei gespeichert. Aus Sicherheitsgründen muss die Delta-Datei mit einer digitalen Signatur versehen werden. Legen Sie den Speicherort der Signaturdatei fest und geben Sie den Namen und den Text des öffentlichen Schlüssels an, der zum Signieren der Delta-Datei in diesem Fenster verwendet wird.

Unter diesem Hilfethema wird das Fenster **Signaturdatei** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Geben Sie die mit IOS IPS zu verwendende Signaturdatei an

Wenn sich die Signaturdatei bereits auf dem PC, im Flash-Speicher oder einem Remote-System befindet, klicken Sie auf **Geben Sie die mit IOS IPS zu verwendende Signaturdatei an**, um ein Dialogfeld anzuzeigen, in dem Sie den Speicherort der Signaturdatei festlegen können.

Rufen Sie die neueste Signaturdatei von CCO ab und speichern Sie sie auf dem PC

Klicken Sie auf **Rufen Sie die neueste Signaturdatei von CCO ab und speichern Sie sie auf dem PC**, falls die Signaturdateien nicht bereits auf dem PC oder im Flash-Speicher des Routers vorhanden sind. Klicken Sie auf **Durchsuchen**, um den Speicherort für die Signaturdatei anzugeben, und klicken Sie anschließend auf **Herunterladen**, um die Datei herunterzuladen. Cisco SDM lädt die Signaturdatei in den angegebenen Ordner herunter.

Konfigurieren eines öffentlichen Schlüssels

Alle Änderungen an der Signaturkonfiguration werden in einer Delta-Datei gespeichert. Diese Datei muss mit einem öffentlichen Schlüssel digital signiert werden. Sie können über Cisco.com einen Schlüssel beziehen und die Daten in die Felder **Name** und **Schlüssel** einfügen.

Hinweis Auch wenn Sie mithilfe der Cisco IOS CLI bereits einen öffentlichen Schlüssel zur Konfiguration hinzugefügt haben, müssen Sie trotzdem in diesem Bildschirm einen öffentlichen Schlüssel angeben. Nach Beenden des Cisco IOS IPS Regelassistenten können Sie zu **Bearbeiten IPS > Globale Einstellungen** wechseln. Im Bildschirm **Globale Einstellungen** können Sie im Bereich **IPS-Voraussetzungen bearbeiten** auf **Bearbeiten** und anschließend auf **Öffentlicher Schlüssel** klicken, um das Dialogfeld **Öffentlicher Schlüssel** anzuzeigen. In diesem Dialogfeld können Sie nicht benötigte öffentliche Schlüssel löschen.

Führen Sie die folgenden Schritte aus, um die Daten für den öffentlichen Schlüssel in die Felder **Name** und **Schlüssel** einzufügen.

Schritt 1 Verwenden Sie den folgenden Link, um den öffentlichen Schlüssel abzurufen:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Schritt 2 Laden Sie den Schlüssel auf den PC herunter.

Schritt 3 Kopieren Sie den Text nach **named-key** in das Feld **Name**. Die Textzeile mit dem Namen kann beispielsweise folgendermaßen lauten:

```
named-key realm-cisco.pub signature
```

Kopieren Sie `realm-cisco.pub signature` in das Feld **Name**.

Schritt 4 Kopieren Sie den Text zwischen `key-string` und `quit` in das Feld **Schlüssel**. Es folgt ein Beispiel:

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

IPS erstellen: Speicherort und Kategorie der Konfigurationsdatei

Geben Sie einen Speicherort für die Signaturinformationen an, die Cisco IOS IPS verwendet. Zu diesen Informationen zählen die Signaturdatei und die Delta-Datei, die erstellt wird, wenn Änderungen an der Signaturinformation vorgenommen werden.

Unter diesem Hilfethema wird das Fenster **Konfigurationsspeicherort** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Konfigurationsspeicherort

Klicken Sie auf die Schaltfläche rechts neben dem Feld **Konfigurationsspeicherort**, um das Dialogfeld aufzurufen, in dem Sie den Speicherort festlegen können. Nachdem Sie die Daten im Dialogfeld eingegeben haben, zeigt Cisco SDM den Pfad zum Speicherort in diesem Feld an.

Kategorie wählen

Da der Router-Speicher und Ressourcenbeschränkungen die Verwendung aller verfügbaren Signaturen möglicherweise nicht zulassen, werden die Signaturen in zwei Kategorien eingeteilt: **Basis** und **Erweitert**. Wählen Sie im Feld **Kategorie wählen** die Kategorie aus, mit der das Cisco IOS IPS reibungslos auf dem Router ausgeführt wird. Die Basiskategorie ist für Router mit weniger als 128 MB verfügbarem Flash-Speicher geeignet. Die erweiterte Kategorie ist für Router mit mehr als 128 MB verfügbarem Flash-Speicher geeignet.

Hinzufügen oder Bearbeiten eines Konfigurationsspeicherorts

Geben Sie einen Speicherort für die Signaturinformationen und die Delta-Datei an, die Cisco IOS IPS verwendet.

Konfigurationsspeicherort auf diesem Router angeben

Klicken Sie zum Festlegen eines Speicherorts auf dem Router auf die Schaltfläche rechts neben dem Feld **Verzeichnisname** und wählen Sie das Verzeichnis aus, in dem die Konfigurationsdaten gespeichert werden sollen.

Hinweis Wenn der Router über ein LEFS-basiertes Dateisystem verfügt, können Sie kein Verzeichnis im Routerspeicher erstellen. In diesem Fall dient der Flash-Speicher als Konfigurationsspeicherort.

Konfigurationsspeicherort mit URL angeben

Um einen Speicherort auf einem Remote-System festzulegen, geben Sie das Protokoll und den Pfad der entsprechenden URL an. Wenn Sie beispielweise die URL http://172.27.108.5/ips-cfg angeben möchten, geben Sie 172.27.108.5/ips-cfg ein.

Hinweis Geben Sie beim Pfad nicht das Protokoll mit an. Cisco SDM fügt das Protokoll automatisch hinzu. Wenn Sie das Protokoll eingeben, zeigt Cisco SDM eine Fehlermeldung an.

Geben Sie in den Feldern **Anzahl der Wiederholungen** und **Timeout** an, wie oft der Router versuchen soll, eine Verbindung zum Remote-System herzustellen, und wie lange der Router auf eine Antwort warten soll, bevor er die Versuche abbricht.

Verzeichnisauswahl

Wählen Sie den Ordner aus, in dem die Konfigurationsinformationen gespeichert werden sollten. Wenn Sie einen neuen Ordner erstellen möchten, klicken Sie auf **Neuer Ordner**, geben Sie im angezeigten Dialogfeld einen Namen für den Ordner ein, wählen Sie ihn aus und klicken Sie auf **OK**.

Signaturdatei

Geben Sie den Speicherort der Signaturdatei für das Cisco IOS IPS an.

Signaturdatei auf Flash angeben

Wenn sich die Signaturdatei im Flash-Speicher eines Routers befindet, klicken Sie auf die Schaltfläche rechts neben dem Feld. Cisco SDM zeigt die Namen der Signaturdateien im richtigen Format an, aus denen Sie auswählen können.

Signaturdatei mit URL angeben

Wenn sich die Signaturdatei auf einem Remote-System befindet, wählen Sie das Protokoll und den Pfad der Datei aus. Wenn sich die Signaturdatei IOS-S259-CLI.pkg beispielsweise auf 10.10.10.5 befindet und das FTP-Protokoll verwendet wird, wählen Sie **ftp** als Protokoll aus und geben Sie

```
10.10.10.5/IOS-S259-CLI.pkg ein.
```

Hinweis Geben Sie beim Pfad nicht das Protokoll mit an. Cisco SDM fügt das Protokoll automatisch hinzu. Wenn Sie das Protokoll eingeben, zeigt Cisco SDM eine Fehlermeldung an. Wenn Sie eine URL verwenden, müssen Sie außerdem einen Dateinamen angeben, der den Benennungskonventionen für die IOS-Snnn-CLI.pkg-Datei entspricht, so wie bei der Datei im vorangehenden Beispiel.

Signaturdatei auf dem PC angeben

Wenn sich die Signaturdatei auf dem PC befindet, klicken Sie auf **Durchsuchen**, navigieren zu dem Ordner, in dem sich die Datei befindet und wählen den Dateinamen aus. Sie müssen ein Cisco SDM-spezifisches Paket des Formats sigv5-SDM-S*xxx*.zip auswählen, wie z. B. sigv5-SDM-S260.zip.

IPS erstellen: Übersicht

Dies ist ein Beispiel einer Cisco IOS IPS-Zusammenfassung auf einem Router, der eine frühere Cisco IOS-Version als 121.4(11)T ausführt.

```
Ausgewählte Schnittstelle: FastEthernet 0/1

IPS-Prüfrichtungen: Beide

Ort der SDF-Datei (Signature Definition File): flash//sdmips.sdf

Integriert aktiviert: Ja
```

Bei diesem Beispiel ist Cisco IOS IPS auf der Schnittstelle FastEthernet 0/1 aktiviert, und der eingehende als auch der ausgehende Datenverkehr wird untersucht. Die SDF-Datei heißt sdmips.sdf und ist im Flash-Speicher des Routers gespeichert. Der Router ist so eingestellt, dass er die im Cisco IOS-Abbild integrierten Signaturdefinitionen des Routers nutzt.

IPS erstellen: Übersicht

Das Übersichtsfenster zeigt die Informationen an, die Sie eingegeben haben, sodass Sie diese nochmals durchlesen können, bevor die Änderungen an den Router gesendet werden.

Unter diesem Hilfethema wird das Fenster **Übersicht** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt. Es folgt ein Beispiel für ein Übersichtsfenster:

```
Die IPS-Regel wird auf den ausgehenden Datenverkehr auf den folgenden
Schnittstellen angewendet.
     FastEthernet0/1
Die IPS-Regel wird auf eingehenden Datenverkehr auf den folgenden Schnittstellen
angewendet.
     FastEthernet0/0
Speicherort der Signaturdatei:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Öffentlicher Schlüssel:
       30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Konfigurationsspeicherort
     flash:/configloc/
Ausgewählte Signaturkategorie:
     erweitert
```

In diesem Beispiel wird die Cisco IOS IPS-Richtlinie auf die Schnittstellen FastEthernet 0/0 und FastEthernet 0/1 angewendet. Die Signaturdatei befindet sich auf dem PC. Der Konfigurationsspeicherort ist im Flash-Speicher des Routers in einem Verzeichnis namens **configloc**.

IPS bearbeiten

In diesem Fenster können Sie Cisco IOS IPS-Schaltflächen zur Konfiguration und Pflege von Cisco IOS IPS-Richtlinien, Sicherheitsmeldungen, Signaturen und einiges mehr aufrufen.

Schaltfläche „IPS-Richtlinien“

Klicken Sie hier, um das Fenster IPS bearbeiten anzuzeigen. Sie können darin die Cisco IOS IPS-Überprüfung einer Schnittstelle ein- oder ausschalten sowie Informationen über das Ansetzen einer Cisco IOS IPS-Regel einholen. Wenn Sie Cisco IOS IPS auf einer Schnittstelle zuschalten, können Sie optional bestimmen, welcher Datenverkehr nach Eindringlingen untersucht werden soll.

Schaltfläche „Globale Einstellungen“

Klicken Sie darauf, um das Fenster IPS bearbeiten: Globale Einstellungen anzuzeigen. Hier können Sie Einstellungen vornehmen, die die Wirkungsweise aller Cisco IOS IPS-Funktionen betreffen.

Autoaktualisierung

Diese Schaltfläche wird angezeigt, wenn das Cisco IOS-Abbild auf dem Router Version 12.4(11)T oder höher entspricht. Mit der Autoaktualisierung können Sie den Router so konfigurieren, dass er automatisch die neuesten Signaturaktualisierungen vom Cisco Security Center abruft. Weitere Informationen finden Sie unter IPS bearbeiten: Autoaktualisierung.

SEAP-Konfiguration

Diese Schaltfläche wird angezeigt, wenn das Cisco IOS-Abbild auf dem Router Version 12.4(11)T oder höher entspricht. Signature Event Action Processing (Signaturereignis-Aktionsverarbeitung, SEAP) ermöglicht eine größere Kontrolle über IOS IPS durch Filtern und Übergehen.

Schaltfläche „SDEE-Meldungen“

SDEE-Meldungen (Secure Device Event Exchange) enthalten Angaben über Initialisierung und Betrieb von Cisco IOS IPS. Klicken Sie hier, um das Fenster IPS bearbeiten: SDEE-Meldungen anzuzeigen. Sie können darin SDEE-Meldungen nachlesen und Anzeigefilter festlegen, um beispielsweise nur Fehler-, Status- oder Warnmeldungen anzuzeigen.

Schaltfläche „Signaturen“

Klicken Sie hier, um das Fenster IPS bearbeiten: Signaturen anzuzeigen. Dort können Sie die Signaturen im Router verwalten.

Schaltfläche „NM CIDS“

Diese Schaltfläche wird angezeigt, wenn im Router ein Cisco Intrusion Detection System-Netzwerkmodul installiert ist. Klicken Sie darauf, um das IDS-Modul zu managen.

IPS bearbeiten: IPS-Richtlinien

Dieses Fenster zeigt den Cisco IOS IPS-Status aller Router-Schnittstellen an. Außerdem können Sie Cisco IOS IPS hier auf den gewünschten Schnittstellen ein- und ausschalten.

Schnittstellen

Verwenden Sie diese Liste zum Filtern der im Bereich der Schnittstellenliste angezeigten Schnittstellen. Wählen Sie eine der folgenden Möglichkeiten:

- **Alle Schnittstellen** – Alle Schnittstellen im Router.
- **IPS-Schnittstellen** – Schnittstellen, auf denen Cisco IOS IPS aktiviert wurde.

Schaltfläche „Aktivieren“

Klicken Sie hierauf, um Cisco IOS IPS auf der angegebenen Schnittstelle zu aktivieren. Sie können festlegen, für welche Datenflussrichtungen die Cisco IOS IPS-Überprüfung aktiviert werden soll und Sie können die ACLs bestimmen, die zur Definition des zu untersuchenden Datenverkehrstyps herangezogen werden. Weitere Informationen finden Sie unter IPS an einer Schnittstelle aktivieren oder bearbeiten.

Schaltfläche „Bearbeiten“

Klicken Sie hier, um die Cisco IOS IPS-Eigenschaften einzustellen, die auf die gewählte Schnittstelle anzuwenden sind.

Schaltfläche „Deaktivieren“

Klicken Sie hierauf, um Cisco IOS IPS auf der angegebenen Schnittstelle zu deaktivieren. Ein Kontextmenü zeigt die Datenverkehrsrichtungen an, auf die Cisco IOS IPS angesetzt wurde, und Sie können die Richtung auswählen, für die Cisco IOS IPS deaktiviert werden soll. Wenn Sie Cisco IOS IPS auf einer Schnittstelle deaktivieren, auf der die Funktion zuvor eingesetzt wurde, hebt Cisco SDM die Beziehung zwischen den Cisco IOS IPS-Regeln und der Schnittstelle auf.

Schaltfläche „Alle deaktivieren“

Klicken Sie darauf, um Cisco IOS IPS auf allen Schnittstellen zu deaktivieren, auf denen die Funktion aktiviert war. Wenn Sie Cisco IOS IPS auf einer Schnittstelle deaktivieren, auf der die Funktion zuvor eingesetzt wurde, hebt Cisco SDM die Beziehung zwischen den Cisco IOS IPS-Regeln und der Schnittstelle auf.

Schnittstellenname

Der Name der Schnittstelle. Beispiel: Serial0/0 oder FE0/1.

IP

Diese Spalte kann die folgenden IP-Adressentypen enthalten:

- Konfigurierte IP-Adresse der Schnittstelle.
- DHCP-Client – Die Schnittstelle erhält von einem DHCP-Server (Dynamic Host Configuration Protocol) eine IP-Adresse.
- Ausgehandelt – Nach Aushandlung der Parameter mit dem Remote-Gerät erhält die Schnittstelle eine IP-Adresse.
- Keine IP-Nummerierung – Der Router verwendet eine IP-Adresse aus einem Adress-Pool, den Ihr Service-Provider für Ihren Router und für die Geräte in Ihrem LAN bereitstellt.
- Nicht zutreffend – Dem Schnittstellentyp kann keine IP-Adresse zugewiesen werden.

Eingangs-IPS/Ausgangs-IPS

- Aktiviert – Cisco IOS IPS ist für diese Richtung des Datenverkehrs aktiviert.
- Deaktiviert – Cisco IOS IPS ist für diese Richtung des Datenverkehrs deaktiviert.

VFR Status

Virtual Fragment Reassembly-(VFR-)Status. Folgende Werte sind möglich:

- Ein – VFR ist aktiviert.
- Aus – VFR ist deaktiviert.

Cisco IOS IPS kann die Inhalte von IP-Fragmenten weder identifizieren noch kann es Portinformationen vom Fragment einholen, um diese mit einer Signatur abzugleichen. Die Fragmente gelangen aus diesem Grunde ohne Untersuchung der Daten bzw. ohne das Anlegen einer dynamischen Zugriffssteuerungsliste (ACL) in das Netzwerk.

Dank VFR kann die Cisco IOS-Firewall geeignete dynamische ACLs anlegen und das Netzwerk auf diese Weise vor verschiedenen Fragmentierungsangriffen schützen.

Beschreibung

Eine Beschreibung der Verbindung, sofern eingegeben.

Details zum IPS-Filter

Wenn der Datenverkehr nicht mit einem Filter versehen ist, enthält dieser Bereich keine Einträge. Wenn ein Filter anwendet wird, wird der Name oder die Nummer der ACL in Klammern angezeigt.

Die Schaltflächen „Eingehender Filter/Ausgehender Filter“

Klicken Sie auf diese Schaltflächen, um die Einträge des Filters anzuzeigen, der auf eingehenden oder ausgehenden Datenverkehr angewendet wird.

Feldbeschreibungen

Aktion - Legt fest, ob der Datenverkehr zugelassen oder abgelehnt wird.

 Zulassen von Quelldatenverkehr.

 Ablehnen des Quelldatenverkehrs

Quelle - Netzwerk- oder Hostadresse oder ein beliebiger Host oder ein Netzwerk

Ziel - Netzwerk- oder Hostadresse oder ein beliebiger Host oder ein Netzwerk

Dienst - Typ des zu filternden Dienstes: IP, TCP, UDP, IGMP oder ICMP.

Protokoll - Angabe, ob verweigerter Datenverkehr protokolliert wird

Attribute - Optionen, die unter Verwendung der CLI konfiguriert sind

Beschreibung - Eine angegebene Beschreibung

IPS an einer Schnittstelle aktivieren oder bearbeiten

In diesem Fenster können Sie die Schnittstellen auswählen, auf denen die Intrusion Detection-Funktion eingeschaltet werden soll. Außerdem können Sie hier die IPS-Filter zur Untersuchung des Datenverkehrs festlegen.

Die Optionen „Beide“, „Eingehend“ und „Ausgehend“

Mithilfe dieser Optionen können Sie Cisco IOS IPS sowohl für eingehenden als auch ausgehenden Datenverkehr, nur für eingehenden Datenverkehr oder nur für ausgehenden Datenverkehr aktivieren.

Eingehender Filter

(Optional) Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die den zu überprüfenden eingehenden Datenverkehr angibt. Die von Ihnen angegebene ACL wird im Fenster **Konfiguration der IPS-Regeln** bei Auswahl der Schnittstelle angezeigt, die mit den Regeln versehen wurde. Wenn Sie nach der Zugriffsregel suchen oder eine neue erstellen müssen, klicken Sie auf die Schaltfläche **...**.

Ausgehender Filter

(Optional) Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die den zu überprüfenden ausgehenden Datenverkehr angibt. Die von Ihnen angegebene ACL wird im Fenster **Konfiguration der IPS-Regeln** bei Auswahl der Schnittstelle angezeigt, die mit den Regeln versehen wurde. Wenn Sie nach der Zugriffsregel suchen oder eine neue erstellen müssen, klicken Sie auf die Schaltfläche **...**.

... (Schaltfläche)

Verwenden Sie diese Schaltfläche, um einen Filter anzugeben. Wenn Sie hierauf klicken, wird ein Menü mit den folgenden Optionen angezeigt:

- **Vorhandene Regel auswählen**. Weitere Informationen finden Sie unter Regel auswählen.
- **Neue Regel (ACL) erstellen und auswählen**. Weitere Informationen finden Sie unter Regel hinzufügen/bearbeiten.
- **Keine (Regelverknüpfung aufheben)**. Verwenden Sie diese Option, um einen Filter aus der Datenverkehrsrichtung zu entfernen, auf die dieser angewendet wurde.

Fragmentprüfung in dieser Schnittstelle aktivieren

(Ist standardmäßig aktiviert). Aktivieren Sie diese Option, wenn die Cisco IOS-Firewall diese Schnittstelle auf IP-Fragmente überprüfen soll. Weitere Informationen finden Sie unter VFR Status.

Fragmentprüfung in andere(n) Schnittstelle(n) aktivieren

Wenn die Fragmentprüfung für ausgehenden Datenverkehr aktiviert ist, muss der Router den eingehenden Datenverkehr überprüfen, der in den Schnittstellen ankommt, die ausgehenden Datenverkehr an die Schnittstellen senden, die konfiguriert werden. Geben Sie diese Schnittstellen hier an.

Wenn das Optionsfeld **Eingehend** aktiviert ist, wird dieser Bereich nicht angezeigt.

Signaturdatei angeben

Das Feld **Signaturdatei angeben** enthält Informationen zur SDF-Version, die der Router ausführt, und ermöglicht die Aktualisierung der SDF auf eine neuere Version. Klicken Sie zum Angeben einer neuen SDF auf die Schaltfläche **...** neben dem Feld **Signaturdatei angeben**, und geben Sie eine neue Datei in das angezeigte Dialogfeld ein.

IPS bearbeiten: Globale Einstellungen

In diesem Fenster können Sie die globalen Cisco IPS-Einstellungen anzeigen und festlegen. Unter diesem Hilfethema wird die Information erläutert, die angezeigt wird, wenn ein früheres Cisco IOS-Abbild als Version 12.4(11)T angezeigt wird.

Tabelle „Globale Einstellungen“

In dieser Tabelle des Fensters **Globale Einstellungen** werden die gegenwärtigen globalen Einstellungen und die eingetragenen Werte angezeigt. Klicken Sie zum Ändern der Werte auf **Bearbeiten**.

Elementname	Elementwert
Syslog	Sofern aktiviert, werden Benachrichtigungen an den Syslog-Server weitergeleitet, der in den **Systemeigenschaften** angegeben ist.
SDEE	Security Device Event Exchange. Wenn diese Option aktiviert ist, werden SDEE-Ereignisse generiert.
SDEE-Ereignisse	Die Anzahl an SDEE-Ereignissen, die im Puffer des Routers gespeichert werden sollen.
SDEE-Abonnement	Anzahl der gleichzeitigen SDEE-Abonnements.

Engine-Optionen	Die Engine-Optionen lauten: • Fail-Closed – Standardmäßig berechnet die Cisco IOS für eine bestimmte Engine eine neue Signatur. Ohne eine Überprüfung der jeweiligen Engine werden die Pakete dabei durchgelassen. Bei Aktivierung dieser Option weist die Cisco IOS während des Berechnungsvorgangs alle Pakete zurück. • Integrierte Signaturen verwenden (als Sicherung) – Wenn die Cisco IOS IPS keine Signaturen finden oder von den angegebenen Speicherorten laden kann, können zum Aktivieren der Cisco IOS IPS die integrierten Signaturen von Cisco IOS verwendet werden. Diese Option ist standardmäßig aktiviert. • **Verweigerung an der IPS-Schnittstelle** – Diese Option empfiehlt sich, wenn der Router einen Lastausgleich durchführt. Wenn diese Option eingeschaltet ist, aktiviert Cisco IOS IPS die ACLs auf den Cisco IOS IPS-Schnittstellen und nicht auf den Schnittstellen, über die der Datenverkehr mit den Angriffen eingetroffen ist.
Abweisungsereignis	Diese Option nutzt den Parameter Shun Time (Abweisungszeit). Die Abweisungszeit (Shun Time) ist die Zeitspanne, über die Abweisungsaktionen wirksam sein sollen. Eine Abweisungsaktion wird eingeleitet, nachdem ein Host oder Netzwerk in eine ACL-Liste aufgenommen wurde, um Daten abzulehnen, die von dem betreffenden Host oder Netzwerk stammen.

Konfigurierte SDF-Speicherorte

Ein Signaturspeicherort ist eine URL, die einen Pfad zu einer SDF enthält. Beim Suchen nach einer SDF versucht der Router Kontakt mit dem ersten Speicherort in der Liste herzustellen. Wenn dies fehlschlägt, wird versucht, Kontakt der Reihe nach mit allen folgenden Speicherorten herzustellen, bis eine SDF gefunden wird.

Schaltfläche „Hinzufügen“

Klicken Sie hier, um einen URL zur Liste hinzuzufügen.

Schaltfläche „Bearbeiten“

Klicken Sie hier, um einen bereits festgelegten Speicherort zu bearbeiten.

Die Schaltfläche Löschen

Klicken Sie hier, um einen festgelegten Speicherort zu löschen.

Schaltflächen Nach oben und Nach unten

Mithilfe dieser Schaltflächen können Sie die Reihenfolge der URLs in der Liste wunschgemäß ändern.

Reload Signatures

Klicken Sie auf diese Option, um die Signaturen aller Signatur-Engines neu zu berechnen. In der Zeitspanne, in der die Signaturen von einer Signatur-Engine erneut berechnet werden, hat die Cisco IOS-Software keine Möglichkeit, Datenpakete mithilfe der Signaturen der betreffenden Engine zu untersuchen.

Globale Einstellungen bearbeiten

Auf den Registerkarten **Syslog**, **SDEE** und **Global Engine** (globale Engine) können Sie in diesem Fenster Einstellungen vornehmen, die sich auf die gesamte Funktionsweise von Cisco IOS IPS auswirken.

Syslog-Benachrichtigung aktivieren (Registerkarten Syslog und SDEE)

Aktivieren Sie dieses Kontrollkästchen, damit der Router Alarm-, Ereignis- und Fehlermeldungen an einen Syslog-Server weiterleitet. Um diese Benachrichtigungsmethode verwenden zu können, muss ein Syslog-Server in den **Systemeigenschaften** identifiziert werden.

SDEE (Registerkarten Syslog und SDEE)

Tragen Sie die Anzahl der gleichzeitigen SDEE-Abonnements (Wertebereich 1 - 3) in das Feld **Anzahl der gleichzeitigen SDEE-Abonnements** ein. Mit einem SDEE-Abonnement werden SDEE-Ereignisse **live** empfangen.

Tragen Sie im Feld **Maximum number of SDEE alerts to store** (Maximale Anzahl zu speichernder SDEE-Warnungen) die Höchstzahl an SDEE-Warnmeldungen ein, die im Router gespeichert werden sollen. Werte zwischen 10 und 2000 sind zulässig. Zur Speicherung von noch mehr Warnmeldungen wird mehr Routerspeicher benötigt.

Tragen Sie im Feld **Maximum number of SDEE messages to store** (Maximale Anzahl zu speichernder SDEE-Meldungen) die Höchstzahl an SDEE-Meldungen ein, die im Router gespeichert werden sollen. Werte zwischen 10 und 500 sind zulässig. Zur Speicherung von noch mehr Meldungen wird mehr Routerspeicher benötigt.

Fail-Close-Engine aktivieren (Registerkarte Global Engine)

Standardmäßig berechnet die Cisco IOS-Software für eine bestimmte Engine eine neue Signatur. Ohne eine Überprüfung der jeweiligen Engine werden die Pakete dabei durchgelassen. Aktivieren Sie diese Option, damit Pakete während der Signaturberechnung von der Cisco IOS-Software gelöscht werden.

Integrierte Signaturen verwenden (als Sicherung) (Registerkarte Global Engine)

Falls Cisco IOS IPS die Signaturen an den genannten Speicherorten nicht finden oder laden kann, kann die Software auf die in Cisco IOS integrierten Signaturen zur Aktivierung von Cisco IOS IPS zurückgreifen. Diese Option ist standardmäßig aktiviert.

Verweigerung an der IPS-Schnittstelle aktivieren (Registerkarte Global Engine)

Diese Option ist anwendbar, wenn Signaturaktionen für **denyAttackerInline** oder **denyFlowInline** konfiguriert sind. Cisco IOS IPS wendet ACLs standardmäßig auf die Schnittstellen an, von denen ein Angriff gestartet wurde, und nicht auf Cisco IOS IPS-Schnittstellen. Wenn Sie diese Option aktivieren, wendet Cisco IOS IPS die ACLs direkt auf die Cisco IOS IPS-Schnittstellen an und nicht auf die Schnittstellen, welche die Datenpakete mit den Angriffen ursprünglich entgegengenommen haben. Wenn der Router keinen Lastausgleich durchführt, sollte diese Einstellung nicht aktiviert werden. Wenn der Router einen Lastausgleich durchführt, ist das Aktivieren dieser Einstellung zu empfehlen.

Timeout (Registerkarte Globale Engine)

Mit dieser Option legen Sie einen Zeitraum in Minuten (zwischen 0 und 65535) fest, in dem Abweisungsaktionen eingeschaltet sein sollen. Der Standardwert ist 30 Minuten. Eine Abweisungsaktion wird eingeleitet, nachdem ein Host oder Netzwerk in eine ACL-Liste aufgenommen wurde, um Daten abzulehnen, die von dem betreffenden Host oder Netzwerk stammen.

Einen Signaturstandort hinzufügen oder bearbeiten

Geben Sie an, aus welchem Verzeichnis Cisco IOS IPS eine SDF laden soll. Um mehrere Standorte anzugeben, öffnen Sie diesen Dialog erneut und geben Sie die Informationen einer weiteren SDF ein.

SDF auf diesem Router angeben

Legen Sie im Dropdown-Menü **Speicherort** den Bereich des Routerspeichers fest, in dem die SDF abgelegt ist. Beispiel: Das Menü könnte unter anderem die Einträge *disk0*, *usbflash1* und *flash* enthalten. Wählen Sie anschließend den Dateinamen aus, indem Sie auf den Pfeil neben dem Feld **Dateiname** klicken oder in das Feld **Dateiname** direkt einen Dateinamen eintragen.

SDF, die eine URL verwendet, angeben

Wenn die SDF auf einem Remote-System liegt, können Sie die URL angeben, wo die Datei liegt.

Protokoll

Wählen Sie das Protokoll aus, dass der Router zum Einlesen einer SDF verwenden soll, zum Beispiel *http* oder *https*.

URL

Geben Sie den URL nach folgendem Muster an:

```
pfad-zur-signaturdatei
```

Hinweis Das im Menü **Protokoll** gewählte Protokoll wird rechts neben dem URL-Feld angezeigt. Die Protokollangabe darf deshalb im URL-Feld *nicht* erneut eingegeben werden.

Die folgende URL dient als Beispiel zur Veranschaulichung des Formats. Dies ist *keine* gültige URL-Angabe zu einer Signaturdatei und enthält das Protokoll, um die URL zu vervollständigen:

```
https://172.16.122.204/mysigs/vsensor.sdf
```

Autosave

Aktivieren Sie diese Option, wenn der Router die SDF bei einem Absturz automatisch speichern soll. Nach der Rückkehr des Routers zur Betriebsbereitschaft muss die Cisco IOS IPS auf diese Weise nicht erneut mit der betreffenden SDF konfiguriert werden.

IPS bearbeiten: SDEE-Meldungen

Dieses Fenster listet die vom Router empfangenen SDEE-Meldungen auf. SDEE-Meldungen werden bei Änderungen an der Cisco IOS IPS-Konfiguration erstellt.

SDEE-Meldungen

Auswahl des anzuzeigenden SDEE-Meldungstyps:

- Alle- SDEE Fehlermeldungen, Statusmeldungen und Warnungen werden gezeigt.
- **Fehler** – Nur die SDEE-Fehlermeldungen werden angezeigt.
- **Status** – Nur die SDEE-Statusmeldungen werden angezeigt.
- Warnungen – Nur Warnungen werden gezeigt.

Ansicht Nach

Auswahl des zu durchsuchenden SDEE-Meldungsfeldes.

Kriterien

Geben Sie den gesuchten Text ein.

Schaltfläche Start

Klicken Sie darauf, um die Suche nach dem Text zu starten, den Sie in das Feld **Kriterien** eingetragen haben.

Typ

Dazu gehören Fehler-, Status- und Warnmeldungen. Klicken Sie auf SDEE-Meldungstext, um mögliche SDEE-Meldungen anzuzeigen.

Zeit

Die Uhrzeit, zu der die Meldung empfangen wurde.

Beschreibung

Verfügbare Beschreibung.

Schaltfläche Aktualisieren

Klicken Sie auf die Taste, um neue SDEE-Meldungen zu sehen.

Taste Schließen

Klicken Sie auf diese Schaltfläche, um das Fenster **SDEE-Meldungen** zu schließen.

SDEE-Meldungstext

Unter diesem Thema werden mögliche SDEE-Meldungen aufgelistet.

IDS Statusmeldungen

Fehlermeldung

```
ENGINE_BUILDING: %s - %d signatures - %d of %d engines
```

Erklärung Wird ausgegeben, wenn Cisco IOS IPS mit der Erstellung der Signatur-Microengine (SME) beginnt.

Fehlermeldung

```
ENGINE_BUILD_SKIPPED: %s - there are no new signature
definitions for this engine
```

Erklärung Wird ausgegeben, wenn keine Signaturdefinitionen oder keine Änderungen an den bestehenden Signaturdefinitionen einer Einbruchserkennungssystem-SME vorliegen.

Fehlermeldung

```
ENGINE_READY: %s - %d ms - packets for this engine will be
scanned
```

Erklärung Wird ausgegeben, wenn eine IDS-SME erstellt wurde und zum Untersuchen der Pakete bereit ist.

Fehlermeldung

```
SDF_LOAD_SUCCESS: SDF loaded successfully from %s
```

Erklärung Wird ausgegeben, wenn eine SDF-Datei erfolgreich von einem angegebenen Speicherort ausgelesen wurde.

Fehlermeldung

```
BUILTIN_SIGS: %s to load builtin signatures
```

Erklärung Wird ausgegeben, wenn der Router zur Sicherheit die integrierten Signaturen lädt.

IDS Fehlermeldungen

Fehlermeldung

```
ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s
```

Erklärung Wird ausgegeben, wenn eine der Engines nach dem Laden einer SDF-Datei von Cisco IOS IPS nicht erstellt werden konnte. Für jeden Engine-Fehlschlag wird eine Meldung ausgegeben. Das bedeutet, dass die Cisco IOS IPS-Engine keine Signaturen für die in der Meldung angegebene Engine importieren konnte. Zu wenig Arbeitsspeicher ist der wahrscheinlichste Grund für dieses Problem. In diesem Fall lehnt Cisco IOS IPS die neu importierte Signatur ab, die von der betreffenden Engine stammt.

Fehlermeldung

```
SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d
```

Erklärung Wird ausgegeben, wenn eine SDF-Datei nicht korrekt interpretiert wurde.

Fehlermeldung

```
SDF_LOAD_FAILED: failed to %s SDF from %s
```

Erklärung Wird ausgegeben, wenn eine SDF-Datei aus irgendeinem Grund nicht geladen wurde.

Fehlermeldung

```
DISABLED: %s - IDS disabled
```

Erklärung IDS wurde deaktiviert. Die Meldung sollte den Grund hierfür angeben.

Fehlermeldung

```
SYSERROR: Unexpected error (%s) at line %d func %s() file %s
```

Erklärung Wird ausgegeben, wenn ein unerwarteter interner Systemfehler auftritt.

IPS bearbeiten: Globale Einstellungen

Einige Cisco IOS IPS-Konfigurationsoptionen sind auf Cisco IOS 12.4(11)T oder höher verfügbar. Diese werden in diesem Hilfethema erläutert. Vor Cisco IOS 12.4(11)T verfügbare Bildschirmsteuerungen und Konfigurationsoptionen, wie beispielsweise globale Einstellungen für Syslog und SDEE, werden in IPS bearbeiten: Globale Einstellungen erläutert.

Unter diesem Hilfethema wird das Fenster **Globale Einstellungen** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Engine-Optionen

Es gibt folgende in Cisco IOS 12.4(11)T und höheren Versionen verfügbare Abbilder:

- Fail-Closed – Standardmäßig berechnet die Cisco IOS für eine bestimmte Engine eine neue Signatur. Ohne eine Überprüfung der jeweiligen Engine werden die Pakete dabei durchgelassen. Bei Aktivieren dieser Option weist die Cisco IOS während des Berechnungsvorgangs alle Pakete zurück.
- **Verweigerung an der IPS-Schnittstelle** – Diese Option empfiehlt sich, wenn der Router einen Lastausgleich durchführt. Wenn diese Option eingeschaltet ist, aktiviert Cisco IOS IPS die ACLs auf den Cisco IOS IPS-Schnittstellen und nicht auf den Schnittstellen, über die der Datenverkehr mit den Angriffen eingetroffen ist.

Tabelle „IPS-Voraussetzungen“ bearbeiten

In dieser Tabelle werden Informationen darüber angezeigt, wie der Router für Cisco IOS IPS bereitgestellt wird. Klicken Sie zum Ändern der Werte auf **Bearbeiten**. Die Beispieldaten in der folgenden Tabelle geben an, dass der Konfigurationsspeicherort das Verzeichnis **configloc** im Flash-Speicher ist, dass der Router die Basiskategorie für Signaturen verwendet und dass ein öffentlicher Schlüssel so konfiguriert wurde, dass der Router Zugriff auf die Informationen im Verzeichnis **configloc** hat.

Elementname	Elementwert
Konfigurationsspeicherort	flash:/configloc/
Ausgewählte Kategorie:	Basis
Öffentlicher Schlüssel	Konfiguriert

Globale Einstellungen bearbeiten

Das Dialogfeld **Globale Einstellungen bearbeiten** enthält die Registerkarten **Syslog**, **SDEE** und **Global Engine**. Klicken Sie für weitere Informationen auf den nachstehenden Link:

- Registerkarten „Syslog“ und „SDEE“
- Registerkarte „Global Engine“

Registerkarten „Syslog“ und „SDEE“

In den Dialogfeldern **Syslog** und **SDEE**, die angezeigt werden, wenn der Router Cisco IOS 12.4(11)T oder höher ausführt, können Sie die Syslog-Benachrichtigung sowie Parameter für SDEE-Abonnements, Ereignisse und Meldungen konfigurieren.

Syslog-Benachrichtigung aktivieren

Aktivieren Sie dieses Kontrollkästchen, damit der Router Alarm-, Ereignis- und Fehlermeldungen an einen Syslog-Server weiterleitet. Um diese Benachrichtigungsmethode verwenden zu können, muss ein Syslog-Server in den **Systemeigenschaften** identifiziert werden.

SDEE

Tragen Sie die Anzahl der gleichzeitigen SDEE-Abonnements (Wertebereich 1 - 3) in das Feld **Anzahl der gleichzeitigen SDEE-Abonnements** ein. Mit einem SDEE-Abonnement werden SDEE-Ereignisse **live** empfangen.

Tragen Sie im Feld **Maximum number of SDEE alerts to store** (Maximale Anzahl zu speichernder SDEE-Warnungen) die Höchstzahl an SDEE-Warnmeldungen ein, die im Router gespeichert werden sollen. Werte zwischen 10 und 2000 sind zulässig. Zur Speicherung von noch mehr Warnmeldungen wird mehr Routerspeicher benötigt.

Tragen Sie im Feld **Maximum number of SDEE messages to store** (Maximale Anzahl zu speichernder SDEE-Meldungen) die Höchstzahl an SDEE-Meldungen ein, die im Router gespeichert werden sollen. Werte zwischen 10 und 500 sind zulässig. Zur Speicherung von noch mehr Meldungen wird mehr Routerspeicher benötigt.

Registerkarte „Global Engine“

Im Dialogfeld **Global Engine**, das angezeigt wird, wenn der Router Cisco IOS 12.4(11)T oder höher ausführt, können Sie die in den folgenden Abschnitten beschriebenen Einstellungen vornehmen.

Fail-Close-Engine aktivieren

Standardmäßig berechnet die Cisco IOS-Software für eine bestimmte Engine eine neue Signatur. Ohne eine Überprüfung der jeweiligen Engine werden die Pakete dabei durchgelassen. Aktivieren Sie diese Option, damit Pakete während der Signaturberechnung von der Cisco IOS-Software gelöscht werden.

Verweigerung an der IPS-Schnittstelle aktivieren

Diese Option ist anwendbar, wenn Signaturaktionen für **denyAttackerInline** oder **denyFlowInline** konfiguriert sind. Cisco IOS IPS wendet ACLs standardmäßig auf die Schnittstellen an, von denen ein Angriff gestartet wurde, und nicht auf Cisco IOS IPS-Schnittstellen. Wenn Sie diese Option aktivieren, wendet Cisco IOS IPS die ACLs direkt auf die Cisco IOS IPS-Schnittstellen an und nicht auf die Schnittstellen, welche die Datenpakete mit den Angriffen ursprünglich entgegengenommen haben. Wenn der Router keinen Lastausgleich durchführt, sollte diese Einstellung nicht aktiviert werden. Wenn der Router einen Lastausgleich durchführt, ist das Aktivieren dieser Einstellung zu empfehlen.

IPS-Voraussetzungen bearbeiten

Das Dialogfeld **IPS-Voraussetzungen bearbeiten** enthält Registerkarten für die folgenden Informationskategorien. Klicken Sie für weitere Informationen auf einen entsprechenden Link:

- Registerkarte „Konfigurationsspeicherort“
- Registerkarte „Kategorieauswahl“
- Registerkarte „Öffentlicher Schlüssel“

Registerkarte „Konfigurationsspeicherort“

Wenn ein Konfigurationsspeicherort auf dem Router konfiguriert wurde, können Sie diesen bearbeiten. Wenn kein Konfigurationsspeicherort konfiguriert wurde und Sie einen hinzufügen möchten, klicken Sie auf **Hinzufügen** und bearbeiten Sie diesen. Die Schaltfläche **Hinzufügen** ist deaktiviert, wenn bereits ein Konfigurationsspeicherort konfiguriert wurde. Die Schaltfläche **Bearbeiten** ist deaktiviert, wenn kein Konfigurationsspeicherort konfiguriert wurde. Weitere Informationen finden Sie unter IPS erstellen: Speicherort und Kategorie der Konfigurationsdatei.

Registerkarte „Kategorieauswahl“

Wenn Sie eine Signaturkategorie angeben, konfiguriert SDM den Router mit einem Teil der Signaturen entsprechend der verfügbaren Menge an Routerspeicher. Sie können auch eine bestehende Kategoriekonfiguration entfernen, wenn Sie bei der Auswahl von Signaturen Kategoriebeschränkungen entfernen möchten.

Kategorie konfigurieren

Klicken Sie auf **Kategorie konfigurieren** und wählen Sie entweder **Basis** oder **Erweitert** aus. Die Basiskategorie ist für Router mit weniger als 128 MB verfügbarem Flash-Speicher geeignet. Die erweiterte Kategorie ist für Router mit mehr als 128 MB verfügbarem Flash-Speicher geeignet.

Kategorie löschen

Wenn Sie eine Kategoriekonfiguration löschen möchten, klicken Sie auf **Kategorie löschen**.

Registerkarte „Öffentlicher Schlüssel“

In diesem Dialogfeld werden die für Cisco IOS IPS konfigurierten öffentlichen Schlüssel angezeigt. Sie können in diesem Dialogfeld Schlüssel hinzufügen oder löschen. Klicken Sie auf **Hinzufügen**, um einen Schlüssel hinzuzufügen, und konfigurieren Sie im angezeigten Dialogfeld die Kriterien ein.

Wählen Sie den Namen des Schlüssels aus, den Sie entfernen möchten, und klicken Sie auf **Löschen**.

Hinzufügen eines öffentlichen Schlüssels

Sie können den Namen des Schlüssels und den Schlüssel von der folgenden Seite auf Cisco.com kopieren:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Kopieren Sie den Namen des Schlüssels und fügen Sie ihn im Feld **Name** in diesem Dialogfeld ein. Kopieren Sie anschließend den Schlüssel vom selben Ort und fügen Sie ihn im Feld **Schlüssel** ein. Detaillierte Anweisungen dazu, welche Teile kopiert und eingefügt werden sollen, finden Sie unter Konfigurieren eines öffentlichen Schlüssels.

IPS bearbeiten: Autoaktualisierung

Aktualisierungen für Signaturdateien finden Sie auf Cisco.com. Cisco SDM kann eine von Ihnen angegebene Signaturdateiaktualisierung herunterladen oder Aktualisierungen automatisch in bestimmten zeitlichen Abständen herunterladen.

Unter diesem Hilfethema wird das Fenster **Autoaktualisierung** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Vor der Konfiguration der Autoaktualisierung

Bevor Sie die Autoaktualisierung konfigurieren, sollten Sie die Routeruhr mit der Uhr auf dem PC synchronisieren. Führen Sie dazu die folgenden Schritte aus:

Schritt 1 Gehen Sie zu **Konfigurieren > Zusätzliche Aufgaben > Router Eigenschaften > Datum/Zeit**.

Schritt 2 Klicken Sie im Fenster **Datum/Zeit** auf **Ändern Einstellungen**.

Schritt 3 Aktivieren Sie die Option **Mit meiner lokalen PC-Uhr synchronisieren**, und klicken Sie auf **Synchronisieren**.

Schritt 4 Schließen Sie das Dialogfeld.

Herunterladen der Signaturdatei von Cisco.com

Wenn Cisco SDM eine bestimmte Signaturdatei von Cisco.com auf Ihren PC herunterladen soll, geben Sie die Datei an, die Cisco SDM herunterladen soll, sowie den Speicherort, wo die Datei gespeichert werden soll. **Verwendetes Signaturpaket** gibt die derzeit vom Cisco IOS IPS verwendete Version an. Zum Herunterladen von Signaturdateien und zum Abrufen von anderen Informationen von den Cisco IOS IPS-Seiten auf Cisco.com ist eine CCO-Anmeldung erforderlich.

Klicken Sie zum Herunterladen der neuesten Signaturdatei auf **Neueste Datei abrufen**. Klicken Sie auf **Durchsuchen**, um festzulegen, wo die Datei gespeichert werden soll, und klicken Sie anschließend auf **Herunterladen**, um die Datei auf dem PC zu speichern.

Um vor dem Herunterladen die verfügbaren Dateien zu durchsuchen, klicken Sie auf **Verfügbare herunterzuladende Dateien auflisten**. Klicken Sie anschließend auf die Schaltfläche rechts neben dem Feld **Liste der Signaturpakete**. Klicken Sie im Kontextmenü auf **Aktualisieren**, um die Liste der verfügbaren Dateien zu durchsuchen. Klicken Sie auf **Readme anzeigen**, um die Readme-Datei zu lesen. Wählen Sie die gewünschte Datei aus, und speichern Sie sie mithilfe der Schaltflächen **Durchsuchen** und **Herunterladen** auf dem PC.

Autoaktualisierung

Klicken Sie auf **Autoaktualisierung aktivieren**, wenn Sie möchten, dass Cisco SDM automatisch Aktualisierungen von einem von Ihnen bestimmten Remote-Server abruft.

IPS-Autoaktualisierung – URL-Einstellungen

Geben Sie den für die Anmeldung beim Server erforderlichen Benutzernamen und das Kennwort ein. Geben Sie anschließend die URL ein, um die Datei im Feld **IPS-Autoaktualisierung – URL-Einstellungen** zu aktualisieren. Es folgt eine Beispiel-URL:

```
tftp//:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

Plan

Legen Sie einen Zeitplan fest, nach dem der Router Aktualisierungen vom Server abrufen soll. Sie können in jeder Spalte mehrere Werte eingeben, um einen Zeitbereich oder mehrere Zeitwerte anzugeben. Um festzulegen, dass von Sonntag bis Donnerstag täglich um 1.00 Uhr Aktualisierungen vom Server abgerufen werden sollen, legen Sie die Werte in der folgenden Tabelle fest.

Minute	Stunde	Datum	Tag
0	1	Wählen Sie 1 und 31.	Aktivieren Sie die Kontrollkästchen für Sonntag bis Donnerstag.

Zum Übertragen der Änderungen in den Autoaktualisierungsfeldern auf den Router klicken Sie auf **Änderungen übernehmen**. Klicken Sie auf **Änderungen verwerfen**, um die Daten, die Sie in die Felder eingegeben haben, zu löschen.

IPS bearbeiten: SEAP-Konfiguration

Cisco IOS IPS verfügbar mit Cisco IOS-Version 12.4(11)T oder höher implementiert Signature Event Action Processing (SEAP). In diesem Fenster werden die SEAP-Funktionen beschrieben, die Sie konfigurieren können. Um mit der Konfiguration zu beginnen, klicken Sie auf eine der Schaltflächen unterhalb der Schaltfläche **SEAP-Konfiguration**.

Sie können SEAP-Einstellungen Cisco IOS IPS vornehmen, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

IPS bearbeiten: SEAP-Konfiguration: Zielwertbewertung

Zielwertbewertung (Target Value Rating, TVR) ist ein benutzerdefinierter Wert, der den vom Benutzer wahrgenommenen Wert des Zielhosts repräsentiert. Dies ermöglicht es dem Benutzer, das Risiko eines Ereignisses zu erhöhen, das mit einem wichtigen System verbunden ist, und das Risiko eines Ereignisses auf einem Ziel niedrigen Werts zu vermindern.

Mithilfe der Schaltflächen neben den Spalten **Zielwertbewertung** und **Ziel-IP-Adresse** können Sie Zieleinträge hinzufügen, entfernen und bearbeiten. Klicken Sie auf **Alles auswählen**, um automatisch alle Zielwertbewertungen zu markieren. Klicken Sie auf **Hinzufügen**, um ein Dialogfeld anzuzeigen, in dem Sie einen neuen TVR-Eintrag erstellen können. Klicken Sie auf **Bearbeiten**, um IP-Adressinformationen für einen Eintrag zu ändern.

Spalte „Zielwertbewertung“

Ziele können als hoch, niedrig, mittel oder aufgabenkritisch eingestuft werden oder verfügen über keinen Wert. Sobald ein Zieleintrag erstellt wurde, kann die Bewertung nicht mehr geändert werden. Wenn Sie die Bewertung ändern müssen, löschen Sie den Zieleintrag und erstellen Sie ihn erneut mit der gewünschten Bewertung.

Spalte „Ziel-IP-Adresse“

Die Ziel-IP-Adresse kann aus einer einzelnen oder mehreren IP-Adressen bestehen. Das folgende Beispiel zeigt zwei Einträge. Einer enthält eine einzelne IP-Adresse, der andere einen Adressbereich.

Zielwertbewertung	Ziel-IP-Adresse
Hoch	192.168.33.2
mittel	10.10.3.1-10.10.3.55

Änderungen übernehmen

Wenn Sie die gewünschten Informationen im Fenster **Zielwertbewertung** eingegeben haben, klicken Sie auf **Änderungen übernehmen**. Die Schaltfläche **Änderungen übernehmen** ist deaktiviert, wenn keine Änderungen an den Router übertragen werden.

Änderungen verwerfen

Wenn Sie Informationen, die Sie im Fenster **Zielwertbewertung** eingegeben, aber nicht an den Router übertragen haben, löschen möchten, klicken Sie auf **Änderungen verwerfen**. Die Schaltfläche **Änderungen verwerfen** ist deaktiviert, wenn keine Änderungen vorgenommen wurden, die an den Router übertragen werden sollen.

Hinzufügen einer Zielwertbewertung

Wenn Sie einen TVR-Eintrag hinzufügen möchten, wählen Sie die Zielwertbewertung aus und geben Sie eine Ziel-IP-Adresse oder einen IP-Adressenbereich ein.

Zielwertbewertung (Target Value Rating, TVR)

Ziele können als hoch, niedrig, mittel oder aufgabenkritisch eingestuft werden oder verfügen über keinen Wert. Sobald eine Bewertung für einen Zieleintrag verwendet wurde, kann sie nicht für weitere verwendet werden. Geben Sie daher alle Ziele, die Sie mit derselben Bewertung versehen möchten, in einen Eintrag ein.

Ziel-IP-Adressen

Sie können wie im folgenden Beispiel gezeigt eine einzelne Ziel-IP-Adresse oder einen Adressenbereich eingeben:

```
192.168.22.33
10.10.11.4-10.10.11.55
```

Die von Ihnen eingegebenen IP-Adressen werden im Fenster **Zielwertbewertung** angezeigt.

IPS bearbeiten: SEAP-Konfiguration: Ereignisaktions-Overrides

Ereignisaktions-Overrides ermöglichen es Ihnen, auf der Basis der Risikobewertung (Risk Rating, RR) eines Ereignisses die mit dem Ereignis verknüpften Aktionen zu ändern. Weisen Sie dazu einen RR-Bereich für jede Ereignisaktion zu. Wenn ein Ereignis eintritt, dessen RR innerhalb des von Ihnen definierten Bereichs liegt, wird diese Aktion zum Ereignis hinzugefügt. Ereignisaktions-Overrides sind eine Möglichkeit, Ereignisaktionen global hinzuzufügen, ohne jede Signatur einzeln konfigurieren zu müssen.

Ereignisaktions-Overrides verwenden

Aktivieren Sie das Kontrollkästchen **Ereignisaktions-Overrides verwenden** für Cisco IOS IPS. Sie können Ereignisaktions-Overrides auch dann hinzufügen und bearbeiten, wenn sie nicht auf dem Router aktiviert sind.

Alles auswählen

Die Schaltfläche **Alles auswählen** funktioniert mit den Schaltflächen **Aktivieren**, **Deaktivieren** und **Löschen**. Wenn Sie alle Ereignisaktions-Overrides aktivieren oder deaktivieren möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Aktivieren** oder **Deaktivieren**. Wenn Sie alle Ereignisaktions-Overrides löschen möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Löschen**.

Schaltflächen „Hinzufügen“ und „Bearbeiten“

Klicken Sie auf **Hinzufügen**, um ein Dialogfeld anzuzeigen, in dem Sie Informationen für ein Ereignisaktions-Override eingeben können. Wählen Sie ein Ereignisaktions-Override aus und klicken Sie auf **Bearbeiten**, um die Informationen für ein Ereignisaktions-Override zu ändern.

Löschen

Wenn Sie die ausgewählten oder alle (nach Klicken auf **Alles auswählen**) Ereignisaktions-Overrides löschen möchten, klicken Sie auf **Löschen**.

Aktivieren und Deaktivieren

Mit den Schaltflächen **Aktivieren** und **Deaktivieren** können Sie Ereignisaktions-Overrides aktivieren oder deaktivieren. Wählen Sie dazu ein Ereignisaktions-Override aus oder klicken Sie zum Aktivieren oder Deaktivieren aller Ereignisaktions-Overrides auf **Alles auswählen**.

Änderungen übernehmen

Wenn Sie die gewünschten Informationen im Fenster **Ereignisaktions-Overrides** eingegeben haben, klicken Sie auf **Änderungen übernehmen**. Die Schaltfläche **Änderungen übernehmen** ist deaktiviert, wenn keine Änderungen an den Router übertragen werden.

Änderungen verwerfen

Wenn Sie Informationen, die Sie im Fenster **Ereignisaktions-Override** eingegeben, aber nicht an den Router übertragen haben, löschen möchten, klicken Sie auf **Änderungen verwerfen**. Die Schaltfläche **Änderungen verwerfen** ist deaktiviert, wenn keine Änderungen vorgenommen wurden, die an den Router übertragen werden sollen.

Hinzufügen oder Bearbeiten von Ereignisaktions-Overrides

Wählen Sie eine Ereignisaktion aus, aktivieren bzw. deaktivieren Sie diese und geben Sie den RR-Bereich an. Bei der Bearbeitung kann die Ereignisaktion nicht geändert werden.

Ereignisaktion

Wählen Sie eine der nachfolgend aufgeführten Ereignisaktionen aus:

- Deny Attacker Inline – Dieses und zukünftige Pakete werden eine bestimmte Zeit lang nicht von der Angreiferadresse weitergeleitet (nur inline).
- Deny Connection Inline – Das aktuelle Paket sowie nachfolgende Pakete werden nicht über diesen TCP-Port weitergeleitet (nur inline).
- Deny Packet Inline – Das betreffende Paket wird nicht weitergeleitet.
- Produce Alert – Schreibt eine <evIdsAlert> in das Protokoll.
- Reset TCP Connection – Schickt TCP RESET-Signale abschicken, um den Datenfluss über den TCP-Port zu unterbinden.

Aktiviert

Klicken Sie zum Aktivieren des Ereignisaktions-Overrides auf **Ja** und zum Deaktivieren auf **Nein**. Sie können Ereignisaktions-Overrides auch im Fenster **Ereignisaktions-Overrides** aktivieren oder deaktivieren.

Risikobewertung

Geben Sie die untere Grenze des RR-Bereichs in das Feld **Min** und die obere Grenze in das Feld **Max** ein. Wenn der RR-Wert eines Ereignisses innerhalb des von Ihnen definierten Bereichs liegt, fügt Cisco IOS IPS das von der Ereignisaktion festgelegte Override hinzu. Wenn beispielsweise Deny Connection Inline ein RR-Bereich von 90 – 100 zugewiesen wurde und ein Ereignis mit einem Wert von 95 eintritt, reagiert das Cisco IOS IPS mit einer Inline-Verweigerung der Verbindung.

IPS bearbeiten: SEAP-Konfiguration: Ereignisaktionsfilter

Ereignisaktionsfilter ermöglichen es dem Cisco IOS IPS, einzelne Aktionen als Reaktion auf Ereignisse durchzuführen, ohne dass alle Aktionen durchgeführt oder das gesamte Ereignis gelöscht werden muss. Mithilfe von Filtern werden Aktionen aus einem Ereignis entfernt. Ein Filter, mit dem alle Aktionen entfernt werden, löscht praktisch das Ereignis. Ereignisaktionsfilter werden als geordnete Liste verarbeitet. Sie können Filter in der Liste nach unten oder oben verschieben, sodass der Router einen Filter vor oder nach einem anderen verarbeitet.

Im Fenster **Ereignisaktionsfilter** werden die konfigurierten Ereignisaktionsfilter angezeigt. Außerdem kann in diesem Fenster die Filterliste neu sortiert werden, sodass Cisco IOS IPS die Filter in der von Ihnen gewünschten Reihenfolge verarbeitet.

Ereignisaktionsfilter verwenden

Aktivieren Sie das Kontrollkästchen **Ereignisaktionsfilter verwenden**, um Ereignisaktionsfilter zu verwenden. Sie können Ereignisaktionsfilter hinzufügen, bearbeiten und löschen. Außerdem können Sie die Liste umsortieren und selbst die Reihenfolge festlegen, in welcher der Router die Filter bearbeitet, unabhängig davon, ob Ereignisaktionsfilter aktiviert sind oder nicht.

Bereich der Ereignisaktionsfilter-Liste

Eine Beschreibung der Spalten im Bereich der Ereignisaktionsfilter-Liste finden Sie unter Hinzufügen oder Bearbeiten eines Ereignisaktionsfilters.

Schaltflächen der Ereignisaktionsfilter-Liste

Mit den Schaltflächen der Ereignisaktionsfilter-Liste können Sie Ereignisaktionsfilter erstellen, bearbeiten und löschen, sowie jeden Ereignisaktionsfilter an der gewünschten Stelle in der Liste platzieren. Die Schaltflächen werden in den folgenden Abschnitten beschrieben.

Alles auswählen

Die Schaltfläche **Alles auswählen** funktioniert mit den Schaltflächen **Aktivieren**, **Deaktivieren** und **Löschen**. Klicken Sie zum Aktivieren oder Deaktivieren aller Ereignisaktionsfilter auf **Alles auswählen** und anschließend auf **Aktivieren** bzw. **Deaktivieren**. Wenn Sie alle Ereignisaktionsfilter löschen möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Löschen**.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um einen Ereignisaktionsfilter am Ende der Liste hinzuzufügen. Im daraufhin angezeigten Dialogfeld können sie Daten für den Filter eingeben.

Davor einfügen

Wenn Sie einen neuen Ereignisaktionsfilter vor einem bestehenden einfügen möchten, wählen Sie den bestehenden Filter aus und klicken Sie auf **Davor einfügen**. Im daraufhin angezeigten Dialogfeld können Sie Daten für den Filter eingeben.

Dahinter einfügen

Wenn Sie einen neuen Ereignisaktionsfilter hinter einem bestehenden einfügen möchten, wählen Sie den bestehenden Filter aus und klicken Sie auf **Dahinter einfügen**. Im daraufhin angezeigten Dialogfeld können Sie Daten für den Filter eingeben.

Nach oben

Wählen Sie einen Ereignisaktionsfilter aus und klicken Sie auf **Nach oben**, um den Filter in der Liste nach oben zu verschieben.

Nach unten

Wählen Sie einen Ereignisaktionsfilter aus und klicken Sie auf **Nach unten**, um den Filter in der Liste nach unten zu verschieben.

Bearbeiten

Klicken Sie zum Bearbeiten eines ausgewählten Ereignisaktionsfilters auf **Bearbeiten**.

Aktivieren

Klicken Sie zum Aktivieren eines ausgewählten Ereignisaktionsfilters auf **Aktivieren**. Wenn Sie alle Ereignisaktionsfilter aktivieren möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Aktivieren**.

Deaktivieren

Klicken Sie zum Deaktivieren eines ausgewählten Ereignisaktionsfilters auf **Deaktivieren**. Wenn Sie alle Ereignisaktionsfilter deaktivieren möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Deaktivieren**.

Löschen

Klicken Sie zum Löschen eines ausgewählten Ereignisaktionsfilters auf **Löschen**. Wenn Sie alle Ereignisaktionsfilter löschen möchten, klicken Sie auf **Alles auswählen** und anschließend auf **Löschen**.

Änderungen übernehmen

Wenn Sie die gewünschten Informationen in diesem Fenster eingegeben haben, klicken Sie auf **Änderungen übernehmen**. Die Schaltfläche **Änderungen übernehmen** ist deaktiviert, wenn keine Änderungen an den Router übertragen werden.

Änderungen verwerfen

Wenn Sie Informationen, die Sie in diesem Fenster eingegeben, aber nicht an den Router übertragen haben, löschen möchten, klicken Sie auf **Änderungen verwerfen**. Die Schaltfläche **Änderungen verwerfen** ist deaktiviert, wenn keine Änderungen vorgenommen wurden, die an den Router übertragen werden sollen.

Hinzufügen oder Bearbeiten eines Ereignisaktionsfilters

Die folgenden Informationen beschreiben die Felder in den Dialogfeldern **Ereignisaktionsfilter hinzufügen** und **Ereignisaktionsfilter bearbeiten**.

Name

SDM enthält Ereignisaktionsfilter-Namen, die mit Q00000 beginnen und bei jedem Hinzufügen eines Ereignisaktionsfilters um 1 ansteigen. Sie können auch einen selbst gewählten Namen eingeben. Wenn Sie einen Ereignisaktionsfilter bearbeiten, ist das Namensfeld schreibgeschützt.

Aktiviert

Klicken Sie zum Aktivieren des Ereignisaktionsfilter auf **Ja** und zum Deaktivieren auf **Nein**. Sie können Ereignisaktionsfilter auch im Fenster **Ereignisaktionsfilter** aktivieren oder deaktivieren.

Signatur-ID

Geben Sie als Signatur-ID einen Signatur-ID-Bereich von 900 bis 65535 oder eine einzelne ID innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 988-5000 ein.

Subsignatur-ID

Geben Sie als Subsignatur-ID einen Subsignatur-ID-Bereich von 0 bis 255 oder eine einzelne Subsignatur-ID innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 70-200 ein.

Hacker-Adresse

Geben Sie als Hacker-Adresse einen Adressenbereich von 0.0.0.0 bis 255.255.255.255 oder eine einzelne Adresse innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 192.168.7.0-192.168.50.0 ein.

Hacker-Port

Geben Sie als Hacker-Port einen Bereich von 0 bis 65535 oder eine einzelne Port-Nummer innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 988-5000 ein.

Opfer-Adresse

Geben Sie als Opfer-Adresse einen Adressenbereich von 0.0.0.0 bis 255.255.255.255 oder eine einzelne Adresse innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 192.168.7.0-192.168.50.0 ein.

Opfer-Port

Geben Sie als Opfer-Port einen Bereich von 0 bis 65535 oder eine einzelne Port-Nummer innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 988-5000 ein.

Risikobewertung

Geben Sie als Risikobewertung einen RR-Bereich zwischen 0 und 100 ein.

Abzuziehende Aktionen

Klicken Sie auf die Aktionen, die Sie von übereinstimmenden Ereignissen abziehen möchten. Wenn Sie mehr als eine Aktion von übereinstimmenden Ereignissen abziehen möchten, halten Sie die **Strg**-Taste gedrückt und wählen Sie weitere Ereignisse aus. Alle für diesen Filter ausgewählten Ereignisse werden im Fenster **Ereignisaktionsfilter** angezeigt.

Bei Übereinstimmung stoppen

Wenn Sie möchten, dass das Cisco IOS IPS stoppt, wenn ein Ereignis mit diesem Ereignisaktionsfilter übereinstimmt, klicken Sie auf **Ja**. Wenn Sie möchten, dass das Cisco IOS IPS übereinstimmende Ereignisse mit anderen Filtern vergleicht, klicken Sie auf **Nein**.

Bemerkungen

Sie können Bemerkungen zur näheren Beschreibung des Zwecks dieses Filters hinzufügen. Dieses Feld ist optional.

IPS bearbeiten: Signaturen

Cisco IOS IPS schützt vor Netzwerkpenetration, indem es die Kommunikationsdaten mit den Signaturen von bekannten Attacken vergleicht. Cisco IOS-Abbilder, die Cisco IOS IPS unterstützen, verfügen über integrierte Signaturen. Sie können Cisco IOS IPS auch so einstellen, dass Signaturen beim Untersuchen des Datenverkehrs für die Verwendung im Router importiert werden. Importierte Signaturen sind in einer SDF-Datei (Signature Definition File) gespeichert.

Dieses Fenster zeigt die konfigurierten Cisco IOS IPS-Signaturen auf dem Router an. Sie können speziell angepasste Signaturen hinzufügen oder Signaturen aus SDFs importieren, die Sie bei Cisco.com herunterladen können. Sie können Signaturen auch bearbeiten, löschen, aktivieren und deaktivieren.

Die mit Cisco IOS IPS gelieferte SDF-Datei enthält eine Reihe von Signaturen zur Speicherung in Ihrem Router. Um mehr über die SDF-Datei zu erfahren, die der Cisco IOS IPS beiliegt, und wie Cisco IOS IPS dazu gebracht werden kann, die Datei zu nutzen, klicken Sie auf Mitgelieferte IPS-Signaturdefinitionsdateien.

Signaturbaum

Der Signaturbaum ermöglicht Ihnen die Filterung der Signaturliste auf der rechten Seite nach dem Signaturtyp, den Sie anzeigen möchten. Wählen Sie als erstes das Unterverzeichnis des allgemeinen Signaturtyps aus, den Sie anschauen wollen. Die Signaturliste zeigt die konfigurierten Signaturen des ausgewählten Typs. Wenn ein Pluszeichen (+) links vom Zweig erscheint, gibt es Unterkategorien, die Sie zur Redefinition des Filters benötigen. Klicken Sie auf das Pluszeichen, um weiter zu verzweigen, und wählen Sie anschließend die Signaturunterkategorie aus, die Sie anschauen wollen. Wenn die Signaturliste leer ist, stehen für diesen Typ keine konfigurierten Signaturen zur Verfügung.

Beispiel: Wenn Sie alle Angriffssignaturen anzeigen wollen, klicken Sie auf die Ordnerverzweigung **Angriff**. Wenn Sie die Unterkategorien sehen wollen, die Sie zur Filterung der Angriffssignaturen einsetzen können, klicken Sie auf das +-Zeichen neben dem Ordner Angriff. Wenn Sie die DoS-Signaturen (Denial of Service) anzeigen wollen, klicken Sie auf den Ordner **DoS**.

Schaltfläche Importieren

Klicken Sie darauf, um eine Signaturdefinitionsdatei vom PC oder vom Router zu importieren. Wenn Sie die Datei angegeben haben, zeigt Cisco IOS IPS die in dieser Datei enthaltenen Signaturen an. Sie können diejenigen auswählen, die Sie an den Router senden möchten. Weitere Informationen über die Auswahl der zu importierenden Signaturen finden Sie unter Signaturen importieren.

Hinweis Sie können Signaturen vom Router nur importieren, wenn der Router über ein DOS-basiertes Dateisystem verfügt.

SDFs stehen bei Cisco zur Verfügung. Klicken Sie auf die nachfolgende URL, um eine SDF von Cisco.com herunterzuladen (Anmeldung erforderlich):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco unterhält ein Alarm-Center, das Informationen zu plötzlich entstehenden Bedrohungen liefert. Weitere Informationen finden Sie unter Cisco Security Center.

View By (Anzeigen nach) und Kriterienliste

Anhand der Dropdown-Listen **View by** (Anzeige nach) und **Kriterienliste** können Sie festlegen, welche Signaturtypen Sie anzeigen lassen möchten und die Einträge dementsprechend filtern. Wählen Sie zuerst die Kriterien aus der Dropdown-Liste **View by** (Anzeige nach) aus und anschließend den Wert für das betreffende Kriterium in der Dropdown-Liste **Kriterien**.

Beispiel: Wenn Sie unter **View by** (Anzeige nach) die Option **Engine** auswählen, wird der Eintrag **Engine** unter **Kriterien** übernommen. Sie haben anschließend die freie Auswahl aus den verfügbaren Engines, z. B. **Atomic.ICMP** und **Service.DNS**.

Wenn Sie **Sig- ID** oder **Sig-Name** auswählen, müssen Sie im Feld **Kriterien** einen Wert eingeben.

Gesamt [*n*] Neu [*n*] Gelöscht [*n*]

Dieser Text gibt die Anzahl der neuen Signaturen und der gelöschten Signaturen an.

Alles auswählen

Klicken Sie auf diese Option, um alle Signaturen in der Liste auszuwählen.

Hinzufügen

Klicken Sie auf **Hinzufügen**, wenn Sie einen der folgenden Schritte ausführen möchten:

- **Neu Hinzufügen** – Wählen Sie diese Option aus, wenn Sie eine neue Signatur hinzufügen möchten. Legen Sie anschließend die Signaturparameter im angezeigten Dialogfeld fest.
- **Klonen** – Diese ist bei Angabe einer Signatur aktiviert, die nicht zu einer fest programmierten Engine gehört. Sie ist deaktiviert, wenn die Signatur eine der fest programmierten Engines verwendet, die in Cisco IOS enthalten sind.

Bearbeiten

Klicken Sie darauf, um die Parameter der angegebenen Signatur zu bearbeiten.

Löschen

Klicken Sie auf **Löschen**, um die angegebene Signatur zum Löschen aus der Liste zu markieren. Um Signaturen anzuzeigen, die Sie gelöscht haben, klicken Sie auf **Details**. Weitere Informationen zum Status und zum Umgang mit diesen Signaturen, finden Sie unter Zum Löschen markierte Signaturen.

Hinweis Sie können TrendMicro OPACL Signaturen anzeigen und überwachen, jedoch nicht bearbeiten, löschen, aktivieren oder deaktivieren. Wenn eine TrendMicro OPACL Signatur ausgewählt wurde, sind die Schaltflächen **Bearbeiten**, **Löschen**, **Aktivieren** und **Deaktivieren** inaktiv. Der Cisco Incident Control Server übernimmt die Steuerung dieser Signaturen.

Aktivieren

Klicken Sie auf **Aktivieren**, um die angegebene Signatur zu aktivieren. Eine aktivierte Signatur ist mit einem grünen Häkchen versehen. Eine Signatur, die deaktiviert war und später aktiviert wurde, ist mit einem gelben Wartesymbol in der Spalte **!** angezeigt, das angibt dass die Änderung im Router übernommen werden muss.

Deaktivieren

Klicken Sie auf **Deaktivieren**, um die angegebene Signatur zu deaktivieren. Eine deaktivierte Signatur ist mit einem roten Symbol versehen. Wenn die Signatur während der aktuellen Sitzung deaktiviert wird, wird ein gelbes Wartesymbol in der Spalte **!** angezeigt, das angibt dass die Änderung im Router übernommen werden muss.

Schaltfläche „Übersicht“ oder „Details“

Klicken Sie darauf, um Signaturen, die zum Löschen markiert sind, ein- oder auszublenden.

Signaturliste

Zeigt die Signaturen an, die vom Router empfangen wurden, sowie alle Signaturen, die von einer SDF hinzugefügt wurden.

Hinweis Signaturen, die nicht auf Importieren eingestellt sind und die mit den bereits geladenen Signaturen übereinstimmen, werden nicht importiert und erscheinen auch nicht in der Signaturliste.

Die Signaturliste kann über die Auswahlsteuerelemente gefiltert werden.

Aktiviert	Aktiviert Signaturen, die durch ein grünes Symbol markiert sind. Wenn diese Option aktiviert ist, werden die angegebenen Aktionen ausgeführt, wenn die Signatur erkannt wird. Deaktiviert Signaturen, die durch ein rotes Symbol markiert sind. Wenn diese Option deaktiviert ist, werden die Aktionen deaktiviert und nicht ausgeführt.
Alarm (!)	Diese Spalte kann das gelbe Wartesymbol enthalten.  Dieses Symbol kennzeichnet neue Signaturen, die nicht an den Router gesendet wurden, oder geänderte Signaturen, die nicht an den Router gesendet wurden.
Sig-ID	Numerische Signatur-ID. Beispiel: Die Sig-ID für ICMP Echo Reply lautet beispielsweise 2000.
SubSig-ID	ID der untergeordneten Signatur.
Name	Der Signaturname. Beispiel: ICMP Echo Reply.
Aktion	Die auszuführende Aktion, wenn die Signatur erkannt wird.
Filter	Eine ACL, die mit der entsprechenden Signatur verknüpft ist.
Schweregrad	Der Schweregrad des Ereignisses. Schweregrade sind Informationsbezogen, Niedrig, Mittel und Hoch.
Suchmaschi-ne	Die Engine, zu der die Signatur gehört.

Kontextmenü über die rechte Maustaste

Wenn Sie mit der rechten Maustaste auf eine Signatur klicken, zeigt Cisco SDM ein Kontextmenü mit folgenden Optionen an:

- **Aktionen** – Klicken Sie hier, um die Aktionen auszuwählen, die bei einer Übereinstimmung mit der Signatur ausgeführt werden sollen. Weitere Informationen finden Sie unter Aktionen zuweisen.
- **Schweregrad einstellen auf** – Klicken Sie hier, um den Schweregrad einer Signatur auf diese Stufen einzustellen: Hoch, Mittel, Niedrig oder Informationsbezogen.
- **Standards wiederherstellen** – Klicken Sie hier, um die Standardwerte der Signatur wiederherzustellen.

- **Filter entfernen** – Klicken Sie hier, um einen auf die Signatur angewendeten Filter zu entfernen.
- **NSDB-Hilfe** (CCO-Konto erforderlich) – Klicken Sie hier, um die Hilfe der Network Security Data Base (NSDB) anzuzeigen.

Zum Löschen markierte Signaturen

Dieser Bereich wird angezeigt, wenn auf die Schaltfläche **Details** geklickt wird. Darin werden die Signaturen aufgelistet, die Sie aus der Signaturliste gelöscht haben, sowie alle zur Löschung markierten Signaturen, weil festgelegt wurde, dass beim Import von Signaturen die bereits im Router konfigurierten zu ersetzen sind. Weitere Informationen finden Sie unter So importieren Sie Signaturen.

Die Option **Zum Löschen markierte Signaturen** bleibt in der Cisco IOS IPS-Konfiguration aktiviert, bis Sie auf **Änderungen übernehmen** klicken. Wenn Sie das Fenster **Signaturen** schließen und Cisco IOS IPS deaktivieren, werden die markierten Signaturen gelöscht, wenn Cisco IOS IPS erneut aktiviert wird.

Schaltfläche Alle wiederherstellen

Klicken Sie darauf, um alle Signaturen wiederherzustellen, die in der Liste der zum Löschen markierten Signaturen eingetragen sind.

Schaltfläche Wiederherstellen

Klicken Sie darauf, um bestimmte Signaturen wiederherzustellen, die zum Löschen markiert sind. Wenn Sie auf diese Schaltfläche klicken, wird die Markierung der Signaturen aufgehoben, und sie erscheinen wieder in der Liste der aktiven Signaturen.

Schaltfläche „Änderungen übernehmen“

Klicken Sie auf diese Schaltfläche, um neu importierte Signaturen, Änderungen an Signaturen und neu aktivierte oder deaktivierte Signaturen an den Router zu senden. Wenn die Änderungen übernommen werden, wird das gelbe Wartesymbol aus der Spalte **!** entfernt. Diese Änderungen werden im Flash-Memory des Routers in der Datei sdmips.sdf gespeichert. Beim ersten Mausklick auf **Änderungen übernehmen** wird diese Datei automatisch angelegt.

Hinweis Beim Import von Signaturen , die mit den bereits geladenen Signaturen ausnahmslos identisch sind, ist die Schaltfläche **Änderungen übernehmen** deaktiviert.

Schaltfläche „Änderungen nicht übernehmen“

Klicken Sie auf diese Schaltfläche, um die vorgenommenen Änderungen nicht zu übernehmen.

Hinweis Beim Import von Signaturen, die mit den bereits geladenen Signaturen ausnahmslos identisch sind, ist die Schaltfläche **Änderungen verwerfen** deaktiviert.

Opfer-Port

Geben Sie als Opfer-Port einen Bereich von 0 bis 65535 oder eine einzelne Port-Nummer innerhalb dieses Bereichs ein. Wenn Sie einen Bereich eingeben, trennen Sie die Unter- und Obergrenze des Bereichs durch ein Minuszeichen (-) voneinander. Geben Sie beispielsweise 988-5000 ein.

Risikobewertung

Geben Sie als Risikobewertung einen RR-Bereich zwischen 0 und 100 ein.

Abzuziehende Aktionen

Klicken Sie auf die Aktionen, die Sie von übereinstimmenden Ereignissen abziehen möchten. Wenn Sie mehr als eine Aktion von übereinstimmenden Ereignissen abziehen möchten, halten Sie die **Strg**-Taste gedrückt und wählen Sie weitere Ereignisse aus. Alle für diesen Filter ausgewählten Ereignisse werden im Fenster **Ereignisaktionsfilter** angezeigt.

Bei Übereinstimmung stoppen

Wenn Sie möchten, dass das Cisco IOS IPS stoppt, wenn ein Ereignis mit diesem Ereignisaktionsfilter übereinstimmt, klicken Sie auf **Ja**. Wenn Sie möchten, dass das Cisco IOS IPS übereinstimmende Ereignisse mit anderen Filtern vergleicht, klicken Sie auf **Nein**.

Bemerkungen

Sie können Bemerkungen zur näheren Beschreibung des Zwecks dieses Filters hinzufügen. Dieses Feld ist optional.

IPS bearbeiten: Signaturen

Cisco IOS IPS schützt vor Netzwerkpenetration, indem es die Kommunikationsdaten mit den Signaturen von bekannten Attacken vergleicht. Cisco IOS-Abbilder, die Cisco IOS IPS unterstützen, verfügen über integrierte Signaturen, von denen Cisco IOS IPS Gebrauch machen kann. Sie können Cisco IOS IPS auch so einstellen, dass Signaturen beim Untersuchen des Datenverkehrs für die Verwendung im Router importiert werden. Importierte Signaturen sind in einer SDF-Datei (Signature Definition File) gespeichert.

Unter diesem Hilfethema wird das Fenster **Signaturen** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Das Fenster **Signaturen** zeigt die konfigurierten Cisco IOS IPS-Signaturen auf dem Router an. Sie können speziell angepasste Signaturen hinzufügen oder Signaturen aus SDFs importieren, die Sie bei Cisco.com herunterladen können. Sie können Signaturen auch bearbeiten, aktivieren, deaktivieren, ausschließen oder erneut aktivieren.

Signaturbaum

Der Signaturbaum ermöglicht Ihnen die Filterung der Signaturliste auf der rechten Seite nach dem Signaturtyp, den Sie anzeigen möchten. Wählen Sie als erstes das Unterverzeichnis des allgemeinen Signaturtyps aus, den Sie anschauen wollen. Die Signaturliste zeigt die konfigurierten Signaturen des ausgewählten Typs. Wenn ein Pluszeichen (+) links vom Zweig erscheint, gibt es Unterkategorien, die Sie zur Redefinition des Filters benötigen. Klicken Sie auf das Pluszeichen, um weiter zu verzweigen, und wählen Sie anschließend die Signaturunterkategorie aus, die Sie anschauen wollen. Wenn die Signaturliste leer ist, stehen für diesen Typ keine konfigurierten Signaturen zur Verfügung.

Beispiel: Wenn Sie alle Angriffssignaturen anzeigen wollen, klicken Sie auf die Ordnerverzweigung **Angriff**. Wenn Sie die Unterkategorien sehen wollen, die Sie zur Filterung der Angriffssignaturen einsetzen können, klicken Sie auf das +-Zeichen neben dem Ordner Angriff. Wenn Sie die DoS-Signaturen (Denial of Service) anzeigen wollen, klicken Sie auf den Ordner **DoS**.

Schaltfläche Importieren

Klicken Sie darauf, um eine Signaturdefinitionsdatei vom PC oder vom Router zu importieren. Wenn Sie die Datei angegeben haben, zeigt Cisco IOS IPS die in dieser Datei enthaltenen Signaturen an. Sie können diejenigen auswählen, die Sie an den Router senden möchten. Weitere Informationen über die Auswahl der zu importierenden Signaturen finden Sie unter Signaturen importieren.

Hinweis Sie können Signaturen vom Router nur importieren, wenn der Router über ein DOS-basiertes Dateisystem verfügt.

SDFs stehen bei Cisco zur Verfügung. Klicken Sie auf die nachfolgende URL, um eine SDF von Cisco.com herunterzuladen (Anmeldung erforderlich):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco unterhält ein Alarm-Center, das Informationen zu plötzlich entstehenden Bedrohungen liefert. Weitere Informationen finden Sie unter Cisco Security Center.

View By (Anzeigen nach) und Kriterienliste

Anhand der Dropdown-Listen **View by** (Anzeige nach) und **Kriterienliste** können Sie festlegen, welche Signaturtypen Sie anzeigen lassen möchten und die Einträge dementsprechend filtern. Wählen Sie zuerst die Kriterien aus der Dropdown-Liste **View by** (Anzeige nach) aus und anschließend den Wert für das betreffende Kriterium in der Dropdown-Liste **Kriterien**.

Beispiel: Wenn Sie unter **View by** (Anzeige nach) die Option **Engine** auswählen, wird der Eintrag **Engine** unter **Kriterien** übernommen. Sie haben anschließend die freie Auswahl aus den verfügbaren Engines, z. B. **Atomic.ICMP** und **Service.DNS**.

Wenn Sie **Sig- ID** oder **Sig-Name** auswählen, müssen Sie im Feld **Kriterien** einen Wert eingeben.

Gesamt [*n*]

Dieser Text gibt die Gesamtzahl der Signaturen auf dem Router an.

Alles auswählen

Klicken Sie auf diese Option, um alle Signaturen in der Liste auszuwählen.

View By (Anzeigen nach) und Kriterienliste

Anhand der Dropdown-Listen **View by** (Anzeige nach) und **Kriterienliste** können Sie festlegen, welche Signaturtypen Sie anzeigen lassen möchten und die Einträge dementsprechend filtern. Wählen Sie zuerst die Kriterien aus der Dropdown-Liste **View by** (Anzeige nach) aus und anschließend den Wert für das betreffende Kriterium in der Dropdown-Liste **Kriterien**.

Beispiel: Wenn Sie unter **View by** (Anzeige nach) die Option **Engine** auswählen, wird der Eintrag **Engine** unter **Kriterien** übernommen. Sie haben anschließend die freie Auswahl aus den verfügbaren Engines, z. B. **Atomic.ICMP** und **Service.DNS**.

Wenn Sie **Sig- ID** oder **Sig-Name** auswählen, müssen Sie im Feld **Kriterien** einen Wert eingeben.

Gesamt [*n*]

Dieser Text gibt die Gesamtzahl der Signaturen auf dem Router an.

Alles auswählen

Klicken Sie auf diese Option, um alle Signaturen in der Liste auszuwählen.

Deaktivieren

Klicken Sie auf **Deaktivieren**, um die angegebene Signatur zu deaktivieren. Eine deaktivierte Signatur ist mit einem roten Symbol versehen. Wenn die Signatur während der aktuellen Sitzung deaktiviert wird, wird ein gelbes Wartesymbol in der Spalte **!** angezeigt, das angibt dass die Änderung im Router übernommen werden muss.

Retire (Ausgeschieden)

Klicken Sie auf **Retire (Ausgeschieden)**, um zu verhindern, dass eine Signatur zum Scannen kompiliert wird.

Unretire (Erneut aktivieren)

Klicken Sie auf **Unretire (Erneut aktivieren)**, um zu erlauben, dass eine Signatur zum Scannen kompiliert wird.

Signaturliste

Zeigt die Signaturen an, die vom Router empfangen wurden, sowie alle Signaturen, die von einer SDF hinzugefügt wurden.

Hinweis Signaturen, die nicht auf Importieren eingestellt sind und die mit den bereits geladenen Signaturen übereinstimmen, werden nicht importiert und erscheinen auch nicht in der Signaturliste.

Die Signaturliste kann über die Auswahlsteuerelemente gefiltert werden.

Aktiviert	Aktiviert Signaturen, die durch ein grünes Symbol markiert sind. Wenn diese Option aktiviert ist, werden die angegebenen Aktionen ausgeführt, wenn die Signatur erkannt wird. Deaktiviert Signaturen, die durch ein rotes Symbol markiert sind. Wenn diese Option deaktiviert ist, werden die Aktionen deaktiviert und nicht ausgeführt.
Alarm (!)	Diese Spalte kann das gelbe Wartesymbol enthalten. Dieses Symbol kennzeichnet neue Signaturen, die nicht an den Router gesendet wurden, oder geänderte Signaturen, die nicht an den Router gesendet wurden.
Sig-ID	Numerische Signatur-ID. Beispiel: Die Sig-ID für ICMP Echo Reply lautet beispielsweise 2000.
SubSig-ID	ID der untergeordneten Signatur.
Name	Der Signaturname. Beispiel: ICMP Echo Reply.
Aktion	Die auszuführende Aktion, wenn die Signatur erkannt wird.
Schweregrad	Der Schweregrad des Ereignisses. Schweregrade sind Informationsbezogen, Niedrig, Mittel und Hoch.
Vertrauens-würdigkeits-bewertung	Die Vertrauenswürdigkeitsbewertung der Signatur.

Ausgeschied-en	Ein Wert (wahr oder falsch). **Wahr**, wenn die Signatur ausgeschlossen wurde. **Falsch**, wenn nicht. Ausgeschlossene Signaturen werden nicht kompiliert.
Suchmaschi-ne	Die Engine, zu der die Signatur gehört.

Kontextmenü über die rechte Maustaste

Wenn Sie mit der rechten Maustaste auf eine Signatur klicken, zeigt Cisco SDM ein Kontextmenü mit folgenden Optionen an:

- **Aktionen** – Klicken Sie hier, um die Aktionen auszuwählen, die bei einer Übereinstimmung mit der Signatur ausgeführt werden sollen. Weitere Informationen finden Sie unter Aktionen zuweisen.
- **Vertrauenswürdigkeitsbewertung** – Klicken Sie darauf, um eine Vertrauenswürdigkeitsbewertung für die Signatur einzugeben.
- **Schweregrad einstellen auf** – Klicken Sie hier, um den Schweregrad einer Signatur auf diese Stufen einzustellen: Hoch, Mittel, Niedrig oder Informationsbezogen.
- **Standards wiederherstellen** – Klicken Sie hier, um die Standardwerte der Signatur wiederherzustellen.
- **NSDB-Hilfe** (CCO-Konto erforderlich) – Klicken Sie hier, um die Hilfe der Network Security Data Base (NSDB) anzuzeigen.

Änderungen übernehmen

Klicken Sie auf **Änderungen übernehmen**, um neu importierte Signaturen, Änderungen an Signaturen und neu aktivierte oder deaktivierte Signaturen an den Router zu senden. Wenn die Änderungen übernommen werden, wird das gelbe Wartesymbol aus der Spalte **!** entfernt. Diese Änderungen werden im Flash-Memory des Routers in der Datei sdmips.sdf gespeichert. Beim ersten Mausklick auf **Änderungen übernehmen** wird diese Datei automatisch angelegt.

Hinweis Beim Import von Signaturen , die mit den bereits geladenen Signaturen ausnahmslos identisch sind, ist die Schaltfläche **Änderungen übernehmen** deaktiviert.

Änderungen verwerfen

Klicken Sie auf **Änderungen verwerfen**, um die vorgenommenen Änderungen nicht zu übernehmen.

Hinweis Beim Import von Signaturen , die mit den bereits geladenen Signaturen ausnahmslos identisch sind, ist die Schaltfläche **Änderungen verwerfen** deaktiviert.

Signatur bearbeiten

Bearbeiten Sie mithilfe der Felder im Dialogfeld **Signatur bearbeiten** die ausgewählte Signatur. Die vorgenommenen Änderungen werden in einer Delta-Datei im Flash-Speicher des Routers gespeichert. Die Signaturelemente werden in den folgenden Abschnitten beschrieben.

Unter diesem Hilfethema wird das Fenster **Signaturen bearbeiten** beschrieben, das angezeigt wird, wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt.

Signatur-ID

Numerischer Wert zur eindeutigen Kennzeichnung der betreffenden Signatur. Anhand dieses Wertes kann Cisco IOS IPS eine bestimmte Signatur identifizieren.

Subsignatur-ID

Numerischer Wert zur eindeutigen Kennzeichnung der Subsignatur. Eine Subsignatur-ID wird zur Identifikation einer genauer definierten Version einer umfassenderen Signatur verwendet.

Schweregrad der Warnung

Wählen Sie eine der folgenden Möglichkeiten zur Kategorisierung des Schweregrads der Warnung: Hoch, Mittel, Niedrig oder Informationsbezogen.

Sig-Vertrauenswürdigkeitsbewertung

Die Signatur-Vertrauenswürdigkeitsbewertung ist ein Wert, der vom Autor der Signatur angegeben wird, um zu quantifizieren, mit welcher Sicherheit die Signatur richtige Positive erzeugt. Dieser Wert wird festgelegt, bevor die Signatur eingesetzt wird, und kann angepasst werden, wenn Daten über die Signaturleistung verfügbar sind.

Promiscuous Delta

Dies ist ein Faktor, der von der Risikobewertung (RR) eines Ereignisses abgezogen wird, wenn der Router im Promiskmodus läuft. Das Promiscuous Delta wird bei jeder Warnung von der Risikobewertung abgezogen, wenn das System im Promiskmodus läuft.

Hinweis Das Promiscuous Delta kann zwar auch auf Signaturbasis konfiguriert werden, es empfiehlt sich jedoch nicht, die voreingestellten Promiscuous Delta-Einstellungen zu ändern.

Sig-Beschreibung

Die Signaturbeschreibung enthält den Signaturnamen und die Version, Warnhinweise des Cisco Security Center, Bemerkungen von Benutzern sowie weitere Informationen.

Suchmaschine

Die Signatur-Engine, die mit dieser Signatur verknüpft ist. Atomic IP ist eine häufig verwendete Engine.

Das Feld **Engine** enthält Felder, mit denen Sie viele verschiedene Signaturparameter einstellen können. Sie können beispielsweise die Aktion festlegen, die ausgeführt werden soll, wenn eine Übereinstimmung mit der Signatur gefunden und ein Ereignis erstellt wird. Außerdem können Sie das Protokoll von Layer 4 so einstellen, dass es nach Ereignissen sucht, die mit dieser Signatur übereinstimmen, und Sie können IP-Parameter wie die Kopfleistenlänge und den Diensttyp angeben.

Event Counter (Ereigniszähler)

Mithilfe der Steuerungen im Feld **Event Counter** (Ereigniszähler) können Sie die in den folgenden Abschnitten beschriebenen Parameter festlegen.

Event Count (Ereignisanzahl)

Die Zahl, wie oft ein Ereignis auftreten muss, bevor eine Warnung erzeugt wird.

Event Count Key (Ereignisanzahl-Schlüssel)

Der zu verwendende Informationstyp, damit ein Ereignis als auftretend gezählt wird. Wenn Sie beispielsweise die **Adressen und Ports von Hacker und Opfer** auswählen, erhöht sich die Ereignisanzahl jedes Mal, wenn diese 4 Informationen auftreten, um 1. Wenn Sie nur die **Hacker-Adresse** auswählen, wird nur diese Information benötigt.

Event Interval (Ereignisintervall)

Die Anzahl der Sekunden, nach denen Ereignisse jeweils an das Protokoll gesendet werden. Wenn Sie **Ja** auswählen, wird ein weiteres Feld angezeigt, in das Sie die Anzahl der Sekunden eingeben können.

Alert Frequency (Warnungsfrequenz)

Mit diesem Parameter können Sie die Anzahl der in das Protokoll geschriebenen Warnungen reduzieren.

Summary Mode (Zusammenfassungsmodus)

Es gibt vier Modi: Fire All (Alle ausgeben), Fire Once (Einmal ausgeben), Summarize (Zusammenfassen) und Global Summarize (Global zusammenfassen). Der Zusammenfassungsmodus wird dynamisch geändert und passt sich an das aktuelle Warnungsvolumen an. Sie können die Signatur beispielsweise auf Fire All (Alle ausgeben) einstellen und festlegen, dass die Warnungen nach Erreichen einer bestimmten Grenze zusammengefasst werden.

Summary Key (Zusammenfassungsschlüssel)

Der zu verwendende Informationstyp zur Festlegung, wann die Zusammenfassung beginnen soll. Wenn Sie beispielsweise die **Adressen und Ports von Hacker und Opfer** auswählen, wird jedes Mal, wenn diese 4 Informationen auftreten, mit der Zusammenfassung begonnen. Wenn Sie nur die **Hacker-Adresse** auswählen, wird nur diese Information benötigt.

Globale Zusammenfassungsgrenze angeben

Sie können optional numerische Grenzen angeben, mit denen festgelegt wird, wann Ereignisse im Protokoll zusammengefasst werden. Wenn Sie **Ja** auswählen, können Sie eine Grenze für die globale Zusammenfassung und ein Zusammenfassungsintervall festlegen.

Status

Im Feld **Status** können Sie festlegen, ob die Signatur aktiviert, deaktiviert oder ausgeschlossen werden soll. Außerdem werden im Feld **Status** als veraltet bewertete Signaturen angezeigt.

Dateiauswahl

In diesem Fenster können Sie eine Datei von Ihrem Router laden. Nur DOSFS-Dateisysteme können in diesem Fenster angezeigt werden.

Die linke Seite des Fensters zeigt einen erweiterbaren Baum, der das Verzeichnissystem auf Ihrem Cisco Router-Flashspeicher und auf den mit dem Router verbundenen USB-Geräten darstellt.

Auf der rechten Seite des Fensters wird eine Liste der Datei- und Verzeichnisnamen angezeigt, die in dem Verzeichnis gefunden wurden, das auf der linken Seite des Fensters ausgewählt ist. Es zeigt auch die Größe jeder Datei in Bytes und Datum und Zeit der letzten Änderung an den Dateien und Verzeichnissen.

Sie können eine Datei in der Liste auf der rechten Seite des Fensters auswählen, damit sie geladen wird. Unterhalb der Liste mit den Dateinamen befindet sich das Dateinamenfeld mit dem vollständigen Pfad der angegebenen Datei.

Hinweis Wenn Sie eine Konfigurationsdatei zur Versorgung Ihres Routers auswählen, muss diese eine CCCD-Datei sein oder die Erweiterung .cfg haben.

Name

Klicken Sie auf **Name**, um die Dateien und Verzeichnisse alphabetisch nach Namen zu sortieren. Wenn Sie erneut auf **Name** klicken, wird die Reihenfolge umgekehrt.

Größe

Klicken Sie auf **Größe**, um die Dateien und Verzeichnisse nach ihrer Größe zu sortieren. Verzeichnisse haben immer eine Größe von 0 Bytes, auch wenn sie nicht leer sind. Wenn Sie erneut auf **Größe** klicken, wird die Reihenfolge umgekehrt.

Zeit geändert

Klicken Sie auf **Zeit der Änderung**, um die Dateien und Verzeichnisse nach Datum und Uhrzeit der Änderung zu sortieren. Wenn Sie nochmals auf **Zeit der Änderung** klicken, wird die Reihenfolge umgekehrt.

Aktionen zuweisen

Dieses Fenster enthält die Aktionen, die bei Übereinstimmung mit einer Signatur ausgeführt werden können. Die verfügbaren Aktionen richten sich nach der Signatur, die häufigsten Aktionen sind nachfolgend aufgeführt:

- **Alarm** – Generiert eine Alarmmeldung. Identisch mit **produce-verbose-alert**.
- **deny-attacker-inline** – Eine ACL wird erstellt, die zum Ablehnen des gesamten von der jeweiligen IP-Adresse stammenden Datenverkehrs führt, bei der das Cisco IOS IPS-System davon ausgeht, dass es sich um eine Angriffsquelle handelt. Identisch mit **denyAttackerInline**.
- **deny-connection-inline** – Das aktuelle Paket sowie alle nachfolgenden Daten ignorieren, die über diesen TCP-Port eintreffen. Identisch mit **produce-alert** und **denyFlowInline**.
- **deny-packet-inline** – Das betreffende Paket nicht weiterleiten (nur inline). Identisch mit **drop**.
- **denyAttackerInline** – Eine ACL wird erstellt, die zum Ablehnen des gesamten von der jeweiligen IP-Adresse stammenden Datenverkehrs führt, bei der das Cisco IOS IPS-System davon ausgeht, dass es sich um eine Angriffsquelle handelt. Identisch mit **deny-attacker-inline**.
- **denyFlowInline** – Erstellt eine ACL, die jeglichen Datenverkehr einer IP-Adresse ablehnt, bei der davon auszugehen ist, dass sie als Quelle für Angriffe nach dem Fünfertupel-Muster einzustufen ist (Quell-IP, Quell-Port, Ziel-IP, Ziel-Port und l4-Protokoll). denyFlowInline arbeitet noch exakter als denyAttackerInline. Identisch mit **produce-alert** und **deny-connection-inline**.

- **drop** - Das angreifende Datenpaket wird gelöscht. Identisch mit **deny-packet-inline**.
- **produce-alert** - Gibt eine Warnung aus. Identisch mit **denyFlowInline** und **deny-connection-inline**.
- **produce-verbose-alert** - Gibt eine Warnung aus, die einen kodierten Auszug aus dem Angriffspaket enthält. Identisch mit **alarm**.
- **reset** - Rücksetzen der Verbindung und Löschen des Angriffspakets. Identisch mit **reset-tcp-connection**.
- **reset-tcp-connection** - TCP RESET-Signale abschicken, um den Datenfluss über den TCP-Port zu unterbinden. Identisch mit **reset**.

Signaturen importieren

Über das Fenster **Import IPS** (IPS importieren) können Sie Signaturen aus einer SDF-Datei oder aus einer anderen Datei auf dem PC laden. Die Informationen in diesem Fenster sagen Ihnen, welche Signaturen von der SDF zur Verfügung stehen und welche bereits auf Ihrem Router eingesetzt werden.

So importieren Sie Signaturen

Zum Importieren von Signaturen gehen Sie folgendermaßen vor:

Schritt 1 Rufen Sie die zu importierenden Signaturen über den Signaturbaum, die Dropdown-Liste **View by** (Anzeige nach) und die Dropdown-Liste **Kriterienliste** auf.

Bei Signaturen, die Sie *nicht* importieren möchten, müssen Sie die zugehörigen **Import**-Kontrollkästchen deaktivieren. Wenn Sie das Kontrollkästchen **Import** aller Signaturen deaktivieren möchten, klicken Sie auf die Schaltfläche **Alles abwählen**. Anschließend wird diese Option durch die Schaltfläche **Alles auswählen** ersetzt.

Schritt 2 Aktivieren Sie das Kontrollkästchen **Importieren Sie keine Signaturen, die als Deaktiviert definiert sind**, damit der Import von Signaturen vermieden wird, die die Routerleistung im Einsatz beeinträchtigen können.

Schritt 3 Klicken Sie auf die Schaltfläche **Zusammenführen**, um die importierten Signaturen mit den bereits im Router geladenen Signaturen zu mischen, oder auf die Schaltfläche **Ersetzen**, um die bereits konfigurierten Signaturen zu überschreiben.

Weitere Informationen dazu finden Sie unter Die Schaltfläche „Zusammenführen“ und Die Schaltfläche „Ersetzen“.

Schritt 4 Klicken Sie im Fenster **Edit IPS** (IPS bearbeiten) auf die Schaltfläche **Änderungen übernehmen**, um die importierten Signaturen zu laden.

Vor dem Einsatz der importierten Signaturen können Sie darin Änderungen vornehmen. Signaturen, die auf Importieren eingestellt sind und die mit bereits geladenen Signaturen übereinstimmen, werden nicht importiert. Wenn alle importierten Signaturen mit den bereits geladenen Signaturen identisch sind, ist die Schaltfläche **Änderungen übernehmen** deaktiviert.

Signaturbaum

Klicken Sie auf den folgenden Link, wenn Sie eine Beschreibung zum Signaturbaum wünschen: Signaturbaum. Sie können den Signaturbaum in diesem Fenster dazu verwenden, die Signaturen, die Sie importieren wollen, Kategorie für Kategorie zusammenzustellen.

Beispiel: Sie möchten Signaturen aus den Kategorien **OS** und **Service** ergänzen. Wählen Sie dazu das Unterverzeichnis **OS** aus dem Baum aus sowie ein beliebiges weiteres Unterverzeichnis aus dem Teil des gewünschten Baums, wie zum Beispiel das Unterverzeichnis **UNIX** oder **Windows**. Wenn die Signaturtypen, die Sie importieren wollen, angezeigt werden, können Sie Ihre Auswahl im Bereich der Signaturliste treffen. Anschließend können Sie die Verzweigung **Service** und die jeweils gewünschten Servicesignaturen auswählen.

View By (Anzeigen nach) und Kriterienliste

Anhand der Listenfelder **View By** (Anzeige nach) sowie **Kriterien** können Sie die Anzeige auf bestimmte Signaturtypen beschränken. Wählen Sie zuerst die Kriterien aus der Liste **View By** (Anzeige nach) aus und rechts daneben anschließend den Wert für das betreffende Kriterium (aus der Kriterienliste).

Beispiel: Wenn Sie in der Liste **View by** (Anzeige nach) die Option **Engine** auswählen, erhält die Kriterienliste die Bezeichnung Engine. Sie haben anschließend die freie Auswahl aus den verfügbaren Engines, z. B. **Atomic.ICMP** und **Service.DNS**.

Wenn Sie **Sig- ID** oder **Sig- Name** auswählen, müssen Sie in die Kriterienliste einen Wert eingeben.

Bereich „Signaturliste“

In der Signaturliste werden die in der SDF-Datei enthaltenen Signaturen entsprechend den von Ihnen im Signaturbaum gewählten Kriterien angezeigt. Der Textinhalt der Signaturen, die bereits im Router vorgefunden wurden, ist dabei blau hervorgehoben.

Der Bereich Signaturliste hat diese Spalten:

- Sig ID – Numerischer Wert zur eindeutigen Kennzeichnung der betreffenden Signatur. Anhand dieses Wertes kann Cisco IOS IPS eine bestimmte Signatur identifizieren.
- Name – Die Bezeichnung der Signatur. Beispiel: *FTP Improper Address*.
- Schweregrad – Hoch, mittel, niedrig oder informationsbezogen.
- Eingesetzt – Enthält den Wert *Ja*, wenn die Signatur bereits auf dem Router eingesetzt wird. Enthält den Wert *Nein*, wenn die Signatur auf dem Router nicht eingesetzt wird.
- Import – Enthält ein Kontrollkästchen zu jeder Signatur. Wenn Sie die Signatur importieren wollen, aktivieren Sie das Kästchen.

Hinweis In der Signaturliste können alle Signaturen angezeigt werden, die aus einer SDF- oder ZIP-Datei mit der Bezeichnung IOS-S*xxx*.zip importiert wurden. Beim Import von Signaturen aus einer ZIP-Datei mit einem anderen Namen werden nur die Signaturen angezeigt, die über die Dropdown-Listen **View By** (Anzeige nach) sowie **Kriterienliste** zu finden sind.

Die Schaltfläche „Zusammenführen“

Klicken Sie darauf, um die zu importierenden Signaturen mit den Signaturen zu mischen, die bereits im Router konfiguriert sind.

Die Schaltfläche „Ersetzen“

Klicken Sie darauf, um die Signaturen, die bereits im Router konfiguriert sind, durch die importierten Signaturen zu ersetzen. Signaturen, die bereits im Router konfiguriert sind, jedoch in der Liste der zu importierenden Signaturen *nicht* erscheinen, werden zur Löschung gekennzeichnet und im Fenster **Edit IPS (IPS bearbeiten) > Signaturen** unter **Zum Löschen markierte Signaturen** aufgelistet. Weitere Informationen finden Sie unter Zum Löschen markierte Signaturen.

Signatur hinzufügen, bearbeiten oder klonen

Dieses Fenster enthält Felder und Werte, die im Abschnitt **Felddefinitionen** erläutert sind. Die Felder variieren je nach Signatur. Daher sind nicht alle Felder aufgeführt, die eventuell angezeigt werden.

Felddefinitionen

Die folgenden Felder befinden sich in den Fenstern **Signaturen hinzufügen**, **Signaturen bearbeiten** und **Signaturen duplizieren**.

- **SIGID** - Numerischer Wert zur eindeutigen Kennzeichnung der betreffenden Signatur. Anhand dieses Wertes kann Cisco IOS IPS eine bestimmte Signatur identifizieren.
- **SigName** – Der betreffenden Signatur zugewiesene Bezeichnung.
- **SubSig** – Numerischer Wert zur eindeutigen Kennzeichnung der betreffenden Subsignatur. Eine SubSig-ID wird zur Identifikation einer genauer definierten Version einer umfassenderen Signatur verwendet.
- **AlarmInterval** – Besonderer Umgang mit Ereignissen mit zeitlichem Bezug. Verwenden Sie **AlarmInterval** Y mit **MinHits** X für X-Alarme in Y Sekundenintervallen.
- **AlarmSeverity** – Schweregrad des Alarms zu der betreffenden Signatur.
- **AlarmThrottle** – Technik, die zum Auslösen des Alarms verwendet wird.
- **AlarmTraits** – Benutzerdefinierte Merkmale, die diese Signatur genauer beschreiben.
- **ChokeThreshold** – Schwellenwert für die Alarme pro Intervall zum automatischen Aktivieren der **AlarmThrottle**-Modi. Wenn **ChokeThreshold** definiert ist, wechselt Cisco IOS IPS automatisch die AlarmThrottle-Modi, wenn eine große Anzahl Alarmmeldungen im ThrottleInterval verzeichnet wird.
- **Aktiviert** – Identifiziert, ob die Signatur aktiviert ist oder nicht. Eine Signatur muss aktiviert sein, damit Cisco IOS IPS Schutzmaßnahmen gegenüber dem Datenverkehr ergreifen kann, der in der Signatur definiert ist.
- **EventAction** – Identifiziert die Aktionen, die Cisco IOS IPS ergreift, wenn diese Signatur einen Treffer erzielt.
- **FlipAddr** – Trifft zu, wenn Ursprungs- und Zieladressen sowie die zugehörigen Ports in der Warnmeldung vertauscht sind. Ist falsch, wenn keine Vertauschung vorliegt (Standard).

- **MinHits** – Gibt die Mindestanzahl an Signaturtreffern an, die vor der Ausgabe einer Warnmeldung erreicht werden müssen. Als Treffer gilt, wenn die Signatur im Adressschlüssel erscheint.
- **SigComment** – Kommentar bzw. ausführlicher Text zu der Signatur.
- **SigVersion** – Version der Signatur.
- **ThrottleInterval** – Anzahl an Sekunden, die ein AlarmThrottle-Intervall definieren. Wird mit dem **AlarmThrottle**-Parameter für die Abstimmung spezieller Alarmbegrenzer verwendet.
- **WantFrag** – Wenn der Wert wahr ist, erfolgt lediglich eine Untersuchung der fragmentierten Pakete. Ist der Wert falsch, werden ausschließlich die nicht fragmentierten Pakete untersucht. Wählen Sie **Nicht definiert**, damit nicht nur die fragmentierten, sondern auch die nicht fragmentierten Pakete untersucht werden.

Cisco Security Center

Das Cisco Security Center liefert Informationen zu plötzlich auftretenden Bedrohungen und enthält Verweise zu den Cisco IOS IPS-Signaturen, die zum Schutz Ihres Netzwerks vor diesen Bedrohungen beitragen. Signaturberichte und -Downloads sind unter folgendem Link verfügbar (Anmeldung erforderlich):

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

Mitgelieferte IPS-Signaturdefinitionsdateien

Damit im Speicher des Routers so viele Signaturen wie möglich geladen sind, wird Cisco SDM mit einer der folgenden SDFs ausgeliefert:

- 256MB.sdf - Wenn mehr als 256 MB RAM zur Verfügung stehen. Die Datei 256MB.sdf enthält 500 Signaturen.
- 128MB.sdf - Wenn der zur Verfügung stehende RAM-Speicher zwischen 128 und 256 MB beträgt. Die Datei 128MB.sdf enthält 300 Signaturen.
- attack-drop.sdf - Wenn 127 MB RAM oder weniger zur Verfügung stehen. Die Datei attack-drop.sdf enthält 82 Signaturen.

Wenn der Router Cisco IOS-Version 12.4(11)T oder höher ausführt, müssen Sie eine SDF-Datei mit dem Namensformat sigv5-SDM-S*xxx*.zip verwenden, wie beispielsweise sigv5-SDM-S260.zip.

Hinweis Auf dem Router muss die Cisco IOS-Version 12.3(14)T oder höher geladen sein, um alle in den Dateien 256MB.sdf und 128MB.sdf zur Verfügung stehenden Signatur-Engines verwenden zu können. Wenn die Version im Router älter ist, stehen nicht alle Signatur-Engines zur Verfügung.

Um eine im Router-Speicher geladene SDF nutzen zu können, müssen Sie feststellen, welche SDF installiert wurde. Anschließend müssen Sie Cisco IOS IPS auf die Verwendung der Datei einstellen. Die nachfolgenden Vorgänge zeigen Ihnen, wie Sie hierbei vorgehen müssen.

Ermitteln, welche SDF-Datei im Speicher geladen ist

Um zu bestimmen, welche SDF-Datei im Speicher des Routers geladen ist, starten Sie eine Telnet-Sitzung zum Router, und geben Sie den Befehl **show flash** ein. Der Router reagiert darauf folgendermaßen:

```
System flash directory:
File  Length   Name/status
  1   10895320  c1710-k9o3sy-mz.123-8.T.bin
  2   1187840  ips.tar
  3   252103   attack-drop.sdf
  4   1038     home.shtml
  5   1814     sdmconfig-1710.cfg
  6   113152   home.tar
  7   758272   es.tar
  8   818176   common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

Bei diesem Beispiel ist die Datei attack-drop.sdf im Speicher des Routers geladen. Bei anderen Routern, die zum Beispiel mit einem Datenträgersystem arbeiten, müssen Sie den Befehl **dir** eingeben, um den Inhalt des Routerspeichers anzuzeigen.

IPS konfigurieren, um eine SDF zu verwenden

Gehen Sie wie folgt vor, um Cisco IOS IPS auf die Verwendung der SDF-Datei im Speicher des Routers einzustellen:

Schritt 1 Klicken Sie auf **Globale Einstellungen**.

Schritt 2 Klicken Sie in der Liste **Konfigurierte SDF-Speicherorte** auf **Hinzufügen**.

Schritt 3 Klicken Sie im anschließenden Dialogfeld auf **Specify SDF on flash** (SDF im Flash angeben), geben Sie den Namen der SDF-Datei ein.

Schritt 4 Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Sicherheits-Dashboard

Mithilfe des Security Dashboard können Sie sicherstellen, dass in Ihrem Router stets die aktuellsten Signaturen zum Schutz vor den neuesten Bedrohungen geladen sind. Bevor Sie Signaturen mithilfe des Security Dashboard einsetzen können, muss Cisco IOS IPS auf dem Router konfiguriert sein.

Die Tabelle mit den häufigsten Bedrohungen

In der Tabelle mit den häufigsten Bedrohungen sind die neuesten und am stärksten verbreiteten Bedrohungen von Cisco aufgeführt, sofern aus dem Status der zugehörigen Signaturen hervorgeht, dass diese entweder für den Routereinsatz bereit oder in der Testphase sind. Einige dieser häufigen Bedrohungen in der Tabelle werden anhand von Signaturen erkannt, die Sie auf Ihrem Router einsetzen können. Der Textinhalt der Signaturen, die bereits im Router geladen sind, ist blau hervorgehoben.

Klicken Sie auf die Schaltfläche **Liste der häufigsten Bedrohungen aktualisieren**, um die Angaben über die häufigsten Bedrohungen auf den neuesten Stand zu bringen.

Hinweis Durch Klicken auf die Cisco SDM-Schaltfläche **Aktualisieren** oder die Auswahl des Aktualisierungsbefehls in Ihrem Browser wird allerdings die Liste mit den häufigsten Bedrohungen nicht aktualisiert.

Die Tabelle **Häufigste Bedrohungen** enthält folgende Spalten:

- **Gerätestatus** – Gibt an, ob die Signatur zu der Bedrohung bereits im Router aktiviert ist. Das folgende Symbol wird möglicherweise in der Spalte **Gerätestatus** angezeigt:

Signatur ist bereits im Router aktiv.

Signatur ist im Router nicht vorhanden, oder sie ist im Router vorhanden, jedoch *nicht* aktiviert.

- **Sig-ID** – Eine Zahl zur eindeutigen Kennzeichnung der Signatur für die Bedrohung.
- **SubSig-ID** – Eine Zahl zur eindeutigen Kennzeichnung der Subsignatur. Wenn die Signatur zu der Bedrohung keine Subsignatur enthält, ist der Wert von **SubSig-ID** 0.
- **Name** – Die Bezeichnung für die jeweilige Bedrohung.
- **Urgency** (Relevanz) – Gibt an, ob es sich um eine sehr ernste (Wartungspriorität) oder um eine normale Bedrohung (Standardwartungsniveau) handelt.
- **Threat Status** (Bedrohungsstatus) – Gibt an, ob die Signatur zu der Bedrohung verfügbar ist, oder ob die Bedrohung noch näher untersucht wird.
- **Deploy** (Einsetzen) – Enthält Kontrollkästchen, über die festgelegt werden kann, ob die Signatur zu einer bestimmten Bedrohung verfügbar und einsatzbereit ist.

SDF auswählen

Klicken Sie auf die Schaltfläche **Durchsuchen**, und wählen Sie die gewünschte Cisco IOS-SDF-Datei aus. Die Cisco IOS-SDF-Datei muss auf dem PC gespeichert sein. Das Format des Dateinamens hängt von der auf dem Router ausgeführten Version von Cisco IOS ab.

- Wenn der Router ein früheres Cisco IOS-Abbild als 12.4(11)T ausführt, muss die SDF-Datei einen Namen im Format IOS-S*xxx*.zip tragen (*xxx* repräsentiert eine dreistellige Zahl). Beispiel: IOS-S193.zip ist ein gültiger Name einer Cisco IOS IPS-SDF-Datei.
- Wenn der Router ein Cisco IOS-Abbild der Version 12.4(11)T oder höher ausführt, muss die SDF-Datei einen Namen im Format sigv5-SDM-S*xxx*.zip tragen, wie beispielsweise sigv5-SDM-S260.zip.

Das Verzeichnis der gewählten Cisco IOS-SDF-Datei wird im Feld mit dem SDF-Dateipfad angezeigt. Das Feld mit dem SDF-Dateipfad ist schreibgeschützt.

Nach dem ersten Übertragen einer Cisco IOS-SDF-Datei bleibt der Verzeichnispfad zu der Datei in Cisco SDM gespeichert. Beim nächsten Start des Security Dashboard wählt Cisco SDM abhängig von der dreistelligen Zahl im Dateinamen die neueste Cisco IOS-SDF-Datei aus.

Hinweis Die Cisco IOS-SDF-Datei mit der höchsten dreistelligen Zahl im Dateinamen ist stets die neueste Cisco IOS-SDF-Datei.

Signaturen aus der Tabelle „Häufigste Bedrohungen übernehmen“

Folgende Voraussetzungen müssen erfüllt sein, bevor Signaturen aus der Tabelle mit den häufigsten Bedrohungen im Router eingesetzt werden können:

- Konfiguriertes Cisco IOS IPS auf dem Router
- Die neuste Cisco IOS-Datei wurde auf den PC heruntergeladen.

So setzen Sie Signaturen aus der Tabelle mit den häufigsten Bedrohungen im Router ein:

Schritt 1 Klicken Sie auf die Schaltfläche **Liste der häufigsten Bedrohungen aktualisieren**, damit Ihnen die neuste Liste mit den häufigsten Bedrohungen vorliegt.

Schritt 2 Aktivieren Sie in der Spalte **Deploy** (Einsetzen) der Tabelle **Häufigste Bedrohungen** das Kontrollkästchen zu jeder Signatur für eine Bedrohung, die Sie übernehmen und aktivieren möchten.

Dabei können nur die Bedrohungen ausgewählt werden, die mit dem Status **Signature available** (Signatur verfügbar) versehen sind. Verfügbare Signaturen, bei denen die Spalte **Applied** (Übernommen) ein rotes Symbol enthält, sind automatisch für den Routereinsatz aktiviert.

Schritt 3 Klicken Sie auf die Schaltfläche **Durchsuchen**, und wählen Sie zur Sicherheit die neueste Cisco IOS-Datei aus, um auf jeden Fall mit der neuesten Signaturdatei zu arbeiten.

Dieser Schritt ist erforderlich, wenn sich der Verzeichnispfad zur neuesten SDF-Datei seit der letzten Pfadeinstellung im Security Dashboard geändert hat, oder wenn die Datei nicht nach dem Muster IOS-S*xxx*.zip benannt ist (wobei *xxx* ein Platzhalter für eine dreistellige Zahl ist).

Schritt 4 Klicken Sie auf die Schaltfläche **Signaturen verwenden**, um die gewählten Signaturen in Ihrem Router zu aktivieren.

Wenn eine der gewählten Signaturen in der Cisco IOS-Datei nicht gefunden wurde, erscheint eine Warnmeldung. Davon abgesehen können aber alle gefundenen Signaturen in den Router übernommen werden. Nach der Übernahme in den Router werden die Signaturen automatisch aktiviert und in die Liste mit den aktiven Routersignaturen eingetragen.

IPS-Migration

Mithilfe des IPS-Migrationsassistenten können Sie eine bestehende Cisco IOS IPS-Konfiguration in Cisco IOS IPS, das in Cisco IOS 12.4(11)T oder höher verfügbar ist, migrieren.

Hinweis Wenn der Router ein Cisco IOS-Abbild der Version 12.4(11)T oder höher ausführt, müssen Sie eine mit einer früheren Version erstellte Konfiguration migrieren, wenn Cisco IOS IPS auf dem Router verwendet werden soll. Wenn Sie die Konfiguration nicht migrieren, ändern sich zwar die Konfigurationsbefehle nicht, aber Cisco IOS IPS kann nicht ausgeführt werden.

Klicken Sie auf die Schaltfläche **IPS-Migrationsassistent starten**, um den Migrationsvorgang zu starten.

Migrationsassistent: Willkommen

Im Willkommensfenster des Migrationsassistenten werden die Aufgaben aufgeführt, die Sie mithilfe des Assistenten durchführen können. Klicken Sie auf **Abbrechen**, wenn Sie den IPS-Migrationsassistenten nicht ausführen möchten.

Der IPS-Migrationsassistent ist verfügbar, wenn auf dem Router Cisco IOS 12.4(11)T oder höher läuft.

Migrationsassistent: Auswählen der IOS IPS Backup-Signaturdatei

Die Backup-Signaturdatei enthält die Cisco IOS IPS Informationen, die migriert werden. Dabei kann es sich beispielsweise um eine SDF-Datei (Signature Definition File), wie z. B. attack-drop.sdf oder 128MB.sdf handeln. Wenn Sie Änderungen an der Signaturinformation vorgenommen haben, wie z. B. Deaktivieren von Signaturen oder Ändern der Attribute bestimmter Signaturen, werden die Änderungen in einer separaten Datei festgehalten. Wenn Sie mithilfe von Cisco SDM Änderungen vorgenommen haben, speichert Cisco SDM diese in einer Datei namens sdmips.sdf im Flash-Speicher des Routers. Wenn Sie manuell Änderungen vorgenommen haben, haben Sie die Datei möglicherweise anders benannt und eine Sicherungskopie der Datei auf dem PC gespeichert.

Klicken Sie auf die Schaltfläche **...** neben dem Feld mit der Backup-Datei , um ein Dialogfeld anzuzeigen, in dem Sie im Flash-Speicher des Routers oder auf dem PC nach der Backup-Signaturdatei suchen können.

Signaturdatei

Geben Sie in diesem Dialogfeld den Speicherort der Backup-Signaturdatei an.

Signaturdatei auf Flash angeben

Wenn sich die Backup-Signaturdatei im Flash-Speicher befindet, klicken Sie auf den nach unten zeigenden Pfeil rechts neben diesem Feld und wählen die Datei aus.

Signaturdatei auf dem PC angeben

Wenn sich die Backup-Signaturdatei auf dem PC befindet, klicken Sie auf die Schaltfläche **Durchsuchen** neben diesem Feld und navigieren zu der Datei.

Heap-Größe für Java

Cisco SDM zeigt das Fenster **Heap-Größe für Java** an, wenn die Heap-Größe für Java zu gering ist, um eine SDM-Funktion zu unterstützen. Führen Sie die folgenden Schritte aus, um die Heap-Größe auf den im Fenster angegebenen Wert festzulegen.

Schritt 1 Beenden Sie Cisco SDM.

Schritt 2 Klicken Sie auf **Start > Systemsteuerung > Java**.

Schritt 3 Öffnen Sie das Dialogfeld **Java Runtime-Einstellungen**. Wo sich dieses Dialogfeld befindet, hängt von der Version ab.

a. Klicken Sie auf die Registerkarte **Erweitert**. Suchen Sie das Dialogfeld **Java Runtime-Einstellungen** und fahren Sie mit Schritt 4 fort. Wenn das Dialogfeld nicht über die Registerkarte **Erweitert** verfügbar ist, fahren Sie mit b. fort.

b. Klicken Sie auf die Registerkarte **Java**. Suchen Sie das Dialogfeld **Java Runtime-Einstellungen**. Klicken Sie, falls nötig, auf **Anzeigen**, um das Dialogfeld anzuzeigen, und fahren Sie mit Schritt 4 fort.

Schritt 4 Geben Sie in der Spalte **Java Runtime-Parameter** den im Fenster angegebenen Wert ein. Beispiel: Wenn im Fenster steht, dass Sie den Wert `-Xmx256m` verwenden sollen, geben Sie diesen Wert in die Spalte **Java Runtime-Parameter** ein. Die folgende Tabelle enthält Beispielwerte.

Produktname	Version	Speicherort	Java Runtime-Parameter
JRE	1.5.0_08	C:\Programme\java\jre1.5.0_08	-Xmx256m

Schritt 5 Klicken Sie im Dialogfeld **Java Runtime-Einstellungen** auf **OK**.

Schritt 6 Klicken Sie im Java Control Panel auf **Anwenden** und anschließend auf **OK**.

Schritt 7 Starten Sie Cisco SDM erneut.

KAPITEL 25

Netzwerk-Modulmanagement

Wenn der Router Netzwerkmodule enthält, die von anderen Anwendungen verwaltet werden, z. B. dem Intrusion Detection System (IDS), dann bietet Secure Router Device Manager (Cisco SDM) Ihnen die Mittel, diese Anwendungen zu starten.

IDS-Netzwerkmodul-Verwaltung

Wenn ein Cisco IDS-Netzwerkmodul auf dem Router installiert ist, werden in diesem Fenster allgemeine Statusinformationen für das Modul angezeigt. Wenn das IDS-Netzwerkmodul konfiguriert wurde, können Sie außerdem die IDM-Software (Intrusion Detection Device Manager) auf dem IDS-Netzwerkmodul starten und in diesem Fenster die Routerschnittstellen auswählen, die das IDS-Netzwerkmodul überwachen soll.

Wenn Cisco SDM ermittelt, dass das IDS-Netzwerkmodul nicht konfiguriert wurde, werden Sie aufgefordert, eine Sitzung für das Netzwerkmodul zu starten, damit Sie es konfigurieren können. Für diese Sitzung können Sie Telnet oder SSH verwenden.

Schaltflächen für die Steuerung des IDS-Netzwerkmoduls

Cisco SDM ermöglicht es Ihnen, von diesem Fenster aus eine Reihe von allgemeinen Befehlen an das IDS-Netzwerkmodul abzusetzen.

Erneut laden

Klicken Sie auf diese Schaltfläche, um das Betriebssystem für das IDS-Netzwerkmodul erneut zu laden.

Zurücksetzen

Klicken Sie auf diese Schaltfläche, um die Hardware des IDS-Netzwerkmoduls zurückzusetzen. Verwenden Sie die Schaltfläche **Zurücksetzen** nur, um nach dem Status **Fehlgeschlagen** eine Wiederherstellung einzuleiten oder nachdem Sie das IDS-Netzwerkmodul heruntergefahren haben.

Beenden

Klicken Sie auf diese Schaltfläche, um das IDS-Netzwerkmodul herunterzufahren. Fahren Sie das Modul immer herunter, bevor Sie es vom Router entfernen.

IDM starten

Klicken Sie auf diese Schaltfläche, um die IDM-Software auf dem IDS-Modul zu starten. Wenn Sie die IDM-Software starten, zeigt Cisco SDM ein Dialogfeld an, in dem Sie nach der IP-Adresse der externen Fast Ethernet-Schnittstelle des IDS-Moduls gefragt werden. Wenn Cisco SDM die richtige Adresse erhält, wird ein IDM-Fenster geöffnet. Weitere Informationen zu diesem Dialogfeld erhalten Sie unter Feststellung der IP-Adresse.

Weitere Informationen über die Ausführung der IDM-Anwendung finden Sie in den Dokumenten unter dem folgenden Link:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Aktualisieren

Klicken Sie auf diese Schaltfläche, um die Statusanzeige zu aktualisieren.

Status von IDS-Netzwerkmodul

In diesem Bereich wird der allgemeine Status des IDS-Netzwerkmoduls angezeigt. Er enthält die folgenden Arten von Informationen:

- Dienstmodul – Der Name des Netzwerkmoduls.
- Status – Der Status des Netzwerkmoduls. Mögliche Statusangaben sind: Bereit, Beenden und/oder Fehlgeschlagen.
- Softwareversion – Die Version der IDM-Software, die auf dem Modul ausgeführt wird.

- Modell – Die Modellnummer des Netzwerkmoduls.
- Speicher – Der auf dem Netzwerkmodul verfügbare Speicher.

Einstellungen für IDS NM-Überwachungsschnittstelle

In diesem Bereich des Fensters wird angezeigt, welche Routerschnittstellen Datenverkehr zur Überwachung an das IDS-Netzwerkmodul senden lassen.

	Ein Häkchen neben dem Namen der Schnittstelle gibt an, dass das IDS-Netzwerkmodul den Datenverkehr auf dieser Schnittstelle überwacht.
	Ein rotes Symbol mit einem X neben dem Namen der Schnittstelle gibt an, dass das IDS-Netzwerkmodul den Datenverkehr auf dieser Schnittstelle nicht überwacht.

Konfigurieren

Klicken Sie auf diese Option, um Schnittstellen zur Liste hinzuzufügen oder daraus zu entfernen. Wenn Sie auf **Konfigurieren** klicken, überprüft Cisco SDM, ob das IDS-Netzwerkmodul konfiguriert wurde und ob der Router alle Konfigurationseinstellungen aufweist, die für die Kommunikation mit dem IDS-Netzwerkmodul benötigt werden. Wenn Konfigurationseinstellungen fehlen, zeigt Cisco SDM in einer Checkliste an, was konfiguriert und was nicht konfiguriert wurde. Sie können auf die nicht konfigurierten Elemente klicken, um die Konfiguration abzuschließen. Anschließend können Sie veranlassen, dass Cisco SDM erneut überprüft, ob diese Elemente konfiguriert wurden, damit Sie Schnittstellen zur Liste **Einstellungen für IDS NM-Überwachungsschnittstelle** hinzufügen oder daraus entfernen können.

IP-Adresse für IDS-Sensorschnittstelle

Cisco SDM muss für die Kommunikation mit dem IDS-Netzwerkmodul die IP-Adresse der internen Fast Ethernet-Schnittstelle des Moduls verwenden. Dieses Fenster wird angezeigt, wenn Cisco SDM diese IP-Adresse nicht ermitteln kann. Sie können darin für Cisco SDM eine Adresse angeben. Wenn das IDS-Netzwerkmodul mit einer statischen IP-Adresse konfiguriert wurde oder mit **Keine IP-Nummerierung** an einer anderen Schnittstelle mit einer IP-Adresse konfiguriert wurde, wird dieses Fenster nicht angezeigt.

Mit der Eingabe einer IP-Adresse in diesem Fenster kann eine neue Loopback-Schnittstelle erstellt werden. Loopback-Schnittstellen können im Fenster **Schnittstellen und Verbindungen** angezeigt werden. Die IP-Adresse, die Sie eingeben, ist nur für den Router sichtbar. Daher kann es eine beliebige Adresse sein, die Sie verwenden möchten.

IP-Adresse

Geben Sie eine IP-Adresse ein, die für die IDS-Sensorschnittstelle verwendet werden soll. Cisco SDM führt folgende Schritte aus:

- Es wird eine Loopback-Schnittstelle erstellt. Sofern verfügbar, wird die Nummer 255 verwendet, ansonsten eine andere Nummer. Diese Loopback-Schnittstelle wird in die Liste im Fenster **Schnittstellen und Verbindungen** aufgenommen.
- Die Loopback-Schnittstelle wird mit der von Ihnen eingegebenen IP-Adresse konfiguriert.
- Das IDS-Netzwerkmodul wird mit **Keine IP-Nummerierung** an der Loopback-Schnittstelle konfiguriert.
- Wenn das IDS-Netzwerkmodul bereits mit **Keine IP-Nummerierung** an einer vorhandenen Loopback-Schnittstelle konfiguriert wurde, die Schnittstelle aber keine gültige IP-Adresse besitzt, erhält die Loopback-Schnittstelle die IP-Adresse, die Sie in diesem Fenster eingeben.

Feststellung der IP-Adresse

Cisco SDM zeigt dieses Fenster an, wenn die IP-Adresse eines Netzwerkmoduls festgestellt werden muss, das Sie verwalten möchten. Dies ist normalerweise die IP-Adresse der externen Ethernet-Schnittstelle des Moduls. Cisco SDM kann die Adresse verwenden, die schon beim letzten Ablauf der Verwaltungsanwendung verwendet wurde, und es kann die IP-Adresse ermittelt oder eine Adresse akzeptiert werden, die Sie in diesem Fenster eingeben.

Wählen Sie eine Methode aus, und klicken Sie auf **OK**. Wenn die ausgewählte Methode fehlschlägt, können Sie eine andere Methode auswählen.

Letzte Cisco SDM bekannte IP-Adresse verwenden

Klicken Sie auf diese Option, damit Cisco SDM die IP-Adresse vom letzten Ablauf der Verwaltungsanwendung für dieses Netzwerkmodul verwendet. Wenn die IP-Adresse des Moduls seit dem letzten Ablauf der Verwaltungsanwendung nicht geändert wurde und Sie nicht wünschen, dass Cisco SDM die Adresse ermittelt, verwenden Sie diese Option.

Cisco SDM IP-Adresse ermitteln lassen

Klicken Sie auf diese Option, wenn Cisco SDM die IP-Adresse des Netzwerkmoduls ermitteln soll. Sie können diese Option verwenden, wenn Sie die IP-Adresse nicht kennen und sich nicht sicher sind, ob die letzte Adresse, die Cisco SDM zum Kontaktieren des Netzwerkmoduls verwendete, noch stimmt.

Angeben

Wenn Sie die IP-Adresse des Netzwerkmoduls kennen, wählen Sie diese Option und geben die Adresse ein. Cisco SDM speichert die Adresse und Sie können das nächste Mal, wenn Sie das Netzwerkmodul starten, die Option **Letzte SDM bekannte IP-Adresse verwenden** auswählen.

Checkliste für IDS NM-Konfiguration

Dieses Fenster wird angezeigt, wenn Sie im Fenster **IDS-Netzwerkmodul-Verwaltung** auf **Konfigurieren** geklickt haben, um die Routerschnittstellen anzugeben, deren Datenverkehr analysiert werden soll, dem IDS-Netzwerkmodul oder dem Router aber eine Konfigurationseinstellung fehlt, die für die Kommunikation zwischen den beiden Geräten benötigt wird. In ihm wird angezeigt, welche Konfigurationseinstellungen benötigt werden, und in einigen Fällen haben Sie die Möglichkeit, die Konfiguration von Cisco SDM aus abzuschließen.

- Ein Häkchen in der Spalte **Aktion** bedeutet, dass die Konfigurationseinstellung vorgenommen wurde.
- Ein X in der Spalte **Aktion** bedeutet, dass die Konfigurationseinstellung vorgenommen werden muss, damit der Router mit dem IDS-Netzwerkmodul kommunizieren kann.

IDS NM-Sensorschnittstelle

- Wenn diese Zeile in der Spalte **Aktion** ein X enthält, wurde die IDS NM-Sensorschnittstelle nicht mit einer IP-Adresse konfiguriert. Doppelklicken Sie in die Zeile, und geben Sie in dem angezeigten Dialogfeld eine IP-Adresse für den IDS-Sensor ein. Die IP-Adresse des IDS-Sensors ist die Adresse, die Cisco SDM und der Router für die Kommunikation mit dem IDS-Netzwerkmodul verwenden. Diese IP-Adresse kann eine private Adresse sein. Sie kann von keinem anderen Host als dem Router erreicht werden, in dem das Modul installiert ist.

Datum & Uhrzeit

- Wenn diese Zeile in der Spalte **Aktion** ein X enthält, wurde die Uhr des Routers nicht konfiguriert. Doppelklicken Sie in diese Zeile, und geben Sie im Fenster **Datums- und Uhrzeiteigenschaften** die Zeit und das Datum ein.

IP CEF-Einstellung

- Wenn diese Zeile in der Spalte **Aktion** ein X enthält, wurde CEF (Cisco Express Forwarding) auf dem Router nicht aktiviert. Doppelklicken Sie in diese Zeile, und klicken Sie auf **Ja**, um IP CEF auf dem Router zu aktivieren.

IDS NM-Anfangseinrichtung

- Wenn diese Zeile in der Spalte **Aktion** ein X enthält, hat Cisco SDM ermittelt, dass die Standard-IP-Adresse des IDS-Netzwerkmoduls nicht geändert wurde. Doppelklicken Sie in diese Zeile. Sie werden in Cisco SDM aufgefordert, eine Sitzung für das IDS-Modul zu starten und die Konfiguration abzuschließen. Sie können Telnet oder SSH für diese Sitzung verwenden.

Weitere Informationen über die Konfiguration des IDS-Moduls finden Sie in den Dokumenten unter dem folgenden Link:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Aktualisieren

- Sobald Sie über feste Konfigurationseinstellungen verfügen, können Sie auf diese Schaltfläche klicken, um die Checkliste zu aktualisieren. Wenn in der Spalte **Aktion** ein X verbleibt, wurde eine Konfigurationseinstellung noch immer nicht vorgenommen.

Konfiguration der IDS NM-Schnittstellenüberwachung

Wählen Sie in diesem Fenster die Routerschnittstellen aus, deren Datenverkehr vom IDS-Netzwerkmodul überwacht werden soll.

Überwachte Schnittstellen

Diese Liste enthält die Schnittstellen, deren Datenverkehr das IDS-Netzwerkmodul überwacht. Um eine Schnittstelle zu dieser Liste hinzuzufügen, wählen Sie aus der Liste **Verfügbare Schnittstellen** eine Schnittstelle aus, und klicken Sie auf die Schaltfläche **<<**. Um eine Schnittstelle aus dieser Liste zu entfernen, wählen Sie die Schnittstelle aus, und klicken Sie auf die Schaltfläche **>>**.

Verfügbare Schnittstellen

Diese Liste enthält die Schnittstellen, deren Datenverkehr das IDS-Netzwerkmodul derzeit nicht überwacht. Um eine Schnittstelle zur Liste **Überwachte Schnittstellen** hinzuzufügen, wählen Sie die Schnittstelle aus, und klicken Sie auf die Schaltfläche **<<**.

Netzwerkmodul-Anmeldung

Geben Sie den Benutzernamen und das Kennwort an, das für die Anmeldung beim Netzwerkmodul erforderlich ist. Diese Anmeldedaten sind nicht unbedingt mit den Angaben identisch, die für die Routeranmeldung benötigt werden.

Feature Unavailable (Funktion nicht vorhanden)

Dieses Fenster wird angezeigt, wenn Sie versuchen, eine Funktion zu konfigurieren, die das Cisco IOS-Abbild auf Ihrem Router nicht unterstützt. Wenn Sie diese Funktion verwenden möchten, besorgen Sie sich ein Cisco IOS-Abbild über Cisco.com, das dies unterstützt.

Switchmodul-Schnittstellenauswahl

Dieses Fenster wird angezeigt, wenn mehr als ein Switchmodul auf dem Router installiert ist und Sie können dasjenige auswählen, das Sie verwalten möchten. Klicken Sie auf die Optionsschaltfläche neben dem Switchmodul, das Sie verwalten möchten, und dann auf **OK**.

KAPITEL 26

Quality of Service

Der Quality of Service (QoS)-Assistent ermöglicht es einem Netzwerkadministrator, Dienstgüte (Quality of Service, QoS) in den WAN-Schnittstellen des Routers zu aktivieren. QoS kann auch in IPSec-VPN-Schnittstellen und -Tunneln aktiviert werden. Die QoS-Bearbeitungsfenster ermöglichen es dem Administrator, Richtlinien, die unter Verwendung des Assistenten erstellt wurden, zu bearbeiten.

QoS-Richtlinie erstellen

Der QoS-Assistent ermöglicht es einem Netzwerkadministrator, QoS in den WAN-Schnittstellen des Routers zu aktivieren. QoS kann auch in IPSec-VPN-Schnittstellen und -Tunneln aktiviert werden.

Die Richtlinie wird auf ausgehenden Datenverkehr in der Schnittstelle angewendet.

Registerkarte „QoS-Richtlinie erstellen“

Klicken Sie auf diese Registerkarte, um eine neue QoS-Richtlinie hinzuzufügen.

Registerkarte „QoS-Richtlinie bearbeiten“

Klicken Sie auf diese Registerkarte, um eine bestehende QoS-Richtlinie zu bearbeiten.

Schaltfläche „QoS-Assistent starten“

Klicken Sie auf diese Schaltfläche, um den QoS-Assistenten zu starten. Mit dem QoS-Assistenten können Sie QoS-Richtlinien in den WAN-Schnittstellen konfigurieren.

QoS-Assistent

Dieses Fenster fasst die Informationen zusammen, die Sie beim Abschluss des QoS-Richtlinienassistenten angeben.

Klicken Sie auf die Schaltfläche **Weiter**, um mit der Konfiguration einer QoS-Richtlinie zu beginnen.

Auswahl der Schnittstelle

Wählen Sie die Schnittstelle aus, in der Sie die QoS-Richtlinie über dieses Fenster konfigurieren möchten. Dieses Fenster listet WAN-Schnittstellen und Schnittstellen auf, in denen keine ausgehende QoS-Richtlinie konfiguriert ist. Die Liste enthält VPN-Schnittstellen. Schnittstellen, die für Easy VPN-Clients verwendet werden, und Schnittstellen mit einer bestehenden QoS-Richtlinie, werden jedoch nicht aufgeführt. QoS wird nicht für Easy VPN-Clients unterstützt.

Schaltfläche „Details“

Klicken Sie auf diese Schaltfläche, um Konfigurationsdetails zur Schnittstelle anzuzeigen. Das Fenster zeigt die IP-Adresse und Subnetzmaske der Schnittstelle, Namen von Zugriffsregeln, Richtlinien, auf die die Schnittstelle angewendet wird, und Verbindungen an, für die die Schnittstelle verwendet wird.

DSCP-Markierung (vertrauenswürdig)

Klicken Sie hier, um Markierungen für Differentiated Services Code Point (DSCP) zur Klassifizierung von Datenverkehr zu verwenden. Cisco Netzwerkgeräte, wie IP-Telefone und Switches, fügen DSCP-Markierungen zu Paketen hinzu. Durch die Konfiguration von DSCP auf dem Router wird die Verwendung dieser Markierungen zur Klassifizierungen von Datenverkehr zugelassen. Wenn das Cisco IOS-Abbild auf dem Router die DSCP-Markierung nicht unterstützt, wird diese Option nicht angezeigt.

NBAR-Protokollerkennung (nicht vertrauenswürdig)

Klicken Sie auf diese Option, um die NBAR (Network-Based Application Recognition)-Protokollerkennung für die Klassifizierung von Datenverkehr zu verwenden. Wenn eine Anwendung über NBAR erkannt und klassifiziert wurde, kann ein Netzwerk Dienste für diese spezielle Anwendung aufrufen. NBAR stellt eine effiziente Ausnutzung der Netzwerkbandbreite sicher, indem Pakete klassifiziert und dann Quality of Service (QoS, Dienstgüte) auf den klassifizierten Datenverkehr angewendet wird. Wenn das Cisco IOS-Abbild auf dem Router keine NBAR-Protokollerkennung unterstützt, wird diese Option nicht angezeigt.

QoS-Richtlinienerstellung

Verwenden Sie dieses Fenster, um die Bandbreite den unterschiedlichen Datenverkehrstypen zuzuweisen, die über die ausgewählte Schnittstelle übertragen werden. Der von Ihnen eingegebene Prozentwert entspricht 1000 KBit/s. Wenn Sie beispielsweise 5 % eingeben, wird für die Bandbreite eine Zuordnung von 5000 KBit/s vorgenommen. Der gesamte Prozentwert für alle Datenverkehrstypen, ausgenommen Best-Effort, darf 75 % nicht überschreiten.

- Sprache – Sprachdatenverkehr. Der Standardwert ist 33 Prozent der Bandbreite.
- Anrufsignalisierung – Die für die Steuerung von Sprachdatenverkehr erforderliche Signalisierung. Der Standardwert ist 5 Prozent der Bandbreite.
- Routing – Datenverkehr, der von diesem und anderen Routern für die Verwaltung des Paket-Routings generiert wird. Der Standardwert ist 5 Prozent der Bandbreite.
- Verwaltung – Telnet, SSH und anderer Datenverkehr, der zur Routerverwaltung generiert wird. Der Standardwert ist 5 Prozent der Bandbreite.
- Transaktionsbezogen – Beispiel dafür ist Datenverkehr, der für Händleranwendungen oder Datenbankaktualisierungen generiert wird. Der Standardwert ist 5 Prozent der Bandbreite.
- Best-Effort – Verbleibende Bandbreite für anderen Datenverkehr, wie E-Mail-Datenverkehr. Der Standardwert ist 47 Prozent der Bandbreite. Der Wert für Best-Effort wird basierend auf dem gesamte Prozentsatz für andere Datenverkehrstypen aktualisiert.

Übersicht über die QoS-Konfiguration

Das Fenster **Übersicht über den Assistenten** für QoS zeigt eine Übersicht der QoS-Richtlinien basierend auf Ihrer Auswahl im Assistenten an. Diese Richtlinienzuordnung wird mit der ausgewählten Schnittstelle verknüpft. Alle vom SDM QoS-Assistenten konfigurierten Klassen werden in diesem Bildschirm zusammengefasst. Danach wird eine Teilansicht angezeigt. In dieser werden die Schnittstelle, an die die Richtlinie gebunden ist, der Klassifizierungstyp (NBAR oder DSCP), der Richtlinienname und mehrere der erstellten QoS-Klassen dargestellt.

```
Schnittstelle: FastEthernet0/0

Klassifizierung: DSCP

Richtlinienname: SDM-QoS-Policy-1

Richtliniendetails

------------------------------------------------------------------------
Klassenname: SDM-Voice-1
------------------------------------------------------------------------
Aktiviert: Ja
DSCP abstimmen: ef
Warteschlangenfunktion: LLQ
Bandbreite in Prozent: 33

------------------------------------------------------------------------
Klassenname: SDM-Signalling-1
------------------------------------------------------------------------
Aktiviert: Ja
DSCP abstimmen: cs3,af31
Warteschlangenfunktion: CBWFQ
Bandbreite in Prozent: 5

------------------------------------------------------------------------
Klassenname: SDM-Routing-1
------------------------------------------------------------------------
Aktiviert: Ja
DSCP abstimmen: cs6
Warteschlangenfunktion: CBWFQ
Bandbreite in Prozent: 5
```

```
------------------------------------------------------------------------
Klassenname: class-default
------------------------------------------------------------------------
Aktiviert: Ja
Protokolle abstimmen:
Warteschlangenfunktion: Fair Queueing
Zufällige Ermittlung: Ja

------------------------------------------------------------------------
Klassenname: SDM-Streaming-Video-1
------------------------------------------------------------------------
Aktiviert: Nein
DSCP abstimmen: cs4
```

QoS-Richtlinie bearbeiten

Im Fenster **QoS-Richtlinie bearbeiten** können Sie konfigurierte QoS-Richtlinien anzeigen und ändern und Richtlinien mit Routerschnittstellen verknüpfen.

Regelnamenliste

Wählen Sie einen QoS-Richtliniennamen aus dieser Liste aus, um die Details dieser Richtlinie anzuzeigen.

Schnittstelle

Wenn die angezeigte Richtlinie mit einer Schnittstelle verknüpft ist, wird der Name dieser Schnittstelle angezeigt, wie beispielsweise FastEthernet 0/0.

Zuordnung

Klicken Sie auf diese Option, um die Verknüpfung einer QoS-Richtlinie mit einer Schnittstelle zu ändern. Wenn die Richtlinie derzeit mit einer Schnittstelle verknüpft ist, können Sie die Verknüpfung mit der Richtlinie aufheben oder die Datenverkehrsrichtung ändern, auf die die Richtlinie angewendet wird. Die Schaltfläche **Zuordnung** ist deaktiviert, wenn im Feld **Schnittstelle** eine serielle Frame-Relay-Schnittstelle angezeigt wird.

Schaltflächen für die QoS-Klasse

Anhand der Schaltflächen über dem Klassenlistenbereich können Sie die Klasseninformationen für die Richtlinie bearbeiten oder neu anordnen.

- Schaltfläche **Hinzufügen** – Klicken Sie auf diese Schaltfläche, um eine QoS-Klasse zur Richtlinie hinzuzufügen.
- Schaltfläche **Bearbeiten** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um diese im angezeigten Dialogfeld zu bearbeiten. Die Schaltfläche **Bearbeiten** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Löschen** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um eine QoS-Klasse aus dieser Richtlinie zu entfernen. Die Schaltfläche **Löschen** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Ausschneiden** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um diese aus ihrer derzeitigen Position in der Liste zu entfernen. Verwenden Sie die Schaltfläche **Einfügen**, um die Klasse an der gewünschten Position abzulegen. Die Schaltfläche **Ausschneiden** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Kopieren** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um die Klasseninformationen zu kopieren. Die Schaltfläche **Kopieren** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Einfügen** – Klicken Sie auf diese Schaltfläche, um die kopierten Klasseninformationen zu bearbeiten und einen neuen Namen für die Klasse anzugeben. Wenn Sie **Diese Klasse zur Richtlinie hinzufügen** wählen, wird die Klasse mit den aktivierten Richtlinien in der Klasse abgelegt. Die Schaltfläche **Einfügen** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Nach oben** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um eine Klasse in der Klassenliste nach oben zu verschieben. Diese Schaltfläche kann nur für das Verschieben aktivierter Klassen verwendet werden. Die Schaltfläche **Nach oben** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.
- Schaltfläche **Nach unten** – Wählen Sie eine Klasse aus, und klicken Sie auf diese Schaltfläche, um eine Klasse in der Klassenliste nach unten zu verschieben. Diese Schaltfläche kann nur für das Verschieben aktivierter Klassen verwendet werden. Die Schaltfläche **Nach unten** ist deaktiviert, wenn eine schreibgeschützte QoS-Klasse ausgewählt ist.

Klassenlistenanzeige

Das Fenster **QoS-Richtlinie bearbeiten** zeigt die Details der QoS-Klassen an, aus denen sich die ausgewählte Richtlinie zusammensetzt.

Symbolspalte

Die erste Spalte kann ein Symbol enthalten, das den Status einer QoS-Richtlinie angibt.

Wenn dieses Symbol neben der QoS-Klasse angezeigt wird, ist diese schreibgeschützt und kann nicht bearbeitet, gelöscht oder an eine andere Position in der Klassenliste verschoben werden.

Klassenname

Der Name der QoS-Klasse. Cisco SDM definiert vorab Namen für QoS-Klassen.

Aktiviert

Ein grünes Häkchen zeigt an, dass diese Klasse aktiviert ist. Ein rotes Symbol mit einem weißen X zeigt an, dass die Klasse nicht für diese Richtlinie aktiviert ist. Um eine Klasse zu aktivieren, klicken Sie auf **Bearbeiten**, und aktivieren Sie die Klasse im Fenster **QoS-Klasse bearbeiten**.

Abstimmen

Hier wird angegeben, ob die QoS-Klasse nach Übereinstimmungen für **Beliebige** oder **Alle** der ausgewählten DSCP-Werte sucht. Wenn Sie **Beliebige** wählen, muss der Datenverkehr nur eines der Übereinstimmungskriterien in der Klassenzuordnung erfüllen. Wenn Sie **Alle** wählen, muss der Datenverkehr alle der Übereinstimmungskriterien in der Klassenzuordnung erfüllen. Die gewählten DSCP-Werte werden in der DSCP-Spalte angezeigt.

Klassifizierung

Dieser Teil der Anzeige enthält folgende Spalten:

- DSCP – Die DSCP-Werte, die für eine mögliche Übereinstimmung gewählt wurden.

- Protokolle – Die in dieser QoS-Klasse enthaltenen Protokolle. Eine QoS-Klasse mit Videodatenverkehr kann Protokolle wie cuseeme, netshow und vdolive enthalten. Eine Routing-QoS-Klasse kann Protokolle wie BGP, EIGRP und OSPF enthalten.
- ACL – Der Name oder die Nummer einer ACL, die den Datenverkehr angibt, auf den diese QoS-Klasse angewendet wird.

Aktion

Dieser Teil der Anzeige enthält folgende Spalten:

- Warteschlangenfunktion – Diese Spalte listet den Wartschlangentyp, Class Based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ) oder Fair Queuing, auf, und zeigt die der Klasse zugeordneten Bandbreite an.
- DSCP festlegen – Der DSCP-Wert, der diesem Datenverkehrstyp von der QoS-Klasse zugeteilt wurde.
- Entfernen – Die Spalte zeigt **Ja** an, wenn dieser Datenverkehrstyp entfernt werden soll, und **Nein**, wenn dieser nicht entfernt werden soll.

Schaltflächen „Änderungen übernehmen“ und „Änderungen verwerfen“

Änderungen, die Sie in diesem Fenster vornehmen, werden nicht unmittelbar an den Router gesendet. Um die vorgenommenen Änderungen zu senden, klicken Sie auf **Änderungen übernehmen**. Wenn die in diesem Fenster vorgenommenen Änderungen nicht an den Router gesendet werden sollen, klicken Sie auf **Änderungen verwerfen**.

Verknüpfung mit QoS-Richtlinie herstellen oder aufheben

Verwenden Sie dieses Fenster, um die Verknüpfungen zu ändern, die zwischen einer QoS-Richtlinie und Routerschnittstellen bestehen.

Spalte „Schnittstelle“

In dieser Spalte werden die Routerschnittstellen aufgeführt.

Hinweis Wenn Sie die Schnittstelle auswählen, die SDM für die Kommunikation mit dem Router verwendet, wird die Verbindung zwischen SDM und dem Router entfernt.

Spalte für „Eingehend“

Aktivieren Sie das Feld in dieser Spalte, wenn die QoS-Richtlinie mit eingehendem Datenverkehr auf der ausgewählten Schnittstelle verknüpft werden soll.

Spalte für „Ausgehend“

Aktivieren Sie das Feld in dieser Spalte, wenn die QoS-Richtlinie mit ausgehendem Datenverkehr auf der ausgewählten Schnittstelle verknüpft werden soll.

QoS-Klassenzuordnung hinzufügen oder bearbeiten

Sie können QoS-Datenverkehrsklassen erstellen und bearbeiten sowie angeben, ob die Klasse zur QoS-Richtlinie hinzugefügt werden soll.

Diese Klasse zur Richtlinie hinzufügen

Aktivieren Sie diese Option, um diese QoS-Klasse in die QoS-Richtlinie aufzunehmen. Wenn diese Option nicht aktiviert ist, ist die ausgewählte QoS-Klasse im Fenster **QoS-Richtlinie bearbeiten** als **Deaktiviert** markiert.

Klassenname

Der QoS-Klassenname wird in diesem Feld angezeigt, wenn Sie eine vorhandene Klasse bearbeiten. Sie müssen einen Klassennamen eingeben, wenn Sie eine neue Klasse zu einer Richtlinie hinzufügen oder Informationen aus einer kopierten QoS-Klasse einfügen.

Klassenstandard

Diese Option wird angezeigt, wenn in der QoS-Richtlinie kein class-default vorhanden ist. Klicken Sie auf **Klassenstandard**, wenn Sie class-default – die Standardklasse – hinzufügen möchten, statt eine neue Klasse zu erstellen. Für class-default ist das Festlegen mehrerer Konfigurationsparameter nicht möglich:

- Feld **Klassifizierung** – Sie können keine Klassifizierungskriterien angeben.
- Feld **Aktion** – Sie können nicht angeben, dass Datenverkehr entfernt werden soll. Darüber hinaus können Sie nur die Verwendung von Fair Queuing angeben.

Klassifizierung

Wählen Sie die Elementtypen und Werte, nach denen der Router den Datenverkehr untersuchen soll. Wenn Sie auf **Alle** klicken, muss der Datenverkehr mit allen Kriterien übereinstimmen. Wenn Sie auf **Beliebige** klicken, muss der Datenverkehr nur mit einem einzelnen Kriterium übereinstimmen. Wählen Sie einen Wertetyp aus der Liste aus, und klicken Sie auf **Bearbeiten**, um die Werte anzugeben. Um anzugeben, dass die Klasse beispielsweise mit http, edonkey und smtp übereinstimmen soll, wählen Sie **Protokoll** und klicken auf **Bearbeiten**. Wählen Sie dann die Protokolle im Dialogfeld **Übereinstimmungs-Protokollwerte bearbeiten**, und klicken Sie auf **OK**. Die ausgewählten Protokolle werden in der Spalte **Wert** der Liste **Klassifikation** angezeigt.

Wenn die Klasse mit dem in einer ACL definierten Datenverkehr übereinstimmen soll, klicken Sie auf **Zugriffsregel** und dann auf **Bearbeiten**. Im angezeigten Dialogfeld können Sie eine vorhandene ACL auswählen, eine neue erstellen oder vorhandene Verknüpfungen entfernen, wenn Sie eine QoS-Klasse bearbeiten.

Aktion

Wählen Sie die Aktion aus, die der Router vornehmen soll, wenn dieser Datenverkehr ermittelt, der mit den angegebenen DSCP-Werten übereinstimmt.

- **Entfernen** – Damit wird der Datenverkehr entfernt. Wenn Sie **Entfernen** auswählen, sind die anderen Optionen im Bereich **Aktion** deaktiviert.
- **DSCP festlegen** – Wählen Sie den DSCP-Wert aus, auf den der Datenverkehr zurückgesetzt werden soll.
- **Warteschlangenfunktion** – LLQ ist verfügbar, wenn der Datenverkehr das RTP-Protokoll verwendet oder für DSCP der Wert EF eingestellt ist. Wenn der Datenverkehr nicht über diese Attribute verfügt, ist die LLQ-Option nicht verfügbar. Wenn Sie die Standardklasse – class-default – hinzufügen oder bearbeiten, ist nur Fair Queuing verfügbar.
- **Bandbreite in Prozent** – Der eingegebene Prozentwert wird als absoluter Prozentwert der gesamten Bandbreite auf der Schnittstelle verwendet.

- **Verbleibende Bandbreite in Prozent** – Der eingegebene Prozentwert wird als relativer Prozentwert der gesamten Bandbreite auf der Schnittstelle verwendet. Sie können beispielsweise angeben, dass 30 Prozent der verfügbaren Bandbreite einer Klasse und 60 Prozent der Bandbreite einer anderen QoS-Klasse zugeordnet werden sollen. Um diese Option verwenden zu können, müssen auch alle anderen Klassen diese Option verwenden. Die Option **Verbleibende Bandbreite in Prozent** ist deaktiviert, wenn **LLQ** ausgewählt ist.
- **Zufällige Ermittlung** – Aktiviert WRED (Weighted Random Early Detection) und DWRED (Distributed WRED) auf dem Router. Diese Option ist deaktiviert, wenn **LLQ** ausgewählt ist. Mit Random Early Detection werden Pakete während der Zeitdauer mit hohem Datenverkehrsaufkommen entfernt, indem der Quellhost angewiesen wird, die Übertragungsrate zu reduzieren.

Übereinstimmungs-DSCP-Werte bearbeiten

Um einen DSCP-Wert zur Übereinstimmungsliste hinzuzufügen, wählen Sie einen Wert aus der Spalte **Verfügbare DSCP-Werte** auf der linken Seite aus, und klicken Sie auf die obere Doppelpfeil-Schaltfläche, um diesen zur Spalte **Ausgewählte DSCP-Werte** hinzuzufügen. Um einen Wert aus der Spalte **Ausgewählte DSCP-Werte** zu entfernen, wählen Sie den Wert aus, und klicken Sie auf die untere Doppelpfeil-Schaltfläche.

Übereinstimmungs-Protokollwerte bearbeiten

Um ein Protokoll zu einer Klasse hinzuzufügen, wählen Sie ein Protokoll aus der Spalte **Verfügbare Protokollwerte** auf der linken Seite aus, und klicken Sie auf die obere Doppelpfeil-Schaltfläche, um dieses zur Spalte **Ausgewählte Protokollwerte** hinzuzufügen. Um einen Wert aus der Spalte **Ausgewählte Protokollwerte** zu entfernen, wählen Sie das Protokoll aus, und klicken Sie auf die untere Doppelpfeil-Schaltfläche.

Benutzerdefinierte Protokolle hinzufügen

Über dieses Fenster können Sie benutzerdefinierte Protokolle hinzufügen, die nicht im Fenster **Übereinstimmungs-Protokollwerte bearbeiten** verfügbar sind. So definierten Sie ein benutzerdefiniertes Protokoll:

Schritt 1 Wählen Sie den Namen des benutzerdefinierten Protokolls aus der Liste **Name** aus.

Schritt 2 Wählen Sie aus, ob das Protokoll als TCP- oder UDP-Protokoll verwendet werden soll.

Schritt 3 Definieren Sie die Portnummern, die dieses Protokoll verwenden soll. Geben Sie eine Portnummer in das Feld **Neue Portnummer** ein, und klicken Sie auf **Hinzufügen**, um diese zur Liste der Portnummern hinzuzufügen. Um eine Portnummer aus der Liste zu entfernen, wählen Sie die Nummer aus und klicken auf **Entfernen**.

Übereinstimmungs-ACL bearbeiten

Wählen Sie entweder **Vorhandene Regel (ACL) auswählen** oder **Neue Regel (ACL) erstellen**, **und auswählen**. Es werden zusätzliche Dialogfelder angezeigt, über die Sie eine vorhandene Regel erstellen oder auswählen können. Wenn Sie vorhandene Regelverknüpfungen löschen möchten, können Sie **Keine (Regelverknüpfung aufheben)** wählen.

Übereinstimmungs-DSCP-Werte bearbeiten

Um einen DSCP-Wert zur Übereinstimmungsliste hinzuzufügen, wählen Sie einen Wert aus der Spalte **Verfügbare DSCP-Werte** auf der linken Seite aus, und klicken Sie auf die obere Doppelpfeil-Schaltfläche, um diesen zur Spalte **Ausgewählte DSCP-Werte** hinzuzufügen. Um einen Wert aus der Spalte **Ausgewählte DSCP-Werte** zu entfernen, wählen Sie den Wert aus, und klicken Sie auf die untere Doppelpfeil-Schaltfläche.

KAPITEL 27

Network Admission Control

Network Admission Control (NAC) schützt die Datennetzwerke des Computers, indem der Zustand von Client-Workstations bewertet und zudem sichergestellt wird, dass die neusten verfügbaren Virensignaturen installiert sind und ihr Zugang zum Netzwerk gesteuert wird.

NAC arbeitet mit einer Antivirensoftware, um den Zustand eines Clients (dem so genannten *Posture* des Clients) zu bewerten, bevor der Client einen Zugang zum Netzwerk erhält. NAC stellt sicher, dass ein Netzwerkclient über eine aktuelle Virensignatur verfügt, die selbst nicht infiziert ist. Wenn der Client eine Aktualisierung der Signatur benötigt, führt ihn NAC durch die Aktualisierung. Wenn der Client gefährdet oder ein Virus ausgebrochen ist, stellt NAC den Client in einen geschützten Netzwerkbereich ab, bis die Beseitigung des Virus erfolgreich abgeschlossen wird.

Weitere Informationen über NAC finden Sie unter den nachfolgenden Links:

- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

NAC Register erstellen

Auf der Registerkarte Create NAC (NAC erstellen) und mit dem NAC-Assistenten können Sie eine NAC-Richtlinie erstellen und einer Schnittstelle zuweisen. Nach dem Erstellen der NAC-Richtlinie können Sie diese bearbeiten, indem Sie auf **NAC Bearbeiten** klicken und die Richtlinie aus der Liste auswählen.

Die NAC-Konfiguration im Router ist nur ein Bestandteil einer vollständigen NAC-Implementierung. Klicken Sie auf Andere Aufgaben einer NAC-Implementierung, um die Aufgaben kennen zu lernen, die bei anderen Geräten durchgeführt werden müssen, um eine NAC zu implementieren.

Taste AAA aktivieren

Authentifizierung, Autorisierung und Accounting (AAA) muss auf dem Router aktiviert sein, bevor Sie eine NAC konfigurieren können. Wenn AAA nicht aktiviert ist, klicken Sie auf die Schaltfläche **AAA aktivieren**. Wenn AAA bereits auf dem Router konfiguriert ist, wird diese Schaltfläche nicht angezeigt.

Taste NAC-Assistent starten

Klicken Sie auf diese Taste, um den NAC-Assistenten zu starten. Der NAC-Assistent teilt die NAC-Konfiguration in mehrere Bildschirme auf, in denen Sie jeweils eine Aufgabe der Konfiguration ausführen.

Wie mache ich Liste

Wenn Sie eine Konfiguration erstellen wollen, durch die Sie dieser Assistent nicht führt, klicken Sie auf die Schaltfläche neben der Liste. Es werden weitere Konfigurationsmöglichkeiten aufgelistet, von denen Sie eine vielleicht durchführen wollen. Um zu erfahren, wie eine der aufgelisteten Konfigurationen erstellt wird, wählen Sie die Konfiguration aus und klicken Sie auf **Los**.

Andere Aufgaben einer NAC-Implementierung

Zu einer vollständigen NAC-Implementierung gehören die folgenden Konfigurationsschritte:

Schritt 1 Installieren und konfigurieren Sie die Cisco Trust Agent (CTA) Software auf den Netzwerkhosts. Dadurch verfügen Sie über Hosts mit einem Posture-Agenten, die in der Lage sind auf EAPoUDP-Anfragen vom Router zu antworten. Schauen Sie in den Links nach, die nach diesen Schritten aufgeführt sind, um die CTA-Software zu bekommen und um zu lernen, wie sie zu installieren und zu konfigurieren ist.

Schritt 2 Installieren und konfigurieren Sie einen AAA Authentifizierungs-EAPoUDP-Server. Der Server muss ein Cisco Secure Access Control Server sein und mit dem Protokoll RADIUS laufen. Dafür ist die Cisco Secure Access Control Server Software Version 3.3 Voraussetzung. Schauen Sie auf die Links, die nach diesen Schritten aufgeführt sind, um mehr über das Installieren und Konfigurieren eines ACS zu erfahren.

Schritt 3 Installieren und konfigurieren Sie den Posture-Gültigkeits- und Wiederherstellungsserver.

Wenn Sie ein registrierter Cisco.com Benutzer sind, können Sie die Cisco Trust Agent (CTA) Software von folgendem Link herunterladen.

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

Das Dokument im folgenden Link erklärt, wie die CTA-Software auf einem Host installiert und konfiguriert werden muss.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

Das Dokument im folgenden Link gibt einen Überblick über den Konfigurationsprozess.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Dokumente im folgenden Link erklären, wie Cisco Secure ACS für Windows Server Version 3.3 installiert und konfiguriert werden muss.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

Willkommen

Mit Hilfe des NAC-Assistenten können Sie Folgendes tun:

- Wählen Sie die Schnittstelle aus, auf der NAC aktiviert werden soll – Hosts, die versuchen über diese Schnittstelle einen Zugang zum Netzwerk zu erhalten, müssen den NAC-Gültigkeitsprozess durchlaufen.
- NAC-Regelserver konfigurieren – Zugangssteuerungsregeln werden auf diesen Servern konfiguriert. Der Router nimmt Verbindung mit ihnen auf, wenn ein Netzwerkhost versucht, Zugang zum Netzwerk zu erhalten. Sie können Informationen für mehrere Server festlegen. NAC-Regelserver arbeiten mit den Protokoll RADIUS.
- Eine NAC-Ausnahmeliste konfigurieren – Hosts, wie z.B. Drucker, IP-Telefone und Hosts ohne installierten NAC-Posture-Agent, müssen den NAC-Prozess wahrscheinlich umgehen. Hosts mit statischen IP-Adressen und anderen Geräten können in einer Ausnahmeliste festgehalten und mit einer verknüpften Ausnahmeregel behandelt werden. Hosts können auch durch ihre MAC-Adresse oder ihren Gerätetyp bestimmt werden
- Eine Regel für einen Host ohne Agent konfigurieren – Wenn Sie eine Regel auf einen Cisco Secure ACS-Server legen wollen, um Hosts ohne einen installierten Posture-Agenten zu behandeln, können Sie dies tun. Wenn der Cisco Secure ACS-Server ein Paket von einem Host ohne Agent erhält, antwortet er mit der Regel für einen Host ohne Agent. Eine Regel für einen Host ohne Agent zu konfigurieren ist sinnvoll, wenn es dynamisch angesprochene Hosts ohne Agenten gibt, wie z.B. DHCP-Clients.
- NAC für den Remote-Zugriff konfigurieren – Hosts, die Cisco SDM zum Verwalten von Routern benutzen, muss der Zugriff auf den Router gewährt werden. Im Assistenten können Sie IP-Adressen für das Remote-Management einrichten, sodass Cisco SDM die NAC ACL so anpasst, dass alle Hosts mit diesen Adressen Zugriff auf den Router erhalten.

Das Konfigurieren von NAC auf dem Router ist der letzte Schritt bei einer NAC-Konfiguration. Bevor Sie den Router mit dieser Funktion konfigurieren, müssen Sie die Schritte erledigen, die im nachfolgenden Link beschrieben sind: Andere Aufgaben einer NAC-Implementierung.

NAC-Richtlinienserver

NAC Zutrittssteuerungsregeln werden in einer Regeldatenbank konfiguriert und gespeichert, die auf RADIUS-Servern liegt, auf denen Cisco Secure ACS Version 3.3 läuft. Der Router muss die Anmeldeinformationen von Netzwerkhosts für gültig erklären, indem er mit dem RADIUS-Server kommuniziert. Benutzen Sie dieses Fenster, um die Informationen einzugeben, die der Router braucht, um den Kontakt mit den RADIUS-Servern aufzunehmen. Auf jedem RADIUS-Server, den Sie festlegen, muss die Cisco Secure Cisco Access Control Server (ACS) Software Version 3.3 installiert und konfiguriert sein.

Die RADIUS-Clientquelle auswählen

Das Konfigurieren der RADIUS-Quelle ermöglicht Ihnen, die Quellen-IP-Adresse festzulegen und in RADIUS-Paketen an den RADIUS-Server zu senden. Wenn Sie weitere Informationen über eine Schnittstelle benötigen, wählen Sie die Schnittstelle aus und klicken Sie auf die Schaltfläche **Details**.

Die Quellen-IP-Adresse in den RADIUS-Paketen, die vom Router gesendet werden, muss als die NAD-IP-Adresse in der Cisco ACS Version 3.3 oder später konfiguriert werden.

Wenn Sie **Router wählt Quelle aus** aktivieren, ist die IP-Quelladresse in den RADIUS-Paketen die Adresse der Schnittstelle, über die die RADIUS-Pakete den Router verlassen.

Wenn Sie eine Schnittstelle auswählen, ist die Quellen-IP-Adresse in den RADIUS-Paketen die Adresse der Schnittstelle, die Sie als die RADIUS-Clientquelle ausgewählt haben.

Hinweis Cisco IOS-Software gestattet die Konfiguration einer Single-RADIUS-Quellschnittstelle auf dem Router. Wenn der Router bereits eine RADIUS-Quelle konfiguriert hat und Sie eine andere Quelle auswählen, ändert sich die IP-Adresse, die in den Paketen an den RADIUS-Server steht, in die IP-Adresse der neuen Quelle und kann dann eventuell nicht mehr mit der NAD-IP-Adresse auf dem konfigurierten Cisco ACS übereinstimmen.

Schaltfläche Details

Klicken Sie auf **Details**, um einen kurzen Einblick in die Informationen über eine Schnittstelle zu erhalten, bevor Sie diese auswählen. Auf dem Bildschirm werden die IP-Adresse und die Subnetzmaske, die der Schnittstelle zugewiesenen Zugriffsregeln und die Prüfregeln, die zugewiesenen IPSec- und QoS-Richtlinien angezeigt und angegeben, ob Easy VPN für die Schnittstelle konfiguriert wurde.

Spalten Server-IP, Timeout und Parameter

Die Spalten Server-IP, Timeout und Parameter enthalten die Informationen, die der Router für den Kontakt mit einem RADIUS-Server braucht. Wenn keine RADIUS-Server Informationen mit der ausgewählten Schnittstelle verknüpft sind, sind diese Spalten leer.

Zweck des Kästchens NAC

Aktivieren Sie dieses Kästchen, wenn Sie die aufgelisteten RADIUS-Server für NAC benutzen wollen. Auf den Servern müssen die erforderlichen Zugangssteuerungsregeln konfiguriert sein, wenn NAC in der Lage ist, die Server zu benutzen.

Tasten Hinzufügen, Bearbeiten und Ping

Um Informationen zu einem RADIUS-Server anzugeben, klicken Sie auf die Taste **Hinzufügen** und geben Sie die Informationen in den angezeigten Bildschirm ein. Wählen Sie eine Zeile aus und klicken Sie auf **Bearbeiten**, um die Informationen zu einem RADIUS-Server zu ändern. Wählen Sie eine Zeile aus und klicken Sie auf **Ping**, um die Verbindung zwischen Router und RADIUS-Server zu testen.

Hinweis Wenn Sie einen Ping-Test durchführen, geben Sie die IP-Adresse der RADIUS-Quellschnittstelle in das Feld **Quelle** im Dialogfeld **Ping** ein. Wenn Sie die Option **Router wählt Quelle** ausgewählt haben, müssen Sie keinen Wert in das Feld **Quelle** im Dialogfeld **Ping** eingeben.

Die Schaltflächen **Bearbeiten** und **Ping** sind deaktiviert, wenn für die ausgewählte Schnittstelle keine RADIUS-Server-Informationen zur Verfügung stehen.

Auswahl der Schnittstelle

Wählen Sie die Schnittstelle aus, auf der NAC in diesem Fenster aktiviert werden soll. Wählen Sie die Schnittstelle aus, durch welche Netzwerkhosts Verbindung zum Netzwerk aufnehmen.

Klicken Sie auf die Schaltfläche **Details**, um die mit der ausgewählten Schnittstelle verknüpften Richtlinien anzuzeigen. Im Fenster werden die Namen der ACLs angezeigt, die auf den eingehenden und ausgehenden Datenverkehr der Schnittstelle angesetzt wurden.

Wenn eine eingehende ACL bereits an der Schnittstelle vorhanden ist, benutzt Cisco SDM diese ACL für NAC, indem SDM entsprechende Erlaubniserklärungen für EAPoUDP-Verkehr hinzufügt. Wenn die IP-Adresse auf der Schnittstelle 192.55.22.33 lautet, auf die NAC angewendet wird, kann eine Erlaubniserklärung wie folgt lauten:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

Die von Cisco SDM erstellte permit-Anweisung verwendet Port Nummer 21862 für das EAPoUDP-Protokoll. Wenn EAPoUDP von den Netzwerkhosts über eine spezielle Portnummer eingesetzt wird, müssen Sie diesen ACL-Eintrag entsprechend ändern und die von den Hosts verwendete Portnummer eintragen.

Wenn keine eingehende ACL an der festgelegten Schnittstelle konfiguriert wurde, können Sie Cisco SDM auffordern, eine ACL an der Schnittstelle anzuwenden. Sie können eine empfohlene Regel oder eine Regel, die einfach berichtete NAC-Postures überwacht, auswählen.

- **Strikte Gültigkeit (empfohlen)** – Cisco SDM wendet eine ACL an, die jeglichen Datenverkehr (**deny ip any any**) ablehnt. Der Zutritt zum Netzwerk wird durch den NAC-Gültigkeitsprozess festgelegt. Standardmäßig wird jeder Datenverkehr abgelehnt, außer wenn der Verkehr durch die konfigurierte Regel auf dem NAC-Regelserver für gültig erklärt wird.
- **NAC Postures überwachen** – Cisco SDM wendet eine ACL an, die jeglichen Verkehr (**permit ip any any**) zulässt. Nach dem NAC-Gültigkeitsprozess kann es sein, dass der Router Regeln vom NAC-Server erhält, die den Zugang zu bestimmten Hosts ablehnen. Sie können die Einstellung **NAC-Postures überwachen** benutzen, um die Wirkungsweise der NAC-Konfiguration auf das Netzwerk zu bestimmen. Im Anschluss können Sie die Richtlinien auf dem NAC-Richtlinienserver anpassen und anschließend NAC auf dem Router auf **Strikte Gültigkeit** umstellen. Dazu verändern Sie mithilfe der Cisco SDM Firewall-Richtlinienfunktion die auf die Schnittstelle angesetzte ACL und geben **deny ip any any** ein.

NAC-Ausnahmeliste

Sie können Hosts festlegen, denen es gestattet werden muss, den NAC-Gültigkeitsprozess zu umgehen. Normalerweise werden Hosts, wie z.B. Drucker, IP-Telefone und Hosts ohne installierte NAC-Posture-Agent-Software der Ausnahmeliste hinzugefügt.

Wenn es auf Ihrem Netzwerk Hosts ohne statische Adressen gibt, wird empfohlen, dass sie in der Hostregel ohne Agent eingetragen werden und nicht in der NAC-Ausnahmeliste. Bei der NAC-Ausnahmeregel kann es sein, dass sie nicht sauber arbeitet, wenn sich Host-IP-Adressen ändern.

Wenn Sie den NAC-Assistenten verwenden und Sie keine NAC-Ausnahmeliste konfigurieren müssen, können Sie auf **Weiter** klicken, ohne Informationen in dieses Fenster einzugeben. Als Alternative oder Ergänzung zur NAC-Ausnahmeliste ermöglicht Ihnen der Assistent, eine Hostregel ohne Agent in einem anderen Fenster zu konfigurieren.

Spalten IP-Adresse/MAC-Adresse/Gerätetyp, Adresse/Gerät und Regel

Diese Spalten enthalten Informationen über einen Host in der Ausnahmeliste. Ein Host kann durch seine IP-Adresse, seine MAC-Adresse oder seinen Gerätetyp bestimmt werden. Wenn er durch eine Adresse bestimmt wird, wird die IP-Adresse oder MAC-Adresse in der Zeile zusammen mit dem Namen der Regel angezeigt, welche den Hostzugang in das Netzwerk regelt.

Tasten Hinzufügen, Bearbeiten und Löschen

Stellen Sie die Ausnahmeliste zusammen, indem Sie auf **Hinzufügen** klicken und Informationen über den Host eingeben. Sie können die Schaltfläche **Hinzufügen** beliebig oft benutzen.

Wählen Sie eine Zeile aus, und klicken Sie auf **Bearbeiten**, um die Informationen über einen Host zu ändern. Klicken Sie auf **Löschen**, um die Informationen über einen Host aus diesem Fenster zu löschen. Die Schaltflächen **Bearbeiten** und **Löschen** sind deaktiviert, wenn in der Liste keine Informationen vorhanden sind.

Einen Eintrag in der Ausnahmeliste hinzufügen oder bearbeiten

In diesem Fenster können Sie die Informationen in einer Ausnahmeliste bearbeiten oder neue hinzufügen.

Listentyp

Hosts werden über die Art und Weise ihrer Identifizierung ausgewählt. Diese Liste enthält die folgenden Auswahlmöglichkeiten:

- IP-Adresse—Wählen Sie diese Möglichkeit aus, wenn Sie den Host über seine IP-Adresse bestimmen wollen.
- MAC-Adresse— Wählen Sie diese Möglichkeit aus, wenn Sie den Host über seine MAC-Adresse bestimmen wollen.
- Cisco IP-Telefon—Wählen Sie diese Möglichkeit aus, wenn Sie die Cisco IP-Telefone im Netzwerk in die Ausnahmeliste aufnehmen wollen.

Feld Adresse bestimmen

Wenn Sie die IP-Adresse oder die MAC-Adresse als den Hosttyp auswählen, geben Sie die Adresse in dieses Feld ein. Wenn Sie einen Gerätetyp auswählen, ist dieses Feld deaktiviert.

Feld Regel

Wenn Sie den Namen der Ausnahmeregel kennen, geben Sie ihn in diesem Feld ein. Klicken Sie auf das Feld mit den drei Punkten, das sich an der rechten Seite des Feldes Regel befindet, um eine bestehende Regel auszuwählen oder ein Dialogfeld anzuzeigen, in dem Sie eine neue Regel erstellen können.

Wählen Sie eine Ausnahmerichtlinie aus

Wählen Sie die Regel aus, die Sie für den Host anwenden wollen. Wenn Sie eine Regel auswählen, erscheint die für die Regel festgelegte umadressierte URL in dem Feld, in dem nur gelesen werden kann.

Wenn in der Liste keine Richtlinien zur Verfügung stehen, klicken Sie auf **Abbrechen**, um zum Assistenten zurückzukehren. Wählen Sie anschließend die Option aus, mit der Sie eine neue Richtlinie hinzufügen können.

Wählen Sie die Richtlinie aus, die Sie auf den erwarteten Host aus der Liste anwenden wollen. Wenn in der Liste keine Richtlinien eingetragen sind, klicken Sie auf **Abbrechen**, um zum Assistenten zurückzukehren. Wählen Sie anschließend **Neue Regel erstellen**, und fügen Sie diese im Fenster Ausnahmeliste hinzu.

URL umlenken: URL-Feld

Dieses Feld kann nur gelesen werden. Es zeigt die umadressierte URL an, die mit der von Ihnen ausgewählten Regel verknüpft ist. Hosts, an denen diese Regel angewendet wird, werden zu dieser URL umadressiert, wenn sie versuchen, Zugang zum Netzwerk zu bekommen.

Vorschau der Zugriffsregel

Die Spalten Aktion, Quelle, Ziel und Service zeigen die Einträge in der Zugriffsregel an, die mit der Regel verknüpft ist. Diese Spalten sind leer, wenn für diese Regel keine ACL verknüpft ist.

Ausnahmerichtlinie hinzufügen

In diesem Fenster können Sie eine neue Ausnahmeregel erstellen.

Um eine neue Ausnahmeregel zu erstellen, geben Sie einen Namen für die Regel ein. Anschließend geben Sie entweder die Zugriffsregel an, welche die IP-Adressen festlegt, über welche die Hosts durch die Ausnahmeregel Zugang erhalten können oder Sie geben eine umadressierte URL ein. In der umadressierten URL sollten die Wiederherstellungsinformationen enthalten sein, mit denen Benutzer Ihre Virendefinitionsdateien aktualisieren können. Sie müssen entweder einen Namen für eine Zugriffsregel oder eine umadressierte URL bereithalten. Sie können beides angeben.

Feld Name

Geben Sie den Namen der Regel in dieses Feld ein. Verwenden Sie für den Namen keine Fragezeichen (?) oder Leerzeichen. Der Regelname darf nicht mehr als 256 Zeichen umfassen.

Feld Zugriffsregel

Geben Sie den Namen für die Zugriffsregel ein, die Sie benutzen wollen oder klicken Sie auf die Taste auf der rechten Seite des Feldes, um nach einer Zugriffsregel zu suchen oder eine neue Zugriffsregel zu erstellen. Die Zugriffsregel muss über Einträge verfügen, welche die IP-Adressen angeben, mit denen Hosts auf der Ausnahmeregel eine Verbindung erstellen können. Die Zugriffsregel muss eine ACL mit Namen sein, nummerierte ACLs werden nicht unterstützt.

Feld umadressierte URL

Geben Sie eine URL ein, welche die Wiederherstellungsinformationen Ihres Netzwerks enthält. In diesen Informationen können z.B. Hinweise für das Herunterladen von Virendefinitionsdateien sein.

Eine Wiederherstellungs-URL könnte wie folgt aussehen:

```
http://172.23.44.9/update
```

Umadressierte URLs haben normalerweise das Format `http://URL` oder `https://URL`.

Regel für agentlosen Host

Wenn auf dem Cisco Secure ACS Server eine Regel für Hosts ohne Agent existiert, kann der Router diese Regel dazu benutzen, um mit Hosts ohne installiertem Posture-Agenten umzugehen. Die Methode zum Umgang mit Hosts ohne Agent kann als Alternative oder Ergänzung zu einer NAC-Ausnahmeliste benutzt werden. Wenn Sie mit dem NAC-Assistenten arbeiten und Sie keine Regel für Hosts ohne Agent konfigurieren müssen, können Sie auf **Weiter** klicken, ohne Informationen in dieses Fenster einzugeben.

Das Kästchen Hosts ohne Agent authentifizieren

Aktivieren Sie dieses Kästchen, um anzugeben, dass Sie die Regel für Hosts ohne Agent auf dem Cisco Secure ACS Server benutzen wollen.

Felder Benutzername und Kennwort

Einige Cisco IOS-Softwareimages erfordern zusammen mit der Anfrage an den Cisco Secure ACL Server die Eingabe eines Benutzernamens und eines Kennworts. Wenn dies verlangt wird, geben Sie den auf dem Cisco Secure ACS Server für diesen Zweck konfigurierten Benutzernamen und das Kennwort ein. Wenn das Cisco IOS-Softwareimage diese Informationen nicht benötigt, erscheinen diese Felder nicht.

NAC für Remotezugriff konfigurieren

Durch das Konfigurieren des NAC für den Remote-Zugriff können Sie die ACLs anpassen, die die NAC-Konfiguration erstellt, sodass Cisco SDM-Datenverkehr zugelassen wird. Geben Sie die Hosts an, die in der Lage sein müssen, Cisco SDM für den Zugriff auf den Router zu benutzen.

Cisco SDM Remote Management aktivieren

Aktivieren Sie diese Option, um Cisco SDM Remote Management an der genannten Schnittstelle zu aktivieren.

Felder Host/Netzwerkadresse

Wenn Cisco SDM die ACL so ändern soll, dass der Cisco SDM-Datenverkehr von einem einzelnen Host zugelassen wird, wählen Sie **Hostadresse** und geben die IP-Adresse eines Hosts ein. Wählen Sie **Netzwerkadresse**, und geben Sie die Adresse eines Netzwerks und einer Subnetzmaske ein, um Cisco SDM-Datenverkehr von Hosts aus dem jeweiligen Netzwerk zuzulassen. Der Host oder das Netzwerk müssen von denen von Ihnen angegebenen Schnittstellen erreichbar sein. Wählen Sie **Beliebige** aus, um Cisco SDM-Datenverkehr von jedem Host zuzulassen, der mit den angegebenen Schnittstellen verbunden ist.

Firewall ändern

Cisco SDM überprüft jede auf die Schnittstelle angewendete ACL, die in dieser Konfiguration angegeben ist, um zu ermitteln, ob Datenverkehr blockiert wird, für den das Passieren durch die Firewall erlaubt werden soll, sodass die von Ihnen zu konfigurierende Funktion funktioniert.

Jede Schnittstelle wird zusammen mit dem Dienst, der auf der jeweiligen Schnittstelle zurzeit blockiert wird, sowie mit der ACL aufgeführt, die für die Blockierung verantwortlich ist. Wenn Cisco SDM die ACL so ändern soll, sodass der aufgelistete Datenverkehr zugelassen wird, aktivieren Sie in der jeweiligen Zeile das Feld **Anpassen**. Um den Eintrag anzuzeigen, bevor Cisco SDM den ACL-Eintrag vornimmt, klicken Sie auf die Schaltfläche **Details**.

In der folgenden Tabelle wurde FastEthernet0/0 für NAC konfiguriert. Diese Schnittstelle wurde mit den in der Spalte Service aufgeführten Diensten konfiguriert.

Schnittstelle	Dienst	ACL	Aktion
FastEthernet0/0	RADIUS Server	101 (EINGEHEND)	[ ] Anpassen
FastEthernet0/0	DNS	100 (EINGEHEND)	[ ] Anpassen
FastEthernet0/0	DHCP	100 (EINGEHEND)	[ ] Anpassen
FastEthernet0/0	NTP	101 (EINGEHEND)	[ ] Anpassen
FastEthernet0/0	VPN	190 (EINGEHEND)	[ ] Anpassen

Fenster Details

Dieses Fenster zeigt die Einträge an, die Cisco SDM zu den ACLs hinzufügt, um Dienste zuzulassen, die für die von Ihnen zu konfigurierenden Dienste benötigt werden. Das Fenster kann Einträge wie den folgenden enthalten:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

In diesem Fall wird Webdatenverkehr mit einer Portnummer größer als 1024 vom Host 10.77.158.84 auf dem lokalen Netzwerk für den Host 10.77.158.1 zugelassen.

Übersicht über die Konfiguration

Dieses Fenster fast die von Ihnen eingegebenen Informationen zusammen und gibt Ihnen die Möglichkeit, alle Angaben in einem einzigen Fenster zu kontrollieren. Sie können mit der Taste Zurück auf die einzelnen Seiten des Assistenten zurückkehren, um Informationen zu ändern. Klicken Sie auf **Beenden**, um die Konfiguration an den Router zu schicken.

Hier finden Sie ein Beispiel für eine Zusammenfassung einer NAC-Konfiguration

```
NAC-Schnittstelle:  FastEthernet0/1.42
Zulassungsname:  SDM_EOU_3


AAA Client-Quellschnittstelle: FastEthernet0/1.40
NAC Policy Server 1:   10.77.158.54

Ausnahmeliste
-------------------------------------------------------------------------
Address/Device     IP Address       (22.22.22.2) newly added
Richtliniendetails:
Richtlinienname:          P55
       URL umlenken:  http://www.fix.com
        Zugriffsregel:   test11

-------------------------------------------------------------------------


Hostregel ohne Agent aktiviert
Benutzername:  bill
Kennwort:   ******
```

Bei diesem Beispiel enthalten die RADIUS-Pakete die IP-Adresse von FastEthernet 0/1.40. NAC ist auf FastEthernet 0/1.42 aktiviert und die NAC-Richtlinie, die der Assistent eingesetzt hat, lautet SDM_EOU_3. In der Ausnahmenliste ist ein Host aufgeführt. Dessen Zugang zu dem Netzwerk wird über die Ausnahmenrichtlinie P55 geregelt.

Register NAC Bearbeiten

Im Register NAC Bearbeiten werden die auf dem Router konfigurierten NAC-Regeln aufgelistet. Sie können dort weitere NAC-Einstellungen vornehmen. Für jede Schnittstelle, an der die Posture-Gültigkeit durchgeführt wird, muss eine NAC-Regel konfiguriert werden.

Taste NAC-Timeouts

Router und Client verwenden das EAPoUDP-Protokoll (Extensible Authentication Protocol over Unformatted Data Protocol), um Posture-Informationen auszutauschen. Standardwerte für EAPoUDP Timeout-Einstellungen sind bereits konfiguriert, Sie können die Einstellungen jedoch ändern. Diese Taste ist deaktiviert, wenn auf dem Router keine NAC-Regel konfiguriert wurde.

Taste Hostregel ohne Agent

Wenn auf dem Cisco Secure ACS Server eine Regel für Hosts ohne Agent existiert, kann der Router diese Regel dazu benutzen, um mit Hosts ohne installiertem Posture-Agenten umzugehen. Diese Methode für den Umgang mit Hosts ohne Agenten kann benutzt werden, wenn solche Hosts keine IP-Adressen haben. Diese Taste ist deaktiviert, wenn auf dem Router keine NAC-Regel konfiguriert wurde.

Tasten Hinzufügen, Bearbeiten und Löschen

Mit diesen Schaltflächen können Sie die NAC-Richtlinienliste verwalten. Klicken Sie auf **Hinzufügen**, um eine neue NAC-Richtlinie zu erstellen. Benutzen Sie die Tasten Bearbeiten und Löschen, um NAC-Regeln anzupassen oder zu löschen. Die Schaltflächen **Bearbeiten** und **Löschen** sind deaktiviert, wenn auf dem Router keine NAC-Richtlinien konfiguriert sind.

Es ist nur die Taste Hinzufügen aktiviert, wenn auf dem Router keine NAC-Regel konfiguriert wurde. Die Taste Hinzufügen ist deaktiviert, wenn alle Router-Schnittstellen mit einer NAC-Regel konfiguriert wurden.

Liste mit den NAC-Regeln

Der Name, die Schnittstelle auf welche die NAC-Regel angewendet wird und die Zugriffsregel, welche die Regel definiert, sind Bestandteile der Liste. Wenn Sie NAC mit dem NAC-Assistenten Erstellen an einer Schnittstelle aktiviert haben, erscheint in dieser Liste die Standard-NAC-Regel SDM_EOU_1.

NAC-Komponenten

In diesem Fenster wird eine kurze Beschreibung der EAPoUDP-Komponenten bereitgestellt, die Sie mit Cisco SDM konfigurieren können.

Fenster Ausnahmeliste

Dieses Platzhalterthema wird entfernt, wenn das Hilfssystem für NAC aufgebaut wird. Dieses Hilfethema wurde bereits im Assistentenmodus geschrieben. Um es anzusehen, klicken Sie auf den folgenden Link:

NAC-Ausnahmeliste

Fenster Ausnahmeregeln

NAC-Ausnahmeregeln steuern den Netzwerkzugang von Hosts in der Ausnahmeliste. Eine NAC-Ausnahmeregel besteht aus einem Namen, einer Zugriffsregel und/oder einer umadressierten URL. Die Zugriffsregel gibt die Zielorte an, zu denen von der Regel bestimmte Hosts Zugang haben. Wenn in der Regel eine umadressierte URL angegeben ist, kann die Regel Webclients auf Seiten führen, die Informationen darüber enthalten, wie der neuste verfügbare Virenschutz bezogen werden kann.

Ein Beispieleintrag einer NAC-Regel wird in der folgenden Tabelle gezeigt:

Name	Zugriffsregel	URL umlenken
NACLess	nac-rule	http://172.30.10/update

Zugriffsregeln, die mit NAC-Regeln verknüpft sind, müssen erweiterte ACLs sein und einen Namen haben. Ein Beispiel einer Zugriffsregel, die in einer NAC-Regel benutzt werden könnte, wird in der folgenden Tabelle gezeigt:

Aktion	Quelle	Ziel	Dienst	Protokoll	Attribute
permit	any	172.30.2.10	ip		

Diese Regel erlaubt jedem Host, der von einer Regel bestimmt wird, IP-Verkehr an die IP-Adresse 172.30.2.10 zu senden.

Tasten Hinzufügen, Bearbeiten und Löschen

Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Ausnahmeregel zu erstellen. Passen Sie mit der Schaltfläche **Bearbeiten** existierende Ausnahmeregeln an. Mit der Schaltfläche **Löschen** können Sie Ausnahmeregeln entfernen. Die Schaltflächen Bearbeiten und Löschen sind deaktiviert, wenn in der Liste keine Ausnahmeregeln vorkommen.

NAC Timeouts

Konfigurieren Sie die Timeoutwerte, die der Router für die EAPoUDP-Kommunikation mit den Netzwerkhosts benutzt. Die Standard-, Minimum- und Maximumwerte werden in der folgenden Tabelle für alle Einstellungen gezeigt.

Wert	Standard	Minimum	Maximum
Hold Period Timeout	180 Sekunden	60 Sekunden	86400 Sekunden
Neuübertragungs-Timeout	3 Sekunden	1 Sekunde	60 Sekunden
Revalidation Timeout	36000 Sekunden	300 Sekunden	86400 Sekunden
Status Query Timeout	300 Sekunden	30 Sekunden	1800 Sekunden

Auswahl der Schnittstelle

Wählen Sie die Schnittstelle aus, auf welche die NAC-Timeouteinstellungen angewendet werden sollen.

Feld Hold Period Timeout

Geben Sie die Anzahl der Sekunden ein, für die der Router Pakete von Clients ignorieren soll, bei denen gerade die Authentifizierung fehlgeschlagen ist.

Feld Retransmit Timeout

Geben Sie die Anzahl der Sekunden ein, die der Router warten soll, bevor er erneut EAPoUDP Meldungen an den Client schickt.

Feld Revalidation Timeout

Der Router fragt in bestimmten Zeitabständen den Posture-Agent auf dem Client ab, um die Einhaltung der Sicherheitsrichtlinie zu kontrollieren. Geben Sie die Anzahl der Sekunden ein, die der Router zwischen den einzelnen Abfragen warten soll.

Feld Status Query Timeout

Geben Sie die Anzahl der Sekunden ein, die der Router zwischen den Anfragen an den Posture-Agent auf dem Host warten soll.

Taste Auf Standardwerte zurücksetzen

Klicken Sie auf diese Taste, um alle NAC-Timeouts auf ihre Standardwerte zurückzusetzen.

Kästchen, in dem diese Timeoutwerte global konfiguriert werden

Aktivieren Sie das Kästchen, damit diese Werte auf alle Schnittstellen angewendet werden.

Eine NAC-Regel konfigurieren

Eine NAC-Regel aktiviert den Posture-Gültigkeitsprozess an einer Routerschnittstelle und kann für die Bestimmung von Verkehrstypen benutzt werden, die im Zutrittssteuerungsprozess von der Posture-Gültigkeitsregel befreit werden sollen.

Feld Name

Geben Sie für die Regel einen Namen ein.

Eine Schnittstellenliste auswählen

Wählen Sie die Schnittstelle aus, an der Sie die NAC-Regel anwenden wollen. Wählen Sie eine Schnittstelle aus, die Netzwerkclients zum Router verbindet.

Feld Zutrittsregel

Sie können eine Zugriffsregel benutzen, um festgelegten Verkehr vom Auslösen des Zutrittssteuerungsprozesses zu befreien. Dies wird nicht verlangt. Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die Sie für die Zutrittsregel benutzen wollen. Sie können auch auf die Taste an der rechten Seite dieses Feldes klicken und nach der Zugriffsregel suchen oder eine neue Zugriffsregel erstellen.

Die Zugriffsregel muss Ablehnungsregelungen beinhalten, aus denen hervorgeht, welcher Verkehr vom Zutrittssteuerungsprozess befreit werden soll. Die Posture-Gültigkeit wird nicht ausgelöst, wenn die Zugriffsregeln ausschließlich aus Ablehnungsregelungen besteht.

Im Folgenden sind Beispieleinträge einer ACL für eine NAC-Zutrittsregel aufgeführt:

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
permit ip any any
```

Die erste Ablehnungsregelung befreit Verkehr mit dem Ziel Port 53 (Domäne) und die zweite Regelung befreit Verkehr mit dem Ziel Port 80 (www). Die Erlaubnisregelung am Ende der ACL stellt sicher, dass die Posture-Gültigkeit durchgeführt wird.

Wie gehe ich vor?

Die folgenden Themen enthalten Verfahren, um Aufgaben durchzuführen, bei denen Sie vom NAC-Assistenten Erstellen keine Hilfe bekommen.

Wie konfiguriere ich einen NAC-Regelserver?

Der Router muss eine Verbindung zu einem Cisco Secure Access Control Server (ACS) haben, auf dem die ACS-Software Version 3.3 läuft. Der ACS muss für die Benutzung des RADIUS-Protokolls konfiguriert sein, damit NAC implementiert werden kann. Das Dokument im folgenden Link gibt einen Überblick über den Konfigurationsprozess.

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns466/c654/cdccont_0900aecd80217e26.pdf

Dokumente im folgenden Link erklären, wie Cisco Secure ACS für Windows Server Version 3.3 installiert und konfiguriert werden muss.

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs33/index.htm

Wie installiere und konfiguriere ich einen Posture-Agent auf einem Host?

Wenn Sie ein registrierter Cisco.com Benutzer sind, können Sie die Cisco Trust Agent (CTA) Software von folgendem Link herunterladen.

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

Das Dokument im folgenden Link erklärt, wie die CTA-Software auf einem Host installiert und konfiguriert werden muss.

http://www.cisco.com/en/US/products/ps5923/products_administration_guide_book09186a008023f7a5.html

Die angegeben Installationsverfahren, die erforderlich sind, um eine dritte Software für Posture-Agenten und den optionalen Wiederherstellungsserver zu installieren, variieren je nach benutzter Software. Schauen Sie in der Dokumentation des Verkäufers nach, um vollständige Informationen darüber zu bekommen.

KAPITEL 28

Routereigenschaftean

Mit den Routereigenschaften können Sie die allgemeinen Attribute des Routers, beispielsweise den Routernamen, den Domänennamen, das Kennwort, den Simple Network Management Protocol (SNMP)-Status, die Serveradresse des Domänennamensystems (DNS), Benutzerkonten, Protokollattribute des Routers, Virtual Type Terminal (vty)-Einstellungen, SSH-Einstellungen und weitere Sicherheitseinstellungen für den Routerzugriff definieren.

Geräteeigenschaften

Der Bildschirm **Eigenschaften – Gerät** enthält Informationen zum Host, der Domäne und dem Kennwort Ihres Routers.

Registerkarte „Geräte“

Die Registerkarte **Gerät** enthält die folgenden Felder.

Host

Geben Sie den gewünschten Namen für den Router in dieses Feld ein.

Domäne

Geben Sie den Domänennamen für Ihre Organisation ein. Wenn Sie den Domänennamen nicht kennen, lassen Sie ihn sich von Ihrem Netzwerkadministrator geben.

Text für Banner eingeben

Geben Sie den Text für das Banner des Routers ein. Das Textbanner des Routers wird immer dann angezeigt, wenn sich jemand beim Router anmeldet. Wir empfehlen, dass Ihr Text-Banner eine Meldung enthalten sollte, die erklärt, dass unautorisierter Zugriff verboten ist.

Registerkarte „Kennwort"

Die Registerkarte **Kennwort** enthält die folgenden Felder.

Geheimes Kennwort aktivieren

Cisco Router and Security Device Manager (Cisco SDM) unterstützt das geheime Kennwort. Mit dem geheimen Kennwort können Sie steuern, wer Konfigurationsbefehle auf diesem Router ausführen darf. Wir empfehlen sehr, dass Sie **geheimes Kennwort aktivieren** einstellen. Das Kennwort kann im Fenster für die Cisco SDM-Geräteeigenschaften nicht gelesen werden und erscheint in der Datei Router-Konfiguration verschlüsselt. Daher sollten Sie sich dieses Kennwort notieren, damit Sie es nicht vergessen.

Die Cisco IOS-Version, die auf dem Router ausgeführt wird, unterstützt möglicherweise zusätzlich das Aktivierungskennwort. Das Aktivierungskennwort funktioniert wie das geheime Kennwort, wurde jedoch in der Konfigurationsdatei verschlüsselt. Wenn das Aktivierungskennwort mit der Befehlszeilenschnittstelle (Command-Line Interface, CLI) konfiguriert wurde, wird es bei der Konfiguration eines geheimen Kennworts ignoriert.

Aktuelles Kennwort

Wenn bereits ein Kennwort festgelegt wurde, werden in diesem Feld Sternchen (*) angezeigt.

Neues Kennwort eingeben

Geben Sie in dieses Feld das neue Aktivierungskennwort ein.

Neues Kennwort erneut eingeben

Geben Sie hier das Kennwort erneut exakt genauso wie im Feld **Neues Kennwort** ein.

Datum und Uhrzeit: Takteigenschaften

In diesem Fenster können Sie die Datums- und Uhrzeiteinstellungen auf dem Router anzeigen.

Datum/Zeit:

Die Datums- und Uhrzeiteinstellungen des Routers werden rechts in der Cisco SDM-Statusleiste angezeigt. Die Datums- und Uhrzeiteinstellungen in diesem Teil des Fensters **Takteigenschaften** werden nicht aktualisiert.

Zeitquelle für Router

Dieses Feld kann die folgenden Werte enthalten:

- NTP - Der Router empfängt Uhrzeitinformationen von einem NTP-Server.
- Benutzerkonfiguration – Die Werte für Datum und Uhrzeit werden manuell über Cisco SDM oder die CLI festgelegt.
- Keine Zeitquelle - Für den Router wurden keine Uhrzeit- oder Datumseinstellungen konfiguriert.

Einstellungen ändern

Klicken Sie auf diese Option, um die Datums- und Uhrzeiteinstellungen auf dem Router zu ändern.

Datums- und Uhrzeiteigenschaften

Stellen Sie in diesem Fenster Datum und Zeit des Routers ein. Sie können Cisco SDM die Einstellungen mit dem PC synchronisieren lassen, oder Sie können diese manuell einstellen.

Mit meiner lokalen PC-Uhr synchronisieren

Aktivieren Sie dieses Kontrollkästchen, um Cisco SDM für die Synchronisierung der Datums- und Uhrzeiteinstellungen des Routers mit den Datums- und Uhrzeiteinstellungen auf dem PC einzurichten.

Synchronisieren

Klicken Sie auf diese Option, um zu veranlassen, dass Cisco SDM die Zeiteinstellungen synchronisiert. Cisco SDM nimmt nur dann eine solche Anpassung für die Datums- und Uhrzeiteinstellungen vor, wenn Sie auf **Synchronisieren** klicken. Cisco SDM führt während folgender Sitzungen keine automatische Neusynchronisierung mit dem PC durch. Diese Schaltfläche ist deaktiviert, wenn Sie die Option **Mit meiner lokalen PC-Uhr synchronisieren** nicht aktiviert haben.

Hinweis Sie müssen die Einstellungen für die Zeitzone sowie Sommer- und Winterzeit auf dem PC vorgenommen haben, bevor Sie Cisco SDM starten, damit Cisco SDM die richtigen Einstellungen empfängt, wenn Sie auf **Synchronisieren** klicken.

Datum und Uhrzeit bearbeiten

Verwenden Sie diesen Bereich, um das Datum und die Uhrzeit manuell einzustellen. Sie können den Monat und das Jahr in den Dropdown-Listen und den Tag des Monats im Kalender auswählen. In die Felder im Bereich **Uhrzeit** müssen Werte im 24-Stunden-Format eingegeben werden. Sie können Ihre Zeitzone basierend auf der Greenwich Mean Time (GMT) eingeben oder die Liste nach größeren Städten in Ihrer Zeitzone durchsuchen.

Wenn Sie möchten, dass der Router die Uhrzeit an die Sommer- und Winterzeit anpasst, aktivieren Sie das Kontrollkästchen **Uhr automatisch an Umstellung von Sommer- und Winterzeit anpassen**.

Übernehmen

Klicken Sie auf diese Option, um die Datums- und Uhrzeiteinstellungen, die Sie in den Feldern **Datum**, **Uhrzeit** und **Zeitzone** vorgenommen haben, zu übernehmen.

NTP

Mit dem Network Time Protocol (NTP) können Router in Ihrem Netzwerk ihre Zeiteinstellungen mit einem NTP-Server synchronisieren. Eine Gruppe von NTP-Clients, die Datums- und Uhrzeitinformationen von einer einzelnen Quelle abrufen, bietet einheitlichere Zeiteinstellungen. In diesem Fenster können Sie die NTP-Serverinformationen anzeigen, die konfiguriert wurden, neue Informationen hinzufügen oder vorhandene Informationen bearbeiten oder löschen.

Hinweis Wenn Ihr Router NTP-Befehle nicht unterstützt, wird dieser Zweig nicht in der Struktur mit den Routereigenschaften angezeigt.

IP-Adresse

Die IP-Adresse eines NTP-Servers.

Wenn Ihre Organisation nicht über einen NTP-Server verfügt, empfiehlt es sich, einen öffentlich verfügbaren Server zu verwenden, wie unter dem folgenden URL erläutert:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Schnittstelle

Die Schnittstelle, über die der Router mit dem NTP-Server kommuniziert.

Bevorzugen

In dieser Spalte wird **Ja** angezeigt, wenn dieser NTP-Server als bevorzugter NTP-Server designiert wurde. Bevorzugte NTP-Server werden vor nicht bevorzugten Servern kontaktiert. Es können mehrere bevorzugte NTP-Server vorhanden sein.

Hinzufügen

Klicken Sie auf diese Option, um NTP-Serverinformationen hinzuzufügen.

Bearbeiten

Klicken Sie diese Option an, wenn Sie eine bestimmte NTP-Serverkonfiguration bearbeiten möchten.

Löschen

Klicken Sie diese Option an, wenn Sie eine bestimmte NTP-Serverkonfiguration löschen möchten.

NTP-Serverdetails bearbeiten/hinzufügen

In diesem Fenster können Sie NTP-Serverinformationen hinzufügen oder bearbeiten.

IP-Adresse

Geben Sie hier die IP-Adresse eines NTP-Servers ein, oder bearbeiten Sie sie.

Bevorzugen

Aktivieren Sie diese Option, wenn dieser Server der bevorzugte NTP-Server sein soll.

Schnittstelle

Wählen Sie die Routerschnittstelle aus, die den Zugriff auf den NTP-Server ermöglicht. Sie können den CLI-Befehl **show IP routes** verwenden, um festzustellen, welche Schnittstelle über eine Route zu diesem NTP-Server verfügt.

Hinweis Eine erweiterte Zugriffsregel wird für Port 123 erstellt und auf die Schnittstelle angewendet, die Sie in diesem Fenster auswählen. Wenn für diese Schnittstelle bereits eine Zugriffsregel vorhanden ist, fügt Cisco SDM Anweisungen hinzu, um für diese Schnittstelle Datenverkehr an Port 123 zuzulassen. Wenn es sich bei der vorhandenen Regel um eine Standardzugriffsregel handelt, ändert Cisco SDM diese in eine erweiterte Regel, damit der Datenverkehrstyp und das Ziel angegeben werden können.

Authentifizierungsschlüssel

Aktivieren Sie dieses Kontrollkästchen, wenn der NTP-Server einen Authentifizierungsschlüssel verwendet, und geben Sie die erforderlichen Informationen in die Felder ein. Die Informationen in diesen Feldern müssen mit den Schlüsselinformationen auf dem NTP-Server übereinstimmen.

Schlüsselnummer

Geben Sie hier die Nummer für den Authentifizierungsschlüssel ein. Die Schlüsselnummern liegen im Bereich von 0 bis 4294967295.

Schlüsselwert

Geben Sie den Schlüssel ein, der vom NTP-Server verwendet wird. Der Schlüsselwert kann aus allen beliebigen Buchstaben von A bis Z in Groß- oder Kleinschreibung bestehen und darf nicht länger als 32 Zeichen sein.

Schlüsselwert bestätigen

Geben Sie den Schlüsselwert zur Bestätigung der Richtigkeit noch einmal ein.

SNTP

Dieses Fenster wird auf Cisco 830 Routern angezeigt. Das Simple Network Time Protocol (SNTP) ist eine weniger komplizierte Version des Network Time Proctocol (NTP). NTP gestattet Routern in Ihrem Netzwerk, ihre Zeiteinstellungen mit einem NTP-Server zu synchronisieren. Eine Gruppe von NTP-Clients, die Datums- und Uhrzeitinformationen von einer einzelnen Quelle abrufen, bietet einheitlichere Zeiteinstellungen. In diesem Fenster können Sie die NTP-Serverinformationen anzeigen, die konfiguriert wurden, um neue Informationen hinzuzufügen oder vorhandene Informationen zu bearbeiten oder zu löschen.

Hinweis Wenn Ihr Router NTP-Befehle nicht unterstützt, wird dieser Zweig nicht in der Struktur mit den Routereigenschaften angezeigt.

Eigenschaft

Der systemdefinierte Name für diesen NTP-Server.

Wert

Die IP-Adresse für diesen NTP-Server.

Hinzufügen

Klicken Sie auf diese Option, um NTP-Serverinformationen hinzuzufügen.

Bearbeiten

Klicken Sie diese Option an, wenn Sie eine bestimmte NTP-Serverkonfiguration bearbeiten möchten.

Löschen

Klicken Sie diese Option an, wenn Sie eine bestimmte NTP-Serverkonfiguration löschen möchten.

NTP-Serverdetails hinzufügen

Geben Sie in dieses Fenster die IP-Adresse eines NTP-Servers ein.

Hinweis Eine erweiterte Zugriffsregel wird für Port 123 erstellt und auf die Schnittstelle angewendet, die Sie in diesem Fenster auswählen. Wenn für diese Schnittstelle bereits eine Zugriffsregel vorhanden ist, fügt Cisco SDM Anweisungen hinzu, um für diese Schnittstelle Datenverkehr an Port 123 zuzulassen. Wenn es sich bei der vorhandenen Regel um eine Standardzugriffsregel handelt, ändert Cisco SDM diese in eine erweiterte Regel, damit der Datenverkehrstyp und das Ziel angegeben werden können.

IP-Adresse

Geben Sie die IP-Adresse des NTP-Servers im Dezimalformat mit Punkten ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Logging

In diesem Fenster können Sie die Protokollierung von Systemmeldungen aktivieren und Logging-Hosts festlegen, auf denen Protokolle gespeichert werden können. Sie können die Ebene der Protokollmeldungen angeben, die Sie senden und sammeln möchten, und den Hostnamen oder die IP-Adresse mehrerer Logging-Hosts eingeben.

IP-Adresse/Hostname

Klicken Sie auf **Hinzufügen**, und geben Sie die IP-Adresse oder den Hostnamen eines Netzwerkhosts ein, an den der Router Logging-Meldungen zum Speichern senden soll. Mit den Schaltflächen **Bearbeiten** und **Löschen** können Sie eingegebene Informationen modifizieren und Einträge löschen.

Geben Sie die Arten der Meldungen an, die an die Logging-Hosts gesendet werden, indem Sie die Logging-Ebene aus der Dropdown-Liste **Logging-Ebene** auswählen. Weitere Informationen finden Sie unter Logging-Ebene.

Logging-Ebene

Folgende Logging-Ebenen sind in den Dropdown-Listen **Logging-Ebene** verfügbar:

- Notfälle (0)
- Alarme (1)
- Wichtig (2)
- Fehler (3)
- Warnungen (4)
- Benachrichtigungen (5)
- Informationen (6)
- Fehlerbereinigung (7)

Das Protokoll erfasst alle Meldungen der ausgewählten Ebene plus aller Meldungen untergeordneter Ebenen oder der Router sendet alle Meldungen der ausgewählten Ebene plus aller Meldungen untergeordneter Ebenen an die Logging-Hosts. Wenn Sie zum Beispiel die Ebene Benachrichtigungen (5) wählen, erfasst oder sendet das Protokoll Meldungen von Ebene 0 bis 5. Für Firewall-Logging-Meldungen ist die Logging-Ebene Fehlerbereinigung (7) erforderlich, und Logging-Meldungen zur Anwendungssicherheit erfordern die Ebene Informationen (6).

Logging an Puffer

Wenn Systemmeldungen im Routerpuffer protokolliert werden sollen, aktivieren Sie das Kontrollkästchen **Protokollierungspuffer** in dem Dialogfeld, das Cisco SDM anzeigt, wenn Sie auf **Bearbeiten** klicken, und geben Sie dann die Puffergröße in das Feld **Puffergröße** ein. Je größer der Puffer ist, desto mehr Einträge können gespeichert werden, bis die ältesten Einträge durch neue Einträge ersetzt werden. Sie sollten jedoch versuchen, ein Gleichgewicht zwischen den Protokollierungsanforderungen und der Routerleistung herzustellen.

Geben Sie die Arten der Meldungen an, die im Protokoll erfasst werden, indem Sie die Logging-Ebene aus der Dropdown-Liste **Logging-Ebene** auswählen. Weitere Informationen finden Sie unter Logging-Ebene.

SNMP

In diesem Fenster können Sie SNMP aktivieren, SNMP-Community-Zeichenfolgen festlegen und Informationen zum SNMP Trap Manager eingeben.

SNMP aktivieren

Aktivieren Sie dieses Kontrollkästchen, um die SNMP-Unterstützung zu aktivieren. Deaktivieren Sie dieses Kontrollkästchen, um die SNMP-Unterstützung zu deaktivieren. SNMP ist standardmäßig aktiviert.

Community-Zeichenfolge

SNMP-Community-Strings sind eingebettete Passwörter in den Management Information Bases (MIBs). MIBs speichern Daten über den Routerbetrieb und sollen auch berechtigten Remote-Benutzern zur Verfügung stehen. Die beiden Arten von Community-Strings bieten Zugriff auf alle Objekte im MIB, außer zu den Community-Strings und sind entweder **public** (öffentlich) mit schreibgeschütztem Zugriff oder **private** mit Lese- und Schreib-Zugriff.

In der Tabelle der Community-Zeichenfolge werden alle konfigurierten Community-Zeichenfolgen mit ihren Typen aufgeführt. Verwenden Sie die Schaltfläche **Hinzufügen**, um das Dialogfeld **Add a Community String** (Community-Zeichenfolge hinzufügen) anzuzeigen und neue Community-Zeichenfolgen zu erstellen. Klicken Sie **Bearbeiten** oder **Löschen**, um die gewählte Community-Zeichenfolge in der Tabelle zu bearbeiten oder zu löschen.

Trap-Empfänger

Geben Sie die IP-Adressen und Community-Zeichenfolgen der Trap-Empfänger ein – d. h. die Adressen, an die die Trap-Informationen gesendet werden sollen. Dabei handelt es sich meist um die IP-Adressen der SNMP-Management-Stationen, die Ihre Domäne überwachen. Wenn Sie nicht sicher sind, um welche Adresse es sich handelt, wenden Sie sich an Ihren Standortadministrator.

Klicken Sie auf **Hinzufügen**, **Bearbeiten** oder **Löschen**, um die Trap-Empfangsinformation zu verwalten.

Standort des SNMP-Servers

Ein Textfeld, in das Sie den Standort des SNMP-Servers eingeben können. Dieser Konfigurationsparameter hat keinen Einfluss auf den Betrieb des Routers.

SNMP-Server-Kontakt

Ein Textfeld, in das Sie Kontaktinformationen für eine Person eingeben können, die den SNMP-Server verwaltet. Dieser Konfigurationsparameter hat keinen Einfluss auf den Betrieb des Routers.

Netflow

In diesem Fenster wird angezeigt, wie Ihr Router für die Überwachung der wichtigsten Netflow-Sprecher auf Schnittstellen konfiguriert ist, welche Netflow konfiguriert haben. Weitere Informationen zu den angezeigten Themen finden Sie unter Netflow-Sprecher.

Sie können Netflow-Parameter auf Ihrem Router überwachen und Statistiken zu den wichtigsten Sprechern anzeigen, indem Sie auf **Monitor > Schnittstellenstatus** bzw. auf **Monitor > Datenverkehrsstatus > Wichtigste N Datenverkehrsflüsse** klicken. Wenn Sie die wichtigsten Netflow-Sprecher *nicht* aktivieren, werden die zehn wichtigsten Netflow-Sprecher überwacht.

Netflow-Sprecher

In diesem Fenster können Sie die Netflow-Überwachung konfigurieren und die wichtigsten Netflow-Sprecher anzeigen.

Häufigste Sprecher aktivieren

Aktivieren Sie das Kontrollkästchen **Enable Top Talkers** (Häufigste Sprecher aktivieren), um die Überwachung der häufigsten Sprecher auf der Schnittstelle zu überwachen, die Netflow konfiguriert haben.

Wichtigste Sprecher

Legen Sie die Anzahl der wichtigsten Sprecher im Nummernfeld **Wichtigste Sprecher** fest. Wählen Sie eine Zahl zwischen 1 und 200. Cisco SDM verfolgt Daten bis zu der von Ihnen festgelegten Anzahl der wichtigsten Sprecher und zeichnet diese auf.

Cache-Timeout

Legen Sie das Timeout in Millisekunden für den Cache der wichtigsten Sprecher im Nummernfeld **Cache-Timeout** fest. Wählen Sie eine Zahl zwischen 1 und 3600000. Der Cache der wichtigsten Sprecher wird bei Erreichen des Timeout-Werts aktualisiert.

Sortieren nach

Legen Sie fest, wie Sie die wichtigsten Sprecher sortieren möchten, indem Sie aus der Dropdown-Liste **Sortieren nach** Byte oder Pakete auswählen.

Routerzugriff

In diesem Fenster wird erläutert, welche Funktionen in den Routerzugriff eingebunden sind.

Benutzerkonten: Benutzerkonten für Routerzugriff konfigurieren

In diesem Fenster können Sie Konten und Kennwörter definieren, mit denen Benutzer sich während der Anmeldung beim Router über HTTP, Telnet, PPP oder über andere Wege selbst authentifizieren können.

Benutzername

Name eines Benutzerkontos.

Kennwort

Kennwort des Benutzerkontos, dargestellt in Form von Sternchen (*).

Hinweis Das Benutzerkennwort ist nicht mit dem geheimen Kennwort identisch, das in den Geräteeigenschaften auf der Registerkarte **Kennwort** konfiguriert wird. Mit dem Benutzerkennwort kann sich der spezielle Benutzer beim Router anmelden und eine limitierte Reihe von Befehlen eingeben.

Berechtigungsstufe

Berechtigungsstufe für den Benutzer.

Namen anzeigen

Wenn eine CLI-Ansicht mit dem Benutzerkonto verknüpft wurde, wird der Name der Ansicht in dieser Spalte angezeigt. Ansichten definieren den Cisco SDM-Zugriff des Benutzers basierend auf der Rolle des Benutzers. Weitere Informationen erhalten Sie, wenn Sie auf Eine Ansicht mit dem Benutzer verknüpfen klicken.

Hinweis Wenn Cisco SDM mit einer benutzerdefinierten Ansicht oder einer geänderten Cisco SDM-definierten Ansicht gestartet wird, arbeitet Cisco SDM im Monitor-Modus, und der Benutzer verfügt nur über Leseberechtigungen. Die Cisco SDM-Funktionen, die zur Überwachung verfügbar sind, hängen von den Befehlen ab, die in der Ansicht vorhanden sind. Es sind möglicherweise nicht alle Funktionen zur Überwachung durch den Benutzer verfügbar.

Welche Aufgabe möchten Sie ausführen?

Aufgabe:	Vorgehensweise:
Neues Benutzerkonto hinzufügen.	Klicken Sie auf **Hinzufügen**. Fügen Sie das Konto dann im Fenster **Benutzernamen hinzufügen** hinzu.
Benutzerkonto bearbeiten.	Wählen Sie das Benutzerkonto, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie das Konto dann im Fenster **Benutzernamen bearbeiten**.
Benutzerkonto löschen.	Wählen Sie das Benutzerkonto, und klicken Sie auf **Löschen**. Bestätigen Sie dann den Löschvorgang in dem daraufhin angezeigten Warnfeld.

Benutzernamen hinzufügen/bearbeiten

In den Feldern in diesem Fenster können Sie ein Benutzerkonto hinzufügen oder bearbeiten.

Benutzername

Geben Sie in dieses Feld den Benutzernamen ein, oder bearbeiten Sie ihn.

Kennwort

Geben Sie in dieses Feld das Kennwort ein, oder bearbeiten Sie es.

Kennwort bestätigen

Geben Sie das Kennwort noch einmal in dieses Feld ein. Wenn das Kennwort und die Kennwortbestätigung nicht übereinstimmen, wird beim Klicken auf **OK** eine Fehlermeldung angezeigt.

Wenn Sie auf **OK** klicken, werden die neuen oder bearbeiteten Kontoinformationen im Fenster **Benutzerkonten für Telnet konfigurieren** angezeigt.

Kontrollkästchen Kennwort mit MD5-Hash-Algorithmus verschlüsseln

Aktivieren Sie dieses Kontrollkästchen, wenn Sie möchten, dass das Kennwort mit dem One-Way Message Digest 5 (MD5)-Algorithmus verschlüsselt wird. Dieser Algorithmus bietet einen großen Verschlüsselungsschutz.

Hinweis Protokolle, für die das Abrufen von klaren Textkennwörtern erforderlich ist, beispielsweise CHAP können nicht zusammen mit MD5-verschlüsselten Kennwörtern verwendet werden. Die MD5-Verschlüsselung kann nicht rückgängig gemacht werden. Wenn Sie das Kennwort in klaren Text zurücksetzen möchten, müssen Sie das Benutzerkonto löschen und neu erstellen und dabei die Option **Kennwort verschlüsseln** deaktiviert lassen.

Berechtigungsstufe

Geben Sie hier die Berechtigungsstufe für den Benutzer ein. Wenn diese Option auf einen CLI-Befehl angewendet wird, kann dieser Befehl nur von Benutzern mit einer Berechtigungsstufe ausgeführt werden, die gleich oder höher ist als die für diesen Befehl festgelegte Berechtigungsstufe.

Eine Ansicht mit dem Benutzer verknüpfen

Dieses Feld wird angezeigt, wenn Sie Benutzerkonten für den Routerzugriff einrichten. Wenn Sie in einem anderen Bereich von Cisco SDM arbeiten, ist es möglicherweise nicht sichtbar.

Aktivieren Sie die Option **Eine Ansicht mit dem Benutzer verknüpfen**, wenn Sie den Benutzerzugriff auf eine bestimmte Ansicht beschränken möchten. Wenn Sie einem Benutzer zu ersten mal eine Ansicht zuweisen, werden Sie aufgefordert, das Ansichtskennwort einzugeben. Diese Option ist nur am Router-Zugriffsknoten des Baums **Zusätzliche Aufgaben** verfügbar.

Namen anzeigen:

Wählen Sie die Ansicht, die Sie mit diesem Benutzer verknüpfen möchten, unter den folgenden Möglichkeiten aus:

- SDM_Administrator – Ein Benutzer, dem die Ansichtsart SDM_Adminstrator zugewiesen ist, verfügt über vollständigen Zugriff auf Cisco SDM und kann alle von Cisco SDM unterstützen Operationen durchführen.
- SDM_Monitor – Ein Benutzer, der mit dem Ansichtstyp SDM_Monitor verknüpft ist, kann alle von Cisco SDM unterstützten Funktionen überwachen. Der Benutzer kann keine Konfigurationen über Cisco SDM senden. Der Benutzer kann in die verschiedenen Bereiche von Cisco SDM navigieren, beispielsweise Schnittstellen und Verbindungen, Firewall und VPN. Die Komponenten der Benutzerschnittstelle in diesen Bereichen sind jedoch deaktiviert.
- SDM_Firewall – Ein Benutzer, dem die Ansicht SDM_Firewall zugewiesen ist, kann die Cisco SDM Firewall und Monitor-Funktionen nutzen. Der Benutzer kann Firewalls und ACLs mit dem Firewall-Assistenten, der Firewallrichtlinienansicht und dem ACL-Editor konfigurieren. Die Komponenten der Benutzerschnittstelle in anderen Bereichen sind für diesen Benutzer deaktiviert.
- SDM_EasyVPN_Remote – Ein Benutzer, dem die Ansicht SDM_EasyVPN_Remote zugewiesen ist, kann die Cisco SDM Easy VPN Remote-Funktionen nutzen. Der Benutzer kann Easy VPN Remote-Verbindungen erstellen und bearbeiten. Die Komponenten der Benutzerschnittstelle in anderen Bereichen sind für diesen Benutzer deaktiviert.

Details

Der Bereich **Benutzer eine Ansicht zuweisen** zeigt Details der angegebenen Ansicht. Genauere Informationen zur angegebenen Ansicht finden Sie unter **Details**.

Kennwort für Ansicht

Wenn Sie einem Benutzer zum ersten Mal eine Ansicht zuweisen, werden Sie aufgefordert, das Ansichtskennwort für Cisco SDM-definierte Ansichten einzugeben. Verwenden Sie dieses Kennwort, um zwischen den Ansichten zu wechseln.

Kennwort für Ansicht eingeben

Geben Sie das Ansichtskennwort aus dem Feld **Kennwort für Ansicht** ein.

vty-Einstellungen

In diesem Fenster werden die Virtual Terminal (vty)-Einstellungen auf Ihrem Router angezeigt. In der Spalte **Eigenschaften** finden Sie konfigurierte Leitungsbereiche und konfigurierbare Eigenschaften für jeden dieser Bereiche. Die Einstellungen für diese Eigenschaften finden Sie in der Spalte **Wert**.

In dieser Tabelle finden Sie die vty-Einstellungen Ihres Routers in den folgenden Spalten:

- Leitungsbereich – Zeigt den Bereich der vty-Verbindungen an, für den die übrigen Einstellungen in der Zeile gelten.
- Zugelassene Eingabeprotokolle – Zeigt die für die Eingabe konfigurierten Protokolle an. Dies kann Telnet, SSH oder sowohl Telnet als auch SSH sein.
- Zugelassene Ausgabeprotokolle – Zeigt die für die Ausgabe konfigurierten Protokolle an. Dies kann Telnet, SSH oder Telnet und SSH sein.
- EXEC-Timeout – Anzahl der Sekunden der Inaktivität, nach deren Ablauf eine Sitzung geschlossen wird.
- Zugriffsklasse (eingehend) – Name oder Nummer der Zugriffsregel, die auf die Eingangsrichtung des Leitungsbereichs angewendet wird.
- Zugriffsklasse (ausgehend) – Name oder Nummer der Zugriffsregel, die auf die Ausgangsrichtung des Leitungsbereichs angewendet wird.
- ACL – Zeigt, falls konfiguriert, die mit den vty-Verbindungen verknüpfte ACL an.

- Authentifizierungsrichtlinie – Die AAA-Authentifizierungsrichtlinie, die mit dieser vty-Leitung verknüpft ist. Dieses Feld wird angezeigt, wenn AAA auf dem Router konfiguriert ist.
- Authentifizierungsrichtlinie – Die AAA-Authentifizierungsrichtlinie, die mit dieser vty-Leitung verknüpft ist. Dieses Feld wird angezeigt, wenn AAA auf dem Router konfiguriert ist.

Hinweis Wenn Sie SSH als Eingangs- oder Ausgangsprotokoll verwenden möchten, müssen Sie es aktivieren, indem Sie in der Struktur **Zusätzliche Aufgaben** auf **SSH** klicken und einen RSA-Schlüssel generieren.

VTY-Leitungen bearbeiten

In diesem Fenster können Sie Virtual Terminal (vty)-Einstellungen auf Ihrem Router bearbeiten.

Leitungsbereich

Geben Sie den Bereich der vty-Leitungen an, für den die in diesem Fenster vorgenommenen Einstellungen gelten sollen.

Timeout

Geben Sie die Anzahl der Sekunden der Inaktivität ein, nach deren Ablauf eine inaktive Verbindung beendet wird.

Eingabeprotokoll

Wählen Sie die Eingabeprotokolle, indem Sie die entsprechenden Kontrollkästchen aktivieren.

Kontrollkästchen Telnet

Aktivieren Sie diese Option, um den Telnet-Zugriff auf Ihren Router zu aktivieren.

Kontrollkästchen SSH

Aktivieren Sie dieses Kästchen, damit SSH-Clients sich beim Router anmelden können.

Ausgabeprotokoll

Wählen Sie die Ausgabeprotokolle, indem Sie die entsprechenden Kontrollkästchen aktivieren.

Kontrollkästchen Telnet

Aktivieren Sie diese Option, um den Telnet-Zugriff auf Ihren Router zu aktivieren.

Kontrollkästchen SSH

Aktivieren Sie diese Option, um die Kommunikation des Routers mit SSH-Clients zu ermöglichen.

Zugriffsregel

Sie können Zugriffsregeln zuordnen, um den eingehenden und ausgehenden Datenverkehr auf den vty-Leitungen im Bereich zu filtern.

Eingehend

Geben Sie den Namen oder die Nummer der Zugriffsregel ein, die den eingehenden Datenverkehr filtern soll, oder klicken Sie auf die Schaltfläche, und suchen Sie nach der Zugriffsregel.

Ausgehend

Geben Sie den Namen oder die Nummer der Zugriffsregel an, mit der Sie ausgehenden Datenverkehr filtern möchten oder klicken Sie auf die Schaltfläche und suchen Sie nach der Zugriffsregel.

Authentifizierung/Autorisierung

Diese Felder werden angezeigt, wenn AAA auf dem Router aktiviert ist. AAA kann durch Klicken auf **Zusätzliche Aufgaben > AAA > aktivieren** aktiviert werden.

Authentifizierungsrichtlinie

Wählen Sie die Authentifizierungsrichtlinie, die Sie für diese vty-Leitung verwenden möchten.

Autorisierungsrichtlinie

Wählen Sie die Autorisierungsrichtlinie, die Sie für diese vty-Leitung verwenden möchten.

Verwaltungszugriffsrichtlinien konfigurieren

In diesem Fenster können Sie vorhandene Verwaltungszugriffsrichtlinien überprüfen und Richtlinien für die Bearbeitung auswählen. Verwaltungszugriffsrichtlinien geben an, welche Netzwerke und Hosts in der Lage sind, auf die Befehlszeilenschnittstelle des Routers zuzugreifen. In der Richtlinie können Sie festlegen, welche Protokolle der Host oder das Netzwerk in der Richtlinie verwenden kann, und welche Routerschnittstelle den Verwaltungsdatenverkehr weiterleitet.

Host/Netzwerk

Eine Netzwerkadresse oder Host-IP-Adresse. Wenn eine Netzwerkadresse angegeben wird, gilt die Richtlinie für alle Hosts in diesem Netzwerk. Wenn eine Hostadresse angegeben wird, gilt die Richtlinie für diesen Host.

Eine Netzwerkadresse wird im Format Netzwerknummer/Netzwerkbits angezeigt, wie in dem folgenden Beispiel dargestellt:

```
172.23.44.0/24
```

Weitere Informationen zu diesem Format und der Verwendung von IP-Adressen und Subnetzmasken finden Sie unter IP-Adressen und Subnetzmasken.

Verwaltungsschnittstelle

Der Routerschnittstelle, über die der Verwaltungsdatenverkehr geleitet wird.

Zulässige Protokolle

In dieser Spalte werden die Protokolle aufgeführt, welche die angegebenen Hosts zur Kommunikation mit dem Router verwenden können. Folgende Protokolle können konfiguriert werden:

- Cisco SDM – Die angegebenen Hosts können Cisco SDM verwenden.
- Telnet – Die angegebenen Hosts können Telnet für den Zugriff auf die CLI des Routers verwenden.
- SSH – Die angegebenen Hosts können die Secure Shell für den Zugriff auf die CLI des Routers verwenden.
- HTTP – Die angegebenen Hosts können das Hypertext Transfer Protocol für den Zugriff auf den Router verwenden. Wenn Cisco SDM festgelegt wird, muss zusätzlich entweder HTTP oder HTTPS eingestellt werden.
- HTTPS – Die angegebenen Hosts können das Hypertext Transfer Protocol Secure für den Zugriff auf den Router verwenden.
- RCP – Die angegebenen Hosts können das Remote Copy Protocol zur Verwaltung der Dateien auf dem Router verwenden.
- SNMP – Die angegebenen Hosts können das Simple Network Management Protocol zur Verwaltung der Dateien auf dem Router verwenden.

Schaltfläche „Hinzufügen“

Klicken Sie auf diese Schaltfläche, um eine Verwaltungsrichtlinie hinzuzufügen, und geben Sie diese Richtlinie im Fenster **Verwaltungsrichtlinie hinzufügen** an.

Schaltfläche „Bearbeiten“

Klicken Sie auf diese Schaltfläche, um eine Verwaltungsrichtlinie zu bearbeiten, und geben Sie diese Richtlinie im Fenster **Verwaltungsrichtlinie bearbeiten** an.

Schaltfläche „Löschen“

Klicken Sie diese Option an, wenn Sie eine bestimmte Management-Richtlinie löschen möchten.

Schaltfläche „Übernehmen“

Klicken Sie auf diese Schaltfläche, um die Änderungen, die Sie im Fenster **Verwaltungsrichtline hinzufügen/bearbeiten** vorgenommen haben, in die Konfiguration des Routers zu übernehmen.

Schaltfläche „Änderungen nicht übernehmen“

Klicken Sie auf diese Schaltfläche, um die Routerkonfigurationsänderungen, die Sie im Fenster **Verwaltungsrichtline hinzufügen/bearbeiten** vorgenommen haben, zu verwerfen. Damit werden alle Ihre Änderungen verworfen und aus dem Fenster **Verwaltungszugriffsrichtlinien konfigurieren** entfernt.

Verwaltungsrichtlinie hinzufügen/bearbeiten

In diesem Fenster können Sie eine Verwaltungsrichtlinie hinzufügen oder bearbeiten.

Typ

Geben Sie an, ob die angegebene Adresse die Adresse eines Hosts oder eines Netzwerks ist.

IP-Adresse/Subnetzmaske

Wenn Sie im Feld **Typ** die Option **Netzwerk** angegeben haben, geben Sie hier die IP-Adresse eines Hosts oder die Netzwerkadresse und Subnetzmaske ein. Weitere Informationen finden Sie unter IP-Adressen und Subnetzmasken.

Schnittstelle

Wählen Sie die Schnittstelle, über die Sie den Verwaltungsdatenverkehr zulassen möchten Die Schnittstelle sollte die direkte Route vom Host oder Netzwerk zum lokalen Router sein.

Verwaltungsprotokolle

Geben Sie Verwaltungsprotokolle an, die der Host bzw. das Netzwerk verwenden darf.

SDM zulassen

Aktivieren Sie diese Option, um dem festgelegten Host oder Netzwerk den Zugriff auf Cisco SDM zu gewähren. Wenn Sie diese Option aktivieren, werden die folgenden Protokolle automatisch aktiviert: Telnet, SSH, HTTP, HTTPS und RCP. Wenn Sie diese Option aktivieren, müssen Sie trotzdem zusätzliche Protokolle zulassen.

Wenn Benutzer bei der Anmeldung bei Cisco SDM sichere Protokolle verwenden sollen, aktivieren Sie die Option **Nur sichere Protokolle zulassen**. Wenn Sie diese Option aktivieren, werden die folgenden Protokolle automatisch aktiviert: SSH, HTTPS, RCP. Wenn Sie ein ungesichertes Protokoll aktivieren, z. B. Telnet, deaktiviert Cisco SDM die Option **Nur gesicherte Protokolle zulassen**.

Sie können Verwaltungsprotokolle einzeln festlegen

Wenn Sie einzelne Protokolle festlegen möchten, die der Host oder das Netzwerk verwenden kann, aktivieren Sie eines der folgenden Kontrollkästchen: Telnet, SSH, HTTP, RCP oder SNMP.

Wenn Telnet und SSH im Fenster **VTYs** nicht aktiviert (mit Häkchen versehen) sind und SNMP im SNMP-Eigenschaftenfenster nicht aktiviert ist, weist Cisco SDM Sie an, diese Protokolle zu aktivieren, wenn sie in diesem Fenster angegeben sind.

Hinweis Wenn die Cisco IOS-Version auf dem Router HTTPS nicht unterstützt, werden die Optionen **Nur sichere Protokolle zulassen** und **HTTPS** deaktiviert.

Fehlermeldungen beim Verwaltungszugriff

Die Verwaltungszugriffsfunktion kann die folgenden Fehlermeldungen generieren.

Fehlermeldung

```
SDM-Warnung: ANY Not Allowed (ALLE nicht zulässig)
```

Erklärung Eine Management-Richtlinie ist schreibgeschützt, wenn eine ihrer Quellen- oder Zielregeleinträge das Schlüsselwort **any** enthält. Solche Richtlinien können im Fenster **Verwaltungszugriff** nicht bearbeitet werden. Eine Richtlinie, die das Schlüsselwort **any** enthält, kann aus den folgenden Gründen ein Sicherheitsrisiko darstellen:

- Falls **any** mit der Quelle verbunden ist, kann Datenverkehr von jedem Netzwerk auf den Router gelangen.
- Falls **any** mit dem Ziel verbunden ist, wird Zugriff auf jeden Knoten im Netzwerk zugelassen, den der Router unterstützt.

Empfohlene Maßnahme Sie können den Zugriffseintrag entfernen, der diese Meldung aufgerufen hat, indem Sie im Fenster **Regeln** die Regel auswählen und auf **Bearbeiten** klicken. Alternativ können Sie auch im Fenster **Schnittstellen und Verbindungen** die Regel von ihrer zugeordneten Schnittstelle trennen.

Fehlermeldung

```
SDM-Warnung: Unsupported Access Control Entry (Nicht
unterstützter Zugriffssteuerungseintrag)
```

Erklärung Eine Verwaltungsrichtlinie wird nur dann gelesen, wenn nicht unterstützte Zugriffssteuerungseinträge (ACEs) mit der Schnittstelle oder vty-Leitung verknüpft sind, auf die Sie die Verwaltungsrichtlinie angewendet haben. Mit der CLI können Sie nicht unterstützte ACEs entfernen. Nicht unterstützte ACEs enthalten Schlüsselwörter oder die Syntax, die Cisco SDM nicht unterstützt.

Fehlermeldung

```
SDM-Warnung: SDM Not Allowed (SDM nicht zulässig)
```

Erklärung Diese Meldung wird angezeigt, wenn Sie weiterhin keine Verwaltungszugriffsrichtlinie für den Zugriff eines Hosts oder Netzwerks auf Cisco SDM auf diesem Router konfiguriert haben.

Empfohlene Maßnahme Sie müssen eine solche Richtlinie bereitstellen, damit Cisco SDM auf diesem Router verfügbar ist. Sie können erst dann zu anderen Funktionen navigieren oder Befehle an den Router senden, nachdem Sie eine Verwaltungszugriffsrichtlinie konfiguriert haben, die einem Host oder Netzwerk den Zugriff auf Cisco SDM ermöglicht.

Fehlermeldung

```
SDM-Warnung: Current Host Not Allowed (Aktueller Host nicht
zulässig)
```

Erklärung Diese Meldung wird angezeigt, wenn Sie keine Verwaltungszugriffsrichtlinie für den Cisco SDM-Zugriff des aktuellen Hosts oder Netzwerks auf diesem Router konfiguriert haben.

Empfohlene Maßnahme Sie sollten eine solche Richtlinie erstellen, damit Cisco SDM für den aktuellen Host oder das aktuelle Netzwerk auf diesem Router verfügbar ist. Wenn Sie dies nicht tun, wird die Verbindung zum Router getrennt, wenn Sie die Konfiguration an Ihren Router senden. Klicken Sie auf **Ja**, um jetzt eine Verwaltungszugriffsrichtlinie für den aktuellen Host oder das aktuelle Netzwerk hinzuzufügen. Klicken Sie auf **Nein**, um fortzufahren, ohne eine Richtlinie für den aktuellen Host oder das aktuelle Netzwerk hinzuzufügen. Die Verbindung zum Router wird während der Übertragung von Befehlen getrennt, und Sie müssen sich über einen anderen Host oder ein anderes Netzwerk bei Cisco SDM anmelden.

SSH

Dieser Router implementiert Secure Shell (SSH)-Server, eine Funktion, die einen SSH-Client aktiviert, um eine sichere, verschlüsselte Verbindung zu einem Cisco-Router herzustellen. Diese Verbindung bietet Funktionen ähnlich der einer eingehenden Telnet-Verbindung, jedoch mit einer hohen Verschlüsselung, die mit der Cisco IOS-Softwareauthentifizierung verwendet werden kann. Der SSH-Server in der Cisco IOS-Software arbeitet mit öffentlich und kommerziell erhältlichen SSH-Clients. Wenn der Router kein IPSEC DES oder keine 3DES Cisco IOS-Version verwendet, wird diese Funktion deaktiviert, und der SSH-Zweig der Struktur Zusätzliche Aufgaben wird nicht angezeigt.

SSH verwendet eine RSA-Verschlüsselung, um Daten zu verschlüsseln, die zwischen dem Router und dem SSH-Client gesendet werden. Durch die Generierung des RSA-Schlüssels in diesem Fenster wird die SSH-Kommunikation zwischen dem Router und den SSH-Clients aktiviert.

Statusmeldungen

Crypto key is not set on this device (Kein Kryptografieschlüssel für dieses Gerät festgelegt)

Dieser Text wird angezeigt, wenn kein Kryptografieschlüssel für das Gerät konfiguriert ist. Wenn kein Schlüssel konfiguriert ist, können Sie die Größe eines Moduls eingeben und einen Schlüssel generieren.

RSA-Schlüssel ist in diesem Router eingerichtet

Dieser Text erscheint, wenn eine Verschlüsselung erstellt wurde. SSH ist auf diesem Router aktiviert.

Schaltfläche Größe des Schlüsselmoduls.

Diese Schaltfläche wird angezeigt, wenn keine Verschlüsselung erstellt wurde. Klicken Sie auf diese Schaltfläche, und geben Sie die Modulgröße für den Schlüssel ein. Wenn Sie einen Modulwert zwischen 512 und 1024 wünschen, geben Sie einen Ganzzahlwert ein, der ein Vielfaches von 64 ist. Wenn Sie einen Wert über 1024 wünschen, können Sie 1536 oder 2048 eingeben. Wenn Sie einen größeren Wert als 512 eingeben, kann die Generierung des Schlüssels mindestens eine Minute dauern.

Schaltfläche RSA-Schlüssel generieren

Klicken Sie auf diese Schaltfläche, um einen Kryptografieschlüssel mit der eingegebenen Modulgröße für den Router zu generieren. Wenn die Verschlüsselung bereits erstellt wurde, ist diese Schaltfläche inaktiv.

DHCP-Konfiguration

Dieses Fenster erklärt, wie Sie DHCP-Konfigurationen auf Ihrem Router verwalten können.

DHCP-Pools

Dieses Fenster zeigt die auf dem Router konfigurierten DHCP-Pools an.

Pool-Name

Der Name des DHCP-Pools.

Schnittstelle

Die Schnittstelle, auf der der DHCP-Pool konfiguriert wurde. Clients, die mit dieser Schnittstelle verbunden sind, erhalten IP-Adressen von diesem DHCP-Pool.

Details zum DHCP-Pool *Name*

In diesem Bereich finden Sie die folgenden Einzelheiten zu dem mit *Name* identifizierten Pool.

- **DHCP-Pool-Bereich** – Der Bereich der IP-Adressen, der Clients gewährt werden kann.
- **Standard-IP-Adresse des Routers** – Wenn der Router eine IP-Adresse in demselben Subnetz wie der DHCP-Pool hat, so wird diese hier angezeigt.
- **DNS-Server** – Die IP-Adressen der DNS-Server, die der Router für DHCP-Clients bereitstellt.

- **WINS-Server** – Die IP-Adressen der WINS-Server, die der Router für DHCP-Clients bereitstellt.
- **Domänenname** – Der auf dem Router konfigurierte Domänenname.
- **Lease-Zeit** – Die Zeitspanne, die der Router eine IP-Adresse einem Client least.
- **Alle importieren** – Gibt an, ob der Router DHCP-Optionsparameter in die DHCP-Server-Datenbank importiert und diese Informationen auch an DHCP-Clients im LAN sendet, wenn diese IP-Adressen anfordern.

Hinzufügen

Wählen Sie diese Option, um einen neuen DHCP-Pool zu erstellen. Der Benutzer muss den DHCP-Poolnamen, das DHCP-Pool Netzwerk, den DHCP-Pool IP-Adressenbereich und die Lease-Zeit angeben. Optional können auch DNS-Server, WIN-Server, Domänenname und der Standardrouter im DHCP-Pool konfiguriert werden.

Bearbeiten

Wählen Sie diese Option, um einen vorhandenen DHCP-Pool zu bearbeiten.

Löschen

Wählen Sie diese Option, um einen DHCP-Pool zu löschen.

DHCP-Pool-Status

Klicken Sie auf dieses Schaltfeld, um die IP-Adresse zu sehen, die vom angegebenen Pool geleast wird. Falls ein DHCP-Pool weitere Parameter enthält, außer dem Pool-Netzwerk, IP-Adressenbereich, der Lease-Zeit, DNS-Server, WINS-Server, dem Domänenname und dem Standardrouter, zeigt Cisco SDM diesen Pool schreibgeschützt an. Falls ein Pool einen unterbrochenen IP-Adressenbereich enthält, wird dieser ebenfalls schreibgeschützt angezeigt.

Add or Edit DHCP Pool (DHCP-Pool hinzufügen oder bearbeiten)

In diesem Fenster können Sie einen DHCP-Pool hinzufügen oder bearbeiten. Cisco SDM-Standardpools können Sie nicht bearbeiten.

DHCP-Pool-Name

Geben Sie in dieses Feld einen Namen für den DHCP-Pool ein.

DHCP-Pool-Netzwerk

Geben Sie das Netzwerk ein, aus dem die IP-Adressen im Pool stammen, zum Beispiel 192.168.233.0. Es darf sich hierbei nicht um die IP-Adresse eines einzelnen Hosts handeln.

Subnetzmaske

Geben Sie die Subnetzmaske ein. Eine Subnet-Maske von 255.255.255.0 liefert 255 IP-Adressen.

DHCP-Pool

Geben Sie die Anfangs- und End-IP-Adressen des Bereichs ein. Z.B., wenn das Netzwerk 192.168.233.0 ist und die Subnetzmaske ist 255.255.255.0, dann ist die Anfangsadresse 192.168.233.1 und die Endadresse 192.168.233.254.

Lease-Dauer

Geben Sie die Zeitspanne an, für die Adressen an Clients geleast werden. Sie können festlegen, dass geleaste Adressen niemals ablaufen, oder Sie können die Lease-Dauer in Tagen, Stunden und Minuten angeben. Gehen Sie nicht über 365 Tage, 23 Stunden oder 59 Minuten.

DHCP-Optionen

Geben Sie Informationen zu den DNS-Servern, WINS-Servern, dem Domänennamen und dem Standardrouter ein. Diese Werte werden an die DHCP-Clients gesendet, wenn sie eine IP-Adresse anfordern.

Alle DHCP-Optionen in die DHCP-Server-Datenbank importieren

Klicken Sie auf diese Option, wenn Sie DHCP-Optionsparameter in die DHCP-Server-Datenbank importieren und diese Informationen auch an DHCP-Clients im LAN senden möchten, wenn diese IP-Adressen anfordern.

DHCP-Bindungen

Dieses Fenster zeigt die bestehenden, manuellen DHCP-Bindungen. Mit einer manuellen DHCP-Bindung können Sie einen bestimmten Client jedesmal dieselbe IP-Adresse zuweisen, wenn dieser Client eine IP-Adresse aus dem verfügbaren DHCP-Pool anfordert.

Sie können auch neue Bindungen hinzufügen und bestehende Bindungen bearbeiten oder löschen.

Bindungsname

Der Name, welcher der DHCP-Bindung zugewiesen wurde.

Host/IP-Maske

IP-Adresse und -Maske, die an den Client gebunden sind.

MAC-Adresse

Die MAC-Adresse dieses Clients.

Typ

Der Typ der MAC-Adresse gehört zu einem der folgenden:

- Ethernet

  Der Client besitzt eine Hardware-Adresse.
- IEEE802

  Der Client besitzt eine Hardware-Adresse.
- <Keine>

  Der Client besitzt einen Client-Identifier.

Clientname

Ein optionaler Name, der dem Client zugewiesen wurde.

Die Schaltfläche Hinzufügen

Klicken Sie auf Hinzufügen, um eine neue DHCP-Bindung hinzuzufügen.

Schaltfläche „Bearbeiten“

Klicken Sie auf diese Option, wenn Sie die angegebene, manuelle DHCP-Bindung bearbeiten möchten.

Schaltfläche „Löschen“

Klicken Sie diese an, wenn Sie die angegebene, manuelle DHCP-Bindung löschen möchten.

DHCP-Bindung hinzufügen oder bearbeiten

In diesem Fenster können Sie bestehende, manuelle DHCP-Bindungen hinzufügen oder bearbeiten.

Name

Geben Sie den Namen ein, den Sie der DHCP-Bindung geben möchten. Wenn Sie die DHCP-Bindung bearbeiten, ist das Namensfeld schreibgeschützt.

Host-IP

Geben Sie die IP-Adresse ein, die Sie an den Client binden möchten. Die Adresse sollte dem Client vom DHCP-Pool aus zur Verfügung stehen. Geben Sie keine Adresse ein, die von einer anderen DHCP-Bindung verwendet wird.

Maske

Geben Sie die Maske ein, die für die Host-IP-Adresse verwendet werden soll.

Identifier

Wählen Sie aus dem Dropdown-Menü eine Methode zur Erkennung des Client mit einer MAC-Adresse.

MAC-Adresse

Geben Sie die MAC-Adresse des Client ein. Geben Sie keine Adresse ein, die von einer anderen DHCP-Bindung verwendet wird.

Typ

Wenn Sie im Dropdown-Menü **Identifier** die Option **Hardware-Adresse** auswählen, wählen Sie **Ethernet** oder **IEEE802**, um den Typ der MAC-Adresse des Client einzustellen.

Client-Name (Optional)

Geben Sie einen Namen ein, um den Client zu erkennen. Beim Namen sollte es sich nur um einen Hostname handeln und nicht um einen Namen im Stil eines Domänennamens. *Router* kann beispielsweise als Name verwendet werden, *router.cisco.com* dagegen nicht.

DNS-Eigenschaften

Das Domain Name System (DNS) ist eine Datenbank mit Internet-Hostnamen und ihren dazugehörigen IP-Adressen, verteilt über designierte DNS-Server. Mit DNS können Netzwerkbenutzer sich nach Namen anstatt IP-Adressen an Hosts wenden, die schwerer im Gedächtnis zu behalten sind. Verwenden Sie dieses Fenster, um die Verwendung von DNS-Servern für die Übersetzung von Hostnamen in Adressen zu aktivieren.

Kontrollkästchen DNS-basierten Hostnamen für die Adressenübersetzung aktivieren

Aktivieren Sie dieses Kontrollkästchen, um die Verwendung von DNS für den Router zu aktivieren. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie DNS nicht verwenden möchten.

DNS-IP-Adresse

Geben Sie die IP-Adressen der DNS-Server ein, an die der Router DNS-Anfragen senden soll.

Klicken Sie auf die Schaltflächen **Hinzufügen**, **Bearbeiten** oder **Löschen**, um DNS-IP-Adressinformationen zu verwalten.

Dynamische DNS-Methoden

Dieses Fenster zeigt eine Liste dynamischer DNS-Methoden.

Jede angezeigte dynamische DNS-Methode sendet den Host- und Domänennamen mit ihrer Aktualisierung, die unter **Konfigurieren > Zusätzliche Aufgaben > Router-Eigenschaften** konfiguriert wurden. Wenn Sie jedoch bei der Konfiguration einer WAN-Schnittstelle eine dynamische DNS-Methode erstellen, können Sie den Host- und Domänennamen überschreiben, die unter **Konfigurieren > Zusätzliche Aufgaben > Router-Eigenschaften** konfiguriert wurden. Die neuen Host- und Domänennamen gelten nur für diese dynamische DNS-Methode.

Manche dynamischen DNS-Methoden sind schreibgeschützt. Sie wurden in der Cisco IOS-Software über das CLI konfiguriert und können weder bearbeitet noch gelöscht werden. Um diese schreibgeschützten Methoden bearbeitbar zu machen, verwenden Sie das CLI, um die internen Cache- oder Hostgruppen-Optionen zu HTTP oder IETF zu machen.

Die Schaltfläche Hinzufügen

Klicken Sie auf **Hinzufügen**, um eine neue, dynamische DNS-Methode zu erstellen.

Schaltfläche „Bearbeiten“

Um eine dynamische DNS-Methode zu bearbeiten, wählen Sie eine aus der Liste der bestehenden DNS-Methoden aus, und klicken Sie auf **Bearbeiten**.

Schaltfläche „Löschen“

Um eine dynamische DNS-Methode zu löschen, wählen Sie eine aus der Liste der bestehenden DNS-Methoden aus, und klicken Sie auf **Löschen**.

Hinweis Wenn Sie dynamische DNS-Methoden löschen möchten, die mit einer oder mehreren Schnittstellen verbunden sind, erhalten Sie eine Warnmeldung.

Dynamische DNS-Methoden hinzufügen oder bearbeiten

In diesem Fenster können Sie dynamische DNS-Methoden hinzufügen oder bearbeiten. Legen Sie die Art der Methode fest, indem Sie **HTTP** oder **IETF** wählen.

HTTP

HTTP ist eine Art dynamischer DNS-Methoden, die einen DNS-Dienstanbieter mit den Änderungen der zugeordneten Schnittstellen-IP-Adressen aktualisiert.

Server

Wenn Sie HTTP verwenden, wählen Sie die Domänenadresse des DNS-Dienstanbieters aus dem Dropdown-Menü.

Benutzername

Wenn Sie HTTP verwenden, geben Sie einen Benutzernamen ein, um auf den DNS-Dienstanbieter zuzugreifen.

Kennwort

Wenn Sie HTTP verwenden, geben Sie einen Benutzernamen ein, um auf den DNS-Dienstanbieter zuzugreifen.

IETF

IETF ist eine Art dynamischer DNS-Methoden, die einen DNS-Server mit den Änderungen der zugeordneten Schnittstellen-IP-Adressen aktualisiert.

Wenn Sie IETF verwenden, konfigurieren Sie einen DNS-Server für den Router über **Konfigurieren > Zusätzliche Aufgaben > DNS**.

KAPITEL 29

ACL-Editor

Regeln definieren, wie der Router auf eine bestimmte Art von Datenverkehr reagiert. Mit Cisco SDM können Sie Zugriffsregeln erstellen, mit denen der Router bestimmte Datenverkehrsarten blockiert und andere Arten zulässt, NAT-Regeln erstellen, die den Datenverkehr definieren, der Adressenübersetzungen empfangen soll, und IPSec-Regeln erstellen, die festlegen, welche Datenverkehrsart verschlüsselt werden soll. Zusätzlich bietet Cisco SDM Standardregeln, die in geleiteten Konfigurationen verwendet werden und die Sie bei der Erstellung eigener Zugriffsregeln untersuchen und verwenden können. Außerdem können Sie nicht mit Cisco SDM erstellte Regeln, so genannte externe Regeln, sowie Regeln mit einer Syntax, die Cisco SDM nicht unterstützt, so genannte nicht unterstützte Regeln, anzeigen.

Auf dem Bildschirm **Regeln** können Sie eine Zusammenfassung der Regeln in der Routerkonfiguration anzeigen und zu anderen Fenstern navigieren, um Regeln zu erstellen, zu bearbeiten oder zu löschen.

Kategorie

Ein Regeltyp. Einer der folgenden Typen:

Zugriffsregeln	Regeln, die den Datenverkehr steuern, der in das Netzwerk eintreten und es verlassen kann. Diese Regeln werden von Routerschnittstellen und von VTY-Leitungen verwendet, über die sich Benutzer beim Router anmelden können.
NAT-Regeln	Regeln, die festlegen, wie private IP-Adressen in gültige Internet-IP-Adressen übersetzt werden.
IPSec-Regeln	Regeln, die festlegen, welcher Datenverkehr in sicheren Verbindungen verschlüsselt wird.
NAC-Regeln	Regeln, die die im Netzwerk zulässigen oder vom Netzwerk zu blockierenden IP-Adressen angeben.
Firewallregeln	Regeln, die die Quell- und Zieladressen und den Datenverkehrstyp definieren und angeben, ob der Datenverkehr zugelassen oder verweigert werden soll.
QoS-Regeln	Regeln, die Datenverkehr angeben, der zur QoS-Klasse gehören soll, mit dem die Regel verknüpft ist.
Nicht unterstützte Regeln	Regeln, die nicht mit Cisco SDM verschlüsselt wurden und die von Cisco SDM nicht unterstützt werden. Diese Regeln sind schreibgeschützt und können mit Cisco SDM nicht modifiziert werden.

Extern definierte Regeln	Regeln, die nicht mit Cisco SDM erstellt wurden, von Cisco SDM jedoch unterstützt werden. Diese Regeln können mit keiner Schnittstelle verknüpft werden.
Cisco SDM-Standardregeln	Diese Regeln sind vordefiniert und werden von Cisco SDM-Assistenten verwendet. Sie können diese in den Fenstern unter **Zusätzliche Aufgaben>ACL-Editor** anwenden.

Anzahl der Regeln

Die Anzahl der Regeln dieses Typs.

Beschreibung

Eine Beschreibung der Regel, falls eine eingegeben wurde.

So konfigurieren Sie Regeln:

Klicken Sie die Regelkategorie im Regelbaum an, um das Fenster für diesen Regeltyp aufzurufen. In diesem Fenster können Sie Regeln erstellen und bearbeiten.

Das Hilfethema für diese Fenster enthält allgemeine Vorgehensweisen, die möglicherweise hilfreich für Sie sein könnten. Nützliche Vorgehensweisen für Zugriffsregeln und Firewalls enthält schrittweise Anleitungen für weitere Aufgaben.

Nützliche Vorgehensweisen für Zugriffsregeln und Firewalls

Dieser Abschnitt enthält Vorgehensweisen, die Ihnen unter Umständen nützlich sein können.

- Wie zeige ich Aktivitäten auf meiner Firewall an?
- Wie konfiguriere ich eine Firewall auf einer nicht unterstützten Schnittstelle?
- Wie konfiguriere ich eine Firewall, nachdem ich ein VPN konfiguriert habe?
- Wie lasse ich bestimmten Datenverkehr über eine DMZ-Schnittstelle zu?
- Wie ändere ich eine existierende Firewall, um Datenverkehr von einem neuen Netzwerk oder Host zuzulassen?
- Wie konfiguriere ich NAT Passthrough für eine Firewall?
- Wie lasse ich über eine Firewall Datenverkehr zu meinem Easy VPN-Konzentrator zu?
- Wie verknüpfe ich eine Regel mit einer Schnittstelle?
- Wie hebe ich die Verknüpfung einer Zugriffsregel mit einer Schnittstelle auf?
- Wie lösche ich eine Regel, die mit einer Schnittstelle verknüpft ist?
- Wie erstelle ich eine Zugriffsregel für eine Java-Liste?

Regelfenster

In diesen Fenstern können Sie Regeln untersuchen, bearbeiten und löschen.

- Fenster **Zugriffsregeln** – Zugriffsregeln definieren meist den Datenverkehr, dem Sie den Zugriff auf Ihr LAN oder das Verlassen Ihres LAN gewähren oder verweigern möchten. Sie können Zugriffsregeln jedoch auch für andere Zwecke verwenden.
- Fenster **NAT-Regeln** – Mit NAT-Regeln können Sie einen Satz von Adressen festlegen, die übersetzt werden sollen.
- Fenster **IPSec-Regeln** – IPSec-Regeln sind erweiterte Regeln, die in IPSec-Richtlinien dazu verwendet werden, festzulegen, welcher Datenverkehr für VPN-Verbindungen verschlüsselt wird.

- Fenster **NAC-Regeln** – Regeln, die die im Netzwerk zulässigen oder vom Netzwerk zu blockierenden IP-Adressen angeben.
- Fenster **Firewallregeln** – Regeln, die die Quell- und Zieladressen und den Datenverkehrstyp definieren und angeben, ob der Datenverkehr zugelassen oder verweigert werden soll.
- Fenster **Qos-Regeln** – Regeln, die Datenverkehr angeben, der zur QoS-Klasse gehören soll, mit der die Regel verknüpft ist.
- Fenster **Nicht unterstützte Regeln** – Nicht unterstützte Regeln enthalten Syntax oder Schlüsselwörter, die Cisco SDM nicht unterstützt. Nicht unterstützte Regeln können die Arbeitsweise des Routers beeinträchtigen, werden von Cisco SDM jedoch als schreibgeschützt markiert.
- Fenster **Extern definierte Regeln** – Extern definierte Regeln wurden nicht mit Cisco SDM erstellt.
- Fenster **Cisco SDM-Standardregeln** – Cisco SDM-Standardregeln sind vordefinierte Zugriffsregeln. Sie werden in geleiteten Erstkonfigurationen verwendet, und Sie können sie bei der Erstellung eigener Zugriffsregeln verwenden.
- Fenster **NAC-Regeln** – NAC-Regeln werden in der NAC-Ausnahmerichtlinie verwendet, um Hosts festzulegen, die vom NAC-Bewertungsprozess ausgenommen werden sollen. Sie werden auch verwendet, um die Hosts oder Netzwerke für die Zulassungssteuerung zu definieren.

Im oberen Bildschirmbereich werden die Zugriffsregeln angezeigt, die auf diesem Router konfiguriert wurden. Diese Liste enthält keine Cisco SDM-Standardregeln. Wenn Sie Cisco SDM-Standardregeln anzeigen möchten, klicken Sie in der Regelstruktur auf den Zweig **SDM-Standardregeln**.

Im unteren Bereich des Fensters werden die Regeleinträge angezeigt, die mit der ausgewählten Regel verknüpft sind. Ein Regeleintrag besteht aus Kriterien, mit denen eingehender oder ausgehender Datenverkehr abgeglichen wird, und der Maßnahme, die für Datenverkehr ergriffen werden muss, der den Kriterien entspricht. Wenn der Datenverkehr keiner der Kriterien in diesem Feld entspricht, wird er entfernt.

Erste Spalte

Diese Spalte kann Symbole enthalten, die den Status einer Regel angeben.

Wenn die Regel schreibgeschützt ist, wird das Schreibgeschützt-Symbol in dieser Spalte angezeigt.

Name/Nummer

Der Name oder die Nummer der Zugriffsregel

Zur Kennzeichnung von Standardzugriffslisten werden die Nummern 1 bis 99 verwendet. Die Nummern 100 bis 199 werden zur Kennzeichnung von erweiterten Zugriffslisten verwendet. Mit Namen, die alphabetische Zeichen enthalten können, können Sie den Bereich von Standardzugriffslisten auf über 99, und den Bereich von erweiterten Zugriffslisten auf über 199 erweitern.

Verwendet von

Der Name der Schnittstelle oder die VTY-Nummern, auf die diese Regel angewendet wurde.

Typ

Der Typ der Regel, entweder Standard oder Erweitert.

Standardregeln vergleichen die Quell-IP-Adresse eines Pakets mit seinen IP-Adresskriterien, um eine Übereinstimmung zu finden. Die IP-Adresskriterien der Regel können eine einzelne IP-Adresse oder Teile einer IP-Adresse sein, die von einer Platzhaltermaske definiert werden.

Erweiterte Regeln können eine größere Bandbreite von Paketfeldern untersuchen, um eine Übereinstimmung zu finden. Erweiterte Regeln können sowohl die Quelle des Pakets als auch die Ziel-IP-Adressen, den Protokolltyp, die Quell- und Ziel-Ports und andere Paketfelder überprüfen.

Zugriffsregeln können entweder Standardregeln oder erweiterte Regeln sein. IPSec-Regeln müssen erweiterte Regeln sein, da sie in der Lage sein müssen, einen Diensttyp festzulegen. Extern definierte und nicht unterstützte Regeln können entweder Standardregeln oder erweiterte Regeln sein.

Beschreibung

Eine Beschreibung der Regel, falls eine eingegeben wurde.

Erste Spalte (Regeleingabebereich)

 Datenverkehr zulassen.

 Datenverkehr verweigern.

Vorgang

Die Aktion, die unternommen werden soll, wenn ein Paket, das den Kriterien dieses Eintrags entspricht, an der Schnittstelle eintrifft. Entweder Zulassen oder Verweigern:

- Zulassen – Datenverkehr zulassen, der den Kriterien in dieser Zeile entspricht.
- Verweigern – Datenverkehr nicht zulassen, der den Kriterien in dieser Zeile entspricht.

Klicken Sie auf Bedeutung der Schlüsselwörter Zulassen und Verweigern, um weitere Informationen zu den Aktionen Zulassen und Verweigern im Kontext eines bestimmten Regeltyps zu erhalten.

Quelle

Die Kriterien für die Quell-IP-Adresse, denen der Datenverkehr entsprechen muss. Diese Spalte kann Folgendes enthalten:

- Eine IP-Adresse und eine Platzhaltermaske. Die IP-Adresse gibt ein Netzwerk an, und die Platzhaltermaske gibt an, zu welchem Anteil der IP-Adresse die IP-Adresse im Paket übereinstimmen muss.
- Das Schlüsselwort **alle. Alle** bedeutet, dass die Quell-IP-Adresse beliebig sein kann.
- Ein Hostname.

Ziel

Bei erweiterten Regeln die Kriterien für die Ziel-IP-Adresse, denen der Datenverkehr entsprechen muss. Die Adresse kann die eines Netzwerks oder eines bestimmten Hosts sein. Diese Spalte kann Folgendes enthalten:

- Eine IP-Adresse und eine Platzhaltermaske. Die IP-Adresse gibt ein Netzwerk an, und die Platzhaltermaske gibt an, zu welchem Anteil der IP-Adresse die IP-Adresse im Paket übereinstimmen muss.
- Das Schlüsselwort **alle. Alle** bedeutet, dass die Quell-IP-Adresse beliebig sein kann.
- Ein Hostname.

Dienst

Für erweiterte Regeln gibt der Dienst den Typ des Datenverkehrs an, den Pakete, die den Regeln entsprechen, enthalten müssen. Dies wird durch Anzeigen des Dienstes, beispielsweise „Echoantwort“, gefolgt von dem Protokoll, zum Beispiel „ICMP“, dargestellt. Eine Regel, die mehrere Dienste zwischen denselben Endpunkten zulässt oder verweigert, muss einen Eintrag für jeden Dienst enthalten.

Attribute

Dieses Feld kann weitere Informationen zu diesem Eintrag enthalten, zum Beispiel, ob das Logging aktiviert wurde.

Beschreibung

Eine kurze Beschreibung des Eintrags.

Was möchten Sie tun?

Aufgabe	Vorgehensweise
Regel hinzufügen.	Klicken Sie auf die Schaltfläche **Hinzufügen**, und erstellen Sie die Regel in den daraufhin angezeigten Fenstern.
Regel oder Regeleintrag bearbeiten.	Wählen Sie die Zugriffsregel aus, und klicken Sie auf **Bearbeiten**. Bearbeiten Sie die Regel dann im daraufhin angezeigten Fenster **Regel bearbeiten**.
Eine Regel mit einer Schnittstelle verknüpfen.	Siehe Wie verknüpfe ich eine Regel mit einer Schnittstelle?
Eine Regel löschen, die nicht mit einer Schnittstelle verknüpft ist.	Wählen Sie die Zugriffsregel aus, und klicken Sie auf **Löschen**.
Eine Regel löschen, die mit einer Schnittstelle verknüpft ist.	Cisco SDM lässt nicht zu, dass Sie eine Regel löschen, die mit einer Schnittstelle verknüpft ist. Wenn Sie die Regel löschen möchten, müssen Sie sie zunächst von der Schnittstelle trennen. Siehe Wie lösche ich eine Regel, die mit einer Schnittstelle verknüpft ist?
Die Aktion, die ich durchführen möchte, ist hier nicht beschrieben.	Unter dem folgenden Link finden Sie Vorgehensweisen, die Sie lesen sollten: Nützliche Vorgehensweisen für Zugriffsregeln und Firewalls.

Regel hinzufügen/bearbeiten

In diesem Fenster können Sie eine Regel hinzufügen oder bearbeiten, die Sie im Fenster **Regeln** ausgewählt haben. Sie können die Regel umbenennen oder mit einer anderen Nummer versehen, Regeleinträge hinzufügen, ändern, neu anordnen oder löschen oder die Beschreibung der Regel hinzufügen oder ändern.

Name/Nummer

Fügen Sie den Namen oder die Nummer der Regel hinzu, oder bearbeiten Sie diese.

Standardregeln müssen im Bereich 1–99 oder 1300–1999 nummeriert sein.

Erweiterte Regeln müssen im Bereich 100–199 oder 2000–2699 nummeriert sein.

Mit Namen, die alphabetische Zeichen enthalten, können Sie einer Zugriffsregel eine aussagekräftige Bezeichnung geben.

Typ

Wählen Sie den Regeltyp aus, den Sie hinzufügen möchten. Bei Standardregeln kann der Router den Quellhost oder das Quellnetzwerk im Paket untersuchen. Bei erweiterten Regeln kann der Router den Quellhost oder das Quellnetzwerk, den Zielhost oder das Zielnetzwerk sowie den Datenverkehrstyp, den das Paket enthält, untersuchen.

Beschreibung

In dieses Feld können Sie eine Beschreibung der Regel eingeben.
Die Beschreibung darf nicht mehr als 100 Zeichen enthalten.

Regeleintragsliste

In dieser Liste werden die Einträge angezeigt, aus denen die Regel besteht. Sie können Einträge hinzufügen, bearbeiten und löschen. Sie können die Einträge auch neu anordnen, um die Reihenfolge zu ändern, in der sie ausgewertet werden.

Beachten Sie bei der Erstellung von Regeleinträgen die folgenden Richtlinien:

- Es muss sich mindestens eine Zulassungsanweisung in der Liste befinden; andernfalls wird der gesamte Datenverkehr verweigert.
- Der letzte Eintrag muss eine „Alle zulassen“-Anweisung oder eine „Alle verweigern“-Anweisung sein.
- Standardeinträge und erweiterte Einträge können innerhalb einer Regel nicht kombiniert werden.
- Es dürfen keine doppelten Einträge in einer Regel vorhanden sein.

Duplizieren

Klicken Sie auf diese Schaltfläche, um den ausgewählten Eintrag als Vorlage für einen neuen Eintrag zu verwenden. Mit dieser Funktion können Sie Zeit sparen und Fehler verringern. Wenn Sie beispielsweise eine Anzahl von erweiterten Regeleinträgen mit derselben Quelle und demselben Ziel, jedoch unterschiedlichen Protokollen oder Ports erstellen möchten, könnten Sie den ersten Eintrag mit der Schaltfläche **Hinzufügen** erstellen. Nachdem Sie den ersten Eintrag erstellt haben, könnten Sie ihn mit der Option **Duplizieren** kopieren und das Protokoll- oder Portfeld ändern, um einen neuen Eintrag zu erstellen.

Schnittstellenverknüpfung

Klicken Sie auf die Schaltfläche **Verknüpfen**, um die Regel auf eine Schnittstelle anzuwenden.

Hinweis Die Schaltfläche **Verknüpfen** ist nur dann aktiviert, wenn Sie eine Regel über das Fenster **Zugriffsregeln** hinzufügen.

Was möchten Sie tun?

Aufgabe	Vorgehensweise
Regeleintrag hinzufügen oder bearbeiten.	Klicken Sie auf **Hinzufügen**, und erstellen Sie den Eintrag im angezeigten Fenster. Oder klicken Sie auf die Schaltfläche **Bearbeiten**, und ändern Sie den Eintrag in dem daraufhin angezeigten Fenster.
Regeleintrag mit einem vorhandenen Eintrag als Vorlage erstellen.	Wählen Sie den Eintrag aus, den Sie als Vorlage verwenden möchten, und klicken Sie auf **Duplizieren**. Erstellen Sie den Eintrag dann in dem daraufhin angezeigten Dialogfeld. In dem Dialogfeld wird der Inhalt des ausgewählten Eintrags angezeigt, den Sie jetzt bearbeiten können, um einen neuen Eintrag zu erstellen.
Regeleinträge neu anordnen, um sicherzustellen, dass der Router bestimmte Einträge auswertet.	Wählen Sie den Regeleintrag aus, und klicken Sie auf die Schaltfläche **Nach oben** oder **Nach unten**, um den Eintrag an die gewünschte Position zu verschieben.
Eine Regel mit einer Schnittstelle verknüpfen.	Klicken Sie auf **Verknüpfen**, und wählen Sie im Fenster **Mit Schnittstelle verknüpfen** die gewünschte Schnittstelle und Richtung aus. Wenn die Schaltfläche **Verknüpfen** nicht aktiviert ist, können Sie die Regel mit einer Schnittstelle verknüpfen, indem Sie im Fenster **Schnittstellen und Verbindungen** auf der Registerkarte **Verknüpfen** auf die Schnittstelle doppelklicken.
Regeleintrag löschen.	Wählen Sie den Regeleintrag aus, und klicken Sie auf **Löschen**. Bestätigen Sie dann den Löschvorgang in dem daraufhin angezeigten Warnfenster.

Aufgabe	Vorgehensweise
Mehr über Regeln erfahren.	Sehen Sie sich die Ressourcen unter Cisco.com an. Über den folgenden Link erhalten Sie weitere Informationen zu IP-Zugriffslisten: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml
Die Aktion, die ich durchführen möchte, ist hier nicht beschrieben.	Unter dem folgenden Link finden Sie Vorgehensweisen, die Sie lesen sollten: Nützliche Vorgehensweisen für Zugriffsregeln und Firewalls

Mit Schnittstelle verknüpfen

In diesem Fenster können Sie eine Regel, die Sie über das Fenster **Zugriffsregeln** erstellt haben, mit einer Schnittstelle verknüpfen und festlegen, ob diese Regel für ausgehenden oder eingehenden Datenverkehr gelten soll.

Schnittstelle auswählen

Wählen Sie die Schnittstelle aus, für die diese Regel gelten soll.

Richtung angeben

Wenn Sie möchten, dass der Router eingehende Pakete an der Schnittstelle prüfen soll, klicken Sie auf **Eingehend**. Der Router sucht nach einer Übereinstimmung mit der Regel, bevor er das Paket weiterleitet; abhängig davon, ob die Regel das Paket zulässt oder verweigert, akzeptiert der Router das Paket oder entfernt es. Wenn Sie möchten, dass der Router das Paket an die ausgehende Schnittstelle weiterleitet, bevor es mit den Einträgen in der Zugriffsregel verglichen wird, klicken Sie auf **Ausgehend**.

Wenn bereits eine andere Regel mit der Schnittstelle verknüpft ist

Wenn ein Informationsfeld angezeigt wird, das Ihnen mitteilt, dass eine andere Zugriffsregel mit der Schnittstelle in der angegebenen Richtung verknüpft ist, können Sie den Vorgang entweder abbrechen oder fortfahren, indem Sie die Regeleinträge an die Regel anhängen, die bereits auf die Schnittstelle angewendet wird, oder indem Sie die Regel von der Schnittstelle trennen und die neue Regel mit dieser Schnittstelle verknüpfen.

Was möchten Sie tun?

Aufgabe	Vorgehensweise
Vorgang abbrechen und die Verknüpfung zwischen der Schnittstelle und der vorhandenen Regel beibehalten.	Klicken Sie auf **Nein**. Die Verknüpfung zwischen der vorhandenen Regel und der Schnittstelle wird beibehalten, und die Regel, die Sie im Fenster **Regel hinzufügen** erstellt haben, wird gespeichert. Sie können die vorhandene Regel und die neue Regel überprüfen und festlegen, ob Sie die vorhandene Regel ersetzen oder die Einträge der neuen Regel mit der vorhandenen Regel zusammenführen möchten.
Fortfahren und die Einträge der erstellten Regel mit den Einträgen der vorhandenen Regel zusammenführen.	Klicken Sie auf **Ja**. Klicken Sie dann, wenn ein Fenster mit der Frage angezeigt wird, ob Sie die vorhandene Regel zusammenführen oder ersetzen möchten, auf **Zusammenführen**. Die für die neue Regel erstellten Einträge werden hinter dem letzten Eintrag an die vorhandene Regel angehängt. **Hinweis** Wenn die Regel, die Sie zusammenführen möchten, nicht mit der vorhandenen Regel kompatibel ist, haben Sie nur die Option, die vorhandene Regel zu ersetzen.
Fortfahren und die vorhandene Regel durch die neu erstellte Regel ersetzen.	Klicken Sie auf **Ja**. Klicken Sie dann, wenn ein Fenster mit der Frage angezeigt wird, ob Sie die vorhandene Regel zusammenführen oder ersetzen möchten, auf **Ersetzen**. Die Regel, die Sie überschreiben, wird nicht gelöscht. Sie wird nur von der Schnittstelle und der Richtung getrennt.

Standardregeleintrag hinzufügen

Mit einem Standardregeleintrag können Sie Datenverkehr zulassen oder verweigern, der von einer bestimmten Quelle stammt. Diese Quelle kann ein Netzwerk oder ein Host innerhalb eines bestimmten Netzwerks sein. Sie können in diesem Fenster einen einzelnen Regeleintrag erstellen, können jedoch auch zu diesem Fenster zurückkehren, um gegebenenfalls zusätzliche Einträge für eine Regel zu erstellen.

Hinweis Datenverkehr, der keiner der Kriterien in den von Ihnen erstellten Regeleinträgen entspricht, wird entfernt. Wenn Sie sicherstellen möchten, dass Datenverkehr, den Sie nicht verweigern möchten, zugelassen wird, müssen Sie explizite Zulassungsregeln an die Regel anhängen, die Sie konfigurieren.

Aktion

Wählen Sie die Aktion, die der Router unternehmen soll, wenn ein Paket den Kriterien des Regeleintrags entspricht. Die Optionen sind **Zulassen** und **Verweigern**. Was die Kriterien **Zulassen** und **Verweigern** bewirken, hängt von dem Regeltyp ab, in dem sie verwendet werden. In Cisco SDM können Standardregeleinträge in Zugriffsregeln, NAT-Regeln und in mit Routenzuordnungen verknüpfte Zugriffslisten verwendet werden. Klicken Sie auf Bedeutung der Schlüsselwörter Zulassen und Verweigern, um weitere Informationen zu den Aktionen **Zulassen** und **Verweigern** im Kontext eines bestimmten Regeltyps zu erhalten.

Quellhost/-netzwerk

Die Kriterien für die Quell-IP-Adresse, denen der Datenverkehr entsprechen muss. Die Felder in diesem Fensterbereich ändern sich je nach dem Wert des Felds **Typ**.

Typ

Wählen Sie eine der folgenden Typen:

- Ein Netzwerk. Wählen Sie diesen Typ aus, wenn Sie die Aktion auf alle IP-Adressen im Netzwerk anwenden möchten.

- Ein Hostname oder eine IP-Adresse. Wählen Sie diesen Typ aus, wenn Sie die Aktion auf einen bestimmten Host oder eine bestimmte IP-Adresse anwenden möchten.
- Beliebige IP-Adresse. Wählen Sie diesen Typ aus, wenn Sie die Aktion auf eine beliebige IP-Adresse anwenden möchten.

IP-Adresse

Wenn Sie **Ein Netzwerk** oder **Ein Hostname oder eine IP-Adresse** ausgewählt haben, geben Sie die IP-Adresse in dieses Feld ein. Wenn die eingegebene Adresse eine Netzwerkadresse ist, geben Sie eine Platzhaltermaske ein, um die Teile der Netzwerkadresse anzugeben, denen entsprochen werden muss.

Maske

Wenn Sie **Ein Netzwerk** oder **Ein Hostname oder eine IP-Adresse** gewählt haben, wählen Sie entweder eine Platzhaltermaske aus dieser Liste aus, oder geben Sie eine benutzerdefinierte Platzhaltermaske ein. Eine binäre 0 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse eines Pakets exakt übereinstimmen muss. Eine binäre 1 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse des Pakets nicht übereinstimmen muss.

Hostname/IP

Wenn Sie im Feld **Typ** die Option **Ein Hostname oder eine IP-Adresse** im Feld ausgewählt haben, geben Sie den Namen oder die IP-Adresse des Hosts ein. Wenn Sie einen Hostnamen eingeben, muss der Router für die Verwendung eines DNS-Servers konfiguriert sein.

Beschreibung

In dieses Feld können Sie eine kurze Beschreibung des Eintrags eingeben. Die Beschreibung darf nicht mehr als 100 Zeichen enthalten.

Entsprechungen für diesen Eintrag protokollieren

Wenn Sie Syslog in den Systemeigenschaften festgelegt haben, können Sie dieses Kontrollkästchen aktivieren; Übereinstimmungen werden dann im Systemprotokoll aufgezeichnet.

Eintrag für erweiterte Regel hinzufügen

Ein erweiterter Regeleintrag ermöglicht es Ihnen, Datenverkehr auf der Grundlage seiner Quelle und seines Ziels sowie des im Paket angegebenen Protokolls und Dienstes zuzulassen oder zu verweigern.

Hinweis Datenverkehr, der keiner der Kriterien in den von Ihnen erstellten Regeleinträgen entspricht, wird entfernt. Wenn Sie sicherstellen möchten, dass Datenverkehr, den Sie nicht verweigern möchten, zugelassen wird, müssen Sie explizite Zulassungsregeln an die Regel anhängen, die Sie konfigurieren.

Aktion

Wählen Sie die Aktion, die der Router unternehmen soll, wenn ein Paket den Kriterien des Regeleintrags entspricht. Die Optionen sind **Zulassen** und **Verweigern**. Wenn Sie einen Eintrag für eine IPSec-Regel erstellen, können Sie wählen, ob die Option **Datenverkehr schützen** aktiviert wird oder nicht.

Was die Kriterien **Zulassen** und **Verweigern** bewirken, hängt von dem Regeltyp ab, in dem sie verwendet werden. In Cisco SDM können erweiterte Regeleinträge in Zugriffsregeln, NAT-Regeln, IPSec-Regeln und in mit Routenzuordnungen verknüpften Zugriffslisten verwendet werden. Klicken Sie auf Bedeutung der Schlüsselwörter Zulassen und Verweigern, um weitere Informationen zu den Aktionen **Zulassen** und **Verweigern** im Kontext eines bestimmten Regeltyps zu erhalten.

Quellhost/-netzwerk

Die Kriterien für die Quell-IP-Adresse, denen der Datenverkehr entsprechen muss. Die Felder in diesem Fensterbereich ändern sich je nach dem Wert des Felds **Typ**.

Typ

Wählen Sie eine der folgenden Typen:

- Eine bestimmte IP-Adresse. Dies kann die Adresse eines Netzwerks oder eines bestimmten Hosts sein.
- Ein Hostname.
- Beliebige IP-Adresse.

IP-Adresse

Wenn Sie **eine bestimmte IP-Adresse** ausgewählt haben, geben Sie die **IP-Adresse** in dieses Feld ein. Wenn die eingegebene Adresse eine Netzwerkadresse ist, geben Sie eine Platzhaltermaske ein, um die Teile der Netzwerkadresse anzugeben, denen entsprochen werden muss.

Maske

Wenn Sie **eine bestimmte IP-Adresse** ausgewählt haben, wählen Sie entweder eine Platzhaltermaske aus dieser Liste aus, oder geben Sie eine benutzerdefinierte Platzhaltermaske ein. Eine binäre 0 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse des Pakets exakt übereinstimmen muss. Eine binäre 1 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse des Pakets nicht übereinstimmen muss.

Hostname

Wenn Sie **einen Hostnamen** im Feld **Typ** ausgewählt haben, geben Sie den Namen des Hosts ein.

Zielhost/-netzwerk

Die Kriterien für die Quell-IP-Adresse, denen der Datenverkehr entsprechen muss. Die Felder in diesem Fensterbereich ändern sich je nach dem Wert des Felds **Typ**.

Typ

Wählen Sie eine der folgenden Typen:

- Eine bestimmte IP-Adresse. Dies kann die Adresse eines Netzwerks oder eines bestimmten Hosts sein.
- Ein Hostname.
- Beliebige IP-Adresse.

Maske

Wenn Sie **eine bestimmte IP-Adresse** ausgewählt haben, wählen Sie entweder eine Platzhaltermaske in dieser Liste aus, oder geben Sie eine benutzerdefinierte Platzhaltermaske ein. Eine binäre 0 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse des Pakets exakt übereinstimmen muss. Eine binäre 1 in einer Platzhaltermaske bedeutet, dass das entsprechende Bit in der IP-Adresse des Pakets nicht übereinstimmen muss.

Hostname

Wenn Sie **einen Hostnamen** im Feld **Typ** ausgewählt haben, geben Sie den Namen des Hosts ein.

Beschreibung

In dieses Feld können Sie eine kurze Beschreibung des Eintrags eingeben. Die Beschreibung darf nicht mehr als 100 Zeichen enthalten.

Protokoll und Dienst

Wählen Sie das Protokoll und den Dienst, falls vorhanden, auf das bzw. den Sie den Eintrag anwenden möchten. Die angegebenen Informationen sind je nach Protokoll unterschiedlich. Klicken Sie auf das Protokoll, um anzuzeigen, welche Informationen Sie eingeben müssen.

Quell-Port

Verfügbar, wenn entweder TCP oder UDP ausgewählt ist. Wenn Sie dieses Feld einstellen, filtert der Router am Quell-Port in einem Paket. Es ist selten erforderlich, einen Quell-Port-Wert für eine TCP-Verbindung festzulegen. Wenn Sie nicht sicher sind, ob Sie dieses Feld verwenden müssen, lassen Sie es auf **= any (alle)** eingestellt.

Ziel-Port

Verfügbar, wenn entweder TCP oder UDP ausgewählt ist. Wenn Sie dieses Feld einstellen, filtert der Router am Ziel-Port in einem Paket.

Wenn Sie folgendes Protokoll auswählen:	…können Sie die folgenden Einstellungen in den Feldern Quell-Port und Ziel-Port vornehmen:
TCP und UDP	Geben Sie den Quell- und den Ziel-Port nach Name oder Nummer an. Wenn Sie sich an den Namen oder die Nummer nicht erinnern, klicken Sie auf die Schaltfläche **...**, und wählen Sie den gewünschten Wert aus dem angezeigten Fenster aus. In dieses Feld können Protokollnummern von 0 bis 65535 eingegeben werden. • =. Der Regeleintrag wird auf den Wert angewendet, den Sie in das rechte Feld eingeben. • !=. Der Regeleintrag wird auf jeden beliebigen Wert ausgenommen dem Wert angewendet, den Sie in das rechte Feld eingeben. • <. Der Regeleintrag wird auf alle Portnummern angewendet, die niedriger als die eingegebene Nummer sind. • >. Der Regeleintrag wird auf alle Portnummern angewendet, die höher als die eingegebene Nummer sind. • Bereich. Der Eintrag wird auf den Bereich von Portnummern angewendet, die Sie in die rechten Felder eingeben.
ICMP	Geben Sie als ICMP-Typ **any (alle)** ein, oder geben Sie einen Typ nach Name oder Nummer ein. Wenn Sie sich an den Namen oder die Nummer nicht erinnern, klicken Sie auf die Schaltfläche **...**, und wählen Sie den gewünschten Wert aus. In dieses Feld können Protokollnummern von 0 bis 255 eingegeben werden.
IP	Geben Sie als IP-Protokoll **any (alle)** ein, oder geben Sie ein Protokoll nach Name oder Nummer ein. Wenn Sie sich an den Namen oder die Nummer nicht erinnern, klicken Sie auf die Schaltfläche **...**, und wählen Sie den gewünschten Wert aus. In dieses Feld können Protokollnummern von 0 bis 255 eingegeben werden.

Eine Tabelle mit Portnamen und -nummern, die in Cisco SDM verfügbar sind, finden Sie unter Dienste und Ports.

Entsprechungen für diesen Eintrag protokollieren

Falls Sie Protokollierung für Firewall-Meldungen konfiguriert haben, können Sie dieses Feld aktivieren, damit Übereinstimmungen, die in der Protokolldatei aufgezeichnet werden, zum syslog-Server gesendet werden. Weitere Informationen finden Sie unter folgendem Link: Firewall-Protokoll.

Regel auswählen

In diesem Fenster können Sie eine zu verwendende Regel auswählen.

Regelkategorie

Wählen Sie die Regelkategorie, aus der Sie auswählen möchten. Die Regeln in der ausgewählten Kategorie werden im Feld unterhalb der Liste angezeigt. Wenn keine Regeln im Feld angezeigt werden, wurden keine Regeln dieser Kategorie definiert.

Name/Nummer

Der Name oder die Nummer der Regel.

Verwendet von

Wie die Regel verwendet wird. Wenn die Regel beispielsweise mit einer Schnittstelle verknüpft wurde, der Name dieser Schnittstelle. Wenn die Regel in einer IPSec-Richtlinie verwendet wird, der Name der Richtlinie. Wenn die Regel dagegen von NAT verwendet wurde, enthält diese Spalte den Wert NAT.

Beschreibung

Eine Beschreibung der Regel.

Vorschau

Dieser Bereich des Bildschirms zeigt die Einträge der ausgewählten Regel an.

Aktion

Entweder **Zulassen** oder **Verweigern**. Klicken Sie auf Bedeutung der Schlüsselwörter Zulassen und Verweigern, um weitere Informationen zu den Aktionen **Zulassen** oder **Verweigern** im Kontext eines bestimmten Regeltyps zu erhalten.

Quelle

Die Kriterien für die Quell-IP-Adresse, denen der Datenverkehr entsprechen muss. Diese Spalte kann Folgendes enthalten:

- Eine IP-Adresse und eine Platzhaltermaske. Die IP-Adresse gibt ein Netzwerk an, und die Platzhaltermaske gibt an, zu welchem Anteil der IP-Adresse die IP-Adresse im Paket übereinstimmen muss.
- Das Schlüsselwort **alle. Alle** bedeutet, dass die Quell-IP-Adresse beliebig sein kann.
- Ein Hostname.

Ziel

Bei erweiterten Regeln die Kriterien für die Ziel-IP-Adresse, denen der Datenverkehr entsprechen muss. Die Adresse kann die eines Netzwerks oder eines bestimmten Hosts sein. Diese Spalte kann Folgendes enthalten:

- Eine IP-Adresse und eine Platzhaltermaske. Die IP-Adresse gibt ein Netzwerk an, und die Platzhaltermaske gibt an, zu welchem Anteil der IP-Adresse die IP-Adresse im Paket übereinstimmen muss.
- Das Schlüsselwort **alle. Alle** bedeutet, dass die Quell-IP-Adresse beliebig sein kann.
- Ein Hostname.

Dienst

Für erweiterte Regeln gibt der Dienst den Typ des Datenverkehrs an, den Pakete, die den Regeln entsprechen, enthalten müssen. Dies wird durch Anzeigen des Dienstes, beispielsweise „Echoantwort“, gefolgt von dem Protokoll, zum Beispiel „ICMP“, dargestellt. Eine Regel, die mehrere Dienste zwischen denselben Endpunkten zulässt oder verweigert, muss einen Eintrag für jeden Dienst enthalten.

KAPITEL 30

Port-to-Application Mapping

Port-to-Application Mapping (PAM) ermöglicht Ihnen die Anpassung von TCP- und UDP-Portnummern für Netzwerkdienste und –anwendungen. PAM benutzt diese Informationen, um Netzwerkumgebungen zu unterstützen, auf denen Dienste laufen, die Ports benutzen, welche sich von den registrierten oder gut bekannten Ports unterscheiden, die mit einer Anwendung verknüpft sind.

Die Informationen, die PAM pflegt, aktivieren Context Based Access Control (CBAC) unterstützte Dienste, um auf nicht standardisierten Ports zu laufen. Früher war CBAC darauf beschränkt, Verkehr zu untersuchen, der von den gut bekannten oder registrierten Ports kommt, die mit einer Anwendung verknüpft sind. In der jetzigen Version ermöglicht PAM Netzwerkadministratoren, die Netzwerkzugangssteuerung für angegebene Anwendungen und Dienste für Ihre Bedürfnisse anzupassen.

Port-to-Application Mappings

Dieses Fenster zeigt die auf dem Router konfigurierten Port-to-Application Mappings an und ermöglicht Ihnen, PAM-Einträge hinzuzufügen, zu bearbeiten und zu löschen. Jede Zeile im Fenster zeigt einen PAM-Eintrag an. Einträge werden nach ihrem Typ gruppiert.

Tasten Hinzufügen, Bearbeiten und Löschen

Benutzen Sie diese Schaltflächen, um PAM-Einträge zu erstellen, zu bearbeiten und zu löschen. Nach dem Klicken auf die Schaltfläche **Hinzufügen** können Sie Einträge erstellen, die Protokollnamen vom Standard abweichende Portnummern zuweisen. Wenn Sie auf **Bearbeiten** klicken, können Sie Änderungen an den benutzerdefinierten Einträgen vornehmen. Einträge mit dem Wert *Systemdefiniert* in der Spalte **Protokolltyp** können nicht bearbeitet oder gelöscht werden.

Spalte Anwendungsprotokoll

Diese Spalte enthält den Namen des Anwendungsprotokolls und den Namen der Protokolltypen. So werden zum Beispiel FTP- und TFTP-Einträge unter dem Protokolltyp Dateitransfer gefunden.

Spalte Porttyp

Diese Liste wird angezeigt, wenn auf dem Router ein Cisco IOS-Image läuft, bei dem Sie angeben können, ob der betreffende Portzuordnungseintrag für TCP- oder UDP-Datenverkehr gelten soll.

Spalte Port

In dieser Spalte befindet sich die Portnummer. Bei einem vom System definierten Eintrag für HTTP steht die Portnummer 80 in dieser Spalte. Bei einem benutzerspezifischen Eintrag für HTTP kann beispielsweise die Portnummer 8080 oder eine andere anwendungsspezifische Nummer in dieser Spalte eingetragen sein.

Spalte Protokolltyp

Eine Zeile in dieser Spalte zeigt einen der folgenden Werte an.

- **Benutzerdefiniert** - Der Eintrag enthält eine nicht standardisierte Zuordnung zwischen Protokoll und Protokollnummer. Der Eintrag könnte mit einer Host-IP-Adresse verknüpft sein, die durch die Zugangssteuerungsliste (Access Control List – ACL) identifiziert wird und deren Nummer in der Spalte Zugangsliste angezeigt wird.
- **Systemdefiniert** - Der Eintrag enthält ein standardisiertes, registriertes Mapping zwischen Protokoll und Protokollnummer, wie zum Beispiel *tftp 69* oder *smtp 25*. Vom System definierte Einträge können nicht bearbeitet oder gelöscht werden. Bei Einträgen, die vom System definiert wurden, enthält die Spalte **Zugriffsliste** keinen Wert, weil diese für sämtliche Hosts im Netzwerk gelten.

Spalte Zugangsliste

Ein PAM-Eintrag gilt für einen einzelnen Host, der durch eine Standard-ACL definiert wird. Diese Spalte zeigt die Nummer der ACL an, die benutzt wird, um den Host zu bestimmen, auf den der PAM-Eintrag anzuwenden ist. Wenn Sie die ACL anzeigen wollen, die für den Host gilt, klicken Sie auf **Zusätzliche Aufgaben > ACL Editor > Zugriffsregeln**. Klicken Sie anschließend auf die Nummer der ACL, die Sie in diesem Fenster gesehen haben.

Spalte Beschreibung

Wenn für einen PAM-Eintrag eine Beschreibung erstellt wurde, wird die Beschreibung in dieser Spalte angezeigt.

Port-Map-Eintrag hinzufügen oder bearbeiten

Sie können Port-Map-Einträge für Kunden- oder Standardprotokolle hinzufügen oder bearbeiten.

Feld Protokoll

Wenn Sie einen Eintrag hinzufügen, geben Sie das Protokoll an, indem Sie auf die Auflistungsschaltfläche (**...**) auf der rechten Seite klicken und ein systemdefiniertes Protokoll auswählen oder indem Sie den Namen eines kundenspezifischen Protokolls eingeben. Sie können keine kundendefinierte Protokollnamen eingeben, wenn für sie bereits ein Port-Mapping existiert.

Wenn Sie einen Eintrag bearbeiten, ist das Protokollfeld deaktiviert. Wenn Sie das Protokoll ändern müssen, löschen Sie den PAM-Eintrag und geben Sie ihn erneut mit den Protokollinformationen ein, die Sie benötigen.

Feld Beschreibung

Dieses Feld erscheint, wenn auf dem Router ein Cisco IOS-Image läuft, bei dem Sie angeben können, ob dieser Portzuordnungseintrag für TCP- oder für UDP-Datenverkehr gelten soll. Sie können optional eine Beschreibung zum Port-Map-Eintrag eingeben. Beschreibungen sind dann hilfreich, wenn Sie Einträge für Kundenprotokolle oder besondere Anwendungen hinzufügen. Wenn Sie zum Beispiel einen Eintrag für eine Kundendatenbankanwendung mit dem Namen **orville** erstellt haben, die auf dem Host sf-5 läuft, dann können Sie **orville –sf-5** eingeben.

Liste Porttyp

Diese Liste wird angezeigt, wenn auf dem Router ein Cisco IOS-Image läuft, bei dem Sie angeben können, ob der betreffende Portzuordnungseintrag für TCP- oder UDP-Datenverkehr gelten soll. Wählen Sie entweder **TCP** oder **UDP** aus. Die Standardeinstellung ist TCP

Feld Portnummer

Geben Sie die Portnummer ein, die Sie auf das von Ihnen angegebene Protokoll abbilden wollen. Wenn auf dem Router ein Cisco IOS-Image läuft, bei dem Sie bestimmen können, ob dieser Portzuordnungseintrag für TCP oder UDP-Datenverkehr gelten soll, können Sie mehrere Portnummern angeben, indem Sie die einzelnen Nummern durch Kommas voneinander trennen oder indem Sie Portnummernbereiche mit Bindestrichen voneinander trennen. Sie können zum Beispiel drei nicht aufeinander folgende Portnummern 310, 313, 318 eingeben oder aber den Bereich 415-419 eingeben.

Wenn auf dem Router kein Cisco IOS-Abbild ausgeführt wird, bei dem Sie eine spezielle Portzuordnung für TCP- oder UDP-Datenverkehr festlegen können, können Sie nur eine einzelne Portnummer eingeben.

Feld Servicehost

Geben Sie die IP-Adresse des Hosts an, auf welche dieses Port-Mapping angewendet werden soll. Wenn Sie für einen anderen Host das gleiche Mapping brauchen, erstellen Sie einen separaten PAM-Eintrag für diesen Host.

KAPITEL 31

Zonenbasierte Richtlinienfirewall (Zone-Based Policy Firewall)

Die zonenbasierte Richtlinienfirewall (auch als „Zone-Policy Firewall“ oder „ZPF“ bezeichnet) ändert die Firewall vom älteren schnittstellenbasierten Modell in ein flexibleres, leichter verständliches zonenbasiertes Konfigurationsmodell. Schnittstellen werden Zonen zugeordnet, und es wird eine Prüfrichtlinie auf Datenverkehr zwischen zwei Zonen angewendet. Richtlinien zwischen den Zonen ermöglichen eine umfassende Flexibilität und exaktere Definition, sodass unterschiedliche Prüfrichtlinien auf mehrere Hostgruppen angewendet werden können, die mit derselben Routerschnittstelle verbunden sind.

Firewallrichtlinien sind mit der Cisco Common Classification Policy Language (C3PL) konfiguriert, die eine hierarchische Struktur für die Prüfung auf Netzwerkprotokolle und für die Gruppen von Hosts nutzt, auf die die Prüfung angewendet wird.

Eine ausführliche Beschreibung zur Implementierung der zonenbasierten Richtlinienfirewall finden Sie in *The Zone-Based Policy Firewall Design Guide* unter cisco.com. Wählen Sie **Support > Product Support > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Configure > Feature Guides**, und klicken Sie auf **Zone-Based Policy Firewall Design Guide**. Dieses Dokument ist auch unter folgendem Link verfügbar:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Reihenfolge der Aufgaben zur Konfiguration

Für die Konfiguration einer zonenbasierten Richtlinienfirewall kann folgende Reihenfolge eingehalten werden:

1. Definieren von Zonen
2. Definieren von Zonenpaaren
3. Definieren von Klassenzuordnungen, die den Datenverkehr beschreiben, für den die Richtlinie angewendet wird, sobald dieser auf ein Zonenpaar trifft
4. Definieren von Richtlinienzuordnungen, um Aktionen auf den Datenverkehr Ihrer Klassenzuordnung anzuwenden
5. Anwenden von Klassenzuordungen auf Zonenpaare
6. Zuweisen von Schnittstellen zu Zonen

Die Reihenfolge der Aufgaben spielt keine Rolle, einige Ereignisse müssen allerdings in einer bestimmten Abfolge abgeschlossen werden. Sie müssen beispielsweise erst eine Klassenzuordnung konfigurieren, bevor Sie eine Klassenzuordnung einer Richtlinienzuordnung zuweisen. Ebenso können Sie auch erst dann eine Zuordnung von einer Richtlinienzuordnung zu einem Zonenpaar vornehmen, nachdem die Konfiguration der Richtlinie erfolgt ist. Wenn Sie versuchen, eine Aufgabe abzuschließen, die von einem anderen Teil der Konfiguration abhängt, für den Sie keine Konfiguration vorgenommen haben, lässt SDM den Abschluss dieser Aufgabe nicht zu.

Fenster „Zone“

Bei einer Zone oder Sicherheitszone handelt es sich um eine Gruppe von Schnittstellen, auf die eine Sicherheitsrichtlinie angewendet werden kann. Die Schnittstellen in einer Zone sollten dieselben allgemeinen Funktionen oder Merkmale verwenden. Zwei Schnittstellen, die mit dem lokalen LAN verbunden sind, könnten beispielsweise in einer Sicherheitszone platziert, und die Schnittstellen, die mit dem Internet verbunden sind, könnten in einer anderen Sicherheitszone platziert werden.

Damit Datenverkehr zwischen allen Schnittstellen in einem Router fließen kann, müssen sämtliche Schnittstellen Mitglieder von bestimmten Sicherheitszonen sein. Es müssen nicht alle Routerschnittstellen Mitglieder von Sicherheitszonen sein.

Unter „Allgemeine zonenbasierte Richtlinienregeln“ werden die Regeln aufgeführt, die das Verhalten der Schnittstellen und den Datenverkehrsfluss zwischen den Schnittstellen festlegen, die Mitglieder von Zonen sind.

Dieses Fenster zeigt den Namen der einzelnen Sicherheitszonen, die darin enthaltenen Schnittstellen und alle verknüpften Zonenpaare an, zu der die Zone als Mitglied gehört. Eine Zone kann Mitglied von mehreren Zonenpaaren sein.

Klicken Sie auf **Hinzufügen**, um eine neue Zone zu erstellen.

Klicken Sie auf **Bearbeiten**, um unterschiedliche Schnittstellen für eine vorhandene Zone auszuwählen.

Klicken Sie auf **Löschen**, um eine Zone zu entfernen. Eine Zone, die Mitglied eines Zonenpaars ist, kann nicht gelöscht werden.

Hinzufügen oder Bearbeiten einer Zone

Um eine neue Zone, auch als Sicherheitszone bezeichnet, hinzuzufügen, geben Sie einen Namen für die Zone ein und wählen die Schnittstellen aus, die in der Zone enthalten sein sollen. Die Schnittstellenliste zeigt die Namen der verfügbaren Schnittstellen an. Da physikalische Schnittstellen nur in einer Zone platziert werden können, werden diese nicht in der Liste angezeigt, wenn diese bereits in einer Zone platziert wurden. Virtuelle Schnittstellen, wie Dialer-Schnittstellen und virtuelle Vorlagenschnittstellen, können in mehreren Zonen platziert werden und werden stets in der Liste aufgeführt.

Hinweis

- Datenverkehr, der an oder ausgehend von dieser Schnittstelle geleitet wird, wird von der Richtlinienzuordnung bestimmt, die mit der Zone verknüpft ist.
- Eine Schnittstelle, die Sie dieser Zone zuordnen, kann für ein Site-to-Site-VPN, DMVPN, Easy VPN, SSL VPN oder einen andere Verbindungstyp verwendet werden, deren Datenverkehr von einer Firewall blockiert werden kann. Wenn Sie in diesem Dialogfeld eine Schnittstelle einer Zone zuordnen, erstellt SDM keine Passthrough-ACL, um solchen Datenverkehr zuzulassen. Es bestehen zwei Möglichkeiten, um den erforderlichen Passthrough für die Richtlinienzuordung zu konfigurieren.

– Wechseln Sie zu **Konfigurieren > Firewall und ACL > Firewallrichtlinie bearbeiten > Regel für neuen Datenverkehr**. Geben Sie im angezeigten Dialogfeld Informationen zur Quell- und Ziel-IP-Adresse sowie den Datenverkehrstyp an, für den das Passieren durch die Firewall zulässig sein muss. Wählen Sie im Feld **Aktion** die Option **ACL zulassen** aus.

– Wechseln Sie zu **Konfigurieren > C3PL > Richtlinienzuordnung > Protokollprüfung**. Geben Sie eine Richtlinienzuordnung für eine Protokollprüfung an, die das Passieren des erforderlichen Datenverkehrs durch die Firewall zulässt.

Nach der Erstellung einer Zone können Sie die der Zone zugeordneten Schnittstellen ändern. Der Name der Zone kann jedoch nicht geändert werden.

Allgemeine zonenbasierte Richtlinienregeln

Die Zugehörigkeit von Router-Netzwerkschnittstellen zu Zonen hängt ebenso wie der Datenverkehr zwischen Schnittstellen, die Mitglieder von Zonen sind, von mehreren Regeln ab, die das Schnittstellenverhalten bestimmen:

- Es muss eine Zone konfiguriert sein, bevor Schnittstellen der Zone zugeordnet werden können.
- Eine Schnittstelle kann nur einer Sicherheitszone zugeordnet werden.
- Sämtlicher Datenverkehr zu/von einer bestimmten Schnittstelle wird ausdrücklich blockiert, wenn die Schnittstelle einer Zone zugewiesen wird, mit Ausnahme des Datenverkehrs zu/von anderen Schnittstellen in derselben Zone und des Datenverkehrs an alle Schnittstellen im Router.
- Der Datenverkehrsfluss zwischen Schnittstellen, die Mitglied derselben Zone sind, wird ausdrücklich zugelassen.
- Um Datenverkehr zu/von einer Schnittstelle zuzulassen, die Mitglied einer Zone ist, muss zwischen dieser Zone und allen anderen Zonen eine Richtlinie konfiguriert werden, die das Zulassen oder Prüfen von Datenverkehr erlaubt.
- Die Zone **Self** stellt die einzige Ausnahme der standardmäßigen Richtlinie **Alle verweigern** dar. Sämtlicher Datenverkehr an beliebige Routerschnittstellen wird zugelassen, bis der Datenverkehr ausdrücklich verweigert wird.

- Es kann kein Datenverkehrsfluss zwischen einer Schnittstelle eines Zonenmitglieds und einer Schnittstelle, die kein Zonenmitglied ist, erfolgen.
- Zwischen zwei Zonen können nur die Aktionen für das Passieren, Prüfen und Entfernen angewendet werden.
- Schnittstellen, die keiner Zonenfunktion als klassische Routerports zugewiesen sind und unter Umständen noch die klassische Stateful Inspection/CBAC-Konfiguration verwenden.
- Wenn eine Schnittstelle im Feld nicht Teil der Zonen-/Firewallrichtlinie sein soll, ist es eventuell trotzdem erforderlich, diese Schnittstelle in einer Zone zu platzieren und eine Richtlinie für das Passieren des gesamten Datenverkehrs (eine Art Dummy-Richtlinie) zwischen dieser Zone und allen anderen Zonen zu konfigurieren, an die der Datenverkehrsfluss erwünscht ist.
- Aus den vorherigen Punkten folgt, dass, sofern Datenverkehr zwischen allen Schnittstellen in einem Router fließen soll, sämtliche der Schnittstellen Teil des Zonenmodells sein müssen (jede Schnittstelle muss ein Mitglied einer bestimmten oder einer anderen bestimmten Zone sein).
- Die einzige Ausnahme aus dem vorherigen Ansatz der standardmäßigen Verweigerung ist der Datenverkehr zum/vom Router, der standardmäßig zugelassen wird. Es kann eine ausdrückliche Richtlinie konfiguriert werden, um solchen Datenverkehr einzuschränken.

Dieser Regelsatz wurde dem Handbuch *The Zone-Based Policy Firewall Design Guide* entnommen, das unter folgendem Link verfügbar ist:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Zonenpaare

Ein Zonenpaar ermöglicht Ihnen die Angabe einer unidirektionalen Firewallrichtlinie zwischen zwei Sicherheitszonen. Die Richtung des Datenverkehrs wird über eine Sicherheitszone für die Quelle und das Ziel angegeben. Ein und dieselbe Zone kann nicht sowohl als Quelle als auch als Ziel definiert werden.

Wenn Datenverkehr in beide Richtungen zwischen zwei Zonen fließen soll, müssen Sie für jede Richtung ein Zonenpaar erstellen. Wenn ein freier Datenverkehrsfluss zwischen allen Schnittstellen erfolgen soll, müssen die einzelnen Schnittstellen in einer Zone konfiguriert sein.

Die folgende Tabelle stellt ein Beispiel für vier Zonenpaare dar.

Zonenpaar	Quelle	Ziel	Richtlinie
LAN-out	zone-VLAN1	zone-FE1	inspection-policymap-a
LAN-in	zone-FE1	zone-VLAN1	inspection-policymap-b
Bkup-out	Self	zone-BRI0	inspection-policymap-c
Bkup-in	zone-BRI0	self	inspection-policymap-c

Bei **LAN-out** und **LAN-in** handelt es sich um Zonenpaare, die für Datenverkehr konfiguriert sind, der zwischen der LAN-Schnittstelle, VLAN1 und der FastEthernet 1-Schnittstelle fließt. Jedes Zonenpaar wird durch eine separate Richtlinie gesteuert. **Bkup-out** und **Bkup-in** sind für Datenverkehr konfiguriert, der vom Router generiert wird. Dieselbe Richtlinie steuert Datenverkehr, der von **zone-BRI0** als Datenverkehr gesendet wird. Dieser wird durch die Zone **Self** dargestellt.

Klicken Sie auf **Hinzufügen**, um ein Zonenpaar zu erstellen.

Klicken Sie auf **Bearbeiten**, um die mit einem Zonenpaar verknüpfte Richtlinie zu ändern.

Klicken Sie auf **Löschen**, um ein Zonenpaar zu entfernen.

Hinzufügen oder Bearbeiten eines Zonenpaars

Um ein neues Zonenpaar zu konfigurieren, geben Sie einen Namen für das Zonenpaar, eine Quellzone, von der der Datenverkehr stammt, eine Zielzone, an die der Datenverkehr gesendet werden soll, und die Richtlinie an, die festlegen soll, welcher Datenverkehr über die Zonen hinweg gesendet werden kann. Die Listen Quellzone und Zielzone enthalten die auf dem Router konfigurierten Zonen sowie die Zone Self. Die Zone **Self** kann verwendet werden, wenn Sie Zonenpaare für Datenverkehr, der vom Router selbst stammt oder für den Router selbst bestimmt ist, konfigurieren, wie für ein Zonenpaar, das für SNMP-Datenverkehr konfiguriert ist. Die Liste **Richtlinie** enthält den Namen jeder Richtlinienzuordnung, die auf dem Router konfiguriert ist.

Wenn Sie ein Zonenpaar bearbeiten, können Sie die Richtlinienzuordnung ändern. Änderungen am Namen oder an den Quell- oder Zielzonen sind jedoch nicht möglich.

Hinzufügen einer Zone

Sie können eine Konfiguration einer Schnittstelle als Mitglied einer Sicherheitszone über die Registerkarte **Schnittstellen und Verbindungen** vornehmen. Die von Ihnen hinzugefügte Zone enthält die Schnittstelle, die Sie als Zonenmitglied bearbeiten.

Hinweis

- Datenverkehr, der an oder von dieser Schnittstelle geleitet wird, wird von der Richtlinienzuordnung bestimmt, die mit der Zone verknüpft ist.
- Eine Schnittstelle, die Sie dieser Zone zuordnen, kann für ein Site-to-Site-VPN, DMVPN, Easy VPN, SSL VPN oder einen andere Verbindungstyp verwendet werden, deren Datenverkehr von einer Firewall blockiert werden kann. Wenn Sie in diesem Dialogfeld eine Schnittstelle einer Zone zuordnen, erstellt SDM keine Passthrough-ACL, um solchen Datenverkehr zuzulassen. Es bestehen zwei Möglichkeiten, um den erforderlichen Passthrough für die Richtlinienzuordung zu konfigurieren.

- Wechseln Sie zu **Konfigurieren > Firewall und ACL > Firewallrichtlinie bearbeiten > Regel für neuen Datenverkehr**. Geben Sie im angezeigten Dialogfeld Informationen zur Quell- und Ziel-IP-Adresse sowie den Datenverkehrstyp an, für den das Passieren durch die Firewall zulässig sein muss. Wählen Sie im Feld **Aktion** die Option **ACL zulassen** aus.
- Wechseln Sie zu **Konfigurieren > C3PL > Richtlinienzuordnung > Protokollprüfung**. Geben Sie eine Richtlinienzuordnung für eine Protokollprüfung an, die das Passieren des erforderlichen Datenverkehrs durch die Firewall zulassen soll.

Zonenname

Geben Sie den Namen der Zone ein, die Sie hinzufügen möchten.

Auswählen einer Zone

Wenn auf dem Router eine Sicherheitszone konfiguriert wurde, können Sie die Schnittstelle hinzufügen, die Sie als Mitglied dieser Zone konfiguriert haben.

Zone für die Schnittstelle auswählen

Wählen Sie die Zone aus, in der die Schnittstelle enthalten sein soll, aus, und klicken Sie auf **OK**.

KAPITEL 32

Authentifizierung, Autorisierung und Accounting

Cisco IOS-Authentifizierung, Autorisation und Accounting (AAA) ist ein architektonisches Rahmenwerk zur Konfiguration von drei voneinander unabhängigen Sicherheitsfunktionen. Dies geschieht auf eine konsistente Art und Weise. AAA bietet eine modulare Möglichkeit zur Anwendung von Authentifizierung, Autorisierung und Accounting-Diensten.

Cisco IOS AAA bietet die folgenden Vorteile:

- Erhöhte Flexibilität und Kontrolle
- Skalierbarkeit
- Standardisierte Authentifizierungsmethoden. Mit Cisco SDM können Sie die Authentifizierungsmethoden RADIUS (Remote Authentication Dialin User Service) und TACACS+ (Terminal Access Controller Access Control System Plus) konfigurieren.

AAA-Hauptfenster

In diesem Fenster erhalten Sie eine Übersicht über die AAA-Konfiguration auf dem Router. Wenn Sie ausführlichere Informationen anzeigen oder die AAA-Konfiguration bearbeiten möchten, klicken Sie auf den entsprechenden Knoten im AAA-Baum.

AAA aktivieren/deaktivieren

AAA ist standardmäßig aktiviert. Wenn Sie auf **Deaktivieren** klicken, werden Sie in Cisco SDM mit einer Meldung darüber informiert, dass Änderungen an der Konfiguration vorgenommen werden, um den Zugriff auf den Router zu gewährleisten. Wenn Sie AAA deaktivieren, können Sie den Router nicht als Easy VPN-Server konfigurieren und Benutzerkonten nicht CLI-Ansichten (Command Line Interface – Befehlszeilenschnittstelle) zuordnen.

AAA-Server und -Gruppen

In diesem schreibgeschützten Feld wird die Anzahl der AAA-Server und -Servergruppen angezeigt. Der Router gibt Authentifizierungs-, Autorisierungs- und Kontozuordnungsanforderungen an AAA-Server weiter. AAA-Server sind in Gruppen organisiert, damit der Router Verbindungen zu anderen Servern aufbauen kann, wenn der erste Server, zu dem eine Verbindung aufgebaut wurde, nicht verfügbar ist.

Authentifizierungsrichtlinien

In diesem schreibgeschützten Feld sind die konfigurierten Authentifizierungsrichtlinien aufgelistet. Authentifizierungsrichtlinien definieren, wie Benutzer identifiziert werden. Wenn Sie Authentifizierungsrichtlinien bearbeiten möchten, klicken Sie in der Baumstruktur mit den AAA-Regeln unter **Authentifizierungsrichtlinien** auf den Unterknoten **Anmeldung**.

Autorisierungsrichtlinien

In diesem schreibgeschützten Feld sind die konfigurierten Autorisierungsrichtlinien aufgelistet. **Autorisierungsrichtlinien definieren die Methoden, mit denen eine Benutzeranmeldung zugelassen oder verweigert wird.** Wenn Sie Autorisierungsrichtlinien bearbeiten möchten, klicken Sie in der Baumstruktur mit den AAA-Regeln auf **Autorisierungsrichtlinien**.

Wenn Sie Autorisierungsrichtlinien für die Exec- und die Netzwerkautorisierung bearbeiten möchten, klicken Sie in der Baumstruktur mit den AAA-Regeln unter dem Knoten **Autorisierungsrichtlinien** auf den Unterknoten **Exec** bzw. **Netzwerk**.

AAA-Server und -Gruppen

In diesem Fenster werden die AAA-Server und -Servergruppen beschrieben.

Fenster „AAA-Server“

In diesem Fenster können Sie einen Snapshot der Informationen über die AAA-Server anzeigen, für deren Nutzung der Router konfiguriert ist. Für jeden Server werden die IP-Adresse, der Servertyp und weitere Parameter angezeigt.

Globale Einstellungen

Klicken Sie auf diese Schaltfläche, um globale Einstellungen für TACACS+- und RADIUS-Server vorzunehmen. Im Fenster **Globale Einstellungen bearbeiten** können Sie angeben, wie lange ein Verbindungsaufbau mit einem AAA-Server versucht werden soll, bevor zum nächsten Server gewechselt wird, welcher Schlüssel beim Verbindungsaufbau mit TACACS+- oder RADIUS-Servern zu verwenden ist und auf welcher Schnittstelle TACACS+- oder RADIUS-Pakete empfangen werden. Diese Einstellungen gelten für alle Server, für die keine serverspezifischen Einstellungen vorgenommen wurden.

Schaltfläche

Klicken Sie auf diese Schaltfläche, um einen TACACS+- oder RADIUS-Server zur Liste hinzuzufügen.

Schaltfläche

Klicken Sie auf diese Schaltfläche, um die Informationen für den ausgewählten AAA-Server zu bearbeiten.

Löschen...

Klicken Sie auf diese Schaltfläche, um die Informationen für den ausgewählten AAA-Server zu löschen.

Server-IP-Adresse

Die IP-Adresse des AAA-Servers.

Typ

Der Servertyp, TACACS+ oder RADIUS.

Parameter

In dieser Spalte werden für jeden Server der Timeout-Wert, der Schlüssel und weitere Parameter aufgelistet.

TACACS+-Server hinzufügen/bearbeiten

In diesem Fenster fügen Sie Informationen für einen TACACS+-Server hinzu oder bearbeiten diese Informationen.

Server-IP oder Host

Geben Sie die IP-Adresse oder den Hostnamen des Servers ein. Wenn der Router nicht für die Verwendung eines DNS-Servers (Domain Name Service) konfiguriert wurde, geben Sie eine IP-Adresse ein.

Einzelverbindung zum Server

Aktivieren Sie dieses Kontrollkästchen, wenn der Router eine einzelne offene Verbindung zum TACACS+-Server beibehalten soll, anstatt bei jeder Kommunikation mit dem Server eine TCP-Verbindung zu öffnen und zu schließen. Eine einzelne offene Verbindung ist effizienter, da der TACACS+-Server eine größere Zahl von TACACS+-Operationen verarbeiten kann.

Hinweis Diese Option wird nur unterstützt, wenn der TACACS+-Server CiscoSecure 1.0.1 oder höher ausführt.

Serverspezifische Einrichtung

Aktivieren Sie dieses Kontrollkästchen, wenn Sie globale AAA-Servereinstellungen überschreiben und einen serverspezifischen Timeout-Wert und Verschlüsselungsschlüssel angeben möchten.

Timeout (Sekunden)

Geben Sie an, wie viele Sekunden der Router einen Verbindungsaufbau mit diesem Server versuchen soll, bevor er zum nächsten Server in der Gruppenliste wechselt. Wenn Sie keinen Wert eingeben, verwendet der Router den Wert, der im Fenster **AAA Server Global Settings** konfiguriert ist.

Schlüssel konfigurieren

Optional. Geben Sie den Schlüssel ein, der für die Verschlüsselung des Datenverkehrs zwischen dem Router und diesem Server verwendet werden soll. Wenn Sie keinen Wert eingeben, verwendet der Router den Wert, der im Fenster **AAA Server Global Settings** konfiguriert ist.

Neuer Schlüssel/Schlüssel bestätigen

Geben Sie den Schlüssel ein, und geben Sie ihn zur Bestätigung noch einmal ein.

RADIUS-Server hinzufügen/bearbeiten

In diesem Fenster fügen Sie Informationen für einen RADIUS-Server hinzu oder bearbeiten diese Informationen.

Server-IP oder Host

Geben Sie die IP-Adresse oder den Hostnamen des Servers ein. Wenn der Router nicht für die Verwendung eines DNS-Servers (Domain Name Service) konfiguriert wurde, geben Sie eine IP-Adresse ein.

Autorisierungsport

Geben Sie den Serverport an, der für Autorisierungsanforderungen verwendet werden soll. Der Standard ist 1645.

Kontozuordnungsport

Geben Sie den Serverport an, der für Kontozuordnungsanforderungen verwendet werden soll. Der Standard ist 1646.

Timeout (Sekunden)

Optional. Geben Sie an, wie viele Sekunden der Router einen Verbindungsaufbau mit diesem Server versuchen soll, bevor er zum nächsten Server in der Gruppenliste wechselt. Wenn Sie keinen Wert eingeben, verwendet der Router den Wert, der im Fenster **AAA Server Global Settings** konfiguriert ist.

Schlüssel konfigurieren

Optional. Geben Sie den Schlüssel ein, der für die Verschlüsselung des Datenverkehrs zwischen dem Router und diesem Server verwendet werden soll. Wenn Sie keinen Wert eingeben, verwendet der Router den Wert, der im Fenster **AAA Server Global Settings** konfiguriert ist.

Neuer Schlüssel/Schlüssel bestätigen

Geben Sie den Schlüssel ein, und geben Sie ihn zur Bestätigung noch einmal ein.

Globale Einstellungen bearbeiten

In diesem Fenster können Sie Kommunikationseinstellungen angeben, die für die gesamte Kommunikation zwischen dem Router und den AAA-Servern gelten. Kommunikationseinstellungen, die für einen spezifischen Router vorgenommen wurden, überschreiben die Einstellungen, die in diesem Fenster vorgenommen wurden.

TACACS+-Server/RADIUS-Server

Klicken Sie auf die entsprechende Schaltfläche, um den Servertyp anzugeben, für den Sie globale Parameter einstellen. Wenn Sie **TACACS+-Server** auswählen, gelten die Parameter für die gesamte Kommunikation mit TACACS+-Servern, für die keine spezifischen Parameter eingestellt sind. Wenn Sie **RADIUS-Server** auswählen, gelten die Parameter für die gesamte Kommunikation mit RADIUS-Servern, für die keine spezifischen Parameter eingestellt sind.

Timeout (Sekunden)

Geben Sie an, wie viele Sekunden auf eine Antwort vom RADIUS- oder TACACS+-Server gewartet werden soll.

Schlüssel

Geben Sie den Verschlüsselungsschlüssel für die gesamte Kommunikation zwischen dem Router und den TACACS+- oder RADIUS-Servern ein.

Wählen Sie die Quellschnittstelle aus

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine einzelne Schnittstelle angeben möchten, auf der der Router TACACS+- oder RADIUS-Pakete empfangen soll.

Schnittstelle

Wählen Sie die Routerschnittstelle, auf der der Router die TACACS+- oder RADIUS-Pakete empfangen soll. Wenn das Kontrollkästchen **Wählen Sie die Quellschnittstelle** nicht aktiviert ist, wird dieses Feld deaktiviert.

Fenster „AAA-Servergruppen“

In diesem Fenster werden die AAA-Servergruppen angezeigt, die auf diesem Router konfiguriert sind. Wenn keine AAA-Server konfiguriert wurden, ist dieses Fenster leer.

Hinzufügen, Bearbeiten und Löschen (Schaltflächen)

Klicken Sie auf **Hinzufügen**, um eine neue RADIUS-Servergruppe zu erstellen. Nachdem Sie diese Gruppe erstellt haben, werden der Name und die Gruppenmitglieder in diesem Fenster angezeigt. Klicken Sie auf **Bearbeiten**, um die Informationen für die markierte Servergruppe zu ändern. Klicken Sie auf **Löschen**, um die Informationen für die markierte Servergruppe zu entfernen.

Gruppenname

Der Name der Servergruppe. Mit Servergruppennamen können Sie einen einzelnen Namen verwenden, um auf mehrere Server hinzuweisen.

Art

Der Typ der Server in der ausgewählten Gruppe, entweder TACACS+ oder RADIUS.

Gruppenmitglieder

Die IP-Adressen oder Hostnamen der AAA-Server in dieser Gruppe.

AAA-Servergruppe hinzufügen oder bearbeiten

Erstellen oder ändern Sie eine AAA-Servergruppe in diesem Fenster.

Gruppenname

Geben Sie für die Gruppe einen Namen ein.

Servertyp

Wählen Sie den Servertyp, entweder RADIUS oder TACACS+.

Hinweis Dieses Feld kann je nach ausgeführter Konfiguration geschützt sein und für einen bestimmten Typ voreingestellt sein.

Wählen der Server, die in diese AAA-Servergruppe aufgenommen werden sollen

Dieser Bereich führt die IP-Adressen aller AAA-Server auf, die auf dem Router des gewählten Typs konfiguriert sind, sowie die verwendeten Authorization- und Accounting-Ports. Aktivieren Sie das Kontrollkästchen **Auswählen** neben den Servern, die Sie hinzufügen möchten.

Authentifizierungs- und Autorisierungs-Richtlinien

Die Fenster Authentifizierungsrichtlinien und Autorisierungsrichtlinen fassen die Informationen der Authentifizierungsrichtlinine auf dem Router zusammen.

Authentifizierungstyp

Der Typ der Authentifizierungsrichtlinie.

Anz. der Richtlinien

Die Anzahl der Richtlinien dieses Typs.

Verwendung

Die Nutzungsbeschreibung für diese Richtlinien.

Die Fenster Authentifizierungs- und Autorisierungs-Richtlinien

Die Fenster Anmeldung, Exec und Netzwerk-Autorisierung zeigen die Methodenliste an, die zur Authentifizierung von Anmeldungen und NAC-Anforderungen sowie zur Autorisierung der Exec-Befehlsebene und Netzwerk-Anforderungen verwendet werden. In diesen Fenstern können Sie diese Methodenliste prüfen und verwalten.

Hinzufügen, Bearbeiten und Löschen (Schaltflächen)

Verwenden Sie diese Schaltflächen, um Methodenlisten zu erstellen, zu bearbeiten oder zu entfernen.

Listenname

Der Methodenlistenname. Eine Methodenliste ist eine sequenzielle Liste, die die Authentifizierungsmethoden beschreibt, die abgefragt werden sollen, um einen Benutzer zu authentifizieren.

Methode 1

Die Methode, die der Router zuerst versucht. Wenn einer der Server in dieser Methode den Benutzer authentifiziert (eine PASS-Antwort sendet), dann ist die Authentifizierung erfolgreich. Wenn ein Server eine FAIL-Antwort zurücksendet, schlägt die Authentifizierung fehl. Wenn keine Server auf die erste Methode reagieren, dann verwendet der Router die nächste Methode auf der Liste. Methoden können geordnet werden, wenn Sie eine Methodenliste erstellen oder bearbeiten.

Methoden 2, 3 und 4

Die Methoden, die der Router zuerst verwendet, wenn die Server, auf die in Methode 1verwiesen wird, nicht antworten. Wenn es weniger als vier Methoden gibt, bleiben die Positionen, für die keine Liste konfiguriert wurden, leer.

Authentifizierungs-NAC

Das Fenster **Authentifizierungs-NAC** zeigt die auf dem Router konfigurierte EAPoUDP-Methodenliste an. Wenn der NAC-Assistent verwendet wurde, um eine NAC-Konfiguration auf dem Router zu erstellen, enthält dieses Fenster den folgenden Eintrag:

Listenname	Methode 1
Standard	Gruppe SDM_NAC_Group

Sie können zusätzliche Methodenlisten in diesem Fenster angeben, wenn der Router die Methoden probieren soll, die Sie eingeben, bevor er die Standardmethodenliste wiederherstellt.

Hinzufügen, Bearbeiten und Löschen (Schaltflächen)

Verwenden Sie diese Schaltflächen, um Methodenlisten zu erstellen, zu bearbeiten oder zu entfernen.

Liste Name Spalte

Der Methodenlistenname. Eine Methodenliste ist eine sequenzielle Liste, die die Authentifizierungsmethoden beschreibt, die abgefragt werden sollen, um einen Benutzer zu authentifizieren.

Spalte der 1. Methode

Die Methode, die der Router zuerst versucht. Wenn einer der Server in dieser Methode den Benutzer authentifiziert (eine PASS-Antwort sendet), dann ist die Authentifizierung erfolgreich. Wenn ein Server eine FAIL-Antwort zurücksendet, schlägt die Authentifizierung fehl. Wenn keine Server auf die erste Methode reagieren, dann verwendet der Router die nächste Methode auf der Liste. Methoden können geordnet werden, wenn Sie eine Methodenliste erstellen oder bearbeiten.

Spalten der 2., 3. und 4. Methoden

Die Methoden, die der Router zuerst verwendet, wenn die Server, auf die in Methode 1verwiesen wird, nicht antworten. Wenn es weniger als vier Methoden gibt, bleiben die Positionen, für die keine Liste konfiguriert wurden, leer.

Authentifizierungs-802.1x

Das Fenster **802.1x-Authentifizierung** zeigt die für die 802.1-Authentifizierung konfigurierten Methodenlisten an. Wenn der LAN-Assistent verwendet wurde, um eine 802.1x-Konfiguration auf dem Router zu erstellen, enthält dieses Fenster den folgenden Eintrag:

Listenname	Methode 1
Standard	group radius (Gruppen-Radius)

Hinweis Sie können keine zusätzlichen Methodenlisten für die 802.1x-Konfiguration angeben.

Hinzufügen, Bearbeiten und Löschen (Schaltflächen)

Verwenden Sie diese Schaltflächen, um Methodenlisten zu erstellen, zu bearbeiten oder zu entfernen.

Liste Name Spalte

Der Methodenlistenname. Eine Methodenliste ist eine sequenzielle Liste, die die Authentifizierungsmethoden beschreibt, die abgefragt werden sollen, um einen Benutzer zu authentifizieren.

Spalte der 1. Methode

Die Methode, die der Router zuerst versucht. Wenn einer der Server in dieser Methode den Benutzer authentifiziert (eine PASS-Antwort sendet), dann ist die Authentifizierung erfolgreich. Wenn ein Server eine FAIL-Antwort zurücksendet, schlägt die Authentifizierung fehl. Wenn keine Server auf die erste Methode reagieren, dann verwendet der Router die nächste Methode auf der Liste. Methoden können geordnet werden, wenn Sie eine Methodenliste erstellen oder bearbeiten.

Spalten der 2., 3. und 4. Methoden

Die Methoden, die der Router zuerst verwendet, wenn die Server, auf die in Methode 1verwiesen wird, nicht antworten. Wenn es weniger als vier Methoden gibt, bleiben die Positionen, für die keine Liste konfiguriert wurden, leer.

Eine Methodenliste zur Authentifikation oder Autorisation hinzufügen oder bearbeiten

Eine Methodenliste ist eine sequenzielle Liste, die die Authentifizierungsmethoden beschreibt, die abgefragt werden sollen, um einen Benutzer zu authentifizieren. Mit Methodenlisten können Sie ein oder mehrere Sicherheitsprotokolle für die Authentifizierung angeben. Auf diese Weise gewährleisten Sie ein Sicherungssystem für die Authentifizierung für den Fall, dass die erste Methode fehlschlägt.

Die Cisco IOS-Software verwendet die erste in der Liste aufgeführte Methode für die Authentifizierung von Benutzern. Wenn für diese Methode keine Antwort eingeht, verwendet die Cisco IOS-Software die nächste Authentifizierungsmethode, die in der Methodenliste aufgeführt ist. Dieser Prozess wird fortgesetzt, bis eine Kommunikation mit einer in der Liste aufgeführten Methode erfolgreich ist oder alle in der Methodenliste definierten Methoden ohne Erfolg versucht wurden.

Wichtig ist, dass die Cisco IOS-Software die Authentifizierung mit der nächsten in der Liste aufgeführten Authentifizierungsmethode nur versucht, wenn für die vorhergehende Methode keine Antwort eingeht. Wenn die Authentifizierung an einem Punkt in diesem Zyklus fehlschlägt (d. h., der Sicherheitsserver oder die lokale Benutzernamendatenbank sendet eine Antwort, in der der Benutzerzugriff verweigert wird), wird der Authentifizierungsprozess gestoppt, und es werden keine weiteren Authentifizierungsmethoden versucht.

Name/Angeben

Wählen Sie in der Liste **Name** den Namen **Standard**, oder wählen Sie **Benutzerdefiniert**, und geben Sie im Feld **Angeben** den Namen einer Methodenliste ein.

Methoden

Eine Methode ist eine konfigurierte Servergruppe. Es können bis zu vier Methoden angegeben und in der Liste in der Reihenfolge platziert werden, in der sie vom Router verwendet werden sollen. Der Router versucht die erste Methode in der Liste. Wenn auf die Authentifizierungsanforderung eine PASS- oder FAIL-Antwort eingeht, führt der Router keine weitere Abfrage durch. Wenn der Router mit der ersten Methode keine Antwort erhält, verwendet er die nächste Methode in der Liste und fährt bis zum Ende der Liste fort, bis er eine PASS- oder FAIL-Antwort erhält.

Hinzufügen

Klicken Sie auf diese Schaltfläche, um eine Methode zur Liste hinzuzufügen. Wenn es keine konfigurierten Servergruppen gibt, die hinzugefügt werden können, haben Sie im angezeigten Fenster die Möglichkeit, eine Servergruppe zu konfigurieren.

Löschen

Klicken Sie auf diese Schaltfläche, um eine Methode aus der Liste zu löschen.

Nach oben/Nach unten

Der Router versucht die Methoden in der Reihenfolge, in der sie in der Liste in diesem Fenster aufgeführt sind. Klicken Sie auf **Nach oben**, um eine Methode in der Liste nach oben zu verschieben. Klicken Sie auf **Nach unten**, um eine Methode in der Liste weiter nach unten zu verschieben.

Die Methode **keine** ist immer die letzte Methode in der Liste. Es kann keine andere Methode in der Liste unter diese Methode verschoben werden. Dies ist eine IOS-Beschränkung. IOS akzeptiert keinen Methodennamen, nachdem der Methodenname **keine** zu einer Methodenliste hinzugefügt wurde.

KAPITEL 33

Routerbereitstellung

Sie können Ihren Router über ein USB-Gerät bereitstellen, das direkt mit Ihrem Router verbunden ist, oder Sie verwenden Secure Device Provisioning (SDP). SDP ist nur dann in Cisco SDM verfügbar, wenn es von der IOS-Ausgabe Ihres Cisco-Servers unterstützt wird.

Secure Device Provisioning

Über dieses Fenster können Sie Secure Device Provisioning (SDP) verwenden, um Aufgaben wie die Registrierung Ihres Routers bei einem CA-Server oder das Konfigurieren Ihres Routers auszuführen. Klicken Sie auf die Schaltfläche **SDP starten**, um zur SDP-Webbrowser-Anwendung zu wechseln und den Vorgang abzuschließen.

Wenn Sie Zertifikate erwerben, zeigt Cisco SDM das Fenster **Zertifikate** an, in dem Sie die Zertifikate anzeigen können, die Sie von der CA erhalten haben.

Weitere Informationen zu den Voraussetzungen für die SDP-Registrierung finden Sie unter Tipps zur SDP-Fehlerbehebung.

Weitere Informationen zu SDP finden Sie unter folgendem Link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

Hinweis Wenn die Schaltfläche **SDP starten** nicht angezeigt wird, wird SDP von Ihrer Cisco IOS-Version nicht unterstützt. Wenn die Schaltfläche **SDP starten** deaktiviert ist, sind Sie nicht als Stammbenutzer, sondern nur als Benutzer mit Ansichtsrechten bei Cisco SDM angemeldet.

Routerbereitstellung über USB

Dieses Fenster teilt Ihnen mit, ob Cisco SDM ein USB-Token oder ein USB-Flash-Gerät auf Ihrem Router ermittelt hat. Sie können auf die Schaltfläche **Routerbereitstellung** klicken, um eine Konfigurationsdatei aus der Liste der USB-Token oder Flash-Speicher zu wählen.

Wenn Sie Ihren Router so bereitstellen möchten, wird die Konfigurationsdatei vom USB-Token oder USB-Flash mit der laufenden Konfigurationsdatei Ihres Routers zusammen geführt und es wird eine neue, aktuelle Konfigurationsdatei erstellt.

Routerbereitstellung über USB (Datei laden)

In diesem Fenster können Sie eine Konfigurationsdatei von einem USB-Token oder USB-Flash laden, das an Ihrem Router angeschlossen ist. Die Datei wird mit der aktuellen Konfigurationsdatei auf Ihrem Router gemischt, um eine neue, aktuelle Konfigurationsdatei zu erstellen.

Um eine Konfigurationsdatei zu laden, führen Sie diese Schritte aus:

Schritt 1 Wählen Sie die Geräteart aus dem Dropdown-Menü.

Schritt 2 Geben Sie für den Dateinamen den Namen der Konfigurationsdatei mit dem vollständigen Pfad ein, oder klicken Sie auf **Durchsuchen**, und wählen Sie die Datei aus dem Dateiauswahlfenster aus.

Schritt 3 Wenn die Geräteart ein USB-Token ist, geben Sie in Token-PIN das Kennwort ein, um sich beim Token anzumelden.

Schritt 4 Wenn Sie eine Vorschau der Datei anzeigen möchten, klicken Sie auf **Dateivorschau**, um den Inhalt der Datei im Detailbereich anzuzeigen.

Schritt 5 Klicken Sie auf **OK**, um die gewünschte Datei zu laden.

Tipps zur SDP-Fehlerbehebung

Beachten Sie diese Informationen, bevor Sie eine Registrierung mit Secure Device Provisioning (SDP) durchführen, um die Verbindung zwischen dem Router und dem Zertifizierungsserver vorzubereiten. Wenn bei der Registrierung Probleme auftreten, können Sie diese Aufgaben überprüfen, um zu ermitteln, wo das Problem liegt.

Richtlinien

- Wenn SDP gestartet wurde, müssen Sie das Browserfenster, das dieses Hilfethema anzeigt, minimieren, um die Webanwendung SDP anzeigen zu können.
- Wenn der Router für die Verwendung von SDP konfiguriert werden soll, sollten Sie diese Konfiguration sofort nach der Konfiguration der WAN-Verbindung vornehmen.
- Wenn Sie die Konfigurationsänderungen in SDP abschließen, müssen Sie zu Cisco SDM zurückkehren und in der Symbolleiste auf **Aktualisieren** klicken, um den Status des Trustpoint im Fenster **Router-Zertifikate** in der Baumstruktur **VPN-Komponenten** anzuzeigen.

Tipps zur Fehlerbehebung

Diese Empfehlungen beziehen sich auf die vorbereitenden Schritte für den lokalen Router und den CA-Server. Sie müssen diese Anforderungen an den Administrator des CA-Servers weitergeben. Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Der lokale Router und der CA-Server sind über eine IP-Verbindung miteinander verbunden. Der lokale Router muss einen erfolgreichen Ping-Vorgang an den Zertifizierungsserver ausführen können, und der Zertifizierungsserver muss einen erfolgreichen Ping-Vorgang an den lokalen Router ausführen können.
- Der CA-Serveradministrator verwendet einen Browser, der JavaScript unterstützt.
- Der CA-Serveradministrator verfügt über Aktivierungsberechtigungen im lokalen Router.

- Die Firewall im lokalen Router lässt Datenverkehr an den und vom Zertifizierungsserver zu.
- Wenn eine Firewall beim Antragsteller und/oder der Registrierungsstelle konfiguriert ist, müssen Sie sicherstellen, dass die Firewall HTTP- oder HTTPS-Datenverkehr vom PC aus zulässt, von dem aus die Cisco SDM-/SDP-Anwendung aufgerufen werden.

Weitere Informationen zu SDP erhalten Sie auf folgender Webseite:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

KAPITEL 34

Cisco Common Classification Policy Language

Cisco Common Classification Policy Language (C3PL) ist ein strukturierter Platzhalter für funktionsspezifische Konfigurationsbefehle. C3PL ermöglicht Ihnen, Datenverkehrsrichtlinien auf der Basis von Ereignissen, Bedingungen und Aktionen zu erstellen. Der SDM verwendet C3PL, um die Richtlinienzuordnungen und Klassenzuordnungen zu erstellen, die in den folgenden Hilfe-Themen beschrieben werden.

Richtlinienzuordnung

Richtlinienzuordnungen geben die Aktionen an, die durchgeführt werden, wenn der Datenverkehr bestimmten definierten Kriterien entspricht. Datenverkehrstypen und Kriterien werden in Klassenzuordnungen definiert, die mit einer Richtlinienzuordnung verknüpft sind. Damit ein Router die Informationen in einer Richtlinienzuordnung und den verbundenen Klassenzuordnungen nutzen kann, muss die Richtlinienzuordnung mit einem Zonenpaar verknüpft sein. Weitere Informationen zur Konfiguration von Zonen und Zonenpaaren finden Sie unter Zonenbasierte Richtlinienfirewall (Zone-Based Policy Firewall).

Richtlinienzuordnungsfenster

Verwenden Sie die Richtlinienzuordnungsfenster, um Richtlinienzuordnungen für QoS, HTTP und andere Datenverkehrstypen zu prüfen, erstellen und bearbeiten. Der obere Teil des Fensters führt die konfigurierten Richtlinienzuordnungen auf, der untere Teil zeigt die Details der markierten Richtlinienzuordnung an. Wenn Sie eine Richtlinienzuordnung bearbeiten müssen oder mehr Details sehen möchten, klicken Sie auf **Bearbeiten**, um ein Dialogfeld anzuzeigen, in dem Sie die Informationen anzeigen und Änderungen vornehmen können.

In diesem Hilfe-Thema finden Sie eine allgemeine Beschreibung der Richtlinienzuordnungsfenster sowie einige Beispieldaten.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um ein Dialogfeld anzuzeigen, in dem Sie eine Richtlinienzuordnung konfigurieren können.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um ein Dialogfeld anzuzeigen, in dem Sie die ausgewählte Richtlinienzuordnung bearbeiten können. Die Schaltfläche **Bearbeiten** ist deaktiviert, wenn keine Richtlinienzuordnungen konfiguriert wurden.

Löschen

Klicken Sie auf **Löschen**, um die ausgewählte Richtlinienzuordnung zu entfernen.

Richtlinienzuordnungslistenbereich

Dieser Bereich listet die Richtlinienzuordnungen auf, die für das jeweilige Protokoll oder die Funktion konfiguriert sind. Wählen Sie eine Richtlinienzuordnung aus, um im unteren Teil des Bildschirms Details anzuzeigen. Das folgende Beispiel zeigt zwei IM-Richtlinien.

Richtlinienzuordnungsname	Beschreibung
im-pmap-g	Gastrichtlinie
im-pmap-e	Mitarbeiterrichtlinie

Details zur Richtlinienzuordnung

Die Details der ausgewählten Richtlinienzuordnung zeigen die Richtlinienzuordnungskonfiguration. Die angezeigten Details variieren je nach Richtlinienzuordnungstyp.

HTTP, IM, P2P, IMAP und POP3 zeigen die Spalten **Klassenname für Übereinstimmung**, **Aktion** und **Protokoll** an. Die folgende Tabelle zeigt Details zu einer IM-Richtlinienzuordnung an Der Router sperrt AOL-Datenverkehr, lässt jedoch alle anderen IM-Datenverkehrstypen zu.

Klassenname für Übereinstimmung	Aktion	Protokoll
aol-cmap	Deaktiviert	Deaktiviert
class-default	Aktiviert	Deaktiviert

Protokollprüfung, SMTP und SUNRPC-Richtlinienzuordnungsdetails umfassen die Spalten **Klassenname für Übereinstimmung** und **Aktion**. Die folgende Tabelle zeigt Details zu einer SUNRPC-Richtlinienzuordnung.

Klassenname für Übereinstimmung	Aktion
cmap-sunrpc1	Zulassen
cmap-sunrpc2	Keine

Hinzufügen oder Bearbeiten einer Richtlinienzuordnung

Verwenden Sie diese Informationen, um eine QoS-Richtlinienzuordnung hinzuzufügen oder zu bearbeiten.

Richtlinienname und Beschreibung

Wenn Sie eine neue Richtlinienzuordnung erstellen, geben Sie dafür in diesen Feldern einen Namen und eine Beschreibung ein. Wenn Sie eine Richtlinienzuordnung bearbeiten, sind diese Felder schreibgeschützt.

Spalten „Klassenzuordnung“, „Warteschlangenfunktion“, „DSCP festlegen“ und „Entfernen“

Diese Spalten fassen die Informationen zu jeder Klassenzuordnung in der Richtlinienzuordnung zusammen. Der folgende Beispieleintrag ist für eine Sprachklassenzuordnung:

```
Voice-FastEthernet0/1  LLQ 70%    ef          No
```

Diese Klassenzuordnung verwendet Low Latency Queuing und 70 % der Bandbreite für diese Schnittstelle. Der DSCP-Wert ist auf „ef“ eingestellt, und Pakete dieses Typs werden nicht entfernt.

Mit den Schaltflächen **Hinzufügen**, **Bearbeiten**, **Löschen**, **Nach oben** und **Nach unten** können die Klassenzuordnungsinformationen in der Liste geändert werden.

Hinzufügen einer Prüfrichtlinienzuordnung

Prüfrichtlinienzuordnungen geben die Aktion an, die vom Router auf Datenverkehr angewandt werden soll, der den Kriterien in den verknüpften Klassenrichtlinien entspricht. Der Router kann den Datenverkehr passieren lassen, entfernen und optional das Ereignis protokollieren oder den Datenverkehr prüfen.

Der eingegebene Name und die Beschreibung werden im Fenster **Prüfrichtlinienzuordnungen** angezeigt. Die Spalten **Klassenzuordnung** und **Aktion** zeigen die mit dieser Richtlinienzuordnung verknüpften Klassenzuordnungen an, sowie die Aktion, die der Router auf den Datenverkehr anwenden soll, der von der Klassenzuordnung beschrieben wird. Klicken Sie auf **Hinzufügen**, um eine neue Klassenzuordnung hinzuzufügen und die Aktion zu konfigurieren. Klicken Sie auf **Bearbeiten**, um die Einstellungen für eine Klassenzuordnung zu ändern. Verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Reihenfolge zu ändern, in der die Klassenzuordnungen bewertet werden.

Richtlinienzuordnung für Layer 7

In diesem Fenster können Sie eine Richtlinienzuordnung für Layer 7 auswählen, die zur Prüfung einer ausgewählten Anwendung verwendet werden soll. Das Fenster zeigt die Richtlinienzuordnungen an, die für diese Anwendung zur Verfügung stehen. Wählen Sie eine Richtlinienzuordnung, und klicken Sie auf **OK**.

Anwendungsprüfung

Anwendungsprüfrichtlinien werden auf Layer 7 des OSI-Modells angewandt, auf der die Anwendungen Nachrichten senden und empfangen, die es den Anwendungen ermöglichen, nützliche Funktionen zu bieten. Manche Anwendungen können unerwünschte oder anfällige Funktionen bieten, sodass die mit diesen Funktionen verknüpften Nachrichten gefiltert werden müssen, um Aktivitäten der Anwendungsdienste einzuschränken.

Die Cisco IOS Software Zone-Policy Firewall bietet eine Anwendungsprüfung und -kontrolle für die folgenden Anwendungsdienste: HTTP-, SMTP-, POP3-, IMAP-, SUNRPC-, P2P- und IMAP-Anwendungen. Weitere Informationen finden Sie unter den folgenden Links:

- Hinzufügen einer HTTP-Prüfklassenzuordnung
- Hinzufügen oder Bearbeiten einer SMTP-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer POP3-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer IMAP-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer SUNRPC-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer Punkt-zu-Punkt-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer Instant Messaging-Klassenzuordnung

Konfigurieren von Deep Packet Inspection

Die (Anwendungs-) Prüfung für Layer 7 erweitert die Prüfung für Layer 4 um die Funktion, dienstspezifische Aktionen erkennen und anwenden zu können, wie beispielsweise selektives Sperren oder Zulassen der Funktionen file-search, file-transfer und text-chat. Die dienstspezifischen Funktionen sind je nach Dienst unterschiedlich.

Wenn Sie eine neue Richtlinienzuordnung erstellen, geben Sie einen Namen in das Feld **Richtlinienzuordnungsname** ein. Sie können auch eine Beschreibung hinzufügen. Klicken Sie auf **Hinzufügen > Neue Klassenzuordnung**, um eine neue Punkt-zu-Punkt-Klassenzuordnung zu erstellen. Hinzufügen oder Bearbeiten einer Punkt-zu-Punkt-Klassenzuordnung enthält Informationen darüber, wie dieser Klassenzuordnungstyp erstellt wird. Klicken Sie auf **Hinzufügen > Klassenstandard**, um die Standard-Klassenzuordnung hinzuzufügen.

Wenn die Klassenzuordnung in der Tabelle angezeigt wird, geben Sie die Aktion an, die ausgeführt werden soll, wenn eine Übereinstimmung gefunden wird, und ob die Übereinstimmung protokolliert werden sollen. Sie können **<Keine>**, **Zurücksetzen** oder **Zulassen** angeben. Im folgenden Beispiel gibt es P2P Klassenzuordnungen für Gnutella und eDonkey.

Klassenname für Übereinstimmung	Aktion	Protokoll
gnutellaCMap	Zulassen	
eDonkeyCMap	Zurücksetzen	X

Klassenzuordnungen

Klassenzuordnungen definieren den Datenverkehr, der von einer Zone-Policy Based Firewall (ZPF) für die Richtlinienanwendung ausgewählt wird. Klassenzuordnungen für Layer 4 sortieren den Datenverkehr auf der Basis der folgenden Kriterien:

- Zugriffsgruppe – Eine standardmäßige, erweiterte oder benannte Zugriffssteuerungsliste (ACL) kann den Datenverkehr auf der Basis von Quell- und Ziel-IP-Adresse sowie Quell- und Ziel-Port filtern.
- Protokoll – Die Protokolle für Layer 4 (TCP, UDP und ICMP) sind Anwendungsdienste wie HTTP, SMTP, DNS usw. Jeder dem PAM bekannte oder benutzerdefinierte Dienst kann angegeben werden.
- Klassenzuordnung – Eine untergeordnete Klassenzuordnung, die zusätzliche Kriterien liefert, kann in einer anderen Klassenzuordnung verschachtelt werden.
- Nicht – Das Kriterium **Nicht** gibt an, dass sämtlicher Datenverkehr, der nicht einem angegebenen Dienst (Protokoll), einer Zugriffsgruppe oder untergeordneten Klassenzuordnung entspricht, für die Klassenzuordnung ausgewählt wird.

Klassenzuordnungen können „match-any“- oder „match-all“-Operatoren anwenden, um zu ermitteln, wie die übereinstimmenden Kriterien angewandt werden sollen. Wenn „match-any“ angegeben ist, muss der Datenverkehr nur eines der übereinstimmenden Kriterien in der Klassenzuordnung erfüllen. Wenn „match-all“ angegeben ist, muss der Datenverkehr alle Kriterien der Klassenzuordnung erfüllen, die zu der Klasse gehören.

Verknüpfen einer Klassenzuordnung

Um eine Klassenzuordnung mit einer Prüfrichtlinienzuordnung zu verknüpfen, führen Sie die folgenden Aufgaben aus.

Schritt 1 Geben Sie einen Klassenzuordnungsnamen an, indem Sie auf die Schaltfläche rechts neben dem Namensfeld klicken, und wählen Sie **Klassenzuordnung hinzufügen**, **Klassenzuordnung auswählen** oder **class-default** aus.

Schritt 2 Klicken Sie im Feld **Aktion** entweder auf **Passieren**, **Entfernen** oder **Prüfen**. Wenn Sie auf **Entfernen** klicken, können Sie optional auf **Protokollieren** klicken, um das Ereignis über das Entfernen zu protokollieren. Wenn Sie auf **Prüfen** klicken, klicken Sie auf **Erweiterte Optionen**, um die Parameterzuordnungen, Prüfrichtlinien oder Richtlinien anzugeben, die Sie für Datenverkehr in dieser Klasse wünschen.

Schritt 3 Klicken Sie auf **OK**, um das Dialogfeld zu schließen und zum Dialogfeld **Richtlinienzuordnung hinzufügen oder bearbeiten** zurückzukehren.

Klassenzuordnung – Erweiterte Optionen

Wenn Sie die Prüfaktion für den Datenverkehr auswählen, können Sie Parameterzuordnungen, Anwendungsprüfung und ZPF-Richtlinien angeben.

Parameterzuordnung für Prüfung

Parameterzuordnungen für die Prüfung geben TCP-, DNS- und UDP-Timeouts sowie Sitzungssteuerungsparameter an. Sie können eine vorhandene Parameterzuordnung auswählen. Wenn keine Parameterzuordnung konfiguriert wurde, ist das Feld deaktiviert. Klicken Sie auf **Ansicht**, um die ausgewählte Parameterzuordnung anzuzeigen, ohne dieses Dialogfeld zu verlassen.

Parameterzuordnung für URL-Filterung

Parameterzuordnungen für die URL-Filterung können URL-Filterserver und lokale URL-Listen angeben. Sie können eine vorhandene Parameterzuordnung auswählen. Wenn keine Parameterzuordnung konfiguriert wurde, ist das Feld deaktiviert. Klicken Sie auf **Ansicht**, um die ausgewählte Parameterzuordnung anzuzeigen, ohne dieses Dialogfeld zu verlassen.

Aktivieren der Anwendungsprüfung

Eine Anwendungsrichtlinie gibt die zu prüfenden Datentypen in Paketen einer bestimmten Anwendung an. Sie können eine vorhandene Anwendungsprüfrichtlinie auswählen. Wenn keine Anwendungsprüfrichtlinie konfiguriert wurde, ist das Feld deaktiviert. Klicken Sie auf **Ansicht**, um die ausgewählte Anwendungsprüfrichtlinie anzuzeigen, ohne dieses Dialogfeld zu verlassen.

Überwachungsrate und Burst

Sie können den Datenverkehr auf eine bestimmte Rate beschränken und einen Burst-Wert angeben. Die Überwachungsrate kann einen Wert zwischen 8.000 und 2.000.000.000 Bit pro Sekunde haben. Die Burst-Rate kann einen Wert zwischen 1.000 und 512.000.000 Byte haben.

QoS-Klassenzuordnung

Verwenden Sie dieses Fenster, um Informationen zu QoS-Klassenzuordnungen anzuzeigen und zu bearbeiten. QoS-Klassenzuordnungen werden in QoS-Richtlinienzuordnungen verwendet, um Datenverkehrstypen zu definieren.

Klicken Sie auf einen Klassenzuordnungsnamen, um Details zur Klassenzuordnung unter **Details des Bereichs Klassenzuordnung** anzuzeigen.

Die Details einer Klassenzuordnung zeigen, welche Protokolle abgeglichen werden, um den Datenverkehr zu definieren. Das folgende Beispiel zeigt Details zu einer Sprachsignalisierungsklassenzuordnung.

```
Details zur Klassenzuordnung SDMSignal-FastEthernet0/1

    Elementname                    Elementwert
Protokolle abgleichen              h323,rtcp
```

H.323 und RTCP sind die Sprachsignalisierungsprotokolle, die abgeglichen werden.

Hinzufügen oder Bearbeiten einer QoS-Klassenzuordnung

Verwenden Sie diese Informationen, um eine QoS-Klassenzuordnung hinzuzufügen oder zu bearbeiten. Wenn Sie eine neue QoS-Klassenzuordnung hinzufügen, klicken Sie auf die Schaltfläche rechts neben dem Feld und wählen entweder **Klassenzuordnung hinzufügen** oder **Klassenzuordnung auswählen** aus dem angezeigten Kontextmenü.

Lesen Sie auch die Informationen in Aktion, um mehr über die Optionen **Entfernen**, **DSCP festlegen** und **Warteschleifenfunktion** zu erfahren.

Hinzufügen oder Bearbeiten einer QoS-Klassenzuordnung

Geben Sie einen Namen und eine Beschreibung für die QoS-Klassenzuordnung ein, die Sie erstellen, damit sie leicht identifiziert und verwendet werden kann. Klicken Sie auf Klassifizierung, um eine Beschreibung der Schaltflächen **Beliebige**, **Alle** und **Bearbeiten** im Feld **Klassifizierung** zu erhalten.

Auswahl einer Klassenzuordnung

Klicken Sie auf den Namen einer Klassenzuordnung, die Sie auswählen möchten, und klicken Sie anschließend auf **OK**. Der Klassenzuordnungseintrag wird in dem Fenster hinzugefügt, über das Sie dieses Dialogfeld aufgerufen haben.

Deep Inspection

Mit der Deep Inspection können Sie Klassenzuordnungen für Parameter einer Anwendung erstellen. So können Sie beispielsweise Klassenzuordnungen für allgemeine P2P-Anwendungen wie beispielsweise eDonkey, Gnutella und Kazaa2 erstellen.

Fenster „Klassenzuordnung“ und „Dienstgruppe“

Verwenden Sie die Klassenzuordnungsfenster, um Klassenzuordnungen für Protokolle wie HTTP, SMTP und POP3 zu überprüfen, erstellen und bearbeiten. Der Bereich **Klassenzuordnung** des Fensters führt die konfigurierten Klassenzuordnungen auf, und der untere Teil zeigt die Details der ausgewählten Klassenzuordnung an. Wenn Sie eine Klassenzuordnung bearbeiten müssen oder mehr Details sehen möchten, klicken Sie auf **Bearbeiten**, um ein Dialogfeld anzuzeigen, in dem Sie die Informationen anzeigen und Änderungen vornehmen können.

Hinzufügen

Klicken Sie auf **Hinzufügen**, um eine neue Klassenzuordnung des ausgewählten Typs zu erstellen und die Konfiguration in das angezeigte Dialogfeld einzugeben.

Bearbeiten

Klicken Sie auf **Bearbeiten**, um die Konfiguration der ausgewählten Klassenzuordnung zu ändern.

Löschen

Klicken Sie auf **Löschen**, um die ausgewählte Klassenzuordnung zu entfernen. Cisco SDM kann Dialogfeld anzeigen, wenn mit dieser Konfiguration Abhängigkeiten verknüpft sind, wie beispielsweise untergeordnete Klassenzuordnungen oder Parameterzuordnungen, die von anderen Klassenzuordnungen verwendet werden könnten.

Klassenzuordnungsbereich

Dieser Bereich zeigt die Klassenzuordnungen an, die für das ausgewählte Protokoll konfiguriert sind. Er enthält die Namen der konfigurierten Klassenzuordnungen und andere relevante Informationen.

QoS-Klassenzuordnungen

QoS-Klassenzuordnungen werden in einer Tabelle mit den Spalten **Klassenzuordnungsname** und **Beschreibung** angezeigt. Es folgt eine Beispieltabelle.

Klassenzuordnungsname	Beschreibung
CMAP-DMZ	FTP- und HTTP-QoS-Klassenzuordnung
CMAP-3	Test

Prüf-, HTTP-, SMTP-, SUN RPC-, IMAP- und POP3-Klassenzuordnungen

Diese Klassenzuordnungstypen verfügen über die Spalten **Klassenzuordnungsname** und **Verwendet von**. Es folgt eine Beispieltabelle für HTTP.

Klassenzuordnungsname	Verwendet von
http-rqst	pmap-5
http-rsp-body	pmap-5

Instant Messaging-Dienstgruppen und Peer-zu-Peer-Anwendungsdienstgruppen

Instant Messaging-Servicegruppen und Peer-zu-Peer (P2P)-Anwendungsdienstgruppen verfügen über eine zusätzliche Spalte, da Klassenzuordnungen für eine bestimmte Anwendung, wie z. B. die Instant Messaging-Anwendung Yahoo! Messenger oder die Gnutella P2P-Anwendung, konfiguriert werden. Die folgende Tabelle zeigt Beispieldaten für P2P-Anwendungsdienstgruppen.

Klassenzuordnungsname	Verwendet von	Klassenzuordnungstyp
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

Details zur Klassenzuordnung

Die Details des Klassenzuordnungsbereichs zeigen die Konfiguration einer bestimmen Klassenzuordnung. Es gibt die Spalten **Elementname** und **Elementwert**.

Elementname

Der Name der Konfigurationseinstellung. Eine HTTP-Klasse kann beispielsweise Einstellungen für Anforderungs-Header, Port-Missbrauch und Protokollverletzung haben.

Elementwert

Der Wert der Konfigurationseinstellung. Der Wert für die Einstellung HTTP-Anforderungs-Header kann beispielsweise **Länge > 500** lauten und die Port-Missbrauch-Markierung kann deaktiviert sein.

Weitere Informationen zu Klassenzuordnungsdetails

Für weitere Informationen zu den in diesen Fenstern angezeigten Klassenzuordnungsdetails klicken Sie auf einen der folgenden Links:

- Hinzufügen oder Bearbeiten einer QoS-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer Prüfklassenzuordnung
- Hinzufügen einer HTTP-Prüfklassenzuordnung

- Hinzufügen oder Bearbeiten einer Instant Messaging-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer Punkt-zu-Punkt-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer SMTP-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer SUNRPC-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer IMAP-Klassenzuordnung
- Hinzufügen oder Bearbeiten einer POP3-Klassenzuordnung

Hinzufügen oder Bearbeiten einer Prüfklassenzuordnung

Durch das Erstellen einer Prüfklassenzuordnung können Sie eine ganze Reihe von Datenverkehr für die Prüfung verfügbar machen. Geben Sie einen Namen in das Feld **Klassenname** ein, um diese Klassenzuordnung zu identifizieren. Sie können auch eine Beschreibung eingeben. Wenn Sie eine Klassenzuordnung bearbeiten, können Sie den Namen nicht ändern. Wenn Sie die Bedingungen angegeben haben, die die Klasse zuordnen soll, klicken Sie auf **OK**.

Geben Sie an, ob die Klasse einigen oder allen Bedingungen entsprechen soll.

Klicken Sie auf **Beliebige**, wenn die Klasse nur einer oder manchen der gewählten Bedingungen entsprechen muss. Klicken Sie auf **Alle**, wenn die Klasse allen Bedingungen entsprechen muss.

Auswählen, womit die Prüfklassenzuordnung übereinstimmen muss

Wählen Sie, womit die Klassenzuordnung in der linken Spalte übereinstimmen muss. Klicken Sie auf das Plus-Zeichen (+) neben einem Knoten, um die untergeordneten Knoten anzuzeigen. Klicken Sie z. B. auf **HTTP**, um die untergeordneten Knoten http und https anzuzeigen. Um ein Element auszuwählen, klicken Sie auf das Element und anschließend auf **Hinzufügen>>**. Um ein Element zu entfernen, das Sie zur Spalte auf der rechten Seite hinzugefügt haben, klicken Sie auf das Element und anschließend auf **<<Entfernen**.

Ändern der Übereinstimmungsreihenfolge

Wenn Sie entscheiden, dass eine der Bedingungen erfüllt sein muss, möchten Sie möglicherweise die Übereinstimmungsreihenfolge der Elemente in der rechten Spalte ändern. Um ein Element in der Liste nach oben zu verschieben, klicken Sie auf das Element und anschließend auf **Nach oben**. Um ein Element in der Liste nach unten zu verschieben, klicken Sie auf das Element und anschließend auf **Nach unten**. Die Schaltfläche **Nach oben** ist deaktiviert, wenn Sie auf das Element ganz oben in der Liste klicken. Die Schaltfläche **Nach unten** ist deaktiviert, wenn Sie auf das Element ganz unten in der Liste klicken.

Verknüpfen der Parameterzuordnung

Dieses Dialogfeld zeigt die Parameterzuordnungen an, die Sie mit dieser Klassenzuordnung verknüpfen können. Klicken Sie auf das Kontrollkästchen **Auswählen** neben der Parameterzuordnung, die Sie mit der Klassenzuordnung verknüpfen möchten.

Hinzufügen einer HTTP-Prüfklassenzuordnung

HTTP-Prüfklassenzuordnungen ermöglichen es Ihnen, eine ganze Reihe von HTTP-Anforderungsdaten, Antwortdaten und Anforderung-Antwort-Daten für die Prüfung verfügbar zu machen.

Gehen Sie wie folgt vor, um eine HTTP-Prüfklassenzuordnung zu erstellen:

Schritt 1 Geben Sie einen Klassennamen ein, um die Klassenzuordnung zu identifizieren. Sie können auch eine Beschreibung eingeben, die im HTTP-Klassenzuordnungsfenster angezeigt wird.

Schritt 2 Klicken Sie auf den Zweig im HTTP-Baum, der den Datentyp enthält, den Sie für die Prüfung verfügbar machen möchten. Sie können eine Klassenzuordnung für HTTP-Anforderungen, Antworten und Anforderung-Antworten erstellen.

Schritt 3 Klicken Sie auf den entsprechenden Unterzweig, um den einzubeziehenden Datentyp weiter zu spezifizieren.

Schritt 4 Konfigurieren Sie in den angezeigten Feldern die Klassenzuordnungsdaten.

Schritt 5 Geben Sie die Bedingungen für die Übereinstimmung an, indem Sie auf **Beliebige der nachfolgenden Bedingungen** klicken, wenn die Klassenzuordnung nur einer oder einigen der Bedingungen entsprechen muss. Klicken Sie auf **Alle der nachfolgend angegebenen Bedingungen**, wenn die Klassenzuordnung allen angegebenen Bedingungen entsprechen muss.

HTTP-Anforderungs-Header

Geben Sie Klassenzuordnungskriterien für HTTP-Anforderungs-Header-Attribute ein.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine globale Anforderungs-Header-Länge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Beschränkung für die Gesamtzahl der Anforderungs-Header-Felder angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Felder ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Feldname und Konfigurationsoptionen

Sie können Felder im Header in die Prüfkriterien einbeziehen und die zu prüfende Länge, Zahl und Zeichenfolgen angeben. Klicken Sie auf **Hinzufügen**, um ein Feld einzubeziehen, und geben Sie im angezeigten Dialogfeld die Kriterien ein.

Felder für HTTP-Anforderungs-Header

Wählen Sie den Header-Feldtyp aus der Liste aus, und geben Sie die Prüfkriterien dafür an.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Länge angeben möchten, die dieses Feld nicht überschreiten sollte, und geben Sie die Zahl der Byte ein. Sie können beispielsweise eine Anforderung sperren, deren Cookie-Feld 256 Byte überschreitet oder deren Benutzeragent-Feld 128 Byte überschreitet.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie angeben möchten, wie oft dieses Feld im Header wiederholt werden kann, und geben eine Zahl ein. Sie können beispielsweise eine Anforderung sperren, die mehrere Inhaltslängen-Header-Zeilen hat, indem Sie den Wert 1 eingeben. Dieses Beispiel ist eine effektive Maßnahme gegen Sitzungsschmuggel.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Feld „Übereinstimmung“

Aktivieren Sie dieses Kontrollkästchen, wenn die Klassenzuordnung mit dem gewählten Feldtyp übereinstimmen soll.

Andere Felder in diesem Dialogfeld

Je nachdem, welches HTTP-Header-Feld Sie wählen, können in diesem Dialogfeld weitere Felder angezeigt werden, über die Sie zusätzliche Kriterien festlegen können. Wenn Sie beispielsweise das Feld **Inhaltstyp** wählen, können Sie eine Prüfung auf nicht übereinstimmende Inhaltstypen zwischen Anforderung und Antwort, auf unbekannte Inhaltstypen sowie Protokollverletzungen des Inhaltstyps durchführen. Wenn Sie das Feld **transfer-encoding** wählen, können Sie eine Prüfung auf verschiedene Komprimierungs- und Codierungstypen durchführen.

HTTP-Anforderungsinhalt

Sie können einen HTTP-Anforderungsinhalt auf Länge und Zeichenfolgen prüfen.

Länge

Aktivieren Sie dieses Kontrollkästchen und wählen Sie **Größer als (>)**, um die obere Grenze für die Länge des Anforderungsinhalts anzugeben. Wählen Sie **Kleiner als (<)**, um eine untere Grenze anzugeben.

Reguläre Ausdrücke

Wenn Sie eine Prüfung auf Zeichenfolgen durchführen möchten, klicken Sie auf dieses Kontrollkästchen und wählen einen vorhandenen regulären Ausdruck für eine Klassenzuordnung aus. Sie können auch einen neuen regulären Ausdruck für eine Klassenzuordnung erstellen, der den Zeichenfolgen entspricht, für die Sie eine Prüfung durchführen. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen aus** und klicken auf **Ansicht**.

Argumente für HTTP-Anforderungs-Header

Sie können die Länge der in einer Anforderung gesendeten Argumente prüfen und eine Prüfung auf Zeichenfolgen durchführen, die von Ihnen konfigurierten regulären Ausdrücken entsprechen.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen und geben Sie die Zahl der Byte an, die die Gesamtlänge der Anforderungs-Header-Argumente nicht überschreiten sollte.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

HTTP-Methode

HTTP-Methoden geben den Zweck einer HTTP-Anforderung an. Wählen Sie die zu prüfenden HTTP-Methoden in der Spalte **Methodenliste** aus, und aktivieren Sie das Kontrollkästchen **Auswählen** neben der Methode.

Port-Missbrauch anfordern

Der HTTP-Port 80 wird manchmal von IM, P2P, Tunnelling und anderen Anwendungen verwendet. Aktivieren Sie die Port-Missbrauch-Typen, auf die Sie prüfen möchten. Sie können eine Prüfung für jeden Port-Missbrauch-Typ durchführen, Port-Missbrauch durch IM-Anwendungen, P2P-Anwendungs-Port-Missbrauch und Missbrauch durch Tunneling-Anwendungen.

URI-Anforderung

Geben Sie die Universal Resource Identifier (URI)-Kriterien ein, die Sie in die Klassenzuordnung aufnehmen möchten.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine URI-Länge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Anwendungsbeispiel

Konfigurieren Sie eine HTTP-Klassenzuordnung, die eine Anforderung sperrt, deren URI einem der folgenden regulären Ausdrücke entspricht:

„.*cmd.exe“

„.*sex“

„.*gambling“

Antwort-Header

Geben Sie die Kriterien für HTTP-Antwort-Header ein, die Sie in die Klassenzuordnung aufnehmen möchten.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine globale Antwort-Header-Länge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Beschränkung für die Gesamtzahl der Antwort-Header-Felder angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Felder ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Antwort-Header-Felder

Wählen Sie den Header-Feldtyp aus der Liste aus, und geben Sie die Prüfkriterien dafür an.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Feldlänge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Beschränkung für die Gesamtzahl der Felder dieses Typs angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Anzahl der Felder ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Andere Felder in diesem Dialogfeld

Je nachdem, welches HTTP-Header-Feld Sie wählen, können in diesem Dialogfeld weitere Felder angezeigt werden, über die Sie zusätzliche Kriterien festlegen können. Wenn Sie beispielsweise das Feld **Inhaltstyp** wählen, können Sie eine Prüfung auf nicht übereinstimmende Inhaltstypen zwischen Anforderung und Antwort, auf unbekannte Inhaltstypen sowie Protokollverletzungen des Inhaltstyps durchführen. Wenn Sie das Feld **transfer-encoding** wählen, können Sie eine Prüfung auf verschiedene Komprimierungs- und Codierungstypen durchführen.

Feld „Übereinstimmung“

Aktivieren Sie dieses Kontrollkästchen, wenn die Klassenzuordnung mit dem gewählten Feldtyp übereinstimmen soll.

HTTP-Antwortinhalt

Geben Sie die Kriterien für den HTTP-Antwortinhalt ein, auf die geprüft werden soll.

Java Applets in HTTP-Antwort

Aktivieren Sie dieses Kontrollkästchen, wenn Sie die HTTP-Antwort auf Java Applets prüfen möchten. Abhängig von den in der Richtlinienzuordnung konfigurierten Aktionen

Länge

Aktivieren Sie dieses Kontrollkästchen und wählen Sie **Größer als (>)**, um die obere Grenze für die Länge des Antwortinhalts anzugeben. Wählen Sie **Kleiner als (<)**, um eine untere Grenze anzugeben.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

HTTP-Antwort + Statuszeile

Aktivieren Sie dieses Kontrollkästchen und geben Sie reguläre Ausdrücke an, die mit Antwort-Statuszeilen verglichen werden sollen. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird.

Anwendungsbeispiel

Konfigurieren Sie den Router so, dass er einen Alarm protokolliert, wenn versucht wird, auf eine verbotene Seite zuzugreifen. Eine verbotene Seite enthält in der Regel den Statuscode 403, und die Statuszeile sieht aus wie „HTTP/1.0 403 page forbidden\r\n.“

Der reguläre Ausdruck hierfür ist der folgende:

```
[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403
```

Die Protokollierung ist in der Richtlinienzuordnung angegeben, mit der die HTTP-Klassenzuordnung verknüpft ist.

Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Anforderungs-/Antwort-Header-Kriterien

Geben Sie Klassenzuordnungskriterien für die HTTP-Anforderungs-/Antwort-Header ein.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine globale Anforderungs-/Antwort-Header-Länge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Beschränkung für die Gesamtzahl der Anforderungs-/Antwort-Header-Felder angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Felder ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Felder für HTTP-Anforderungs-/Antwort-Header

Wählen Sie das HTTP-Anforderungs-/Antwort-Header-Feld, das Sie in die Klassenzuordnung aufnehmen möchten.

Länge größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Feldlänge angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Zahl der Byte ein.

Zählung größer als

Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Beschränkung für die Gesamtzahl der Felder dieses Typs angeben möchten, die ein Paket nicht überschreiten sollte, und geben Sie die Anzahl der Felder ein.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Andere Felder in diesem Dialogfeld

Je nachdem, welches HTTP-Header-Feld Sie wählen, können in diesem Dialogfeld weitere Felder angezeigt werden, über die Sie zusätzliche Kriterien festlegen können. Wenn Sie beispielsweise das Feld **Inhaltstyp** wählen, können Sie eine Prüfung auf nicht übereinstimmende Inhaltstypen zwischen Anforderung und Antwort, auf unbekannte Inhaltstypen sowie Protokollverletzungen des Inhaltstyps durchführen. Wenn Sie das Feld **transfer-encoding** wählen, können Sie eine Prüfung auf verschiedene Komprimierungs- und Codierungstypen durchführen.

Feld „Übereinstimmung“

Aktivieren Sie dieses Kontrollkästchen, wenn die Klassenzuordnung mit dem gewählten Feldtyp übereinstimmen soll.

Anforderungs-/Antwortinhalt

Der Router kann auf Anforderungs-/Antwortinhalt-Länge und spezielle Textzeichenfolgen im Inhalt der Anforderung/Antwort prüfen.

Länge

Aktivieren Sie dieses Kontrollkästchen und wählen Sie **Größer als (>)**, um die obere Grenze für die Länge des Anforderungs-/Antwortinhalts anzugeben. Wählen Sie **Kleiner als (<)**, um eine untere Grenze anzugeben.

Reguläre Ausdrücke

Aktivieren Sie dieses Kontrollkästchen, um reguläre Ausdrücke anzugeben, mit denen ein Vergleich erfolgen soll. Wählen Sie einen vorhandenen regulären Ausdruck einer Klassenzuordnung aus oder erstellen Sie einen neuen, der mit den zu prüfenden Zeichenfolgen verglichen wird. Weitere Informationen zum Erstellen regulärer Ausdrücke finden Sie unter Hinzufügen oder Bearbeiten eines regulären Ausdrucks. Um eine vorhandene Zuordnung zu prüfen, ohne dieses Dialogfeld zu verlassen, wählen Sie sie in der Liste **Bestehende Zuordnung auswählen** aus und klicken auf **Ansicht**.

Anforderungs-/Antwort-Protokollverletzung

Um auf Protokollverletzungen in HTTP-Anforderungen/-Antworten zu prüfen, klicken Sie auf **Protokollverletzung**.

Hinzufügen oder Bearbeiten einer IMAP-Klassenzuordnung

Das Erstellen einer Klassenzuordnung für die Internet Message Access Protocol (IMAP)-Prüfung kann dazu beitragen sicherzustellen, dass Benutzer sichere Authentifizierungsmechanismen verwenden, um einem Missbrauch der Benutzeranmeldeinformationen vorzubeugen.

Geben Sie einen Namen in das Feld **Klassenname** ein, um diese Klassenzuordnung zu identifizieren. Sie können auch eine Beschreibung eingeben. Wenn Sie eine Klassenzuordnung bearbeiten, können Sie den Namen nicht ändern.

Klicken Sie auf **Anmeldezeichenfolge im Klartext**, damit der Router IMAP-Datenverkehr auf unsichere Anmeldungen prüft.

Klicken Sie auf **Anmeldezeichenfolge im Klartext**, damit der Router IMAP-Datenverkehr auf unsichere Anmeldungen prüft.

Hinzufügen oder Bearbeiten einer SMTP-Klassenzuordnung

Simple Mail Transfer Protocol (SMTP)-Klassenzuordnungen ermöglichen Ihnen, die Inhaltslänge zu beschränken und die Protokoll-Compliance umzusetzen.

Geben Sie einen Namen in das Feld **Klassenname** ein, um diese Klassenzuordnung zu identifizieren. Sie können in das vorgesehene Feld auch eine Beschreibung eingeben.

Geben Sie die **Maximal erlaubte Datenübertragung** in das Feld **Übereinstimmungskriterien** ein.

Hinzufügen oder Bearbeiten einer SUNRPC-Klassenzuordnung

Mit SUN Remote Procedure Call (SUNRPC)-Klassenzuordnungen können Sie die Nummer des Programms angeben, dessen Datenverkehr der Router prüfen soll.

Geben Sie einen Namen in das Feld **Klassenname** ein, um diese Klassenzuordnung zu identifizieren. Sie können auch eine Beschreibung eingeben. Wenn Sie eine Klassenzuordnung bearbeiten, können Sie den Namen nicht ändern.

Klicken Sie auf im Feld **Programmnummer für Übereinstimmung** auf **Hinzufügen**, um eine Programmnummer hinzuzufügen.

Hinzufügen oder Bearbeiten einer Instant Messaging-Klassenzuordnung

Instant Messaging (IM)-Klassenzuordnungen erlauben Ihnen, den Instant Messaging-Typ anzugeben und festzulegen, ob der Datenverkehr aller IM-Dienste geprüft werden soll oder ob nur der Datenverkehr des Textchat-Dienstes geprüft werden soll.

Wählen Sie im Feld **Klassenzuordnungstyp aol** für America Online (AOL), **msnmsgr** für Microsoft Networks Messenger oder **ymsgr** für Yahoo! Messenger.

Klicken Sie im Feld **Übereinstimmungskriterien** auf **Alle Dienste** oder klicken Sie auf **Textchat-Dienste**, wenn Sie nur den Textchat-Datenverkehr prüfen möchten.

Hinzufügen oder Bearbeiten einer Punkt-zu-Punkt-Klassenzuordnung

Eine P2P-Klassenzuordnung gibt eine P2P-Anwendung und die Übereinstimmungskriterien an. Pro Klassenzuordnung kann jeweils nur eine Anwendung angegeben werden.

Klassenname

Geben Sie einen neuen Klassennamen ein, um eine neue Klassenzuordnung zu erstellen. Wenn Sie auf die Schaltfläche rechts neben dem Feld klicken, können Sie vorhandene Klassenzuordnungen zur Bearbeitung auswählen. Sie können die Übereinstimmungskriterien für eine Klassenzuordnung bearbeiten, aber nicht den Klassenzuordnungstyp ändern.

Klassenzuordnungstyp

Sie können eine P2P-Klassenzuordnung für die folgenden P2P-Diensttypen erstellen:

- **eDonkey**
- **Fasttrack**
- **Gnutella**
- **Kazaa2**

Übereinstimmungskriterien und -wert

Klicken Sie auf **Hinzufügen**, um die Übereinstimmungskriterien einzugeben und den Verbindungstyp anzugeben, der von der Datenverkehrsklasse identifiziert werden soll.

Geben Sie Übereinstimmungskriterien ein, um den Verbindungstyp anzugeben, der von der Datenverkehrsklasse identifiziert werden soll. Sie können angeben, dass die Dateiübertragungsverbindungen von der Datenverkehrsklasse für fasttrack, gnutella und kazaa2 identifiziert werden sollen. Für eDonkey können Sie angeben, dass die Dateiübertragungsverbindungen, Dateinamenanforderungen (search-file-name) und Textchats von der Datenverkehrsklasse identifiziert werden sollen. Der Wert für die Übereinstimmungskriterien kann ein regulärer Ausdruck sein. Wenn Sie beispielsweise angeben möchten, dass alle Dateiübertragungsverbindungen identifiziert werden sollen, geben Sie * ein.

Hinzufügen einer P2P-Regel

Geben Sie Übereinstimmungskriterien ein, um den Verbindungstyp anzugeben, der von der Datenverkehrsklasse identifiziert werden soll. Sie können angeben, dass die Dateiübertragungsverbindungen von der Datenverkehrsklasse für fasttrack, gnutella und kazaa2 identifiziert werden sollen. Für eDonkey können Sie angeben, dass die Dateiübertragungsverbindungen, Dateinamenanforderungen (search-file-name) und Textchats von der Datenverkehrsklasse identifiziert werden sollen. Der Wert für die Übereinstimmungskriterien kann ein regulärer Ausdruck sein. Wenn Sie beispielsweise angeben möchten, dass alle Dateiübertragungsverbindungen identifiziert werden sollen, geben Sie * ein.

Hinzufügen oder Bearbeiten einer POP3-Klassenzuordnung

Das Erstellen einer Klassenzuordnung für die Post Office Protocol Version 3 (POP3)-Prüfung kann dazu beitragen sicherzustellen, dass Benutzer sichere Authentifizierungsmechanismen verwenden, um einem Missbrauch der Benutzeranmeldeinformationen vorzubeugen.

Geben Sie einen Namen in das Feld **Klassenname** ein, um diese Klassenzuordnung zu identifizieren. Sie können auch eine Beschreibung eingeben. Wenn Sie eine Klassenzuordnung bearbeiten, können Sie den Namen nicht ändern.

Klicken Sie auf **Anmeldezeichenfolge in Klartext**, damit der Router den POP3-Datenverkehr auf unsichere Anmeldungen prüft.

Klicken Sie auf **Ungültiger Protokollbefehl**, damit der Router den POP3-Datenverkehr auf ungültige Befehle prüft.

Parameterzuordnungen

Parameterzuordnungen geben das Prüfverhalten für die Zone-Policy Firewall an, für Parameter wie z. B. Denial-of-Service-Schutz, Sitzungs- und Verbindungstimer und Anmeldeeinstellungen. Parameterzuordnungen werden auch mit Klassen- und Richtlinienzuordnungen für Layer 7 angewandt, um anwendungsspezifisches Verhalten zu definieren, wie beispielsweise HTTP-Objekte, POP3- und IMAP-Authentifizierungsanforderungen und andere anwendungsspezifische Informationen.

Parameterzuordnungsfenster

Die Parameterzuordnungsfenster listen die konfigurierten Parameterzuordnungen für Protokollinformationen, URL-Filterung, reguläre Ausdrücke und andere Parameterzuordnungstypen auf. Wenn die Parameterzuordnung mit einer Klassenzuordnung verknüpft wurde, wird der Name der Klassenzuordnung in der Spalte **Verwendet von** angezeigt. Die Details der ausgewählten Parameterzuordnung werden in der unteren Hälfte des Fensters angezeigt. Sie können Parameterzuordnungen hinzufügen, bearbeiten und löschen. Der SDM informiert Sie, wenn Sie versuchen, eine Parameterzuordnung zu löschen, die von einer Klassenzuordnung verwendet wird.

Für weitere Informationen zu den in diesen Fenstern angezeigten Parameterzuordnungen klicken Sie auf einen der folgenden Links:

- Timeouts und Grenzwerte für Prüfparameterzuordnungen und CBAC
- Hinzufügen oder Bearbeiten einer Parameterzuordnung für Protokollinformationen
- Allgemeine Einstellungen für die URL-Filterung
- Hinzufügen oder Bearbeiten von URL-Filter-Servern
- Liste lokaler URLs
- Hinzufügen oder Bearbeiten eines regulären Ausdrucks

Hinzufügen oder Bearbeiten einer Parameterzuordnung für Protokollinformationen

Es kann notwendig sein, Server für bestimmte Anwendungstypen, wie beispielsweise IM-Anwendungen, zu identifizieren, sodass Sie die Verwendung auf eine bestimmte Aktivität, wie beispielsweise Textchat, einschränken können.

Parameterzuordnungsname

Geben Sie einen Namen ein, der die Verwendung dieser Parameterzuordnung beschreibt. Wenn Sie beispielsweise eine Serverliste für Yahoo! Instant Messenger-Textchat-Server erstellen, können Sie den Namen ymsgr-pmap verwenden.

Serverdetails

Dieser Bildschirmbereich enthält eine Liste der Servernamen, Server-IP-Adressen oder IP-Adressbereiche.

Hinzufügen oder Bearbeiten eines Servereintrags

Sie können den Hostnamen oder die IP-Adresse eines einzelnen Servers oder einen Bereich von IP-Adressen, der einer Gruppe von Servern zugewiesen ist, angeben.

Sie können den Hostnamen in das Feld **Name** eingeben, wenn der Router einen DNS-Server im Netzwerk kontaktieren kann, um die IP-Adresse des Servers aufzulösen. Wenn Sie die IP-Adresse für einen Server eingeben möchten, geben Sie sie in das Feld **Einzelne IP-Adresse** ein. Gibt es mehrere Server, die einen IP-Adressbereich nutzen, verwenden Sie das Feld **IP-Bereich**. Geben Sie die niedrigste IP-Adresse in das Feld auf der linken Seite und die höchste IP-Adresse in das Feld auf der rechten Seite ein. Um beispielsweise den Bereich 103.24.5.67 bis 99 einzugeben, geben Sie `103.24.5.67` in das linke Feld und `103.24.5.99` in das rechte Feld ein.

Hinzufügen oder Bearbeiten eines regulären Ausdrucks

Ein regulärer Ausdruck stimmt entweder buchstabengetreu mit einer Zeichenfolge überein, oder Sie können *Metazeichen* verwenden, sodass Übereinstimmungen mit mehreren Varianten einer Textzeichenfolge gefunden werden. Sie können einen regulären Ausdruck verwenden, um Übereinstimmungen des Inhalts eines bestimmten Anwendungsdatenverkehrs zu finden; so können Sie beispielsweise nach Übereinstimmungen mit dem Textinhalt eines HTTP-Pakets suchen.

Von Ihnen erstellte reguläre Ausdrücke können überall verwendet werden, wo in den Bildschirmen der Zone-Based Policy Firewall ein regulärer Ausdruck benötigt wird. Metazeichen für regulären Ausdruck enthält eine Liste von Metazeichen für reguläre Ausdrücke und Informationen darüber, wie diese verwendet werden.

Name

Geben Sie einen Namen ein, um den regulären Ausdruck zu identifizieren. Wenn Sie den regulären Ausdruck bearbeiten, ist das Namensfeld schreibgeschützt.

Musterliste

Ein regulärer Ausdruck kann mehrere Muster enthalten. Klicken Sie auf **Hinzufügen**, um ein Dialogfeld anzuzeigen, in dem Sie ein neues Muster für einen regulären Ausdruck eingeben können. Jedes von Ihnen erstellte Muster wird automatisch zur Liste hinzugefügt. Wenn Sie ein Muster von einem anderen regulären Ausdruck kopieren möchten, klicken Sie auf **Muster kopieren**, klicken auf das Pluszeichen (+) neben dem Namen des regulären Ausdrucks, klicken in das gewünschte Muster und klicken auf **OK**.

```
parameter-map type regex ref_regex
pattern „\.delfinproject\.com"
pattern „\.looksmart\.com"
parameter-map type regex host_regex
pattern „secure\.keenvalue\.com"
pattern „\.looksmart\.com"
parameter-map type regex usragnt_regex
pattern „Peer Points Manager"
```

Durch Tabelle ersetzen.

Hinzufügen eines Musters

Das von Ihnen in diesem Fenster eingegebene Muster wird unten zur Parameterzuordnung des regulären Ausdrucks hinzugefügt, den Sie bearbeiten. Wenn Sie die Muster in der Parameterzuordnung neu anordnen möchten, können Sie dies im Fenster **Regulären Ausdruck bearbeiten** tun.

Muster

Geben Sie das Muster ein, das Sie zum regulären Ausdruck hinzufügen möchten.

Schaltfläche „Anleitung"

Klicken Sie auf diese Schaltfläche, um das Dialogfeld Regulären Ausdruck erstellen anzuzeigen, das Ihnen bei der Erstellung eines regulären Ausdrucks behilflich ist. Wenn Sie auf **Anleitung** klicken, wird sämtlicher in das Feld **Muster** eingegebener Text im Feld Regulärer Ausdruck des Dialogfelds **Regulären Ausdruck erstellen** angezeigt.

Regulären Ausdruck erstellen

Mithilfe des Dialogfelds **Regulären Ausdruck erstellen** können Sie einen regulären Ausdruck aus Zeichen und Metazeichen erstellen. Felder, die Metazeichen einfügen, nehmen das Metazeichen in Klammern in den Feldnamen auf.

Build-Snippet

Mit diesem Bereich können Sie Snippets von regulärem Text erstellen oder ein Metazeichen in das Feld **Regulärer Ausdruck** einfügen.

- Beginnt am Anfang der Zeile (^) – Gibt an, dass das Snippet am Anfang einer Zeile beginnen sollte, unter Verwendung des Caret-Metazeichens (^). Achten Sie darauf, ein Snippet mit dieser Option am Anfang des regulären Ausdrucks einzufügen.
- Zeichenfolge angeben – Geben Sie manuell eine Textzeichenfolge ein.
  - Zeichenfolge – Geben Sie eine Zeichenfolge ein.
  - Escape-Sonderzeichen – Wenn Sie Metazeichen in eine Textzeichenfolge eingegeben haben, die buchstabengetreu verwendet werden sollen, aktivieren Sie dieses Kontrollkästchen, um das Escape-Zeichen Backslash (\) davor einzufügen. Wenn Sie beispielsweise „example.com“ eingeben, konvertiert diese Option den Text in „example\.com“.
  - Groß-/Kleinschreibung ignorieren – Wenn die Groß- und Kleinschreibung bei Zeichen ignoriert werden soll, fügt dieses Kontrollkästchen automatisch Text hinzu, um beide Fälle zu berücksichtigen. Der eingegebene Text „cats“ wird beispielsweise in „[cC][aA][tT][sS]“ konvertiert.

Zeichen angeben

Lässt Sie ein Metazeichen angeben, das in den regulären Ausdruck eingefügt wird.

- Zeichen negieren – Gibt an, dass das jeweils eingegebene Zeichen nicht übereinstimmen soll.
- Beliebiges Zeichen (.) – Fügt das Metazeichen Punkt (.) ein, das für ein beliebiges Zeichen steht. Die Zeichenfolge **d.g** entspricht beispielsweise „dog“, „dag“, „dtg“ und jedem anderen Wort, das diese Zeichen enthält, wie zum Beispiel „doggonnit“.
- Zeichensatz – Fügt einen Zeichensatz ein. Der Text kann jedem Zeichen im Zeichensatz entsprechen. Zu den Zeichensätzen gehören:

  [0-9A-Za-z]

  [0-9]

  [A-Z]

  [a-z]

  [aeiou]

  [\n\f\r\t] (was einer neuen Zeile, einem Seitenvorschub, einem Zeilenumbruch oder einem Tabulator entspricht)

  Wenn Sie beispielsweise [0-9A-Za-z] angeben, dann entspricht dieses Snippet Zeichen von A bis Z (groß oder klein geschrieben) oder einer Zahl von 0 bis 9.
- Sonderzeichen – Fügt ein Zeichen ein, dass ein Escape erfordert, einschließlich \, ?, *, +, |, ., [, (oder ^. Das Escape-Zeichen ist der Backslash (\), der automatisch eingefügt wird, wenn Sie diese Option wählen.
- Leerstelle – Leerstellen beinhalten \n (neue Zeile), \f (Seitenvorschub), \r (Zeilenumbruch) oder \t (Tabulator).
- Oktalnummer mit drei Ziffern – Entspricht einem ASCII-Zeichen in Oktalschreibweise (bis zu drei Ziffern). Das Zeichen \040 beispielsweise steht für ein Leerzeichen. Der Backslash (\) wird automatisch eingefügt.
- Hexadezimalnummer mit zwei Zeichen – Entspricht einem ASCII-Zeichen in Hexadezimalschreibweise (genau zwei Ziffern). Der Backslash (\) wird automatisch eingefügt.
- Angegebenes Zeichen – Geben Sie ein einzelnes Zeichen ein.

Snippet-Vorschau

Nur anzeigen. Zeigt das Snippet so, wie es in den regulären Ausdruck aufgenommen wird.

- Snippet anhängen – Hängt das Snippet an das Ende des regulären Ausdrucks an.
- Snippet als Alternative anhängen – Fügt das Snippet am Ende des regulären Ausdrucks an und trennt diesen vom nächsten zu vergleichenden Ausdruck durch das Pipe-Zeichen (|). Beispiel: **dog|cat** entspricht „dog“ oder „cat“.
- Snippet bei Cursor einfügen – Fügt das Snippet beim Cursor ein.

Regulärer Ausdruck

Dieser Bereich enthält Text eines regulären Ausdrucks, den Sie manuell eingeben und mit Snippets erstellen können. Anschließend können Sie Text im Feld **Regulärer Ausdruck** auswählen und einen Quantifizierer auf die Auswahl anwenden.

- Auswahl der Vorkommen – Wählen Sie Text im Feld **Regulärer Ausdruck** aus, klicken Sie auf eine der folgenden Optionen und klicken Sie anschließend auf **Auf Auswahl anwenden**. Wenn der reguläre Ausdruck beispielsweise „test me“ lautet und Sie „me“ auswählen und **Einmal oder mehrmals** auswählen, dann ändert sich der reguläre Ausdruck in „test (me)+“.
  - Null oder mehrmals (?) – Ein Quantifizierer, der angibt, dass es 0 oder 1 Vorkommnis des vorherigen Ausdrucks gibt. Beispiel: **lo?se** entspricht „lse“ oder „lose“.
  - Einmal oder mehrmals (+) – Ein Quantifizierer, der angibt, dass es mindestens 1 Vorkommnis des vorherigen Ausdrucks gibt. Beispiel: **lo+se** entspricht „lose“ und „loose“, aber nicht „lse“.
  - Einmal oder mehrmals (+) – Ein Quantifizierer, der angibt, dass es mindestens 1 Vorkommnis des vorherigen Ausdrucks gibt. Beispiel: **lo+se** entspricht „lose“ und „loose“, aber nicht „lse“.
  - Alle Anzahl an Vorkommen (*) – Ein Quantifizierer, der angibt, dass es 0, 1 oder eine beliebige Anzahl von Vorkommnissen des vorherigen Ausdrucks gibt. Beispiel: **lo*se** entspricht „lse“, „lose“, „loose“ usw.

  - Mindestens – Mindestens *x*-mal wiederholen. Beispiel: **ab(xy){2,}z** entspricht „abxyxyz“, „abxyxyxyz“ usw.
  - Exakt – Genau *x*-mal wiederholen. Beispiel: **ab(xy){3}z** entspricht „abxyxyxyz“.
- Auf Auswahl anwenden – Wendet den Quantifizierer auf die Auswahl an.
- Test – Testet einen regulären Ausdruck mit einem Beispieltext.

Metazeichen für regulären Ausdruck

Die folgende Tabelle führt die Metazeichen auf, die besondere Bedeutungen haben.

Zeichen	Beschreibung	Hinweise
.	Punkt	Steht für ein einzelnes Zeichen. Die Zeichenfolge **d.g** entspricht beispielsweise „dog“, „dag“, „dtg“ und jedem anderen Wort, das diese Zeichen enthält, wie zum Beispiel „doggonnit“.
(*exp*)	Unterausdruck	Ein Unterausdruck trennt Zeichen von umgebenden Zeichen, sodass Sie andere Metazeichen im Unterausdruck verwenden können. So entspricht **d(o|a)g** beispielsweise „dog“ und „dag“, **do|ag** jedoch „do“ und „ag“. Ein Unterausdruck kann auch mit Wiederholungsquantifizierern verwendet werden, um die Zeichen, die sich wiederholen sollen, zu unterscheiden. Beispiel: **ab(xy){3}z** entspricht abxyxyxyz.
|	Alternative	Entspricht einem der Ausdrücke, der davon getrennt wird. Beispiel: **dog|cat** entspricht „dog“ oder „cat“.
?	Fragezeichen	Ein Quantifizierer, der angibt, dass es 0 oder 1 Vorkommnis des vorherigen Ausdrucks gibt. Beispiel: **lo?se** entspricht „lse“ oder „lose“. **Hinweis** Sie müssen **Strg+V** drücken und dann das Fragezeichen eingeben, andernfalls wird die Hilfe-Funktion aufgerufen.

Zeichen	Beschreibung	Hinweise
*	Sternchen	Ein Quantifizierer, der angibt, dass es 0, 1 oder eine beliebige Zahl von Vorkommnissen des vorherigen Ausdrucks gibt. Beispiel: **lo*se** entspricht „lse“, „lose“, „loose“ usw.
+	Pluszeichen	Ein Quantifizierer, der angibt, dass es mindestens 1 Vorkommnis des vorherigen Ausdrucks gibt. Beispiel: **lo+se** entspricht „lose“ und „loose“, aber nicht „lse“.
{*x*}	Wiederholungsquantifizierer	Genau *x*-mal wiederholen. Beispiel: **ab(xy){3}z** entspricht abxyxyxyz.
{*x*,}	Quantifizierer für Mindestwiederholungen	Mindestens *x*-mal wiederholen. Beispiel: **ab(xy){2,}z** entspricht „abxyxyz“, „abxyxyxyz“ usw.
[*abc*]	Zeichenklasse	Entspricht einem beliebigen Zeichen in den Klammern. Beispiel: **[abc]** entspricht a, b oder c.
[^*abc*]	Negierte Zeichenklasse	Entspricht einem einzigen Zeichen, das nicht in den Klammern enthalten ist. **[^abc]** entspricht beispielsweise einem anderen Zeichen als a, b oder c. **[^A-Z]** entspricht einem beliebigen Zeichen, das kein Großbuchstabe ist.
[*a*-*c*]	Zeichenbereichsklasse	Entspricht einem beliebigen Zeichen im Bereich. **[a-z]** entspricht einem beliebigen Kleinbuchstaben. Sie können Zeichen und Bereich mischen: **[abcq-z]** entspricht a, b, c, q, r, s, t, u, v, w, x, y, z, genau wie **[a-cq-z]**. Der Bindestrich (-) ist nur buchstabengetreu, wenn er das letzte oder erste Zeichen in den Klammern ist: **[abc-]** oder **[-abc]**.
""	Fragezeichen	Erhalten nachfolgende oder vorausgehende Leerzeichen in der Zeichenfolge. Beispiel: **„ test“** erhält das vorausgehende Leerzeichen, wenn nach einer Entsprechung gesucht wird.
^	Caret-Zeichen	Kennzeichnet den Anfang einer Zeile.
\	Escape-Zeichen	Wird es zusammen mit einem Metazeichen verwendet, entspricht es genau einem Zeichen. Beispiel: **\[** entspricht einer linken eckigen Klammer.

Zeichen	Beschreibung	Hinweise
char	Zeichen	Wenn es kein Metazeichen ist, entspricht es genau dem Zeichen.
\r	Zeilenumbruch	Entspricht einem Zeilenumbruch 0x0d.
\n	Neue Zeile	Entspricht einer neuen Zeile 0x0a.
\t	Tabulator	Entspricht einem Tabulator 0x09.
\f	Seitenvorschub	Entspricht einem Seitenvorschub 0x0c.
\x*NN*	Zahl in Hexadezimalschreibweise mit Escape	Entspricht einem ASCII-Zeichen in Hexadezimalschreibweise (genau zwei Ziffern).
NNN	Oktal-Zahl mit Escape	Entspricht einem ASCII-Zeichen in Oktalschreibweise (genau drei Ziffern). Das Zeichen 040 beispielsweise steht für ein Leerzeichen.

KAPITEL 35

URL-Filterung

Mit URL-Filterung können Sie den Zugriff auf Internet-Websites steuern, indem Sie den Zugang für bestimmte Websites auf der Grundlage von Informationen aus einer URL-Liste zulassen oder ablehnen. Sie können eine Liste lokaler URLs auf dem Router verwalten und URL-Listen verwenden, die auf Websense- oder Secure Computing URL-Filterlisten-Servern gespeichert sind. Die URL-Filterung erfolgt durch die Konfiguration einer Richtlinie zur Anwendungssicherheit, welche diese Filterung aktiviert.

Auch wenn keine Richtlinie zur Anwendungssicherheit auf dem Router konfiguriert ist, können Sie trotzdem eine Liste lokaler URLs und eine URL-Filter-Server-Liste verwalten, die für die URL-Filterung verwendet werden kann, sobald eine Richtlinie erstellt wird, die diese Filterung aktiviert.

Dieses Kapitel enthält die folgenden Abschnitte:

- Fenster URL-Filterung
- Liste lokaler URLs
- URL-Filter-Server

Weitere Informationen zur URL-Filterung finden Sie unter folgendem Link:

Firewall Websense URL Filtering

Informationen zur Verwendung von Richtlinien zur URL-Filterung erhalten Sie durch Klicken auf Vorrang bei der URL-Filterung.

Fenster URL-Filterung

In diesem Fenster werden die globalen Einstellungen für die URL-Filterung auf dem Router angezeigt. Sie können die lokale URL-Liste und die URL-Filter-Server-Liste auf den Bildschirmen für zusätzliche Aufgaben oder in den Fenstern zur Anwendungssicherheit verwalten. Die globalen Einstellungen für die URL-Filterung können nur über dieses Fenster für zusätzliche Aufgaben verwaltet werden. Verwenden Sie die Schaltfläche **Globale Einstellungen bearbeiten**, um diese Werte zu ändern.

Eine Beschreibung der einzelnen Einstellungen, die in diesem Fenster angezeigt werden, finden Sie unter Globale Einstellungen bearbeiten.

Eine Beschreibung der URL-Filterungsfunktionen, die Cisco SDM bereitstellt, finden Sie in den einführenden Informationen unter URL-Filterung.

Globale Einstellungen bearbeiten

In diesem Fenster können Sie die globalen Einstellungen für die URL-Filterung bearbeiten.

Hinweis Die Protokollierung muss aktiviert sein, damit der Router URL-Filter-Warnungen, Meldungen der Überwachungsliste und Systemmeldungen bezüglich des URL-Filter-Servers melden kann.

Zulassen-Modus

Aktivieren Sie diese Option, damit der Router in den Zulassen-Modus wechseln kann, wenn er keine Verbindung zu einem der URL-Filterungsserver in der Serverliste herstellen kann. Wenn sich der Router im Zulassen-Modus befindet, werden alle HTTP-Anforderungen durchgelassen, wenn der Router keine Verbindung zu einem der URL-Filterungsserver in der Serverliste herstellen kann. Der Zulassen-Modus ist standardgemäß deaktiviert.

URL-Filter-Warnung

Aktivieren Sie dieses Kontrollkästchen, damit der Router die Meldungen der URL-Filter-Warnungen protokollieren kann. URL-Filter-Warnungen melden Ereignisse wie den Ausfall eines URL-Filterungsservers oder eine HTTP-Anforderung mit einem URL, der für eine Lookup-Anforderung zu lang ist. Diese Option ist standardmäßig deaktiviert.

Überwachungsliste

Aktivieren Sie diese Option, damit der Router eine Überwachungsliste im Protokoll verwalten kann. Der Router zeichnet Statusmeldungen der URL-Anforderungen auf, die angeben, ob eine HTTP-Anforderung zugelassen oder abgelehnt wurde, sowie andere Meldungen aus der Überwachungsliste. Diese Option ist standardmäßig deaktiviert.

Bericht für URL-Filter-Server

Aktivieren Sie diese Option, damit der Router Systemmeldungen zum URL-Filter-Server im Protokoll aufzeichnen kann. Diese Option ist standardmäßig deaktiviert.

Cache-Größe

Sie können die maximale Größe des Cache festlegen, der die zuletzt angeforderten IP-Adressen und ihren jeweiligen Autorisierungsstatus speichert. Die Standardgröße dieses Cache ist 5000 Byte. Der Größenbereich liegt zwischen 0 Byte und 2147483647. Der Cache wird alle 12 Stunden geleert.

Maximale Anzahl zwischengespeicherter HTTP-Anforderungen

Sie können die maximale Anzahl ausstehender HTTP-Anforderungen festlegen, die der Router zwischenspeichern kann. Der Router speichert vorübergehend standardmäßig bis zu 1000 Anforderungen. Sie können zwischen 1 und 2147483647 Anforderungen angeben.

Maximale Anzahl zwischengespeicherter HTTP-Antworten

Sie können die maximale Anzahl von HTTP-Antworten des URL-Filterungsservers festlegen, die der Router zwischenspeichern kann. Wenn diese Anzahl erreicht ist, lässt der Router weitere Antworten nicht mehr durch. Der Standardwert ist 200. Sie können einen Wert zwischen 0 und 20000 festlegen.

Allgemeine Einstellungen für die URL-Filterung

Vergeben Sie für den URL-Filter einen Namen, geben Sie an, welche Aktion der Router vornehmen soll, wenn eine Übereinstimmung ermittelt wird, und konfigurieren Sie Parameter für Protokolle und die Cache-Größe. Sie können auch eine Quellschnittstelle angeben, wenn die URL-Filterparameterzuordung auf alle anderen Routerschnittstellen angewendet werden soll.

URL-Filtername

Geben Sie einen Namen ein, der vermittelt, wie dieser URL-Filter konfiguriert ist oder verwendet wird. Wenn Sie beispielsweise eine Quellschnittstelle von FastEthernet 1 angeben, könnten Sie den Namen `fa1-parzuord` eingeben. Wenn der Filter einen Websense URL-Filterserver bei IP-Adresse 192.128.54.23 verwendet, könnten Sie für den Namen `websense23-parzuord` eingeben.

Zulassen-Modus

Aktivieren Sie diese Option, damit der Router in den Zulassen-Modus wechseln kann, wenn er keine Verbindung zu einem der URL-Filterungsserver in der Serverliste herstellen kann. Wenn sich der Router im Zulassen-Modus befindet, werden alle HTTP-Anforderungen durchgelassen, wenn der Router keine Verbindung zu einem der URL-Filterungsserver in der Serverliste herstellen kann. Der Zulassen-Modus ist standardgemäß deaktiviert.

URL-Filter-Warnung

Aktivieren Sie dieses Kontrollkästchen, damit der Router die Meldungen der URL-Filter-Warnungen protokollieren kann. URL-Filter-Warnungen melden Ereignisse wie den Ausfall eines URL-Filterungsservers oder eine HTTP-Anforderung mit einem URL, der für eine Lookup-Anforderung zu lang ist. Diese Option ist standardmäßig deaktiviert.

Überwachungsliste

Aktivieren Sie diese Option, damit der Router eine Überwachungsliste im Protokoll verwalten kann. Der Router zeichnet Statusmeldungen der URL-Anforderungen auf, die angeben, ob eine HTTP-Anforderung zugelassen oder abgelehnt wurde, sowie andere Meldungen aus der Überwachungsliste. Diese Option ist standardmäßig deaktiviert.

Bericht für URL-Filter-Server

Aktivieren Sie diese Option, damit der Router Systemmeldungen zum URL-Filter-Server im Protokoll aufzeichnen kann. Diese Option ist standardmäßig deaktiviert.

Cache-Größe

Sie können die maximale Größe des Cache festlegen, der die zuletzt angeforderten IP-Adressen und ihren jeweiligen Autorisierungsstatus speichert. Die Standardgröße dieses Cache ist 5000 Byte. Der Größenbereich liegt zwischen 0 Byte und 2147483647. Der Cache wird alle 12 Stunden geleert.

Maximale Anzahl zwischengespeicherter HTTP-Anforderungen

Sie können die maximale Anzahl ausstehender HTTP-Anforderungen festlegen, die der Router zwischenspeichern kann. Der Router speichert vorübergehend standardmäßig bis zu 1000 Anforderungen. Sie können zwischen 1 und 2147483647 Anforderungen angeben.

Maximale Anzahl zwischengespeicherter HTTP-Antworten

Sie können die maximale Anzahl von HTTP-Antworten des URL-Filterungsservers festlegen, die der Router zwischenspeichern kann. Wenn diese Anzahl erreicht ist, lässt der Router weitere Antworten nicht mehr durch. Der Standardwert ist 200. Sie können einen Wert zwischen 0 und 20000 festlegen.

Erweiterte

Im Feld **Erweiterte** können Sie die Quellschnittstelle wählen. Wählen Sie die Schnittstellen aus der Liste der Quellschnittstellen aus.

Liste lokaler URLs

Wenn das Cisco IOS-Abbild auf dem Router die URL-Filterung unterstützt, jedoch keine zonenbasierte Richtlinienfirewall (Zone-Based Policy Firewall, ZPF), können Sie die lokale URL-Liste auf dem Router beibehalten. Diese Liste wird von allen Richtlinien zur Anwendungssicherheit verwendet, für welche die URL-Filterung aktiviert ist. Das Cisco IOS-Abbild der Version 12.4(9)T und höher unterstützt sämtliche ZPF-Funktionen, die von SDM unterstützt werden. In einer ZPF-Konfiguration kann eine lokale URL-Liste für jede Parameterzuordnung der URL-Filterung erstellt werden.

Sie können Cisco SDM verwenden, um Listeneinträge zu erstellen, und Einträge aus einer auf Ihrem PC gespeicherten Liste importieren. Wenn eine Liste lokaler URLs zusammen mit URL-Filter-Servern verwendet wird, werden die lokalen Einträge zuerst verwendet. Weitere Informationen finden Sie unter Vorrang bei der URL-Filterung.

Verwalten der Liste lokaler URLs

Sie können Cisco SDM verwenden, um eine Liste lokaler URLs zu verwalten, indem Sie Einträge einzeln hinzufügen und löschen und eine URL-Liste von Ihrem PC importieren und festlegen, welche Aktionen Cisco SDM mit den einzelnen Einträgen vornehmen soll. Verwenden Sie die Schaltflächen **Hinzufügen** und **Löschen**, um bestimmte Einträge in der Liste auf dem Router zu verwalten, und klicken Sie auf die Schaltfläche **URL-Liste importieren**, um eine URL-Liste von Ihrem PC zu importieren.

Hinweis Wenn ein Eintrag aus der lokalen Liste gelöscht wird und der Router für die Verwendung von URL-Filterungservern konfiguriert ist, sind auf diesen Servern möglicherweise noch Einträge vorhanden, die mit den Einträgen übereinstimmen, die Sie aus der lokalen Liste löschen.

Klicken Sie auf die Schaltfläche **Alle löschen**, um alle Einträge vom Router zu löschen. Wenn keine lokale Liste auf dem Router konfiguriert ist, muss der Router auf die konfigurierten URL-Filter-Server zurückgreifen. Wenn Sie die URL-Liste, die Sie löschen, zu einem späteren Zeitpunkt wieder aufrufen möchten, verwenden Sie die Schaltfläche **URL-Liste exportieren**, um die URL-Liste auf Ihrem PC zu speichern, bevor Sie alle Einträge löschen. Wenn Sie die URL-Liste auf Ihrem PC speichern, erhält sie die Erweiterung .CSV.

Importieren von URL-Listen von Ihrem PC

Klicken Sie auf die Schaltfläche **URL-Liste importieren**, um eine URL-Liste von Ihrem PC auf den Router zu importieren. Die ausgewählte URL-Liste muss die Erweiterung .txt oder .CSV haben. Nachdem Sie die Liste auf Ihrem PC ausgewählt haben, zeigt Cisco SDM ein Dialogfeld an, in dem Sie festlegen können, welche Aktionen Sie mit den einzelnen Einträgen in der Liste vornehmen möchten. Weitere Informationen finden Sie unter URL-Liste importieren.

Lokalen URL hinzufügen oder bearbeiten

In diesem Fenster können Sie einen URL-Eintrag für die Liste lokaler URLs auf dem Router hinzufügen oder bearbeiten. Geben Sie einen vollständigen oder teilweisen Domänennamen ein, und wählen Sie aus, ob Sie Anforderungen für diesen URL **Genehmigen** oder **Ablehnen** möchten.

Wenn Sie einen vollständigen Domänennamen eingeben, zum Beispiel www.Einedomäne.com, werden alle Anforderungen, die diesen Domänennamen enthalten, zum Beispiel www.Einedomäne.com/news oder www.Einedomäne.com/index abhängig von der in diesem Dialogfeld festgelegten Einstellung genehmigt oder abgelehnt. Diese Anforderungen werden nicht an die URL-Filterungsserver gesendet, für deren Verwendung der Router konfiguriert ist.

Wenn Sie einen teilweisen Domänennamen eingeben, zum Beispiel .Einedomäne.com, werden alle Anforderungen, die mit dieser Zeichenfolge enden, zum Beispiel www.Einedomäne.com/Produkte oder wwwin.Einedomäne.com/eng abhängig von der in diesem Dialogfeld festgelegten Einstellung genehmigt oder abgelehnt. Diese Anforderungen werden nicht an die URL-Filterungsserver gesendet, für deren Verwendung der Router konfiguriert ist.

URL-Liste importieren

In diesem Dialogfeld können Sie die URL-Liste überprüfen, die Sie von Ihrem PC auf den Router importieren, und festlegen, was Sie mit den einzelnen Einträgen in der Liste tun möchten. Wenn sich ein URL-Eintrag in diesem Dialogfeld nicht bereits auf dem Router befindet, können Sie ihn zu der Liste auf dem Router hinzufügen, indem Sie auf **Anhängen** klicken. Wenn sich ein URL-Eintrag bereits auf dem Router befindet, Sie ihn jedoch durch den Eintrag in diesem Dialogfeld ersetzen möchten, klicken Sie auf **Ersetzen**.

Die Kontrollkästchen in der Spalte **Importieren** sind alle standardmäßig aktiviert. Wenn Einträge dabei sind, die Sie nicht an den Router senden möchten, deaktivieren Sie das Kästchen neben diesen Einträgen. Wenn Sie alle Kontrollkästchen deaktivieren möchten, klicken Sie auf **Alles abwählen**. Wenn Sie auf **Alles auswählen** klicken, werden alle Kontrollkästchen aktiviert.

Anhängen fügt einen beliebigen aktivierten Eintrag zur URL-Liste hinzu, der nicht bereits in der Liste vorhanden ist. Wenn Sie versuchen, einen Eintrag hinzuzufügen, der sich bereits in der URL-Liste befindet, wird er nicht hinzugefügt, auch wenn die für die Domäne im Eintrag festgelegte Aktion sich von der Aktion unterscheidet, die sich bereits in der Liste befindet.

Verwenden Sie die Schaltfläche **Ersetzen**, um eine andere Aktion für einen Eintrag festzulegen, der sich bereits in der URL-Liste des Routers befindet. Wenn sich der aktivierte Eintrag nicht bereits in der Router-Liste befindet, hat die Aktion **Ersetzen** keine Auswirkung.

URL-Filter-Server

Der Router kann HTTP-Anforderungen an URL-Filterungsserver senden, die viel größere URL-Listen als der Router speichern können. Wenn der Router mit einer URL-Filter-Server-Liste konfiguriert ist, sendet er Anforderungen, die nicht mit Einträgen in der lokalen Liste übereinstimmen, an den verbundenen URL-Filter-Server und genehmigt die Anforderung oder lehnt sie ab, abhängig von der vom Server empfangenen Antwort. Wenn der Server ausfällt, mit dem der Router verbunden ist, kontaktiert der Router den jeweils nächsten Server in der Liste, bis er eine Verbindung herstellt.

Listen mit URL-Filter-Servern können zusammen mit den Listen lokaler URLs verwendet werden. Klicken Sie auf Vorrang bei der URL-Filterung, um zu erfahren, wie der Router beide Ressourcen verwenden kann.

Klicken Sie auf **Hinzufügen**, und wählen Sie entweder **Secure Computing** oder **Websense**, um den Servertyp festzulegen, den Sie hinzufügen.

Hinweis Die Cisco IOS-Software kann nur einen Typ von URL-Filterungsservern verwenden und lässt nicht zu, dass Sie einen Server eines anderen Typs zur Liste hinzufügen. Wenn beispielsweise eine URL-Filter-Server-Liste mit Websense-Servern auf dem Router konfiguriert ist, erhalten Sie eine Fehlermeldung, wenn Sie versuchen, einen Secure Computing-Server zur Liste hinzuzufügen. Wenn die URL-Filter-Server-Liste gegenwärtig einen Servertyp enthält, und Sie zu dem anderen Typ wechseln möchten, müssen Sie alle Servereinträge aus der Liste löschen, bevor Sie einen Eintrag des neuen Typs hinzufügen können.

In diesem Fenster wird die Konfiguration für jeden URL-Filter-Server in der Liste angezeigt. Eine Beschreibung der einzelnen Konfigurationswerte finden Sie unter Hinzufügen oder Bearbeiten von URL-Filter-Servern.

Hinzufügen oder Bearbeiten von URL-Filter-Servern

Geben Sie die Informationen zu dem URL-Filter-Server für Websense oder Secure Computing an.

IP-Adresse/Hostname

Geben Sie die IP-Adresse oder den Hostnamen des Servers ein. Wenn Sie einen Hostnamen eingeben, muss der Router eine Verbindung zu einem DNS-Server haben, damit der Hostname in eine IP-Adresse aufgelöst werden kann.

Richtung

Wählen Sie **Innen**, wenn der URL-Filter-Server zu einem inneren Netzwerk gehört. Hierbei handelt es sich meist um eines der Netzwerke, zu dem die LAN-Schnittstellen des Routers eine Verbindung herstellen. Wählen Sie **Außen**, wenn sich der Router in einem äußeren Netzwerk befindet. Hierbei handelt es sich meist um eines der Netzwerke, zu dem die WAN-Schnittstellen des Routers eine Verbindung herstellen. Die Standardeinstellung ist **Innen**.

Portnummer

Enthält automatisch die Standard-Portnummer für den Typ des URL-Filter-Servers, den Sie hinzufügen. Wenn Sie einen Websense-Server hinzufügen, lautet der Standardwert 15868. Wenn Sie einen Secure Computing-Server hinzufügen, lautet der Standardwert 4005. Ändern Sie diesen Wert zu dem Wert für den Port, an dem der Server kontrolliert, wenn sich dieser Wert vom Standardwert unterscheidet. In dieses Feld können Werte zwischen 1 und 65535 eingegeben werden.

Neuübertragungszählung

Optionales Feld. Geben Sie hier die Anzahl der Versuche ein, die der Router unternimmt, um die Anforderung neu zu übertragen, wenn der Server nicht antwortet. Der Standardwert ist zwei Versuche. In dieses Feld können Werte zwischen 1 und 10 eingegeben werden.

Neuübertragungs-Timeout

Optionales Feld. Geben Sie hier die Anzahl der Sekunden ein, die der Router auf eine Antwort vom Server wartet, bevor er die Anforderung neu überträgt. Der Standardwert ist 5 Sekunden.

Vorrang bei der URL-Filterung

Aktivieren Sie die URL-Filterung, indem Sie zu **Konfigurieren > Firewall und ACL > Anwendungssicherheit > URL-Filterung** wechseln und auf **URL-Filterung aktivieren** klicken. Sie können diesen Vorgang nur ausführen, wenn eine Richtlinie zu Anwendungssicherheit auf dem Router konfiguriert ist.

Wenn die URL-Filterung aktiviert ist, legt der Router folgendermaßen fest, wie eine HTTP-Anforderung behandelt wird:

- Wenn der URL in der Anforderung mit einem Eintrag in der Liste lokaler URLs auf dem Router übereinstimmt, genehmigt der Router die Anforderung auf Grundlage dieses Eintrags oder lehnt sie ab.
- Wenn der URL in der Anforderung mit einem der Einträge in der Liste lokaler URLs übereinstimmt, leitet der Router die HTTP-Anforderung an den URL-Filterungsserver weiter, mit dem er verbunden ist. Auf der Grundlage der Informationen, die der Server zurückgibt, wird die Anforderung genehmigt oder abgelehnt.

- Wenn der Zulassen-Modus deaktiviert ist und der Router keine Verbindung zu einem URL-Filter-Server herstellen kann, lehnt der Router die Anforderung ab. Der Zulassen-Modus ist standardgemäß deaktiviert.
- Wenn der Zulassen-Modus aktiviert ist und der Router keine Verbindung zu einem URL-Filter-Server herstellen kann, genehmigt der Router die Anforderung. Der Zulassen-Modus kann im Dialogfeld Globale Einstellungen bearbeiten aktiviert werden.

Es kann nur eine URL-Liste und eine URL-Filter-Server-Liste auf dem Router konfiguriert werden. Alle konfigurierten Richtlinien zur Anwendungssicherheit verwenden dieselbe URL-Liste und URL-Filter-Server-Liste. Diese Listen können in den Fenstern zur Anwendungssicherheit oder über die Optionen **Zusätzliche Aufgaben > URL-Filterung** verwaltet werden. Wenn alle Richtlinien zur Anwendungssicherheit gelöscht sind, können die URL-Liste und die URL-Filter-Server-Liste weiterhin in den Fenstern für zusätzliche Aufgaben verwaltet werden. Der Router führt jedoch nur dann eine URL-Filterung aus, wenn die URL-Filterung in einer Richtlinie zur Anwendungssicherheit aktiviert ist.

KAPITEL 36

Konfigurationsverwaltung

Mit Cisco SDM können Sie die Konfigurationsdatei des Routers bearbeiten und die Routerkonfiguration auf die werkseitigen Standardeinstellungen zurücksetzen. Da Sie beim direkten Bearbeiten der Konfigurationsdatei und Zurücksetzen des Routers auf die werkseitigen Standardeinstellungen die Verbindung zwischen PC und Router verlieren können, achten Sie darauf, dass Sie die Online-Hilfe für alle Bildschirme in diesem Bereich von Cisco SDM lesen.

Manuelles Bearbeiten der Konfigurationsdatei

Mit Cisco SDM können Sie die Routerkonfigurationsdatei bearbeiten, indem Sie einen Configuration Editor verwenden, um eine Konfigurationsdatei zu importieren oder Cisco IOS CLI-Befehle direkt einzugeben.

Cisco SDM unterstützt die häufigsten Cisco IOS-Befehle und -Schlüsselwörter, kann jedoch nicht jeden CLI-Befehl unterstützen. Wenn Sie mit der Cisco IOS-CLI vertraut sind und genau verstehen, wie die eingegebenen Konfigurationsbefehle die Funktionsweise des Routers und das Netzwerk, in dem sich der Router befindet, beeinflussen, stellen Sie möglicherweise fest, dass die Verwendung des Configuration Editor schneller ist als die Verwendung von Cisco SDM-Dialogfeldern. Wenn Sie eine Konfiguration hinzufügen möchten, die von Cisco SDM nicht unterstützt wird, müssen Sie dies entweder mit dem Config Editor tun oder eine Telnet-Sitzung auf dem Router öffnen und die Cisco IOS-CLI verwenden.

Durch die Verwendung des Config Editor wird die Cisco SDM-Validierung umgangen. Cisco SDM gibt zwar IOS-Fehlermeldungen zurück, es kann jedoch Ihre Konfigurationsänderungen nicht mit der aktiven Konfiguration vergleichen und Sie über daraus entstehende Konflikte informieren. Wenn Sie beispielsweise Cisco SDM-Dialogfelder zur Eingabe einer VPN-Konfiguration auf einem Router verwenden, der bereits über eine Firewall-Konfiguration verfügt, untersucht Cisco SDM die Firewall, ermittelt die Zulassungsanweisungen, die hinzugefügt werden müssen, damit VPN-Datenverkehr passieren kann, und richtet diese Anweisungen für Sie ein. Wenn Sie jedoch den Config Editor verwenden, müssen Sie ermitteln, welche Konflikte auftreten können, indem Sie die vorhandene Konfiguration untersuchen und zusätzliche Änderungen vornehmen, die erforderlich sind, um diese Konflikte zu lösen. Überwachen Sie anschließend das Verhalten des Routers, um festzustellen, ob der Datenverkehr nach Ihren Vorstellungen abgewickelt wird.

Es ist zwar nicht erforderlich, wird jedoch dringend empfohlen, dass Sie die Sicherung der aktuellen Konfiguration durch Cisco SDM zulassen. Wenn Cisco SDM diese Sicherung durchführt, verwendet es jedes Mal denselben Dateinamen und überschreibt die jeweils frühere Version der Backup-Datei.

Config Editor

Mit dem Config Editor können Sie die aktive Konfiguration anzeigen und Änderungen daran vornehmen, indem Sie bestimmte Befehle bearbeiten oder die gesamte Konfigurationsdatei durch eine Datei ersetzen, die Sie von Ihrem PC importieren. Sie können die aktive Konfiguration während der Durchführung von Änderungen anzeigen oder das gesamte Fenster nutzen, um die Konfiguration anzuzeigen, die Sie an den Router senden.

Aktive Konfiguration

In diesem Feld wird standardmäßig die aktive Konfiguration des Routers angezeigt. Sie können dieses Feld ausblenden, indem Sie in der oberen rechten Ecke des Fensters auf **Ausblenden** klicken. Zeigen Sie dieses Feld wieder an, indem Sie auf **Anzeigen** klicken.

Konfiguration bearbeiten

In diesem Feld können Sie die Konfiguration bearbeiten. Dieses Feld ist standardmäßig leer. Geben Sie die aktive Konfiguration des Routers in dieses Feld ein, indem Sie auf **Import > running config** (Aktive Konfiguration importieren) klicken. Geben Sie eine Konfigurationsdatei auf dem PC in dieses Feld ein, indem Sie auf **Import > config from PC** (Konfiguration vom PC importieren) klicken. Vergrößern Sie dieses Feld, indem Sie das Feld **Aktive Konfiguration** ausblenden.

Zusammenführen mit aktiver Konfiguration

Wenn Sie die Änderungen, die Sie im Feld **Konfiguration bearbeiten** vorgenommen haben, mit der aktiven Routerkonfiguration zusammenführen möchten, klicken Sie auf **Mit aktiver Konfiguration zusammenführen**. Die Änderungen werden an den Router gesendet und sofort wirksam, nachdem der Router sie empfangen hat.

Ersetzen der aktiven Konfiguration

Wenn Sie die aktive Routerkonfiguration durch den Inhalt des Felds **Konfiguration bearbeiten** ersetzen möchten, klicken Sie auf **Aktive Konfiguration ersetzen**. Verwenden Sie diese Schaltfläche nur, wenn Sie in das Feld **Konfiguration bearbeiten** eine Konfiguration eingegeben haben, die Sie vom Router importiert und bearbeitet oder von Ihrem PC importiert haben.

Wiederherstellen

Wenn Sie die aktive Konfiguration vor der Verwendung des Config Editor gespeichert haben, können Sie diese Konfiguration durch Klicken auf diese Schaltfläche auf dem Router speichern. Die wiederhergestellte Konfiguration wird in die Startkonfiguration des Routers kopiert und der Router neu geladen. Wenn keine Sicherungskopie der Routerkonfiguration vorhanden ist, zeigt Cisco SDM eine Meldung an, die Sie darüber informiert, dass die Konfiguration nicht wiederhergestellt werden kann.

Auf werksseitige Einstellungen zurücksetzen

Sie können die Konfiguration des Routers auf die werksseitigen Einstellungen zurücksetzen und die aktuelle Konfiguration zur späteren Verwendung in einer Datei speichern. Wenn Sie die LAN-IP-Adresse des Routers vom werksseitig eingestellten Wert 10.10.10.1 geändert haben, wird die Verbindung zwischen dem Router und dem PC getrennt, da diese IP-Adresse wieder in 10.10.10.1 geändert wird, wenn Sie die Einstellungen zurücksetzen.

Hinweis

- Die Funktion für das Zurücksetzen auf werksseitige Einstellungen wird nicht für Cisco Router der Serien 3620, 3640, 3640A und 7000 unterstützt.
- Die Funktion **Auf werkseitige Einstellungen zurücksetzen** wird nicht unterstützt, wenn Sie eine auf dem Computer installierte Kopie von Cisco SDM ausführen.

Bevor Sie beginnen, sollten Sie wissen, wie Sie Ihrem PC eine statische IP-Adresse im 10.10.10.0-Subnetz zuweisen können, sodass Sie die Verbindung wieder herstellen können, nachdem Sie die Einstellungen zurückgesetzt haben. Die werksseitige Konfiguration umfasst keine DHCP-Serverkonfiguration im Router, und der Router weist dem PC keine IP-Adresse zu. Zusätzlich beschränkt die werkseitige Konfiguration den HTTP- oder HTTPS-Zugriff auf den Router auf die LAN-Schnittstelle und auf das auf dieser Schnittstelle definierte interne Subnetz. Nachdem Sie einmal auf den Router zugegriffen haben, können Sie die standardmäßige IP-Adresse des Routers ändern und auf das Zulassen von Remote-Zugriff einstellen.

Anleitung zum Zuweisen einer dynamischen oder statischen IP-Adresse zum PC nach dem Zurücksetzen der Einstellungen

Wenn Sie Cisco SDM nach dem Zurücksetzen der Einstellungen verwenden möchten, müssen Sie dem PC eine statische oder dynamische IP-Adresse zuweisen. Diese richtet sich nach Ihrem Routertyp. Verwenden Sie die folgende Tabelle, um den Adressentyp zu ermitteln, der dem PC zugewiesen werden muss.

Router, die dynamische Adressen erfordern	Router, die statische Adressen erfordern
SB10x Cisco 83x, 85x, und 87x Cisco 1701, 1710 und 171x Cisco 180x und 181x	Cisco 1721, 1751 und 1760 Cisco 1841 Cisco 2600XM, und 2691 Cisco 28xx, 36xx, 37xx, und 38xx

Der Prozess der Zuweisung einer statischen oder dynamischen IP-Adresse zum PC richtet sich nach der vom PC ausgeführten Version von Microsoft Windows.

Hinweis Konfigurieren Sie den PC erst dann neu, wenn Sie den Router zurückgesetzt haben.

Microsoft Windows NT

Doppelklicken Sie in der Systemsteuerung auf das Symbol **Netzwerk**, um das Fenster **Netzwerk** anzuzeigen. Klicken Sie auf **Protokolle**, wählen Sie den ersten TCP/IP-Protokolleintrag aus, und klicken Sie auf **Eigenschaften**. Wählen Sie im Fenster **Eigenschaften** den für diese Verbindung verwendeten Ethernet-Adapter aus. Klicken Sie auf **IP-Adresse automatisch beziehen**, um eine dynamische IP-Adresse zu erhalten. Klicken Sie für eine statische IP-Adresse auf **IP-Adresse angeben**. Geben Sie die IP-Adresse 10.10.10.2 oder eine beliebige andere Adresse aus dem Subnetz 10.10.10.0 ein, die größer als 10.10.10.1 ist. Geben Sie das Subnetz 255.255.255.248 ein. Klicken Sie auf **OK**.

Microsoft Windows 98 und Microsoft Windows ME

Doppelklicken Sie in der Systemsteuerung auf das Symbol **Netzwerk**, um das Fenster **Netzwerk** anzuzeigen. Doppelklicken Sie auf den TCP/IP-Protokolleintrag mit dem Ethernet-Adapter, der für diese Verbindung verwendet wird, um die TCP/IP-**Eigenschaften** anzuzeigen. Klicken Sie in der Registerkarte **IP-Adresse** auf **IP-Adresse automatisch beziehen**, um eine dynamische IP-Adresse zu erhalten. Klicken Sie für eine statische IP-Adresse auf **IP-Adresse angeben**. Geben Sie die IP-Adresse 10.10.10.2 oder eine beliebige andere Adresse aus dem Subnetz 10.10.10.0 ein, die größer als 10.10.10.1 ist. Geben Sie das Subnetz 255.255.255.248 ein. Klicken Sie auf **OK**.

Microsoft Windows 2000

Wählen Sie in der Systemsteuerung **Netzwerk- und DFÜ-Verbindungen/LAN-Verbindung**. Wählen Sie im Feld **Verbindung herstellen unter Verwendung von** den Ethernet-Adapter aus. Wählen Sie **Internetprotokoll**, und klicken Sie auf **Eigenschaften**. Klicken Sie auf **IP-Adresse automatisch beziehen**, um eine dynamische IP-Adresse zu erhalten. Klicken Sie für eine statische IP-Adresse auf **IP-Adresse angeben**. Geben Sie die IP-Adresse 10.10.10.2 oder eine beliebige andere Adresse aus dem Subnetz 10.10.10.0 ein, die größer als 10.10.10.1 ist. Geben Sie das Subnetz 255.255.255.248 ein. Klicken Sie auf **OK**.

Microsoft Windows XP

Klicken Sie auf **Start**, wählen Sie **Einstellungen**, **Netzwerkverbindungen**, und wählen Sie dann die LAN-Verbindung aus, die Sie verwenden möchten. Klicken Sie auf **Eigenschaften**, wählen Sie **Internetprotokoll TCP/IP**, und klicken Sie auf die Schaltfläche **Eigenschaften**. Klicken Sie auf **IP-Adresse automatisch beziehen**, um eine dynamische IP-Adresse zu erhalten. Klicken Sie für eine statische IP-Adresse auf **IP-Adresse angeben**. Geben Sie die IP-Adresse 10.10.10.2 oder eine beliebige andere Adresse aus dem Subnetz 10.10.10.0 ein, die größer als 10.10.10.1 ist. Geben Sie das Subnetz 255.255.255.248 ein. Klicken Sie auf **OK**.

So stellen Sie den Router auf die werksseitigen Einstellungen zurück

Schritt 1 Lassen Sie die Option **Aktive Konfiguration in PC speichern** in **Schritt 1** im Bildschirm aktiviert, und geben Sie einen Namen für die Konfigurationsdatei an. Cisco SDM liefert einen Standardpfad und -namen. Sie brauchen ihn nicht ändern, können dies jedoch tun.

Schritt 2 Lesen Sie sich die Informationen im Feld **Anleitung zur erneuten Verbindung** in **Schritt 2** im Bildschirm durch, sodass Sie nach dem Wiederherstellen der Einstellungen eine Verbindung für den Router herstellen können. Falls erforderlich, informieren Sie sich unter **Anleitung zum Zuweisen einer dynamischen oder statischen IP-Adresse zum PC nach dem Zurücksetzen der Einstellungen.**

Schritt 3 Klicken Sie auf **Router zurücksetzen**.

Schritt 4 Klicken Sie auf **Ja**, um das Zurücksetzen zu bestätigen.

Schritt 5 Folgen Sie den Anleitungen im Feld **Anleitung zur erneuten Verbindung**, **Schritt 2**, um eine erneute Verbindung herzustellen.

Durch das Zurücksetzen zur werksseitigen Standardkonfiguration wird die innere IP-Adresse des Routers zurück in 10.10.10.1 geändert. Wenn Sie sich das nächste Mal über den Browser am Router anmelden, geben Sie die IP-Adresse 10.10.10.1 im IP-Adressenfeld des Browserfeld ein.

This Feature Not Supported (Diese Funktion wird nicht unterstützt)

Dieses Fenster wird angezeigt, wenn eine Cisco SDM-Funktion nicht unterstützt wird. Das kann daran liegen, dass der Router ein Cisco IOS-Image verwendet, das diese Funktion nicht unterstützt, oder dass Cisco SDM auf einem Computer ausgeführt wird und die Funktion nicht unterstützen kann.

KAPITEL 37

Weitere Informationen...

Diese Themen bieten weitere Informationen zu Bereichen, die in der Cisco SDM-Online-Hilfe erläutert werden.

IP-Adressen und Subnetzmasken

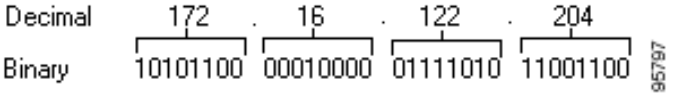
Dieses Thema bietet Hintergrundinformationen zu IP-Adressen und Subnetzmasken und zeigt Ihnen, wie diese Informationen bei der Eingabe von Adressen und Masken in Cisco SDM verwendet werden.

IP-Adressen der Version 4 weisen eine Länge von 32 Bits bzw. 4 Bytes auf. Dieser **Adressraum** wird verwendet, um Folgendes zu bestimmen:

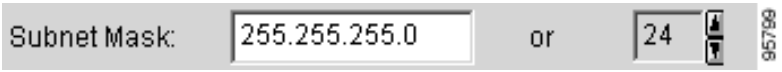
- Netzwerknummer
- Optionale Subnetznummer
- Eine Hostnummer

Hinweis Cisco SDM unterstützt nicht IP Version 6.

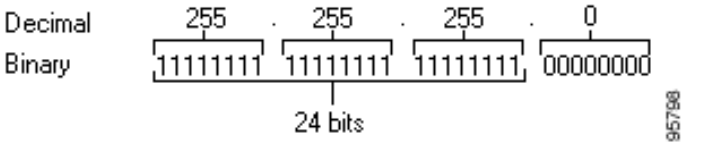
Cisco SDM erfordert die Eingabe der IP-Adressen im durch Punkte getrennten Dezimalformat. Dieses Format erleichtert den Benutzern das Lesen und die Handhabung der Adressen. Die 32 Bits werden in 4 Oktette gruppiert, die in Dezimalzahlen angezeigt werden, die durch Punkte oder *Dots* getrennt sind, wie z. B. 172.16.122.204. Die Dezimaladresse 172.16.122.204 steht für eine binäre IP-Adresse, die in der folgenden Abbildung dargestellt ist:



Die Subnetzmaske wird dazu verwendet anzugeben, wie viele der 32 Bits für die Netzwerknummer und wie viele für die Subnetznummer (bei Subnetzbildung) verwendet werden. Es handelt sich um eine binäre Maske mit 1 Bit an jeder Position, das von den Netzwerk- und Subnetznummern verwendet wird. Wie die bei der IP-Adresse handelt es sich um einen 32-Bit-Wert, der im Dezimalformat ausgedrückt wird. Die folgende Abbildung zeigt eine Subnetzmaske, die in Cisco SDM eingegeben wurde. Cisco SDM zeigt die Subnetzmaske und die entsprechende Anzahl an Bits in der Maske an.

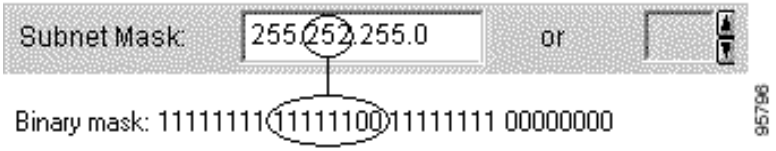


Diese in Cisco SDM eingegebenen Werte stehen für die binäre Maske, die in der folgenden Abbildung dargestellt wird:



Diese Subnetzmaske gibt an, dass die ersten 24 Bits der IP-Adresse für die Netzwerknummer und Subnetzmaske stehen und dass die letzten 8 Bits für die Hostnummer innerhalb dieses Netzwerks und Subnetzes stehen. Sie können die Maske im durch Punkte getrennten Dezimalformat, das im Feld **Subnetzmaske** angezeigt wird, eingeben, oder Sie können die Anzahl an Bits im entsprechenden Feld auswählen. Wenn Sie einen Wert in einem Feld eingeben oder auswählen, passt Cisco SDM automatisch das andere Feld an.

Cisco SDM zeigt eine Warnmeldung an, wenn Sie eine Dezimalmaske eingeben, die zu binären Nullwerten (0) im Netzwerk-/Subnetzbereich der Maske führt. Das folgende Subnetzmaskenfeld enthält einen Dezimalwert, der zu binären Nullwerten im Netzwerk-/Subnetznummernteil der Maske führen würde. Beachten Sie, dass das Bits-Feld auf der rechten Seite leer ist, um anzuzeigen, dass ein ungültiger Wert in das Feld **Subnetzmaske** eingegeben wurde.



Wenn eine Netzwerkadresse in den Cisco SDM-Fenstern angezeigt wird, wird die zugehörige IP-Adresse und Subnetzmaske eventuell im Netzwerkadressen-/Subnetz-Bits-Format angezeigt, wie im folgenden Beispiel dargestellt:

```
172.28.33.0/24
```

Die Netzwerkadresse in diesem Beispiel ist 172.28.33.0. Die Zahl 24 zeigt die Anzahl der verwendeten Subnetz-Bits an. Sie können sich diese als Kurzform der entsprechenden Subnetzmaske of 255.255.255.0 vorstellen.

Adressen, die im öffentlichen Internet verwendet werden, müssen für die Zeitdauer ihrer Nutzung eindeutig sein. In privaten Netzwerken sind die Adressen eventuell nur im privaten Netzwerk oder Subnetz eindeutig.

Adressen können auch unter Verwendung von Schemata, wie NAT und PAT übersetzt werden, und können temporär unter Verwendung von DHCP zugewiesen werden. Sie können Cisco SDM verwenden, um NAT, PAT und DHCP zu konfigurieren.

Hostfeld und Netzwerkfeld

Dieses Thema erläutert, wie Host- oder Netzwerkinformationen in Fenstern bereitgestellt werden, über die Sie Netzwerk- oder Hostadressen bzw. Hostnamen angeben können.

Geben Sie das Netzwerk oder den Host an.

Typ

Einer der folgenden Typen:

- **Ein Netzwerk** – Wenn Sie diesen Typ wählen, geben Sie eine Netzwerkadresse in das Feld **IP-Adresse** ein. Beachten Sie, dass Sie mit der Platzhaltermaske eine Netzwerknummer eingeben können, die mehrere Subnetze angeben kann.
- **Ein Hostname oder eine IP-Adresse** – Wenn Sie diesen Typ wählen, geben Sie eine Host-IP-Adresse oder einen Hostnamen im nächsten Feld an.
- **Beliebige IP-Adresse** – Wenn Sie diesen Typ wählen, wird die von Ihnen angegebene Aktion allen Hosts oder Netzwerken zugewiesen.

IP-Adresse/Platzhaltermaske

Geben Sie eine Netzwerkadresse und dann die Platzhaltermaske ein, um anzugeben, zu welchem Teil eine Übereinstimmung der Netzwerkadresse erforderlich ist.

Wenn Sie z. B. die Netzwerkadresse 10.25.29.0 und die Platzhaltermaske 0.0.0.255 eingeben, werden alle Java Applets mit einer Quelladresse, die 10.25.29 enthält, gefiltert. Wenn die Platzhaltermaske 0.0.255.255 lautet, werden alle Java Applets mit einer Quelladresse, die 10.25 enthält, gefiltert.

Hostname/IP

Dieses Feld wird angezeigt, wenn Sie **Ein Hostname oder eine IP-Adresse** als Typ ausgewählt haben. Wenn Sie einen Hostnamen eingeben, muss ein DNS-Server im Netzwerk verfügbar sein, der den Hostnamen in eine IP-Adresse auflösen kann.

Verfügbare Schnittstellenkonfigurationen

Die Konfigurationstypen, die für jeden Schnittstellentyp verfügbar sind, werden in der folgenden Tabelle aufgeführt.

Wenn Sie dieses ausgewählt haben:	Können Sie Folgendes hinzufügen:
Eine Ethernet-Schnittstelle	• Eine PPPoE-Verbindung • Eine Tunnelschnittstelle • Eine Loopback-Schnittstelle
Eine der folgenden Konfigurationen: • Ethernet mit einer PPPoE-Verbindung • Dialer-Schnittstelle, die mit einer ADSL- oder G.SHDSL-Konfiguration verknüpft ist • Serielle Schnittstelle mit einer PPP- oder HDLC-Konfiguration • Serielle Unterschnittstelle mit einer Frame Relay-Konfiguration • Nicht unterstützte WAN-Schnittstelle	• Eine Tunnelschnittstelle • Eine Loopback-Schnittstelle
Eine ATM-Schnittstelle ohne Kapselung	• Eine ADSL-Schnittstelle • Eine G.SHDSL-Schnittstelle • Einen Tunnel oder Loopback für eine der oben aufgeführten Konfigurationen

Eine serielle Schnittstelle	• Eine Frame Relay-Verbindung • Eine PPP-Verbindung • Eine Tunnelschnittstelle • Eine Loopback-Schnittstelle
Eine ATM-Unterschnittstelle Eine Ethernet-Unterschnittstelle Eine Dialer-Schnittstelle, die nicht mit einer ATM-Schnittstelle verknüpft ist Einen Loopback Einen Tunnel	• Eine Tunnelschnittstelle • Eine Loopback-Schnittstelle

DHCP-Adressen-Pools

Die IP-Adressen, die der DHCP-Server zuweist, werden von einem allgemeinen Pool bezogen, den Sie konfigurieren, indem der Bereich für die Start-IP-Adressen und der Bereich für die End-IP-Adressen angegeben wird.

Der von Ihnen angegebene Adressenbereich sollte sich innerhalb des folgenden privaten Adressenbereichs befinden:

- 10.1.1.1 bis 10.255.255.255
- 172.16.1.1 bis 172.31.255.255

Der von Ihnen angegebene Adressenbereich muss sich auch im selben Subnetz wie die IP-Adresse der LAN-Schnittstelle befinden. Der Bereich kann maximal für 254 Adressen stehen. Die folgenden Beispiele sind gültige Bereiche:

- 10.1.1.1 bis 10.1.1.254 (wenn sich die LAN-IP-Adresse im Subnetz 10.1.1.0 befindet)
- 172.16.1.1 bis 172.16.1.254 (wenn sich die LAN-IP-Adresse im Subnetz 172.16.1.0 befindet)

Cisco SDM konfiguriert den Router so, dass die IP-Adresse der LAN-Schnittstelle automatisch aus dem Pool ausgeschlossen wird.

Reservierte Adressen

Die folgenden Adressen dürfen nicht in dem von Ihnen angegebenen Adressenbereich verwendet werden:

- Die Netzwerk-/Subnetz-IP-Adresse
- Die Broadcast-Adresse im Netzwerk

Bedeutung der Schlüsselwörter Zulassen und Verweigern

Regeleinträge können in Zugriffsregeln, NAT-Regeln, IPSec-Regeln und in Zugriffsregeln, die mit Routenzuordnungen verknüpft sind, verwendet werden. **Zulassen** und **Verweigern** haben unterschiedliche Bedeutungen, je nach dem Regeltyp, in dem diese Schlüsselwörter verwendet werden.

Regeltyp	Bedeutung von Zulassen	Bedeutung von Verweigern
Zugriffsregel	Zulassen von eingehendem und ausgehendem Datenverkehr, für den eine Übereinstimmung besteht, in der Schnittstelle, auf die die Regel angewendet wurde	Entfernen von Datenverkehr, für den eine Übereinstimmung besteht
NAT-Regel	Übersetzen der IP-Adresse von Datenverkehr, für den eine Übereinstimmung besteht, in die angegebene innere lokale Adresse oder äußere lokale Adresse	Adresse wird nicht übersetzt.
IPSec-Regel (Nur erweitert)	Verschlüsseln von Datenverkehr mit Adresse, für die eine Übereinstimmung besteht	Datenverkehr wird nicht verschlüsselt. Kann unverschlüsselt gesendet werden.
Zugriffsregel, die in Routenzuordnung verwendet wird	Schützen von Adressen, für die eine Übereinstimmung besteht, vor NAT-Übersetzung	Kein Schützen von Adressen, für die eine Übereinstimmung besteht, vor NAT-Übersetzung

Dienste und Ports

Dieses Thema listet die Dienste, die Sie in Regeln angeben können, sowie ihre zugehörigen Portnummern auf. Es enthält darüber hinaus eine kurze Beschreibung von jedem Dienst.

Dieses Thema ist in folgende Bereiche unterteilt:

TCP-Dienste

TCP-Dienst	Portnum-mer	Beschreibung
bgp	179	Border Gateway Protocol. BGP tauscht Erreichbarkeitsinformationen mit anderen Systemen aus, die das BGP-Protokoll verwenden.
chargen	19	Zeichengenerator (Character Generator)
cmd	514	Remote-Befehle (Remote Commands). Ähnlich wie exec mit der Ausnahme, dass cmd über eine automatische Authentifizierung verfügt.
daytime	13	Tageszeit
discard	9	Nicht übernehmen
domain	53	Domänennamensserver. System, das im Internet verwendet wird, um Namen von Netzwerkknoten in Adressen zu übersetzen.
echo	7	Echo-Anforderung. Meldung, die gesendet wird, wenn ein Ping-Befehl ausgegeben wird.
exec	512	Ausführung eines Remote-Prozesses

TCP-Dienst	Portnum-mer	Beschreibung
finger	79	Finger. Anwendung, mit der festgestellt werden kann, ob eine Person über ein Konto auf einer bestimmten Internetsite verfügt.
ftp	21	File Transfer Protocol. Protokoll der Anwendungsschicht, das für die Übertragung von Dateien zwischen Netzwerkknoten verwendet wird.
ftp-data	20	FTP-Datenverbindungen
gopher	70	Gopher. Ein verteiltes Dokumentsendesystem
hostname	101	Hostname des NIC-Servers
ident	113	Identifizierungsprotokoll
irc	194	Internet Relay Chat. Ein weltweit genutztes Protokoll, mit dem Benutzer Textmitteilungen untereinander in Echtzeit austauschen können.
klogin	543	Kerberos-Anmeldung (Kerberos Login). Kerberos ist ein Entwicklungsstandard für die Authentifizierung von Netzwerkbenutzern.
kshell	544	Kerberos-Shell.
login	513	Anmeldung
lpd	515	Zeilendruckdämon (Line Printer Daemon). Ein Protokoll, das zum Senden von Druckaufträgen innerhalb von UNIX-Systemen verwendet wird.
nntp	119	Netzwerknachrichtenübertragungs-Protokoll (Network News Transport Protocol)
pim-auto-rp	496	Protokollunabhängiges Multicast-Auto-RP (Protocol-Independent Multicast Auto-RP). PIM ist eine Multicast-Routing-Architektur, die das Hinzufügen von Multicast-IP-Routing zu bestehenden IP-Netzwerken ermöglicht.
pop2	109	Post Office Protocol v2. Protokoll, das Client-E-Mail-Anwendungen verwenden, um E-Mails von Mailservern abzurufen.
pop3	110	Post Office Protocol v3

TCP-Dienst	Portnum-mer	Beschreibung
smtp	25	Simple Mail Transport Protocol. Internetprotokoll, das E-Mail-Dienste bereitstellt.
sunrpc	111	SUN-Remote-Verfahrensaufruf (SUN Remote Procedure Call). Siehe rpc.
Syslog	514	Systemprotokoll (System Log).

UDP-Dienste

UDP-Dienst	Portnum-mer	Beschreibung
biff	512	Wird von Mailsystemen verwendet, um Benutzer zu benachrichtigen, wenn neue Mails empfangen wurden
bootpc	69	Bootstrap Protocol-(BOOTP-)Client
bootps	67	Bootstrap Protocol-(BOOTP-)Server
discard	9	Nicht übernehmen
dnsix	195	DNSIX-Sicherheitsprotokollprüfung (DNSIX Security Protocol Auditing)
domain	53	Domänennamensserver (DNS)
echo	7	Siehe echo.
isakmp	500	Internet Security Association- und Schlüsselverwaltungsprotokoll (Internet Security Association and Key Management Protocol)
mobile-ip	434	Mobile IP-Registrierung
nameserver	42	IEN116-Namensdienst (nicht mehr gebräuchlich)
netbios-dgm	138	NetBios-Datagrammdienst. Grundlegendes Netzwerk-Eingabe-/Ausgabesystem (Network Basic Input Output System). Ein API, das von Anwendungsanforderungsdiensten von Netzwerkprozessen niedrigerer Ebenen verwendet wird.
netbios-ns	137	NetBios-Namensdienst
netbios-ss	139	NetBios-Sitzungsdienst
ntp	123	Network Time Protocol. TCP-Protokoll, das eine exakte lokale Zeitangabe sicherstellt, nutzt Radio- und Atomuhren im Internet als Referenz.

UDP-Dienst	Portnum-mer	Beschreibung
pim-auto-rp	496	Protokollunabhängiges Multicast, Reverse-Path-Leitung, hohe Dichte (Protocol Independent Multicast, Reverse Path Flooding, Dense Mode)
rip	520	Routing Information Protocol. Ein Protokoll, das verwendet wird, um Routeninformationen zwischen Routern auszutauschen.
snmp	161	Simple Network Management Protocol. Ein Protokoll, das für die Überwachung und Steuerung von Netzwerkgeräten verwendet wird.
snmptrap	162	SNMP-Trap. Eine Systemverwaltungsbenachrichtigung über ein Ereignis, dass im Remote-Verwaltungssystem aufgetreten ist.
sunrpc	111	SUN-Remote-Verfahrensaufruf (SUN Remote Procedure Call). RPCs sind Verfahrensaufrufe, die von Clients erstellt oder angegeben und auf Servern ausgeführt werden. Die Ergebnisse werden über das Netzwerk an den Client zurückgegeben.
Syslog	514	Systemprotokolldienst (System Log Service).
tacacs	49	Terminalzugriffs-Controller-Zugriffssteuerungssystem (Terminal Access Controller Access Control System). Authentifizierungsprotokoll, das Remote-Zugriffsauthentifizierung und verwandte Dienste, wie Logging, bereitstellt.
talk	517	Talk. Ein Protokoll, das ursprünglich für die Kommunikation zwischen Teletyp-Terminals entwickelt wurde, jetzt aber ein Rendezvous-Port von dem aus eine TCP-Verbindung hergestellt werden kann.
tftp	69	Trivial File Transfer Protocol. Vereinfachte Version von FTP, mit der Dateien zwischen Netzwerkknoten übertragen werden.
time	37	Zeit
who	513	Port für Datenbanken, der anzeigt, wer an Geräten in einem lokalen Netzwerk angemeldet ist und wie das Gerät durchschnittlich ausgelastet ist
xdmcp	177	X-Display Manager Client Protocol. Ein Protokoll, das für die Kommunikation zwischen X-Displays (Clients) und X-Display-Managern verwendet wird.
non500-isakmp	4500	Internet Security Association- und Schlüsselverwaltungsprotokoll (Internet Security Association and Key Management Protocol). Dieses Schlüsselwort wird verwendet, wenn eine Floating-Übertragung über NAT-Ports hinweg erforderlich ist.

ICMP-Meldungstypen

ICMP-Meldungen	Portnum-mer	Beschreibung
alternate-address	6	Alternative Hostadresse
conversion-error	31	Wird gesendet, um einen Datagrammkonvertierungsfehler zu melden
echo	8	Meldungstyp, der gesendet wird, wenn ein Ping-Befehl ausgegeben wird
echo-reply	0	Antwort auf eine Echo-Anforderungsmeldung (Ping)
information-reply	16	Nicht mehr gebräuchlich. Antwort auf Mitteilungen, die vom Host gesendet wurden, um die Nummer des Netzwerks zu ermitteln, in dem er sich befindet. Ersetzt durch DHCP.
information-request	15	Nicht mehr gebräuchlich. Mitteilung, die vom Host gesendet wurde, um die Nummer des Netzwerks zu ermitteln, in dem er sich befindet. Ersetzt durch DHCP.
mask-reply	18	Antwort auf Mitteilungen, die vom Host gesendet wurden, um die Netzwerkmaske des Netzwerks zu ermitteln, in dem er sich befindet.
mask-request	17	Nicht mehr gebräuchlich. Mitteilung, die vom Host gesendet wurde, um die Netzwerkmaske des Netzwerks zu ermitteln, in dem er sich befindet.
mobile-redirect	32	Mobile Host-Redirect-Meldung. Wird gesendet, um einen mobilen Host über einen besseren First Hop-Knoten im Pfad zu einem Ziel zu informieren.
parameter-problem	12	Mitteilung, die als Antwort auf ein Paket generiert wird, für das ein Problem im Header besteht
redirect	5	Wird gesendet, um einen Host über einen besseren First Hop-Knoten im Pfad zu einem Ziel zu informieren
router-advertisement	9	Wird in periodischen Abständen gesendet oder als Antwort auf eine Router-Solicitation (Routeranfrage)
router-solicitation	10	Mitteilungen, die gesendet werden, um Router dazu zu veranlassen, Router-Advertisement-Meldungen (Routerankündigungen) schnell zu generieren

ICMP-Meldungen	Portnum-mer	Beschreibung
source-quench	4	Wird gesendet, wenn nicht genügend Pufferspeicher verfügbar ist, um Pakete zur Next Hop-Übertragung in die Warteschlange zu stellen, oder wenn im Zielrouter nicht genügend Puffer verfügbar ist, da Pakete zu schnell ankommen, um verarbeitet zu werden
time-exceeded	11	Wird gesendet, um anzuzeigen dass das **Time-to-Live**-Feld des empfangenen Pakets, das die Zeitdauer angibt, bis zu der das Paket abgeliefert sein muss, den Wert Null erreicht hat
timestamp-reply	14	Antwort auf Anforderung eines Zeitstempels (Timestamp), der für die Synchronisierung zwischen zwei Geräten verwendet wird
timestamp-request	13	Anforderung eines Zeitstempels, der für die Synchronisierung zwischen zwei Geräten verwendet wird
traceroute	30	Mitteilung, die in einer Antwort an einen Host gesendet wird, der eine Traceroute-Anforderung ausgegeben hat
unreachable	3	Ziel nicht erreichbar. Paket kann nicht gesendet werden, die Ursache liegt nicht in einer Überlastung.

IP-Dienste

IP-Dienste	Portnum-mer	Beschreibung
aahp	51	
eigrp	88	Enhanced Interior Gateway Routing Protocol. Erweiterte, von Cisco entwickelte Version von IGRP.
esp	50	Prozessor für erweiterte Dienste (Extended Services Processor)
icmp	1	Internet Control Message Protocol. Netzwerkschichtprotokoll, das Fehler meldet und andere, für die Verarbeitung von IP-Paketen relevante Informationen bereitstellt.
igmp	2	Internet Group Management Protocol. Wird von IP-Hosts verwendet, um deren Multicast-Gruppenmitgliedschaften an benachbarte Multicast-Router zu melden.
ip	0	Internet Protocol. Netzwerkschichtprotokoll, das einen anbindungslosen Internetarbeitsdienst bietet.

IP-Dienste	Portnum-mer	Beschreibung
ipinip	4	IP-in-IP-Kapselung
nos	94	Netzwerkbetriebssystem (Network Operating System). Ein verteiltes Dateisystemprotokoll.
ospf	89	Open Shortest Path First. Ein hierarchischer Link-State-(Verbindungsstatus-)Routing-Algorithmus
pcp	108	Nutzlastkompressionsprotokoll (Payload Compression Protocol)
pim	103	Protokollunabhängiges Multicast (Protocol-Independent Multicast). PIM ist eine Multicast-Routing-Architektur, die das Hinzufügen von Multicast-IP-Routing zu bestehenden IP-Netzwerken ermöglicht.
tcp	6	Transmission Control Protocol. Verbindungsorientiertes Transportschichtprotokoll, das zuverlässige Vollduplex-Datenübertragung bietet.
udp	17	User Datagram Protocol. Verbindungsloses Transportschichtprotokoll im TCP/IP-Protokollstapel.

Dienste, die in Prüfregeln definiert werden können

Protokoll	Beschreibung
cuseeme	Videokonferenzprotokoll
fragment	Gibt an, dass die Regel eine Fragmentprüfung ausführen soll
ftp	Siehe ftp.
h323	Siehe H.323.
http	Siehe HTTP.
icmp	Siehe icmp.
netshow	NetShow. Ein Streaming-Video-Protokoll.
rcmd	Remote-Befehl (Remote Command). Ein Protokoll, das verwendet wird, wenn Befehle in einem Remote-System von einem lokalen System ausgeführt werden.
realaudio	RealAudio. Ein Streaming-Audio-Protokoll.

Protokoll	Beschreibung
rpc	Remote-Verfahrensaufruf (Remote Prodedure Call). RPCs sind Verfahrensaufrufe, die von Clients erstellt oder angegeben und auf Servern ausgeführt werden. Die Ergebnisse werden über das Netzwerk an den Client zurückgegeben.
rtsp	Echtzeit-Streaming-Protokoll (Real-Time Streaming Protocol). Ein Protokoll der Anwendungsebene, das verwendet wird, um das Senden von Daten mit Echtzeit-Eigenschaften zu steuern.
sip	Session Initiation Protocol. Sip ist ein Telefonieprotokoll, das verwendet wird, um Telefoniedienste und Datendienste zu integrieren.
skinny	Ein Telefonieprotokoll, dass Telefonieclients eine H.323-Kompatibilität ermöglicht
smtp	Siehe smtp.
sqlnet	Protokoll für netzwerkfähige Datenbanken
streamworks	StreamWorks-Protokoll. Ein Streaming-Video-Protokoll.
tcp	Siehe tcp.
tftp	Siehe tftp.
udp	Siehe udp.
vdolive	VDOLive-Protokoll. Ein Streaming-Video-Protokoll.

Weitere Informationen zu NAT

Dieser Abschnitt stellt Informationen in Beispielszenarios bereit, die Ihnen helfen, die erforderlichen Angaben in den Fenstern der NAT-Übersetzungsregeln zu machen, und andere Informationen, die erläutern, warum über die CLI erstellten NAT-Regeln nicht in Cisco SDM bearbeitet werden können.

Beispielszenarios für die statische Adressenübersetzung

Die folgenden Beispielszenarios zeigen Ihnen, wie Sie die Regeln für die statische Adressenübersetzung verwenden können.

Szenario 1

Sie müssen eine IP-Adressenzuordnung für einen einzelnen Host zu einer öffentlichen Adresse vornehmen. Die Adresse des Hosts ist 10.12.12.3. Die öffentliche Adresse ist 172.17.4.8.

Die folgende Tabelle zeigt, wie die Felder im Fenster Adressen-Übersetzungsregel hinzufügen verwendet werden.

Statisch/Dynamisch	Felder Von Schnittstelle übersetzen		Felder In Schnittstelle übersetzen	
	IP-Adresse	Netzwerkmaske	IP-Adresse	Weiterleitungs-Port
Statisch	10.12.12.3	Nicht ausfüllen	172.17.4.8	Nicht aktivieren

Ergebnis

Die Quelladresse 10.12.12.3 wird in die Adresse 172.17.4.8 für Pakete übersetzt, die den Router verlassen. Wenn es sich dabei um die einzige NAT-Regel in diesem Netzwerk handelt, ist 10.12.12.3 die einzige Adresse im Netzwerk, die übersetzt wird.

Szenario 2

Sie müssen für jede IP-Adresse in einem Netzwerk eine Zuordnung zu einer öffentlichen IP-Adresse vornehmen, und Sie möchten nicht für jede Zuordnung eine separate Regel erstellen. Die Quellnetzwerknummer ist 10.l2.12.0, und das Zielnetzwerk ist 172.17.4.0. In diesem Szenario müssen die Quell- und Zielnetzwerknummern jedoch nicht bekannt sein. Es genügt, die Hostadressen und eine Netzwerkmaske einzugeben.

Die folgende Tabelle zeigt, wie die Felder im Fenster Adressen-Übersetzungsregel hinzufügen verwendet werden.

Statisch/Dynamisch	Felder Von Schnittstelle übersetzen		Felder In Schnittstelle übersetzen	
	IP-Adresse	Netzwerkmaske	IP-Adresse	Weiterleitungs-Port
Statisch	10.12.12.35 (Host)	255.255.255.0	172.17.4.8 (Host)	Nicht aktivieren

Ergebnis

NAT leitet die **Übersetzen von**-Netzwerkadresse aus der IP-Hostadresse und der Subnetzmaske ab. NAT leitet die **Übersetzen in**-Netzwerkadresse aus der in den Feldern **Übersetzen von** eingegebenen Netzwerkmaske und aus der **Übersetzen in**-IP-Adresse ab. Die Quell-IP-Adresse in allen Paketen, die das ursprüngliche Netzwerk verlassen, wird in eine Adresse im Netzwerk 172.17.4.0 übersetzt.

Szenario 3

Sie möchten dieselbe globale IP-Adresse für mehrere Hosts im vertrauenswürdigen Netzwerk verwenden. Der eingehende Datenverkehr enthält eine andere Portnummer, die sich nach dem Zielhost richtet.

Die folgende Tabelle zeigt, wie die Felder im Fenster Adressen-Übersetzungsregel hinzufügen verwendet werden.

Statisch/Dynamisch	Felder Übersetzen von...		Felder Übersetzen in...	
	IP-Adresse	**Netzwerkmaske**	**IP-Adresse**	**Weiterleitungs-Port**
Statisch	10.12.12.3	Nicht ausfüllen	172.17.4.8	UDP Ursprünglicher Port 137 Übersetzter Port 139

Ergebnis

Die Quelladresse 10.12.12.3 wird in die Adresse 172.17.4.8 für Pakete übersetzt, die den Router verlassen. Die Portnummer im Feld **Weiterleitungs-Port** ändert sich von 137 in 139. Zurücklaufender Datenverkehr mit der Zieladresse 172.17.4.8 wird an Portnummer 137 des Hosts mit der IP-Adresse 10.12.12.3 geleitet.

Sie müssen einen separaten Eintrag für jede zu erstellende Host-/Portzuordnung vornehmen. Sie können dieselbe **Übersetzen in**-IP-Adresse für jeden Eintrag verwenden, Sie müssen jedoch eine andere **Übersetzen von**-IP-Adresse und unterschiedliche Portnummernsätze für jeden Eintrag verwenden.

Szenario 4

Übersetzen von-Quelladressen sollen die IP-Adresse verwenden, die der Fast Ethernet 0/1-Schnittstelle 172.17.4.8 zugewiesen ist. Zudem soll dieselbe globale IP-Adresse für mehrere Hosts im vertrauenswürdigen Netzwerk verwendet werden. Der eingehende Datenverkehr enthält eine andere Portnummer, die sich nach dem Zielhost richtet. Die folgende Tabelle zeigt, wie die Felder im Fenster **Adressenübersetzungsregel hinzufügen** verwendet werden:

Statisch/Dynamisch	Felder Übersetzen von...		Felder Übersetzen in...	
	IP-Adresse	**Netzwerkmaske**	**IP-Adresse**	**Weiterleitungs-Port**
Statisch	10.12.12.3	Nicht ausfüllen	FastEthernet 0/1	UDP Ursprünglicher Port 137 Übersetzter Port 139

Ergebnis

Die Quelladresse 10.12.12.3 wird in die Adresse 172.17.4.8 für Pakete übersetzt, die den Router verlassen. Die Portnummer im Feld **Weiterleitungs-Port** ändert sich von 137 in 139. Zurücklaufender Datenverkehr mit der Zieladresse 172.17.4.8 und der Portnummer 139 wird an den Port Nummer 137 des Hosts mit der IP-Adresse 10.12.12.3 geleitet.

Beispielszenarios für die dynamische Adressenübersetzung

Die folgenden Beispielszenarios zeigen Ihnen, wie Sie Regeln für die dynamische Adressenübersetzung verwenden können. Diese Szenarios gelten für die Richtungen **Von innen nach außen** oder **Von außen nach innen**.

Szenario 1

Übersetzen von-Quelladressen sollen die IP-Adresse verwenden, die der Fast Ethernet 0/1-Schnittstelle 172.17.4.8 zugewiesen ist. Es soll eine Port Address Translation (PAT) verwendet werden, um eine Unterscheidung mit Datenverkehr, der mit anderen Hosts verknüpft ist, vornehmen zu können. Die von Ihnen verwendete ACL-Regel für die Definition der **Übersetzen von**-Adressen ist wie nachfolgend angezeigt konfiguriert:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

Diese Zugriffsregel würde bei der Verwendung in einer NAT-Regel jeden Host im Netzwerk 10.10.10.0 für die Adressenübersetzung zulassen, mit Ausnahme des Hosts mit der Adresse 10.10.10.1.

Die folgende Tabelle zeigt, wie die Felder im Fenster Adressen-Übersetzungsregel hinzufügen verwendet werden.

Statisch/Dynamisch	Felder Übersetzen von...	Felder Übersetzen in...		
	ACL-Regel	Typ	Schnittstelle	Adressen-Pool
Dynamisch	7	Schnittstelle	FastEthernet0/1	Deaktiviert

Ergebnis

Für Datenverkehr von allen Hosts im Netzwerk 10.10.10.0 würde die Quell-IP-Adresse in 172.17.4.8 übersetzt werden. PAT würde verwendet werden, um eine Unterscheidung mit Datenverkehr, der mit anderen Hosts verknüpft ist, vornehmen zu können.

Szenario 2

Sie möchten, dass die in access-list 7 im vorherigen Szenario angegebenen Hostadressen Adressen von einem von Ihnen definierten Pool verwenden. Wenn die Adressen im Pool aufgebraucht sind, soll der Router PAT verwenden, um auf zusätzliche Anfragen nach Adressen aus dem Pool reagieren zu können.

Die folgende Tabelle zeigt an, wie die Felder im Fenster **Adressen-Pool** für dieses Szenario verwendet werden müssten.

Pool-Name	Port Address Translation	Felder IP-Adresse		Netzwerkmaske
Pool 1	Aktiviert	172.16.131.2	172.16.131.10	255.255.255.0

Die folgende Tabelle zeigt an, wie die Felder im Fenster **Adressenübersetzungsregel hinzufügen** für dieses Szenario verwendet werden müssten.

Statisch/Dynamisch	Felder Übersetzen von...	Felder Übersetzen in...		
	ACL-Regel	Typ	Schnittstelle	Adressen-Pool
Dynamisch	7	Adressen-Pool	Deaktiviert	Pool 1

Ergebnis

Die IP-Adressen der Hosts im Netzwerk 10.10.10.0 werden in IP-Adressen im Bereich von 172.16.131.2 bis 172.16.131.10 übersetzt. Wenn die Anforderungen nach Adressenübersetzungen die verfügbaren Adressen in Pool 1 übersteigen, wird dieselbe Adresse verwendet, um Folgeanfragen gerecht werden zu können, und PAT wird verwendet, um Unterscheidungen zwischen Hosts vornehmen zu können, die die Adresse verwenden.

Ursachen, warum Cisco SDM keine NAT-Regel bearbeiten kann

Eine zuvor konfigurierte NAT-Regel ist schreibgeschützt und kann nicht konfiguriert werden, wenn eine statische NAT-Regel unter Verwendung der folgenden Befehle konfiguriert wurde:

- Die Cisco IOS-Befehle **inside source static** und **destination**
- Der Befehl **inside source static network** mit einem der Schlüsselwörter **extendable**, **no-alias** oder **no-payload**
- Der Befehl **outside source static network** mit einem der Schlüsselwörter **extendable**, **no-alias** oder **no-payload**

- Der Befehl **inside source static tcp** mit einem der Schlüsselwörter **no-alias** oder **no-payload**
- Der Befehl **inside source static udp** mit einem der Schlüsselwörter **no-alias** oder **no-payload**
- Der Befehl **outside source static tcp** mit einem der Schlüsselwörter **no-alias** oder **no-payload**
- Der Befehl **outside source static udp** mit einem der Schlüsselwörter **no-alias** oder **no-payload**
- Der Befehl **inside source static** mit einem der Schlüsselwörter **no-alias**, **no-payload**, **extendable**, **redundancy**, **route-map** oder **vrf**
- Der Befehl **outside source static** mit einem der Schlüsselwörter **no-alias**, **no-payload**, **extendable** oder **add-route**
- Der Befehl **inside source static** mit dem Schlüsselwort **esp**
- Der Befehl **inside source static** mit dem Befehl **interface**

Eine dynamische NAT-Regel ist mit der Loopback-Schnittstelle konfiguriert.

Weitere Informationen zu VPN

Diese Themen enthalten weitere Informationen über VPN, DMVPN, IPSec und IKE.

Ressourcen unter Cisco.com

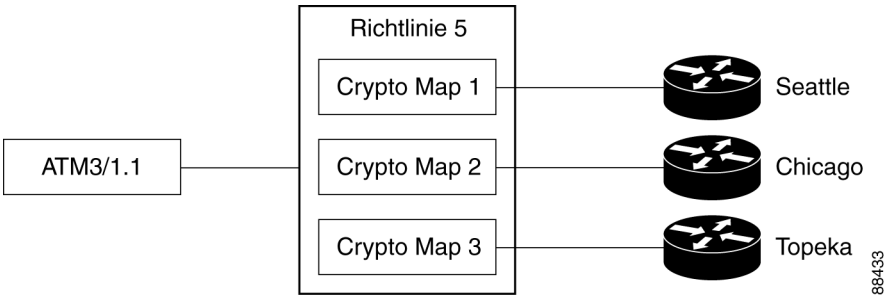
Über die folgenden Links erhalten Sie TAC-Ressourcen und andere Informationen zu VPN-Themen.

- How Virtual Private Networks Work
- Dynamic Multipoint IPSec VPNs
- TAC-authored articles on IPSec
- TAC-authored articles on Cisco SDM
- Security and VPN Devices
- IPSecurity Troubleshooting–Understanding and Using Debug Commands
- Field Notices

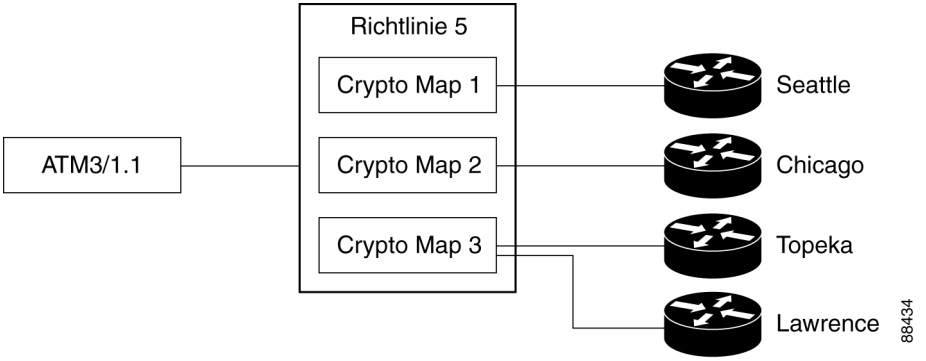
Weitere Informationen zu VPN-Verbindungen und IPSec-Richtlinien

Eine VPN-Verbindung ist eine Verknüpfung zwischen einer Routerschnittstelle und einer IPSec-Richtlinie. Der Baustein einer IPSec-Richtlinie ist die Crypto Map. Eine Crypto Map gibt Folgendes an: Einen Transformationssatz und andere Parameter zum Steuern der Verschlüsselung, die Identität eines oder mehrerer Peers und eine IPSec-Regel, die angibt, welcher Datenverkehr verschlüsselt wird. Eine IPSec-Richtlinie kann mehrere Crypto Maps enthalten.

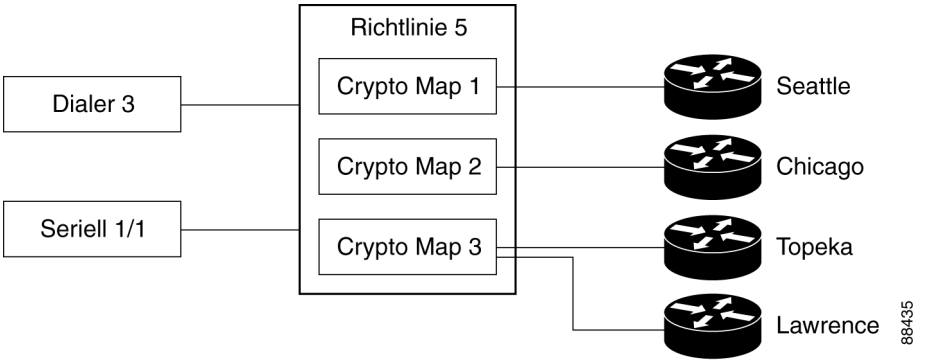
Das folgende Diagramm zeigt eine Schnittstelle (ATM 3/1.1) an, die mit einer IPSec-Richtlinie verknüpft ist. Die Richtlinie verfügt über drei Crypto Maps, von denen jede ein anderes Peer-System angibt. Die ATM 3/1.1-Schnittstelle ist daher mit drei VPN-Verbindungen verknüpft.



Eine Crypto Map kann mehr als einen Peer für eine Verbindung angeben. Das kann erforderlich sein, um Redundanz zu erzeugen. Das folgende Diagramm zeigt dieselbe Schnittstelle und Richtlinie an, die Crypto Map CM-3 gibt jedoch zwei Peers an: Topeka und Lawrence.



Eine Routerschnittstelle kann nur mit einer IPSec-Richtlinie verknüpft werden. Eine IPSec-Richtlinie kann jedoch mit mehreren Routerschnittstellen verknüpft werden, und eine Crypto Map kann mehr als einen Peer für eine Verbindung angeben. Das folgende Diagramm zeigt zwei Routerschnittstellen an, die mit einer Richtlinie und einer Crypto Map, die zwei Peers angibt, verknüpft sind:



In dieser Konfiguration bestehen sechs VPN-Verbindungen, da sowohl Dialer 3 als auch Serial 1/1 über Verbindungen zu Seattle, Chicago, Topeka und Lawrence verfügen. Cisco SDM würde die Verbindungen zu Topeka und Lawrence als eine Verbindung für beide Schnittstellen anzeigen.

Weitere Informationen zu IKE

IKE führt die folgenden Aufgaben aus:

- Authentifizierung
- Sitzungsaushandlung
- Schlüsselaustausch
- IPSec-Tunnelaushandlung und -Konfiguration

Authentifizierung

Die Authentifizierung ist wohl die wichtigste Aufgabe, die von IKE ausgeführt wird, und mit Sicherheit auch die komplizierteste. Immer wenn Aushandlungen stattfinden, ist es von größter Bedeutung zu wissen, mit wem die Aushandlung gerade ausgeführt wird. IKE kann eine von zahlreichen Methoden verwenden, um eine gegenseitige Authentifizierung von Parteien, die eine Aushandlung vornehmen, durchzuführen.

- **Pre-shared Key**. IKE verwendet eine Hash-Technik, um sicherzustellen, dass nur Parteien, die über denselben Schlüssel verfügen, IKE-Pakete verschicken können.
- **DSS oder digitale RSA-Signaturen**. IKE verwendet digitale Signaturverschlüsselung mit öffentlichem Schlüssel, um sicherzustellen, dass jede Partei auch wirklich die von ihr angegebene Identität besitzt.
- **RSA-Verschlüsselung**. IKE verwendet eine der beiden Methoden, um die Aushandlung in ausreichendem Maß zu verschlüsseln, sodass nur eine Partei mit dem korrekten privaten Schlüssel mit der Aushandlung fortfahren kann.

Hinweis Cisco SDM unterstützt die Authentifizierungsmethode **Pre-Shared Key**.

Sitzungsaushandlung

Während einer Sitzungsaushandlung erlaubt IKE den Parteien auszuhandeln, wie diese die Authentifizierung vornehmen und wie sie zukünftige Aushandlungen (d. h. IPSec-Tunnelaushandlungen) schützen möchten. Die folgenden Elemente werden ausgehandelt:

- **Authentifizierungsmethode**. Dies ist eine der oben aufgeführten Authentifizierungsmethoden.
- **Key Exchange Algorithm**. Dies ist eine mathematische Technik für den sicheren Austausch von kryptografischen Schlüsseln über ein öffentliches Medium (d. h. Diffie-Hellman). Die Schlüssel werden in Verschlüsselungs- und Paketsignaturalgorithmen verwendet.
  - **Verschlüsselungsalgorithmus**: DES, 3DES oder AES
  - **Paketsignaturalgorithmus**: MD5 oder SHA-1

Schlüsselaustausch

IKE verwendet die ausgehandelte Schlüsselaustauschmethode (siehe **Sitzungsaushandlung** oben), um genügend Bits an kryptografischem Schlüsselmaterial für zukünftige Transaktionen zu erstellen. Diese Methode stellt sicher, dass jede IKE-Sitzung durch einen neuen, sicheren Schlüsselsatz geschützt wird.

Authentifizierung, Sitzungsaushandlung und Schlüsselaustausch stellen Phase 1 einer IKE-Aushandlung dar.

IPSec-Tunnelaushandlung und -Konfiguration

Nachdem IKE die Aushandlung einer sicheren Methode zum Informationsaustausch abgeschlossen hat (Phase 1), wird IKE verwendet, um einen IPSec-Tunnel auszuhandeln. Dies wird in der IKE-Phase 2 durchgeführt. Bei diesem Austausch erstellt IKE neues zu verwendendes Schlüsselmaterial für den IPSec-Tunnel (entweder, indem als Grundlage die Schlüssel der IKE-Phase 1 verwendet werden oder indem ein neuer Schlüsselaustausch durchgeführt wird). Die Verschlüsselungs- und Authentifizierungsalgorithmen für diesen Tunnel werden ebenfalls ausgehandelt.

Weitere Informationen zu IKE-Richtlinien

Wenn die IKE-Aushandlung gestartet wird, sucht IKE nach einer IKE-Richtlinie, die in beiden Peers identisch ist. Der Peer, der die Aushandlung initiiert, sendet seine gesamten Richtlinien an den Remote-Peer, und der Remote-Peer versucht, eine Übereinstimmung zu finden. Der Remote-Peer führt die Suche nach einer Übereinstimmung durch, indem er seine Richtlinie mit der höchsten Priorität mit den vom anderen Peer erhaltenen Richtlinien vergleicht. Der Remote-Peer überprüft sämtliche seiner Richtlinien entsprechend der Prioritätsreihenfolge (die höchste Priorität zuerst), bis eine Übereinstimmung ermittelt wurde.

Eine Übereinstimmung erfolgt, wenn beide Richtlinien von beiden Peers dieselben Verschlüsselungs-, Hash-, Authentifizierungs- und Diffie-Hellman-Parameterwerte enthalten und wenn die Richtlinie des Remote-Peers eine Gültigkeitsdauer angibt, die kleiner oder gleich der Gültigkeitsdauer der Richtlinie ist, mit der der Vergleich durchgeführt wird. Wenn die Gültigkeitsdauer nicht identisch ist, wird die kürzere Gültigkeitsdauer von der Richtlinie des Remote-Peers angewendet.

Zulässige Transformationskombinationen

Um einen Transformationssatz zu definieren, geben Sie eine bis drei Transformationen an. Jede Transformation steht für ein IPSec-Sicherheitsprotokoll (AH oder ESP) und für einen Algorithmus, den Sie verwenden möchten. Wenn ein bestimmter Transformationssatz während Aushandlungen für IPSec Security Associations verwendet wird, muss der gesamte Transformationssatz (die Kombination aus Protokollen, Algorithmen und anderen Einstellungen) mit einem Transformationssatz im Remote-Peer übereinstimmen.

Die folgende Tabelle listet die zulässige Kombinationsauswahl von Transformationen für AH- und ESP-Protokolle auf.

AH-Transformation (***Eine auswählen***)	**ESP-Verschlüsselungs-transformation** (***Eine auswählen***)	**Authenti-fizierungs-transformation** (***Eine auswählen***)	**IP-Kompressions-transformation** (***Eine auswählen***)	**Beispiele** *(Insgesamt sind 3 Transformationen zulässig)*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	**1.** ah-md5-hmac **2.** esp-3des und esp-md5-hmac **3.** ah-sha-hmac, esp-des und esp-sha-hmac

In der folgenden Tabelle werden die einzelnen Transformationen beschrieben.

Transformation	**Beschreibung**
ah-md5-hmac	AH mit dem MD5-Authentifizierungsalgorithmus (HMAC-Variante)
ah-sha-hmac	AH mit dem SHA-Authentifizierungsalgorithmus (HMAC-Variante)
esp-des	ESP mit dem 56-Bit-DES-Verschlüsselungsalgorithmus
esp-3des	ESP mit dem 168-Bit-DES-Verschlüsselungsalgorithmus (3DES oder Tripel DES)
esp-null	Null-Verschlüsselungsalgorithmus
esp-seal	ESP mit Verschlüsselungsalgorithmus Software Encryption Algorithm (SEAL) mit 160-Bit-Schlüssel
esp-md5-hmac	ESP mit MD5-Authentifizierungsalgorithmus (HMAC-Variante)
es-aes-128	ESP mit Advanced Encryption Standard (AES). Verschlüsselung mit einem 128-Bit-Schlüssel
esp-aes-192	ESP mit AES. Verschlüsselung mit einem 192-Bit-Schlüssel
esp-aes-256	ESP mit AES. Verschlüsselung mit einem 256-Bit-Schlüssel

Transformation	Beschreibung
esp-sha-hmac	ESP mit SHA-Authentifizierungsalgorithmus (HMAC-Variante)
comp-lzs	IP-Kompression mit LZS-Algorithmus

Beispiele

Im Folgenden finden Sie Beispiele für zulässige Transformationskombinationen:

- ah-md5-hmac
- esp-des
- esp-3des und esp-md5-hmac
- ah-sha-hmac, esp-des und esp-sha-hmac
- comp-lzs

Ursachen, warum eine serielle Schnittstellen- oder Unterschnittstellenkonfiguration schreibgeschützt sein kann

Eine zuvor konfigurierte serielle Schnittstelle oder Unterschnittstelle ist schreibgeschützt und kann nicht konfiguriert werden, wenn Folgendes zutrifft:

- Die Schnittstelle ist mit den Cisco IOS-Befehlen **encapsulation ppp** und **ppp multilink ...** konfiguriert.
- Die Schnittstelle ist mit den Befehlen **encapsulation hdlc** und **ip address negotiated** konfiguriert.
- Die Schnittstelle ist Teil einer SERIAL_CSUDSU_56K WIC.
- Die Schnittstelle ist Teil einer Sync/Async-WIC, die mit dem Befehl **physical-layer async** konfiguriert ist.
- Die Schnittstelle ist mit dem Befehl **encapsulation frame-relay** mit einer IP-Adresse in der Hauptschnittstelle konfiguriert.
- Die Schnittstellenverschlüsselung ist nicht **hdlc**, **ppp** oder **frame-relay**.

- Der Befehl **encapsulation frame-relay ...** umfasst die Option **mfr ...**.
- Die Schnittstelle ist mit dem Befehl **encapsulation ppp** konfiguriert, die PPP-Konfiguration enthält jedoch nicht unterstützte Befehle.
- Die Schnittstelle ist mit den Befehlen **encapsulation frame-relay** und **frame-relay map ...** konfiguriert.
- Die Hauptschnittstelle ist mit den Befehlen **encapsulation frame-relay** und **frame-relay interface-dlci ...** konfiguriert.
- Die Hauptschnittstelle ist mit dem Befehl **encapsulation frame-relay** und die Unterschnittstelle mit dem Befehl **frame-relay priority-dlci-group ...** konfiguriert.
- Die Unterschnittstelle ist mit dem Befehl **interface-dlci ...** konfiguriert, der eines der Schlüsselwörter **ppp**, **protocol** oder **switched** enthält.
- Der Unterschnittstellentyp ist **Multipoint** statt **Point-to-Point**.
- Die Unterschnittstelle ist mit einer anderen Kapselung als **frame-relay** konfiguriert.

Ursachen, warum eine ATM-Schnittstellen- oder Unterschnittstellenkonfiguration schreibgeschützt sein kann

Eine zuvor konfigurierte ATM-Schnittstelle oder Unterschnittstelle ist schreibgeschützt und kann nicht konfiguriert werden, wenn Folgendes zutrifft:

- Sie verfügt über eine PVC-Verbindung mit dem Befehl **dialer pool-member**.
- Sie verfügt über eine PVC-Verbindung, bei der anhand des Befehls **protocol** nicht **ip** als Protokoll festgelegt wurde.
- Sie verfügt über eine PVC-Verbindung mit mehreren Befehlen **protocol ip**.
- Die Kapselung in der PVC-Verbindung ist weder **aal5mux** noch **aal5snap**.
- Das Kapselungsprotokoll in **aal5mux** lautet nicht **ip**.
- Die IP-Adresse ist nicht in der PVC-Verbindung mit dem Befehl **protocol ip** konfiguriert.
- Die Option **dial-on-demand** ist im Befehl **pppoe-client** konfiguriert.

- Es ist mehr als eine PVC-Verbindung in der Schnittstelle konfiguriert.
- Die Kapselung ist nicht im verknüpften Dialer angegeben oder lautet nicht **ppp**.
- Es ist keine IP-Adresse im verknüpften Dialer konfiguriert.
- VPDN ist erforderlich (wird dynamisch vom Cisco IOS-Abbild ermittelt), ist jedoch nicht für diese Verbindung konfiguriert.
- Der Betriebsmodus in einer SHDSL-Schnittstelle ist **CO** (nur ATM-Hauptschnittstelle).
- Es ist keine IP-Adresse in der Schnittstelle konfiguriert, und die Schnittstelle ist nicht für PPPoE konfiguriert (ATM-Unterschnittstellen).
- Die Schnittstelle verfügt über eine IP-Adresse, nicht jedoch über eine verknüpfte PVC-Verbindung.
- Die Schnittstelle verfügt über eine PVC-Verbindung, nicht jedoch über eine verknüpfte IP-Adresse, und ist nicht für PPPoE konfiguriert.
- Der Befehl **bridge-group** ist in der Schnittstelle konfiguriert.
- Die Hauptschnittstelle verfügt über eine oder mehrere PVC-Verbindungen und über eine oder mehrere Schnittstellen.
- Die Hauptschnittstelle ist nicht konfigurierbar (nur ATM-Unterschnittstellen).
- Es handelt sich um eine Multipoint-Schnittstelle (nur ATM-Unterschnittstellen).

Ursachen, warum eine Ethernet-Schnittstellenkonfiguration schreibgeschützt sein kann

Eine zuvor konfigurierte Ethernet-LAN- oder WAN-Schnittstelle ist schreibgeschützt und kann nicht konfiguriert werden, wenn Folgendes zutrifft:

- Die LAN-Schnittstelle wurde als DHCP-Server und mit einer IP-Hilfsadresse konfiguriert.

Ursachen, warum eine ISDN BRI-Schnittstellenkonfiguration schreibgeschützt sein kann

Eine zuvor konfigurierte ISDN BRI-Schnittstelle ist schreibgeschützt und kann nicht konfiguriert werden, wenn Folgendes zutrifft:

- Eine IP-Adresse ist mit der ISDN BRI-Schnittstelle verknüpft.
- Die in der ISDN BRI-Schnittstelle konfigurierte Kapselung ist nicht **ppp**.
- Der Befehl **dialer-group** oder **dialer string** ist in der ISDN BRI-Schnittstelle konfiguriert.
- **dialer pool-member** <*x*> ist in der ISDN BRI-Schnittstelle konfiguriert, die entsprechende Dialer-Schnittstelle <*x*> ist jedoch nicht vorhanden.
- Mehrere **dialer pool-member**-Befehle sind in der ISDN BRI-Schnittstelle konfiguriert.
- Der Befehl **dialer map** ist in der ISDN BRI-Schnittstelle konfiguriert.
- Die in der Dialer-Schnittstelle konfigurierte Kapselung ist nicht **ppp**.
- Entweder der Befehl **dialer-group** oder **dialer-pool** ist nicht in der Dialer-Schnittstelle konfiguriert.
- **dialer-group** <*x*> ist in der Dialer-Schnittstelle konfiguriert, der entsprechende Befehl **dialer-list** <*x*> **protocol** ist jedoch nicht konfiguriert.
- **dialer idle-timeout** <*num*> mit optionalem Schlüsselwort (either/inbound) ist in der Dialer-Schnittstelle konfiguriert.
- Befehl **dialer string** mit optionalem Schlüsselwort **class** ist in der Dialer-Schnittstelle konfiguriert.
- Wenn die ISDN BRI-Verbindung als Backupverbindung verwendet wird, wird die Backupverbindung als schreibgeschützt angezeigt, sobald die Konfiguration der Backupverbindung durch Cisco SDM durchgeführt wird, wenn eine der nachfolgend aufgeführten Bedingungen zutrifft:
  - Die Standardroute durch die primäre Schnittstelle wurde entfernt.
  - Die Standardroute der Sicherheitsschnittstelle ist nicht konfiguriert.
  - Die lokale IP-Richtlinie wurde entfernt.

- **track /rtr** oder **both** ist nicht konfiguriert.
- Routenzuordnung wurde entfernt.
- Die Zugriffsliste wurde entfernt, oder die Zugriffsliste wurde geändert (z. B. die Tracking-IP-Adresse wurde geändert).
- Die Cisco SDM-unterstützten Schnittstellen sind mit nicht unterstützten Konfigurationen konfiguriert.
- Die primären Schnittstellen werden nicht von Cisco SDM unterstützt.

Ursachen, warum eine Analogmodem-Schnittstellenkonfiguration schreibgeschützt sein kann

Eine zuvor konfigurierte Analogmodem-Schnittstelle ist schreibgeschützt und kann nicht konfiguriert werden, wenn Folgendes zutrifft:

- Eine IP-Adresse ist mit der asynchronen Schnittstelle verknüpft.
- Die in der asynchronen Schnittstelle konfigurierte Kapselung ist nicht **ppp**.
- Der Befehl **dialer-group** oder **dialer string** ist in der asynchronen Schnittstelle konfiguriert.
- Der Async-Modus **interactive** ist in der asynchronen Schnittstelle konfiguriert.
- **dialer pool-member** <*x*> ist in der asynchronen Schnittstelle konfiguriert, die entsprechende Dialer-Schnittstelle <*x*> ist jedoch nicht vorhanden.
- Es sind mehrere **dialer pool-member**-Befehle in der asynchronen Schnittstelle konfiguriert.
- Die in der Dialer-Schnittstelle konfigurierte Kapselung ist nicht **ppp**.
- Entweder der Befehl **dialer-group** oder **dialer-pool** ist nicht in der Dialer-Schnittstelle konfiguriert.
- **dialer-group** <*x*> ist in der Dialer-Schnittstelle konfiguriert, der entsprechende Befehl **dialer-list** <*x*> **protocol** ist jedoch nicht konfiguriert.
- **dialer idle-timeout** <*num*> mit optionalem Schlüsselwort (either/inbound) ist in der Dialer-Schnittstelle konfiguriert.

- Im Leitungskonfigurations-Sammelmodus ist **modem inout** nicht konfiguriert.
- Im Leitungskonfigurations-Sammelmodus ist **autoselect ppp** nicht konfiguriert.
- Wenn die Analogmodem-Verbindung als Backupverbindung verwendet wird, wird die Backupverbindung als schreibgeschützt angezeigt, sobald die Konfiguration der Backupverbindung durch Cisco SDM durchgeführt wird, wenn eine der nachfolgend aufgeführten Bedingungen zutrifft:
  - Die Standardroute durch die primäre Schnittstelle wurde entfernt.
  - Die Standardroute der Sicherheitsschnittstelle ist nicht konfiguriert.
  - Die lokale IP-Richtlinie wurde entfernt.
  - **track /rtr** oder **both** ist nicht konfiguriert.
  - Routenzuordnung wurde entfernt.
  - Die Zugriffsliste wurde entfernt, oder die Zugriffsliste wurde geändert (z. B. die Tracking-IP-Adresse wurde geändert).
  - Die Cisco SDM-unterstützten Schnittstellen sind mit nicht unterstützten Konfigurationen konfiguriert.
  - Die primären Schnittstellen werden nicht von Cisco SDM unterstützt.

Beispielszenario zur Verwendung der Firewallrichtlinien

Informationen zur Firewall-Richtlinienverwaltung sowie detaillierte Einsatzmöglichkeiten finden Sie in einem Dokument unter folgendem Link:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration_09186a0080230754.pdf

Empfehlungen zur DMVPN-Konfiguration

Dieses Hilfethema enthält Empfehlungen dazu, wie Sie bei der Routerkonfiguration in einem DMVPN verfahren sollten.

Zuerst Konfigurieren des Hubs

Es ist wichtig, zuerst die Hub-Konfiguration vorzunehmen, da Spokes, die die Hub-Informationen verwenden, konfiguriert sein müssen. Wenn Sie einen Hub konfigurieren, können Sie mit der Spoke-Konfigurationsfunktion, die im Übersichtsfenster zur Verfügung steht, eine Textdatei generieren, die ein Verfahren enthält. Diese können Sie an Spoke-Administratoren senden, damit diese die Spokes mit den richtigen Hub-Informationen konfigurieren können. Bevor Sie mit der Konfiguration eines Spokes beginnen, müssen Sie über die korrekten Informationen zum Hub verfügen.

Zuweisen von Spoke-Adressen

Alle Router im DMVPN müssen sich im selben Subnetz befinden. Daher muss der Hub-Administrator den Spoke-Routern Adressen im Subnetz zuweisen, damit keine Adressenkonflikte auftreten und von allen Beteiligten dieselbe Subnetzmaske verwendet wird.

Empfehlungen zur Konfiguration von Routing-Protokollen für DMVPN

Im Folgenden finden Sie Richtlinien, die Sie bei der Konfiguration von Routing-Protokollen für DMVPN beachten sollten. Sie können diese Richtlinien ignorieren, Cisco SDM wurde jedoch nicht für Szenarios, auf die diese Richtlinien nicht zutreffen, getestet. Cisco SDM lässt unter Umständen das Bearbeiten von Konfigurationen nicht zu, nachdem Sie diese eingegeben haben.

Bei den folgenden Empfehlungen sind die wichtigsten Punkte zuerst aufgeführt:

- Wenn ein Routing-Prozess besteht, der innere Netzwerke ankündigt, verwenden Sie diesen Prozess, um Netzwerke für das DMVPN anzukündigen.
- Wenn ein Routing-Prozess besteht, der Tunnelnetzwerke für VPNs ankündigt, wie beispielsweise GRE over IPSec-Tunnel, verwenden Sie diesen Prozess, um die DMVPN-Netzwerke anzukündigen.

- Wenn ein Routing-Prozess besteht, der Netzwerke für die WAN-Schnittstellen ankündigt, stellen Sie sicher, dass eine AS-Nummer oder eine Prozess-ID, die die WAN-Schnittstellen nicht für die Ankündigung von Netzwerken einsetzen, verwendet wird.
- Wenn Sie DMVPN-Routing-Informationen konfigurieren, überprüft Cisco SDM, ob die von Ihnen eingegebene autonome Systemnummer (EIGRP) oder Bereichs-ID (OSPF) bereits zum Ankündigen von Netzwerken für die physikalische Schnittstelle des Routers verwendet wird. Wenn der Wert bereits verwendet wird, werden Sie von Cisco SDM darüber informiert, und Cisco SDM empfiehlt entweder die Verwendung eines neuen Werts oder die Auswahl eines anderen Routing-Protokolls zum Ankündigen von Netzwerken im DMVPN.

Verwenden von Schnittstellen mit DFÜ-Konfigurationen

Wenn Sie eine Schnittstelle, die eine DFÜ-Verbindung verwendet, auswählen, kann dies dazu führen, dass die Verbindung ständig aktiv ist. Sie können über das Fenster **Schnittstellen und Verbindungen** die unterstützten Schnittstellen untersuchen, um zu ermitteln, ob eine DFÜ-Verbindung, wie beispielsweise eine ISDN- oder Async-Verbindung, für die von Ihnen ausgewählte physikalische Schnittstelle konfiguriert wurde.

Ping-Vorgang an den Hub, bevor Sie mit der Spoke-Konfiguration beginnen

Bevor Sie mit der Spoke-Routerkonfiguration beginnen, sollten Sie die Hub-Konnektivität testen, indem Sie einen Ping-Befehl ausgeben. Wenn der Ping-Test nicht erfolgreich ist, müssen Sie eine Route zum Hub konfigurieren.

White Papers zu Cisco SDM

Es sind eine Reihe von White Papers verfügbar, welche die Verwendung von Cisco SDM beschreiben. Diese White Papers können unter dem folgenden Link abgerufen werden:

http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/appnote/index.htm

KAPITEL 38

Erste Schritte

Cisco Router and Security Device Manager (Cisco SDM) ist ein einfach zu verwendendes, Internet-Browser-basiertes Software-Tool, das für die Konfiguration von LAN-, WAN- und Sicherheitsfunktionen auf einem Router konzipiert wurde. Cisco SDM ist für Wiederverkäufer und Netzwerkadministratoren von kleinen und mittleren Unternehmen bestimmt, die mit LAN-Grundlagen und allgemeinem Netzwerkdesign vertraut sind.

Damit Sie Ethernet-Netzwerke, WAN-Konnektivität, Firewalls und VPNs (Virtual Private Networks – virtuelle private Netzwerke) schnell und effizient konfigurieren können, werden Sie in Cisco SDM mit Assistenten durch den Einrichtungsvorgang geleitet und zur Eingabe von Daten aufgefordert. Die Assistenten verwenden eine Sequenz von Bildschirmen, in denen die Konfiguration in einzelne Schritte aufgeteilt und erläutert wird. Sie können dann die erstellte Grundkonfiguration bearbeiten, um eine bessere Kontrolle über Router und Netzwerk zu erhalten. Für Cisco SDM werden keine Erfahrungen mit Cisco-Geräten oder der Cisco-CLI (Command Line Interface – Befehlszeilenschnittstelle) vorausgesetzt.

Wenn Sie Cisco SDM starten, wird die Startseite angezeigt, ein Fenster mit einer Übersicht über das System und die Konfiguration. In diesem Fenster erhalten Sie wichtige Informationen über die Hardware und Software des Routers. Damit können Sie bestimmen, was konfiguriert werden soll. Nachdem Sie eine Konfiguration definiert haben, können Sie diese mithilfe von Cisco SDM testen und eventuelle Fehler beheben. Dadurch wird sichergestellt, dass die Konfiguration einwandfrei funktioniert.

Cisco SDM verfügt zudem über einen Monitor-Modus, mit dem Sie die Routerleistung überwachen und Statistikdaten sammeln können, die im Zusammenhang mit den von Ihnen definierten Routerkonfigurationen stehen.

Was ist neu an dieser Ausgabe?

Diese Ausgabe unterstützt die folgenden neuen Funktionen:

- Certificate Authority (CA)-Server – Sie können den Router als Certificate Authority (CA)-Server konfigurieren und diesen für die Hosts im Netzwerk Zertifikate ausstellen lassen. Die Verwendung eines CA-Servers in Ihrem eigenen Netzwerk vereinfacht den Einsatz der VPN-Technologie, indem lokale Hosts Zertifikate von einem von Ihnen konfigurierten CA-Server anfordern können, anstelle diese von einem öffentlichen CA-Server anzufordern.
- 802.1x-Authentifizierung – Der Router kann so konfiguriert werden, dass eine IEEE 802.1x-Authentifizierung erfolgt. Damit kann sich ein Client über die Computer-Identität anstatt über die IP-Adresse authentifizieren.
- Dynamic Virtual Tunnel Interfaces – DVTI ermöglicht es Ihnen, eine Easy VPN-Verbindung mit einer virtuellen Schnittstelle zu konfigurieren.
  Die dynamischen virtuellen Tunnel liefern auf Anforderung eine separate virtuelle Zugangsschnittstelle für jede Easy VPN-Verbindung.
  Die Konfiguration der virtuellen Zugangsschnittstellen wird von einer virtuellen Vorlagenkonfiguration geklont, die die IPSec-Konfiguration und sämtliche Cisco IOS-Software-Funktionen beinhaltet, die auf der virtuellen Vorlagenschnittstelle konfiguriert sind, wie beispielsweise QoS, NetFlow oder Zugriffssteuerungslisten (ACLs).
- Zone-Based Policy Firewall – Zone-Based Policy Firewalls verwenden ein zonenbasiertes Konfigurationsmodell, das flexibler ist als schnittstellenbasierte Firewalls. Schnittstellen werden Zonen zugeordnet, und Zonen werden in Zonenpaaren platziert, um die Datenverkehrsquelle und die Zielschnittstellen zu definieren. Auf Zonenpaare können Prüfrichtlinien angewandt werden, um den Datenverkehr zu steuern, der in einem Zonenpaar von den Quellschnittstellen zu den Zielschnittstellen fließt.
- Cisco Common-Classification Policy Language – C3PL erlaubt Ihnen, klassenbasierte Richtlinien zu erstellen. Klassen identifizieren Datenverkehrstypen, wie beispielsweise P2P- und IM-Datenverkehr. Richtlinien ordnen Datenverkehrsklassen und Aktionen zu. Sie geben die Aktion an, die vom Router auf den Datenverkehr einer bestimmten Klasse angewandt werden soll, beispielsweise Datenverkehr prüfen, passieren lassen oder entfernen. Diese Richtlinien können auf Zonenpaare angewandt werden.

- IPS Enhancements – In Cisco IOS Version 12.4(11)T enthaltene Cisco IOS IPS Enhancements werden unterstützt. Es wird ein neues Format der Signature Definition File (SDF, Signaturdefinitionsdatei) unterstützt sowie andere Funktionen wie beispielsweise der Signaturereignis-Aktionsprozessor. Der SEAP ermöglicht eine größere Kontrolle über die Filterung, indem Sie Signaturereignis-Aktionsfilter (SEAF) erstellen können und Signaturereignis-Aktions-Overrides (SEAO) zuweisen können.
- Quality of Service-Verbesserungen – Der QoS wurde verbessert, sodass Sie für den Datenverkehr entweder DSCP- oder NBAR-Markierungen angeben können und mit C3PL QoS-Richtlinien erstellen können.

Mehr über diese Ausgabe finden Sie:

http://www.cisco.com/go/sdm

Klicken Sie auf den Link „General Information“ und dann auf „Release Notes“.

Unterstützte Cisco IOS-Versionen

Welche Cisco IOS-Versionen Cisco SDM unterstützt, erfahren Sie unter folgender URL:

http://www.cisco.com/go/sdm

Klicken Sie auf den Link „Technical Documentation“ und dann auf „Release Notes“.

KAPITEL 39

Anzeigen von Router-Informationen

Im Monitor-Modus des Cisco Router and Security Device Manager (Cisco SDM) können Sie eine aktuelle Momentaufnahme der Informationen zu Ihrem Router, den Router-Schnittstellen, der Firewall und gegebenenfalls aktiven VPN-Verbindungen anzeigen. Zusätzlich können Sie Meldungen im Ereignisprotokoll des Routers anzeigen.

Hinweis Das Monitor-Fenster wird nicht automatisch mit den neuesten Informationen aktualisiert. Wenn Sie die Informationen anzeigen möchten, die sich seit dem letzten Öffnen dieses Fensters geändert haben, klicken Sie auf **Aktualisieren**.

Der Monitor-Modus funktioniert durch Überprüfen des Router-Protokolls und Anzeigen der Ergebnisse von Cisco IOS **Anzeigen**-Befehlen. Bei Funktionen des Monitor-Modus, die auf Protokolleinträgen basieren, beispielsweise Firewall-Statistiken, muss die Protokollierung aktiviert sein. Die Protokollierung wird von Cisco SDM standardmäßig aktiviert, Sie können diese Einstellung jedoch über das Fenster **Zusätzliche Aufgaben > Routereigenschaften > Logging** ändern. Zusätzlich müssen einzelne Regeln möglicherweise konfiguriert werden, damit sie Ereignisse für Protokolle generieren können. Weitere Informationen finden Sie unter dem Hilfethema Wie zeige ich Aktivitäten auf meiner Firewall an?

Aufgabe	Vorgehensweise
Informationen zu Routerschnittstellen anzeigen	Klicken Sie in der Symbolleiste auf **Monitor**, und klicken Sie dann im linken Bereich auf **Schnittstellenstatus**. Wählen Sie im Feld **Schnittstelle auswählen** die Schnittstelle aus, für die Sie Informationen anzeigen möchten, und wählen Sie dann in der Gruppe der verfügbaren Elemente die Informationen aus, die Sie anzeigen möchten. Klicken Sie anschließend auf **Details anzeigen**.
Grafiken der CPU- oder Speicherauslastung anzeigen.	Klicken Sie in der Symbolleiste auf **Monitor**. Die Übersichtsseite umfasst Grafiken der CPU- und Speicherauslastung.
Informationen zur Firewall anzeigen	Klicken Sie in der Symbolleiste auf **Monitor**, und klicken Sie dann im linken Bereich auf **Firewallstatus**.
Informationen zu VPN-Verbindungen anzeigen	Klicken Sie in der Symbolleiste auf **Monitor**, und klicken Sie dann im linken Bereich auf **VPN-Status**. Wählen Sie dann die Registerkarte für IPSec-Tunnel, DMVPN-Tunnel, Easy VPN-Server oder IKE-SAs.
Meldungen im Ereignisprotokoll des Routers anzeigen.	Klicken Sie in der Symbolleiste auf **Monitor**, und klicken Sie dann im linken Bereich auf **Logging**.

Übersicht

Der Bildschirm **Übersicht** des Monitor-Modus zeigt eine Übersicht über die Aktivitäten und Statistiken Ihres Routers und bietet eine Zusammenfassung der Informationen, die in den anderen Bildschirmen des Monitor-Modus angezeigt werden. Darin sind die Informationen enthalten, die unter diesem Hilfethema erläutert werden.

Hinweis Wenn Sie Informationen zu einer Funktion, die unter diesem Hilfethema erläutert wird, nicht im Bildschirm **Übersicht** wiederfinden, wird die Funktion vom Cisco IOS-Abbild nicht unterstützt. Beispiel: Wenn der Router ein Cisco IOS-Abbild verwendet, das Sicherheitsfunktionen nicht unterstützt, erscheinen die Bereiche Firewallstatus und VPN-Status nicht auf dem Bildschirm.

Schaltfläche Wireless-Anwendung starten

Wenn der Router mit Funkschnittstellen ausgestattet ist, können Sie auf diese Schaltfläche klicken, um die Funkschnittstellen zu überwachen und zu konfigurieren. Das Fenster **Monitor - Übersicht** enthält Informationen über den Status dieser Schnittstellen, die Funkschnittstellen werden jedoch im Fenster **Monitor - Schnittstellenstatus** nicht aufgeführt.

Diese Schaltfläche wird nicht angezeigt, wenn der Router über keine Funkschnittstellen verfügt.

Schaltfläche Aktualisieren

Ruft aktuelle Informationen vom Router ab und aktualisiert somit die auf diesem Bildschirm angezeigten Informationen.

Ressourcenstatus

Zeigt grundlegende Informationen zu Ihrer Router-Hardware an und enthält die folgenden Felder:

CPU-Auslastung

Zeigt die CPU-Auslastung in Prozent an.

Speicherauslastung

Zeigt die Auslastung des Arbeitsspeichers in Prozent an.

Flash-Auslastung

Zeigt den Anteil des verfügbaren Flash-Speichers am gesamten auf dem Router installierten Flash-Speicher an.

Schnittstellenstatus

Zeigt grundlegende Informationen zu den auf dem Router installierten Schnittstellen mit ihrem jeweiligen Status an.

Hinweis In dieser Statistik sind nur die von Cisco SDM unterstützten Schnittstellentypen aufgeführt. Nicht unterstützte Schnittstellen werden nicht berücksichtigt.

Gesamtzahl der aktiven Schnittstellen

Gesamtzahl der auf dem Router aktivierten Schnittstellen.

Gesamtzahl der inaktiven Schnittstellen

Gesamtzahl der auf dem Router deaktivierten Schnittstellen.

Schnittstelle

Der Name der Schnittstelle.

IP

Die IP-Adresse der Schnittstelle.

Status

Der Status der Schnittstelle, entweder aktiv oder inaktiv.

Bandbreitenverwendung

Die verwendete Schnittstellenbandbreite in Prozent.

Beschreibung

Verfügbare Beschreibung der Schnittstelle. Cisco SDM fügt unter Umständen Beschreibungen wie beispielsweise $FW_OUTSIDE$ oder ETH_LAN hinzu.

Firewallstatusgruppe

Zeigt grundlegende Informationen zu den Router-Ressourcen an und enthält die folgenden Felder:

Anzahl der verweigerten Versuche

Zeigt die Anzahl der Protokollmeldungen an, die durch Verbindungsversuche generiert wurden (von Protokollen wie Telnet, HTTP, Ping und anderen), die von der Firewall verweigert wurden. Beachten Sie, dass für einen verweigerten Verbindungsversuch nur dann ein Protokolleintrag generiert werden kann, wenn die ZugriffsRegel, die den Verbindungsversuch verweigert hat, für die Generierung von Protokolleinträgen konfiguriert ist.

Firewall-Protokoll

Zeigt die Anzahl der Firewall-Protokolleinträge an, falls aktiviert.

QoS

Die Anzahl der Schnittstellen, die mit einer QoS-Richtlinie verknüpft sind.

VPN-Statusgruppe

Zeigt grundlegende Informationen zu den Router-Ressourcen an und enthält die folgenden Felder:

Anzahl von offenen IKE-SAs

Zeigt die Anzahl der IKE Security Associations (SAs) an, die derzeit konfiguriert und aktiv sind.

Anzahl von offenen IPSec-Tunneln

Zeigt die Anzahl der IPSec Virtual Private Networks (VPNs) an, die derzeit konfiguriert und aktiv sind.

Anzahl der DMVPN-Clients

Wenn der Router als ein DMVPN-Hub konfiguriert ist, die Anzahl der DMVPN-Clients.

Anzahl der aktiven VPN-Clients

Wenn der Router als ein EasyVPN-Server konfiguriert ist, wird in diesem Feld die Anzahl der Easy VPN Remote-Clients angezeigt.

NAC-Statusgruppe

Zeigt einen elementaren Snapshot des Network Admission Control (NAC) Status auf dem Router an.

Das Feld Anzahl der NAC-fähigen Schnittstellen

Die Anzahl der Routerschnittstellen, auf denen NAC aktiviert ist.

Das Feld Anzahl der bestätigten Hosts

Die Anzahl der Hosts mit Posture-Agents, die vom Zulassungssteuerungsprozess bestätigt wurden.

Protokollgruppe

Zeigt grundlegende Informationen zu den Router-Ressourcen an und enthält die folgenden Felder:

Gesamtzahl der Protokolleinträge

Gesamtzahl der derzeit im Routerprotokoll gespeicherten Einträge.

Hoher Schweregrad

Die Anzahl der gespeicherten Protokolleinträge, die einen Schweregrad von 2 oder niedriger haben. Bei dieser Meldung ist ein sofortiges Eingreifen erforderlich. Wenn keine Meldungen mit hohem Schweregrad vorhanden sind, ist diese Liste leer.

Warnung

Die Anzahl der gespeicherten Protokolleinträge mit einem Schweregrad von 3 oder 4. Diese Meldungen können auf ein Problem mit dem Netzwerk hindeuten, es sind jedoch meist keine sofortigen Maßnahmen erforderlich.

Informationsbezogen

Die Anzahl der gespeicherten Protokolleinträge, die einen Schweregrad von 6 oder höher haben. Diese Informationsmeldungen melden normale Netzwerkereignisse.

Schnittstellenstatus

Auf dem Bildschirm **Schnittstellenstatus** wird der aktuelle Status der verschiedenen Schnittstellen auf dem Router sowie die Anzahl der Pakete, Byte oder Datenfehler angezeigt, die die ausgewählte Schnittstelle passiert haben. Die auf diesem Bildschirm angezeigten Statistiken sind gehäuft, da die Zähler oder die ausgewählte Schnittstelle seit dem letzten Neustart des Routers zurückgesetzt wurden.

Überwachungsschnittstelle und Schaltfläche Überwachung beenden

Klicken Sie auf diese Schaltfläche, um die Überwachung der ausgewählte Schnittstelle zu starten oder anzuhalten. Die Schaltflächenbezeichnung ändert sich, je nachdem, ob Cisco SDM die Schnittstelle überwacht oder nicht.

Schaltfläche „Verbindung testen“

Klicken Sie auf diese Schaltfläche, um die ausgewählte Verbindung zu testen. Daraufhin wird ein Dialogfeld angezeigt, in dem Sie einen Remote-Host festlegen können, der während dieser Verbindung Ping-Befehle aussendet. Das Dialogfeld meldet dann den Erfolg oder das Scheitern des Tests. Wenn der Test fehlschlägt, werden Informationen zu der Ursache des Fehlschlagens sowie Informationen angegeben, welche Schritte Sie unternehmen müssen, um das Problem zu beheben.

Schnittstellenliste

Wählen Sie die Schnittstelle aus, für die Sie Statistiken aus dieser Liste anzeigen möchten. Die Liste enthält den Namen, die IP-Adresse und die Subnetzmaske, den Steckplatz und den Port, an dem sie sich befindet, sowie gegebenenfalls eingegebene Cisco SDM- oder Benutzerbeschreibungen.

Gruppe „Darstellungstyp zur Überwachung auswählen“

Diese Kontrollkästchen sind die Datenelemente, für die Cisco SDM Statistiken auf der ausgewählten Schnittstelle anzeigen kann. Dabei handelt es sich um folgende Datenelemente:

- Paket - Eingabe - Die Anzahl der auf der Schnittstelle eingegangenen Pakete.
- Paket - Ausgabe - Die Anzahl der von der Schnittstelle gesendeten Pakete.
- Bandbreitenverwendung – Die prozentuale Auslastung der Bandbreite durch die Schnittstelle. So wird die Bandbreitenauslastung berechnet:

  Bandbreite in Prozent = (KBit pro Sek./BB) * 100

  Dabei gilt:

  Bits pro Sekunde = ((Eingabeveränderung+Ausgabeveränderung) * 8) / Abfrageintervall

  KBit/s = Bits proSekunde/1024

  BB = Bandbreitenkapazität der Schnittstelle

Da die Differenz zwischen Eingabebytes und Ausgabebytes erst nach dem zweiten Anzeigeintervall berechnet werden kann, geht aus der Grafik der Bandbreiten-Prozentwerte die korrekte Bandbreitennutzung erst ab dem zweiten Anzeigeintervall hervor. Siehe den Abschnitt *Intervall anzeigen* dieses Dokuments für Informationen zu Abfrageintervallen und Anzeigeintervallen.

- Bytes - Eingabe - Die Anzahl der auf der Schnittstelle eingegangenen Bytes.
- Bytes - Ausgabe - Die Anzahl der von der Schnittstelle gesendeten Bytes.
- Fehler - Eingabe - Die Anzahl der Fehler, die während des Datenempfangs auf der Schnittstelle aufgetreten sind.
- Fehler - Ausgabe - Die Anzahl der Fehler, die beim Datenversand über die Schnittstelle aufgetreten sind.
- Paketfluss - Die Anzahl der auf der gewählten Schnittstelle transportierten Pakete. Dieser Eintrag wird nur angezeigt, wenn die Einstellung für die betreffende Schnittstelle unter **Konfigurieren > Schnittstellen und Verbindungen > Bearbeiten > Anwendungsdienst** entsprechend gewählt wurde.
- Byte-Fluss - Die Anzahl an Bytes der auf der gewählten Schnittstelle transportierten Pakete. Dieser Eintrag wird nur angezeigt, wenn die Einstellung für die betreffende Schnittstelle unter **Konfigurieren > Schnittstellen und Verbindungen > Bearbeiten > Anwendungsdienst** entsprechend gewählt wurde.
- Gesamter Datenfluss - Die Gesamtanzahl der auf der gewählten Schnittstelle transportierten Pakete von den Datenursprüngen bis zu den Zieladressen. Dieser Eintrag wird nur angezeigt, wenn die Einstellung für die betreffende Schnittstelle unter **Konfigurieren > Schnittstellen und Verbindungen > Bearbeiten > Anwendungsdienst** entsprechend gewählt wurde.

Hinweis Wenn Netflow vom Cisco IOS-Abbild des Routers nicht unterstützt wird, stehen keine Datenflusszählerwerte zur Verfügung.

So zeigen Sie Statistiken für eines dieser Elemente an:

Schritt 1 Wählen Sie die Elemente, die Sie anzeigen möchten, indem Sie die dazugehörigen Kontrollkästchen aktivieren.

Schritt 2 Klicken Sie auf **Schnittstelle überwachen**, um Statistiken für alle ausgewählten Datenelemente anzuzeigen.

Bereich „Schnittstellenstatus“

Intervall anzeigen

In diesem Pulldown-Feld werden die für jedes Element angezeigte Datenmenge und die Häufigkeit angezeigt, mit der die Daten aktualisiert werden. Das Feld bietet die folgenden Optionen:

Hinweis Die aufgeführten Abfragehäufigkeiten sind ungefähre Werte und können leicht von den aufgelisteten Zeitpunkten abweichen.

- Real Time-Daten alle 10 Sek. – Bei dieser Option wird der Router fortlaufend maximal zwei Stunden abgefragt. Dies führt zu ca. 120 Datenpunkten.
- 10 Minuten lang zyklische Abfrage von Daten, Abfrage alle 10 Sekunden
- 60 Minuten lang zyklische Abfrage von Daten, Abfrage jede Minute
- 12 Stunden lang zyklische Abfrage von Daten, Abfrage alle 10 Minuten

Hinweis Bei den letzten drei Optionen werden maximal 60 Datenpunkte abgerufen. Nachdem 60 Datenpunkte empfangen wurden, fragt Cisco SDM weiterhin Daten ab und ersetzt dabei die ältesten Datenpunkte durch die neuesten.

Tabelle anzeigen/Tabelle ausblenden

Klicken Sie auf diese Schaltfläche, um die Leistungsdiagramme anzuzeigen oder auszublenden.

Schaltfläche „Zurücksetzen“

Klicken Sie auf diese Schaltfläche, um die Zähler der Schnittstellenstatistiken auf Null zurückzusetzen.

Darstellungsbereich

In diesem Bereich werden die Darstellungen und einfachen numerischen Werte für die angegebenen Daten angezeigt.

Hinweis Bei den letzten drei Optionen werden maximal 30 Datenpunkte abgerufen. Nachdem 30 Datenpunkte empfangen wurden, fragt Cisco SDM weiterhin Daten ab und ersetzt dabei die ältesten Datenpunkte durch die neuesten.

Firewallstatus

In diesem Fenster werden folgende statistische Angaben zu der Firewall angezeigt, die im Router konfiguriert ist:

- Anzahl der zur Prüfung konfigurierten Schnittstellen - Die Anzahl der Routerschnittstellen, bei denen die Überprüfung eines bestimmten Datenverkehrs durch eine Firewall eingeschaltet ist.
- Anzahl der TCP-Paket(e)-Zählungen - Die Gesamtzahl an TCP-Paketen die über die überwachten Schnittstellen übertragen worden sind.
- Anzahl der UDP-Paket(e)-Zählungen - Die Gesamtzahl an UDP-Paketen die über die überwachten Schnittstellen übertragen worden sind.
- Gesamtzahl aktiver Verbindungen - Die Summe aus allen laufenden Sitzungen.

Das Fenster Firewallstatus zeigt ebenfalls die Firewallsitzungen anhand einer Tabelle an, die folgende Spalten enthält:

- IP-Quell-Adresse - Die IP-Adresse des Hosts, von dem das Paket ursprünglich ausgegeben wurde.
- IP-Ziel-Adresse - Die IP-Adresse des Zielhosts für das Paket.
- Protokoll - Das untersuchte Netzwerkprotokoll.
- Zahl der Übereinstimmungen - Die Anzahl an Paketen, die die Firewallbedingungen erfüllen.

Die Schaltfläche Aktualisierung

Klicken Sie auf diese Schaltfläche, um die eingetragenen Firewallsitzungen in der Tabelle zu aktualisieren und die aktuellsten Daten vom Router anzuzeigen.

Zone-Based Policy Firewall-Status

Sie können den Status der Firewall-Aktivitäten für jedes Zonenpaar auf dem Router anzeigen, wenn der Router ein Cisco IOS-Abbild ausführt, das eine Zone-Based Policy Firewall-Funktion unterstützt.

Firewallrichtlinien-Listenbereich

Der Firewallrichtlinien-Listenbereich zeigt den Richtliniennamen, die Quellzone und Zielzone für jedes Zonenpaar an. Die folgende Tabelle enthält Beispieldaten für zwei Zonenpaare.

Zonenpaarname	Richtlinienname	Quellzone	Zielzone
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

In dieser Beispieltabelle ist ein Zonenpaar für den eingehenden und eines für den abgehenden Datenverkehr des DMZ konfiguriert.

Wählen Sie das Zonenpaar aus, dessen Firewallstatistiken Sie anzeigen möchten.

Intervall anzeigen

Wählen Sie eine der folgenden Optionen, um festzulegen, wie Daten gesammelt werden:

- Real Time-Daten alle 10 Sek. – Die Daten werden alle 10 Sekunden gemeldet. Jedes Häkchen auf der horizontalen Achse der Grafiken **Entfernte Pakete** und **Zugelassene Pakete** repräsentiert 10 Sekunden.
- 60 Minuten lang zyklische Abfrage von Daten, Abfrage jede Minute – Die Daten werden jede Minute gemeldet. Jedes Häkchen auf der horizontalen Achse der Grafiken **Entfernte Pakete** und **Zugelassene Pakete** repräsentiert 1 Minute.
- 12 Stunden lang zyklische Abfrage von Daten, Abfrage alle 12 Minuten – Die Daten werden alle 12 Minuten gemeldet. Jedes Häkchen auf der horizontalen Achse der Grafiken **Entfernte Pakete** und **Zugelassene Pakete** repräsentiert 12 Minuten.

Richtlinie überwachen

Klicken Sie auf **Richtlinie überwachen**, um Firewalldaten für die ausgewählte Richtlinie zu sammeln.

Überwachung beenden

Klicken Sie auf **Überwachung beenden,** um das Sammeln von Firewalldaten zu stoppen.

Statistikbereich

In diesem Bereich werden die Firewallstatistiken für das ausgewählte Zonenpaar angezeigt. Durch Klicken auf Knoten im Baum auf der linken Seite können Sie die Anzeige steuern. In den folgenden Abschnitten wird beschrieben, was beim Klicken auf die einzelnen Knoten angezeigt wird.

Aktive Sitzungen

Wenn Sie auf **Aktive Sitzungen** klicken, wird der Datenverkehrstyp, die Quell-IP-Adresse und die Ziel-IP-Adresse für den Datenverkehr dargestellt, die im ausgewählten Zonenpaar geprüft werden.

Entfernte Pakete

Wenn Sie für das ausgewählte Zonenpaar auf **Entfernte Pakete** klicken, wird in der Grafik die gehäufte Anzahl an entfernten Paketen im Zeitintervall, das in der Liste **Intervall anzeigen** ausgewählt wurde, dargestellt. Es werden Daten über den Datenverkehr gesammelt, der so konfiguriert ist, dass er entfernt und in der Richtlinienzuordnung für Layer 4 protokolliert wird.

Zugelassene Pakete

Wenn Sie für das ausgewählte Zonenpaar auf **Zugelassene Pakete** klicken, wird in der Grafik die gehäufte Anzahl an zugelassenen Paketen im Zeitintervall, das in der Liste **Intervall anzeigen** ausgewählt wurde, dargestellt. Es werden Daten über den Datenverkehr gesammelt, der laut Konfiguration in der Richtlinienzuordnung für Layer 4 passieren kann.

VPN-Status

In diesem Fenster wird eine Baumstruktur mit VPN-Verbindungen angezeigt, die mit dem Router möglich sind. Sie können eine der folgenden VPN-Kategorien aus der Baumdarstellung mit den VPN-Verbindungen auswählen:

- IPSec-Tunnel
- DMVPN-Tunnel
- Easy VPN-Server
- IKE-SAs
- SSL VPN-Komponenten

Zur Anzeige statistischer Daten zu einer aktiven VPN-Kategorie wählen Sie diese aus der Baumstruktur mit den VPN-Verbindungen aus.

IPSec-Tunnel

In dieser Gruppe werden Statistiken zu jeder einzelnen IPSec-VPN angezeigt, die auf dem Router konfiguriert ist. Jede Reihe in der Tabelle stellt ein IPSec-VPN dar. Die Tabelle enthält Spalten mit den folgenden Informationen:

- Spalte **Schnittstelle**

  Die WAN-Schnittstelle auf dem Router, auf der der IPSec-Tunnel aktiv ist.

- Spalte **Lokales IP**

  Die IP-Adresse der lokalen IPSec-Schnittstelle

- Spalte **Remote-IP**

  Die IP-Adresse der Remote-IPSec-Schnittstelle

- Spalte **Peer**

  Die IP-Adresse des Remote-Peer.

- Tunnelstatus

  Der aktuelle Status des IPSec-Tunnels. Folgende Werte sind möglich:

  - Aktiv – Der Tunnel ist aktiv
  - Inaktiv – Der Tunnel ist aufgrund eines Fehlers oder Hardware-Ausfalls inaktiv.

- Spalte **Gekapselte Pakete**

  Die Anzahl der Pakete, die über die IPSec-VPN-Verbindung gekapselt wurden.

- Spalte **Entkapselte Pakete**

  Die Anzahl der Pakete, die über die IPSec-VPN-Verbindung entkapselt wurden.

- Spalte **Fehlerpakete senden**

  Die Anzahl der Fehler, die während der Versendung von Paketen aufgetreten sind.

- Spalte **Empfangene Fehlerpakete**

  Die Anzahl der Fehler, die während des Empfangs von Paketen aufgetreten sind.

- Spalte **Verschlüsselte Pakete**

  Die Anzahl der Pakete, die über die Verbindung verschlüsselt wurden.

- Spalte **Entschlüsselte Pakete**

  Die Anzahl der Pakete, die über Verbindung entschlüsselt wurden.

Schaltfläche Tunnel überwachen

Klicken Sie darauf, um den in der Tabelle **IPSec-Tunnel** gewählten IPSec-Tunnel zu überwachen. Siehe Überwachen eines IPSec-Tunnels.

Tunnel testen... (Schaltfläche)

Klicken Sie auf diese Schaltfläche, um einen ausgewählten VPN-Tunnel zu testen. Die Ergebnisse des Tests werden in einem weiteren Fenster angezeigt.

Die Schaltfläche Aktualisierung

Klicken Sie auf diese Schaltfläche, um die Tabelle der IPSec-Tunnel zu aktualisieren und die aktuellsten Daten vom Router anzuzeigen.

Überwachen eines IPSec-Tunnels

Anhand folgender Arbeitsschritte überwachen Sie einen IPSec-Tunnel:

Schritt 1 Wählen Sie in der Tabelle **IPSec-Tunnel** den zu überwachenden IPSec-Tunnel aus.

Schritt 2 Aktivieren Sie die Kontrollkästchen unter **Zu überwachendes Element wählen**, und wählen Sie die zu verfolgenden Angaben aus.

Schritt 3 Wählen Sie aus der Dropdown-Liste **Intervall anzeigen** die Zeitspanne für die Echtzeitkurve aus.

DMVPN-Tunnel

In dieser Gruppe werden die folgenden Statistiken zu Dynamic Multi-point VPN (DMVPN)-Tunneln angezeigt. Jede Reihe stellt einen VPN-Tunnel dar.

- Spalte **Remote-Subnetz**

  Die Netzwerkadresse des Subnetzes, mit dem der Tunnel verbunden ist.

- Spalte **Remote-Tunnel-IP**

  Die IP-Adresse des Remote-Tunnels Hierbei handelt es sich um die private IP-Adresse, die der Tunnel vom Remote-Gerät erhalten hat.

- Spalte **IP von öffentlicher Schnittstelle des Remote-Routers**

  IP-Adresse der öffentlichen (äußeren) Schnittstelle des Remote-Routers.

- Spalte „Status“

  Der Status des DMVPN-Tunnels.

- Spalte **Ablaufzeit**

  Die Uhrzeit und das Datum, an dem bzw. zu der die Tunnelregistrierung abläuft und der DMVPN-Tunnel beendet wird.

Schaltfläche Tunnel überwachen

Klicken Sie darauf, um den in der Tabelle **DMVPN-Tunnel** gewählten DMVPN-Tunnel zu überwachen. Siehe Überwachen eines DMVPN-Tunnels.

Die Schaltfläche Aktualisierung

Klicken Sie auf diese Schaltfläche, um die DMVPN-Tunneltabelle zu aktualisieren und die aktuellsten Daten vom Router anzuzeigen.

Schaltfläche Zurücksetzen

Klicken Sie hierauf, um die statistischen Zählerwerte zur Tunnelliste wieder auf Null zu stellen. Die Anzahl der gekapselten und entkapselten Pakete, die Anzahl gesendeter und empfangener Fehler sowie die Anzahl verschlüsselter und entschlüsselter Pakete werden wieder auf Null gesetzt.

Überwachen eines DMVPN-Tunnels

Anhand folgender Arbeitsschritte überwachen Sie einen DMVPN-Tunnel:

Schritt 1 Wählen Sie in der Tabelle **DMVPN-Tunnel** den zu überwachenden Tunnel aus.

Schritt 2 Aktivieren Sie die Kontrollkästchen unter **Zu überwachendes Element wählen**, und wählen Sie die zu verfolgenden Angaben aus.

Schritt 3 Wählen Sie aus der Dropdown-Liste **Intervall anzeigen** die Zeitspanne für die Echtzeitkurve aus.

Easy VPN-Server

In dieser Gruppe werden die folgenden Informationen zu den einzelnen Easy VPN-Servergruppen angezeigt:

- Gesamtzahl der Server-Clients (in der oberen rechten Ecke)
- Gruppenname
- Anzahl an Clientverbindungen

Schaltfläche Gruppendetails

Durch Klicken auf die Schaltfläche **Gruppendetails** werden folgende Informationen zur ausgewählten Gruppe angezeigt.

- Gruppenname
- Schlüssel
- Pool-Name
- DNS-Server
- WINS-Server
- Domänenname
- ACL
- Sicherungsserver
- Firewall-R-U-There
- Include-Local-LAN
- Gruppensperre
- Kennwort speichern
- Für diese Gruppe zugelassene maximale Anzahl von Verbindungen
- Max. Anzahl an Anmeldungen pro Benutzer

Clientverbindungen in dieser Gruppe

In diesem Bereich werden folgende Informationen zur ausgewählten Gruppe angezeigt.

- Öffentliche IP-Adresse
- Zugewiesene IP-Adresse
- Verschlüsselte Pakete
- Entschlüsselte Pakete
- Entfernte ausgeh. Pakete
- Entfernte eingeh. Pakete
- Status

Die Schaltfläche Aktualisierung

Klicken Sie auf diese Schaltfläche, um die neuesten Daten vom Router anzuzeigen.

Die Trennen-Schaltfläche

- Wählen Sie eine Zeile in der Tabelle aus und klicken Sie auf Trennen, um die Verbindung zum Client abzubrechen.

IKE-SAs

In dieser Gruppe werden die folgenden Statistiken zu jeder aktiven IKE-Security Association angezeigt, die auf dem Router konfiguriert ist:

- Spalte **Quell-IP**

  Die IP-Adresse des Peers, der Ursprung der IKE-SA ist.

- Spalte **Ziel-IP**

  Die IP-Adresse des Remote-IKE-Peers.

- Spalte **Status**

  Beschreibt den aktuellen Status der IKE-Aushandlungen. Folgende Status sind möglich:

  - MM_NO_STATE – Die Internet Security Association und Key Management-Protokoll (ISAKMP)-SA wurde erstellt, es ist jedoch weiter nichts geschehen.
  - MM_SA_SETUP – Die Peers haben Parameter für die ISAKMP-SA ausgehandelt.
  - MM_KEY_EXCH – Die Peers haben öffentliche Diffie-Hellman-Schlüssel ausgehandelt und einen gemeinsamen geheimen Schlüssel generiert. Die ISAKMP-SA ist weiterhin nicht authentifiziert.
  - MM_KEY_AUTH – Die ISAKMP-SA wurde authentifiziert. Wenn der Router diesen Austausch gestartet hat, wechselt dieser Status sofort zu QM_IDLE, und es beginnt ein Austausch im Schnellmodus.
  - AG_NO_STATE – Die ISAKMP-SA wurde erstellt, es ist jedoch weiter nichts geschehen.

  - AG_INIT_EXCH – Die Peers haben den ersten Austausch im Aggressive-Modus vorgenommen, die SA ist jedoch noch nicht authentifiziert.
  - AG_AUTH – Die ISAKMP-SA wurde authentifiziert. Wenn der Router diesen Austausch gestartet hat, wechselt dieser Status sofort zu QM_IDLE, und es beginnt ein Austausch im Schnellmodus.
  - QM_IDLE – Die ISAKMP-SA befindet sich im Ruhezustand. Sie ist weiterhin beim Peer authentifiziert und kann für zukünftige Austauschvorgänge im Schnellmodus verwendet werden.
- Schaltfläche **Aktualisieren** - Klicken Sie auf diese Schaltfläche, um die IKE SA-Tabelle zu aktualisieren und die aktuellsten Daten vom Router anzuzeigen.
- Schaltfläche **Löschen** - Wählen Sie eine Zeile in der Tabelle aus, und klicken Sie auf **Löschen**, um die IKE-SA-Verbindung zu löschen.

SSL VPN-Komponenten

Wenn Sie im Überwachungsfenster auf die Schaltfläche **VPN-Status** klicken, beginnt der Router mit der Überwachung der SSL VPN-Aktivitäten. In diesem Fenster werden die Daten angezeigt, die in allen auf dem Router konfigurierten SSL VPN-Kontexten gesammelt wurden.

In der Standardeinstellung werden diese Daten alle 10 Sekunden auf den neuesten Stand gebracht. Wenn Ihnen 10 Sekunden als Zeitspanne bis zur nächsten Aktualisierung zu kurz ist, können Sie ein automatisches Aktualisierungsintervall der **Echtzeit-Daten einmal pro Minute** einschalten.

Wählen Sie einen Kontext im SSL VPN-Baum, um die Daten für den jeweiligen Kontext sowie die Daten der Benutzer anzuzeigen, die auf den betreffenden Kontext eingestellt sind.

Systemressourcen

In diesem Bereich wird der Prozentsatz an CPU- und Arbeitsspeicherressourcen angezeigt, die der SSL VPN-Datenverkehr in allen aktiven Kontexten in Anspruch nimmt.

Anz. verbundener Benutzer

In dieser Grafik wird die Anzahl der aktiven Benutzer in einen bestimmten Zeitraum dargestellt. Oben in der Grafik kann der Spitzenwert für die Anzahl aktiver Benutzer seit Beginn der Überwachung abgelesen werden. Der Zeitpunkt für den Überwachungsbeginn wird unten links in der Grafik angezeigt, und die aktuelle Zeitangabe kann mittig unterhalb der Grafik entnommen werden.

Registerkartenbereich

In diesem Bereich des Fensters sind mehrere Registerkarten untergebracht, über die die unterschiedlichen Statistikdaten übersichtlich aufgerufen werden können.

Klicken Sie auf einen beliebigen Link weiter unten, um eine Erläuterung zu den angezeigten Daten auf der Registerkarte zu erhalten.

Benutzersitzungen

URL-Mangling

Port-Weiterleitung

CIFS

Full Tunnel

Hinweis Wenn eine Funktion wie z. B. die Port-Weiterleitung oder ein Tunnel auf dem Router nicht konfiguriert ist, enthält die Registerkarte zu der jeweiligen Funktion keine Daten.

Einige Statistikdaten werden immer dann neu gesammelt, wenn der Router die Überwachungsdaten auf den neuesten Stand bringt. Andere Statistiken, wie z. B. der Spitzenwert für die Anzahl aktiver Benutzer werden zum Aktualisierungszeitpunkt ermittelt, jedoch denselben Daten gegenübergestellt, die zu Beginn der Überwachung gesammelt wurden. Die Überwachung sämtlicher VPN-Aktivitäten einschließlich SSL VPN beginnt, sobald Sie auf die Schaltfläche **VPN-Status** klicken.

SSL VPN-Kontext

In diesem Fenster werden die gleichen Informationen wie im Fenster **SSL VPN-Komponenten** angezeigt, allerdings erscheinen hier nur die zu dem gewählten Kontext gesammelten Daten. Klicken Sie auf SSL VPN-Komponenten, um eine Erläuterung zu den dargestellten Informationen zu erhalten.

Benutzersitzungen

Auf dieser Registerkarte werden die folgenden Informationen zu den SSL VPN-Benutzersitzungen angezeigt.

- **Aktive Benutzersitzungen** – Die Anzahl von SSL VPN-Benutzersitzungen aller Datenverkehrstypen, die seit Aktualisierung der Überwachungsdaten aktiv waren.
- **Spitzen-Benutzersitzungen** – Die höchste Anzahl aktiver SSL VPN-Benutzersitzungen seit Beginn der Überwachung.
- **Aktive Benutzer-TCP-Verbindungen** – Die Anzahl TCP-basierter SSL VPN-Benutzersitzungen, die seit Aktualisierung der Überwachungsdaten aktiv waren.
- **Zuordnungsfehler bei Sitzung** - Die Anzahl an Sitzungszuweisungsfehlern, die seit Beginn der Überwachung aufgetreten sind.
- **VPN-Sitzungs-Timeout** - Die Anzahl an VPN-Sitzungs-Timeouts, die seit Beginn der Überwachung aufgetreten sind.
- **Benutzer hat VPN-Sitzungen gelöscht** - Die Anzahl an VPN-Sitzungen, die seit Beginn der Überwachung gelöscht wurden.
- **AAA anstehende Anforderungen** - Die Anzahl noch ausstehender AAA-Anforderungen seit der Aktualisierung der Überwachungsdaten.
- **Spitzenzeit** - Die längste verzeichnete Benutzersitzung seit Beginn der Überwachung.
- **Beendete Benutzersitzungen** - Die Anzahl an Benutzersitzungen, die seit Beginn der Überwachung beendet wurden.
- **Authentifizierungsfehler** - Die Anzahl an Sitzungen mit gescheiterter Authentifizierung seit Beginn der Überwachung.
- **VPN-Ruhezustand-Timeout** - Die Anzahl an VPN-Timeouts bei Inaktivität, die seit Beginn der Überwachung aufgetreten sind.

- **Limit für Kontextbenutzer überschritten** - Die Anzahl der Vorfälle seit Beginn der Überwachung, bei denen ein Benutzer eine Sitzung versucht hat zu starten, jedoch das für den Kontext geltende Sitzungslimit bereits erreicht war.
- **Limit für Benutzeranzahl überschritten** - Die Anzahl der Vorfälle seit Beginn der Überwachung, bei denen ein Benutzer eine Sitzung versucht hat zu starten, jedoch das gesamte Sitzungslimit bereits erreicht war.

URL-Mangling

Auf dieser Registerkarte werden Informationen über URL-Mangling-Aktivitäten angezeigt. Weitere Informationen erhalten Sie in der Befehlsreferenz, die über folgenden Link abrufbar ist:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Port-Weiterleitung

Auf dieser Registerkarte werden Informationen angezeigt, die im Zusammenhang mit der Port-Weiterleitung gesammelt wurden. Weitere Informationen erhalten Sie in der Befehlsreferenz, die über folgenden Link abrufbar ist:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

Auf dieser Registerkarte werden Informationen zu CIFS-Anfragen, -Antworten- und Verbindungen angezeigt. Weitere Informationen erhalten Sie in der Befehlsreferenz, die über folgenden Link abrufbar ist:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Full Tunnel

Diese Registerkarte enthält Informationen über Full-Tunnel-Verbindungen zwischen SSL VPN-Clients und -Servern im Intranet des Unternehmens.

- Aktive Tunnel-Verbindungen - Die Anzahl aktiver Full-Tunnel-Verbindungen, die seit Aktualisierung der Daten aktiv waren. Die Daten können alle 10 Sekunden oder einmal pro Minute aktualisiert werden.
- Aktive Verbindungen zur Spitzenzeit - Die Full-Tunnel-Verbindung mit der längsten Dauer seit Beginn der Überwachung.
- Aktive Tunnel-Verbindungen zur Spitzenzeit - Die höchste Anzahl aktiver Full-Tunnel-Verbindungen seit Beginn der Überwachung.
- Versuche zur Tunnelverbindung fehlgeschlagen - Die Anzahl an Full-Tunnel-Verbindungsversuchen, die seit Beginn der Überwachung fehlgeschlagen sind.
- Versuche zur Tunnelverbindung erfolgreich - Die Anzahl an erfolgreich hergestellten Full-Tunnel-Verbindungen seit Beginn der Überwachung.

Server:

- An Server gesendete IP-Pakete - Die Anzahl der IP-Pakete von Full-Tunnel-Clients, die der Router an die Server im firmeninternen Intranet weitergeleitet hat.
- An Server gesendeter IP-Verkehr in Byte - Das mengenmäßige IP-Verkehrsaufkommen in Byte, das von den Full-Tunnel-Clients an die Server im firmeninternen Intranet weitergeleitet wurde.
- Vom Server empfangene IP-Pakete - Die Anzahl der IP-Pakete, die der Router von Servern mit Full-Tunnel-Verbindungen zu Clients entgegengenommen hat.
- Vom Server empfangener IP-Verkehr in Byte - Das mengenmäßige IP-Verkehrsaufkommen in Byte, das von den Servern im firmeninternen Intranet mit Full-Tunnel-Verbindungen zu den Clients empfangen wurde.

Benutzerliste

In diesem Fenster werden die Benutzerinformationen zu dem Kontext angezeigt, der im SSL VPN-Komponentenbaum ausgewählt wurde. Da für den Kontext viele Gruppenrichtlinien definiert sein können, von denen sich jede einer eigenen URL-Liste und Serverliste bedient, enthält dieser Bildschirm wertvolle Informationen darüber, wie einzelne Benutzer von Ihren SSL VPN-Verbindungen Gebrauch machen.

Den individuellen Gebrauch von SSL VPN können Sie in diesem Fenster steuern, indem Sie einen Benutzer auswählen und auf die Schaltfläche **Trennen** klicken.

Benutzerlistenbereich

In diesem Bereich werden alle aktiven Benutzer aller Gruppen aufgeführt, die für den jeweiligen Kontext konfiguriert sind. In dem Bereich werden folgende Informationen angezeigt:

- Benutzername – Der Benutzername entsprechend der Authentifizierung beim AAA-Server.
- Client-IP-Adresse – Die SSL VPN-IP-Adresse, die dem Benutzer für die betreffende Sitzung zugewiesen wurde. Diese IP-Adresse stammt aus dem Adress-Pool, der für den betreffenden Kontext definiert ist.
- Kontext – Der SSL VPN-Kontext, in dem die Gruppenrichtlinien für den betreffenden Benutzer konfiguriert wurden.
- Anzahl der Verbindungen – Die Anzahl der aktiven Verbindungen des Benutzers. Zum Beispiel kann der Benutzer eineVerbindung zu einem Mailserver haben und zugleich auf einem Server im Netzwerk nach Dateien suchen.
- Erstellt – Der Zeitpunkt, zu dem die Sitzung erstellt wurde.
- Zuletzt verwendet - Der Zeitpunkt, zu dem der Benutzer das letzte Mal Daten über eine aktive Verbindung übertragen hat.
- Cisco Secure Desktop - wahr oder falsch. Gibt an, ob Cisco Secure Desktop auf den PC des Benutzers heruntergeladen wurde.
- Gruppenname - Der Name der Gruppenrichtlinie, der die Konfiguration des Benutzers zugeordnet wurde. In der Gruppenrichtlinie sind die URL-Liste, die für die Benutzer verfügbaren Dienste, die WINS-Server zur Auflösung von Servernamen sowie die Server definiert, die den Benutzern bei der Suche nach Dateien im firmeninternen Intranet angeboten werden.

- URL-Listenname - Der Name der URL-Liste, die auf der Portalseite des Benutzers angezeigt wird. Die URL-Liste ist für die Gruppe festgelegt, zu der der Benutzer gehört. Weitere Informationen finden Sie unter Gruppenrichtlinie: Registerkarte Clientless.
- Leerlauf-Timeout - Die Anzahl an Sekunden, die eine Sitzung im Leerlauf bleiben kann, bevor sie vom Router beendet wird. Dieser Wert ist für die Gruppe festgelegt, zu der der Benutzer gehört. Weitere Informationen finden Sie unter Gruppenrichtlinie: Registerkarte Allgemein.
- Sitzungs-Timeout - Die maximale Anzahl an Sekunden, die eine Sitzung aktiv bleiben darf, bevor sie beendet wird. Dieser Wert ist für die Gruppe festgelegt, zu der der Benutzer gehört. Weitere Informationen finden Sie unter Gruppenrichtlinie: Registerkarte Allgemein.
- Port-Weiterleitungsliste Name - Dieser Wert ist für die Gruppe festgelegt, zu der der Benutzer gehört. Weitere Informationen finden Sie unter Gruppenrichtlinie: Registerkarte Thin Client.
- WINS Name Service Listenname - Dieser Wert ist für die Gruppe festgelegt, zu der der Benutzer gehört. Weitere Informationen finden Sie unter Gruppenrichtlinie: Registerkarte Clientless.

Datenverkehrsstatus

In diesem Fenster wird eine Baumstruktur mit verschiedenen Datenverkehrskategorien angezeigt, die auf einer Schnittstelle überwacht werden können. Vor dem Beginn der Überwachung muss der Datenverkehrstyp zumindest auf einer Schnittstelle aktiviert sein.

Sie können eine der folgenden Datenverkehrskategorien aus der Baumdarstellung **Datenverkehrsstatus** auswählen:

- Wichtigste Sprecher (Netflow)
- QoS
- Anwendung/Protokoll Datenverkehr

  Bei diesem Typ wird zur Datenverkehrsüberwachung NBAR (Network-based Application Recognition) eingesetzt.

Wichtigste Sprecher (Netflow)

Wenn mit **Konfigurieren > Schnittstellen und Verbindungen > Schnittstelle/Verbindung bearbeiten** die Erfassung von Netflow-Statistiken auf zumindest einer Schnittstelle eingeschaltet wurde, können Sie die Netflow-Statistik einsehen. Wählen Sie dazu aus der Baumstruktur **Datenverkehrsstatus** die Befehle **Wichtigste N Datenverkehrsflüsse > Häufigste Protokolle > Häufigste Sprecher** (Ursprungsadressen mit starkem Verkehrsaufkommen) aus.

Hinweis Wenn Netflow von dem Cisco IOS-Abbild im Router nicht unterstützt wird, stehen in der Baumstruktur **Datenverkehrsstatus** keine Netflow-Optionen zur Auswahl zur Verfügung.

Häufigste Protokolle

Dieses Fenster enthält eine Tabelle mit den folgenden Spalten:

- Protokoll - Das untersuchte Protokoll.
- Gesamtzahl Datenflüsse - Die Summe der Datenflüsse mit dem jeweiligen Protokoll.
- Datenflüsse/Sek. - Aktive Datenflüsse pro Sekunde unter Verwendung des Protokolls.
- Pakete/Datenfluss - Pro Datenfluss übertragene Pakete.
- Byte/Paket - Anzahl an Byte pro übertragenem Paket.
- Pakete/Sek. - Pro Sekunde übertragene Pakete.

Schaltfläche Aktualisieren

Aktualisiert den Informationsstand in dem Fenster mit den neuesten Daten zum Datenverkehrsfluss.

Wichtigste Sprecher

Dieses Fenster enthält eine Tabelle mit den folgenden Spalten:

- **IP-Quell-Adresse** - Die IP-Quell-Adresse des Host mit dem stärksten Verkehrsaufkommen.

  Wählen Sie eine IP-Quell-Adresse aus, um unter **Datenfluss-Status für die Quelladresse** weitere Informationen einzusehen.
- **Pakete** - Die Gesamtzahl an Paketen, die von der IP-Quell-Adresse eingegangen sind.
- **Byte** - Die Gesamtzahl an Byte, die von der IP-Quell-Adresse eingegangen sind.
- **Datenflüsse** - Die Anzahl der Datenflüsse, die von der IP-Ursprungs-Adresse stammen.

Hinweis Wenn die Netflow-Erfassung von Adressen mit dem stärksten Verkehrsaufkommen unter **Konfigurieren > Zusätzliche Aufgaben > Router-Eigenschaften > NetFlow** nicht aktiviert ist, werden statistische Erhebungen zu den zehn Adressen mit dem stärksten Verkehrsaufkommen angezeigt.

Datenfluss-Status für die Quelladresse

In dieser Tabelle werden folgende Angaben über den Datenfluss zu der gewählten IP-Quell-Adresse angezeigt:

- **IP-Ziel-Adresse** - Die IP-Ziel-Adresse des Host mit dem stärksten Verkehrsaufkommen.
- **Protokolle** - Die Protokolle, die beim Datenaustausch mit der IP-Ziel-Adresse benutzt wurden.
- **Anzahl Pakete** - Die Anzahl an Paketen, die mit der IP-Ziel-Adresse ausgetauscht wurden.

Schaltfläche Aktualisieren

Aktualisiert den Informationsstand in dem Fenster mit den neuesten Daten zum Datenverkehrsfluss.

QoS

Im Fenster QoS-Status können Sie überwachen, wie sich der Datenverkehr in QoS-konfigurierten Schnittstellen verhält. (Siehe Einer Schnittstelle QoS-Richtlinien zuweisen.) Dieses Fenster ermöglicht Ihnen darüber hinaus die Überwachung der Bandbreitennutzung und der Bytes, die für Schnittstellen ohne QoS-Konfiguration gesendet wurden. Die Überwachung von eingehendem Datenverkehr in QoS-Schnittstellen zeigt die Statistiken nur auf Protokollebene an. Statistiken auf Protokollebene andere Schnittstellen als QoS-Schnittstellen werden für Datenverkehr beider Richtungen zusammengestellt.

Über dieses Fenster können Sie die folgenden Statistiken überwachen:

- Bandbreitennutzung für Cisco SDM-definierte Datenverkehrstypen
  - Bandbreitennutzung pro Klasse unter jedem Datenverkehrstyp
  - Bandbreitennutzung für Protokolle unter jeder Klasse

  Die Bandbreitennutzung wird in KBit/s angezeigt.
- Summe der eingehenden und ausgehenden Bytes für jeden Datenverkehrstyp
  - Eingehende und ausgehende Bytes für jede unter dem Datenverkehrstyp definierte Klasse
  - Eingehende und ausgehende Bytes für jedes Protokoll für jede Klasse

  Wenn der Wert größer als 1.000.000 ist, zeigt der Graph die Bytes eventuell als ein Vielfaches von 10^6 an. Wenn der Wert größer als 1.000.000.000 ist, zeigt der Graph die Bytes eventuell als ein Vielfaches von 10^9 an.
- Statistiken zu entfernten Paketen für jeden Datenverkehrstyp

Schnittstelle – IP/Maske – Slot/Port – Beschreibung

Dieser Bereich listet die Schnittstellen mit verknüpften QoS-Richtlinien, deren IP-Adressen und Subnetzmasken, Slot-/Portinformationen, falls vorhanden, und verfügbare Beschreibungen auf.

Wählen Sie die Schnittstelle, die überwacht werden soll, aus dieser Liste aus.

Intervall anzeigen

Wählen Sie das Intervall aus, in dem Statistiken erstellt werden sollen:

- **Jetzt** – Statistiken werden erstellt, wenn Sie auf **Überwachung starten** klicken.
- **Jede Minute** – Statistiken werden erstellt, wenn Sie auf **Überwachung starten** klicken. Diese werden in einminütigen Intervallen aktualisiert.
- **Alle 5 Minuten** – Statistiken werden erstellt, wenn Sie auf **Überwachung starten** klicken. Diese werden in fünfminütigen Intervallen aktualisiert.
- **Jede Stunde** – Statistiken werden erstellt, wenn Sie auf **Überwachung starten** klicken. Diese werden in einstündigen Intervallen aktualisiert.

Überwachung starten

Klicken Sie auf diese Option, um die Überwachung der QoS-Statistiken zu starten.

QoS-Parameter für Überwachung auswählen

Wählen Sie die Datenverkehrsrichtung und den Typ der Statistik für die Überwachung aus.

Richtung

Klicken Sie entweder auf **Eingabe** oder auf **Ausgabe**.

Statistik

Wählen Sie eine der folgenden Optionen:

- Bandbreite
- Bytes
- Entfernte Pakete

Gesamter Datenverkehr – Echtzeit – Unternehmenskritisch – Unkritisch

Cisco SDM zeigt Statistiken für alle Datenverkehrsklassen in Form eines Balkendiagramms an, basierend auf dem von Ihnen ausgewählten Statistiktyp. Cisco SDM zeigt eine Meldung statt eines Balkendiagramms an, wenn keine geeigneten Statistiken für einen bestimmten Datenverkehrstyp vorhanden sind.

Einer Schnittstelle QoS-Richtlinien zuweisen

Schritt 1 Klicken Sie auf **Schnittstellen und Verbindungen > Schnittstelle/Verbindung bearbeiten**.

Schritt 2 Wählen Sie in der Schnittstellenliste diejenige aus, die Sie mit einer QoS-Richtlinie belegen wollen.

Schritt 3 Klicken Sie auf die Schaltfläche **Bearbeiten**.

Schritt 4 Klicken Sie auf die Registerkarte **Anwendungsdienst**.

Schritt 5 Wählen Sie eine QoS-Richtlinie aus der Dropdownliste **Eingehend** aus, um sie auf den eingehenden Datenverkehr der Schnittstelle anzusetzen.

Schritt 6 Wählen Sie eine QoS-Richtlinie aus der Dropdownliste **Ausgehend** aus, um sie auf den ausgehenden Datenverkehr der Schnittstelle anzusetzen.

Anwendung/Protokoll Datenverkehr

In diesem Fenster können Sie den Datenverkehr von Anwendungen und Protokollen nachprüfen, der mit NBAR (Network-based Application Recognition), einem Verfahren zur Erkennung von Protokollen und Anwendungen, erfasst wurde. NBAR dient zur Klassifizierung von Paketen, um einen effizienteren Umgang mit dem Netzwerkdatenverkehr aiuf einer bestimmten Schnittstelle zu ermöglichen.

Hinweis Wenn NBAR vom Cisco IOS-Abbild des Routers nicht unterstützt wird, steht dieses Statusfenster nicht zur Verfügung.

NBAR aktivieren

Damit der NBAR-Status einer bestimmten Schnittstelle angezeigt werden kann, muss NBAR zunächst auf dieser Schnittstelle aktiviert werden. So aktivieren NBAR:

Schritt 1 Klicken Sie auf **Schnittstellen und Verbindungen > Schnittstelle/Verbindung bearbeiten**.

Schritt 2 Wählen Sie in der Schnittstellenliste diejenige aus, auf der Sie NBAR aktivieren wollen.

Schritt 3 Klicken Sie auf die Schaltfläche **Bearbeiten**.

Schritt 4 Klicken Sie auf die Registerkarte **Anwendungsdienst**.

Schritt 5 Aktivieren Sie das Kontrollkästchen **NBAR**.

NBAR Status

Die NBAR-Statustabelle enthält folgende Statistikangaben zu der Schnittstelle, die in der Dropdown-Liste **Schnittstelle auswählen** gewählt wurde:

- Paketzahl Eingabe - Die Anzahl an Paketen des jeweiligen Protokolls, die auf der gewählten Schnittstelle eingegangen sind.
- Paketzahl Ausgabe - Die Anzahl an Paketen des jeweiligen Protokolls, die auf der gewählten Schnittstelle ausgegangen sind.
- Bitrate (bps) - Die Geschwindigkeit in Bit pro Sekunde, mit der der Datenverkehr über die Schnittstelle transportiert wurde.

NAC-Status

Wenn auf dem Router NAC konfiguriert ist, kann Cisco SDM Snapshot-Informationen über die NAC-Sitzungen auf dem Router, die Schnittstellen, auf denen NAC konfiguriert ist, und NAC-Statistiken für die ausgewählten Schnittstellen anzeigen.

Die obere Zeile in dem Fenster zeigt die Anzahl der aktiven NAC-Sitzungen an, die Anzahl der initialsierten NAC-Sitzungen sowie eine Schaltfläche, mit der Sie alle aktiven und initialisierten NAC-Sitzungen löschen können.

Das Fenster führt die Routerschnittstellen auf, mit denen NAC-Richtlinien verbunden sind.

```
FastEthernet0/0    10.10.15.1/255.255.255.0   0
```

Wenn Sie auf einen Schnittstelleneintrag klicken, wird die Information angezeigt, die von den Posture-Agents zurückgesendet wurden, die auf dem Host im Subnetz dieser Schnittstelle installiert sind. Ein Beispiel der Schnittstelleninformation folgt:

```
10.10.10.5      Remote EAP Policy      Infected       12
```

10.10.10.1 ist die IP-Adresse des Hosts. Die Remote-EAP-Richtlinie ist die Art der geltenden Authentifizierungsrichtlinie. Die aktuelle Posture des Hosts ist infiziert und es ist 12 Minuten her, seit der Host den Zulassungssteuerungsprozess abgeschlossen hat.

Hinweis Dieser Bereich des Fensters enthält keine Daten, wenn keine Posture-Information von den Hosts auf dem gewählten Subnetz zurückgesendet wurde.

Die Authentifizierungsarten sind:

- **Lokale Ausnahmerichtlinie** Eine auf dem Router konfigurierte Ausnahmerichtlinie wird zur Überprüfung des Hosts verwendet.
- **Remote EAP-Richtlinie** - Der Host sendet eine Posture zurück und es wird eine Ausnahmerichtlinie verwendet, die von einem ACS-Server zugewiesen wurde.
- **Remote Generische Zugriffsrichtlinie** Es ist kein Posture-Agent auf dem Host installiert, und der ACS-Server weist eine agentenlose Hostrichtlinie zu.

Die Posture-Agents auf den Hosts können folgende Posture-Tokens zurücksenden:

- **Healthy** - Es befinden sich keine bekannten Viren auf dem Host und es sind die neuesten Virenerkennungsdateien gespeichert.
- **Checkup** - Der Posture-Agent ermittelt, ob die neuesten Virenerkennungsdateien installiert sind.
- **Quarantäne** - Es sind nicht die neuesten Virenerkennungdateien auf dem Host installiert. Der Benutzer wird zur angegebenen Virenerkennungs-Site umgeleitet, die Anweisungen zum Downloaden der neuesten Virenerkennungsdateien enthält.
- **Infiziert** - Der Host ist mit einem unbekannten Virus infiziert. Der Benutzer wird auf eine Virenerkennungs-Site umgeleitet, wo er Virenerkennungsdatei-Aktualisierungen erhalten kann.
- **Unbekannt** - Die Posture des Hosts ist unbekannt.

Logging

Cisco SDM bietet folgende Protokollmöglichkeiten:

- Syslog - Das Protokoll des Routers
- Firewall-Bericht - Wenn auf dem Router eine Firewall konfiguriert wurde, enthält dieser Bericht die Einträge, die von der Firewall generiert wurden.
- Anwendungssicherheitsbericht - Wenn auf dem Router eine Anwendungs-Firewall konfiguriert wurde, enthält dieser Bericht die Einträge, die von der Firewall generiert wurden.
- SDEE-Meldungsbericht - Wenn SDEE auf dem dem Router konfiguriert wurde, enthält dieser Bericht die SDEE-Meldungen.

Zum Öffnen eines Berichts klicken Sie die Registerkarte mit der Bezeichnung des jeweiligen Berichts.

Syslog

Der Router enthält ein Protokoll, bei dem die Ereignisse wie beim UNIX-Syslog-Dienst nach Schweregrad gestaffelt sind.

Hinweis Das Routerprotokoll wird auch dann angezeigt, wenn Protokollmeldungen an einen Syslog-Server weitergeleitet werden.

Logging-Puffer

Zeigt an, ob der Logging-Puffer und das Syslog-Logging aktiviert sind. Wenn beide aktiviert sind, wird der Text „Enabled“ angezeigt. Der Logging-Puffer reserviert eine bestimmte Speichermenge für Protokollmeldungen. Die Einstellung in diesem Feld geht bei einem Neustart des Routers verloren. Standardmäßig ist in diesen Feldern die Aktivierung des Logging-Puffers mit einem Speicher von 4096 Byte eingestellt.

Logging-Hosts

Zeigt die IP-Adresse eines beliebigen Syslog-Hosts an, an den Protokollmeldungen weitergeleitet werden. Dieses Feld ist schreibgeschützt. Wenn Sie die IP-Adressen von Syslog-Hosts konfigurieren möchten, rufen Sie das Fenster **Zusätzliche Aufgaben > Routereigenschaften > Logging** auf.

Logging-Ebene (Puffer)

Zeigt die Logging-Ebene, die auf dem Router für den Puffer konfiguriert ist.

Anzahl an Meldungen in Protokoll

Zeigt die Gesamtzahl der im Routerprotokoll gespeicherten Meldungen an.

Logging-Ebene zur Ansicht auswählen

Wählen Sie in diesem Feld den Schweregrad der Meldungen aus, die Sie im Protokoll anzeigen möchten. Wenn Sie die Einstellung in diesem Feld ändern, wird die Liste der Protokollmeldungen aktualisiert.

Protokoll

Zeigt alle Meldungen mit dem Schweregrad an, der in dem Feld **Logging-Ebene zur Ansicht auswählen** angegeben ist. Die Protokollereignisse enthalten die folgenden Informationen:

- Spalte **Schweregrad**

  Zeigt den Schweregrad des Logging-Ereignisses an. Der Schweregrad wird in Form einer Zahl zwischen 1 und 7 angezeigt, wobei niedrigere Zahlen schwerwiegendere Ereignisse kennzeichnen. Die Schweregrade können folgendermaßen beschrieben werden:

  - 0 - Notfälle

    Das System kann nicht verwendet werden
  - 1 - Alarme

    Sofortiger Benutzereingriff erforderlich
  - 2 - Kritisch

    Es liegt ein kritischer Zustand vor
  - 3 - Fehler

    Es liegt ein Fehler vor
  - 4 - Warnungen

    Es liegt eine Warnung vor
  - 5 - Benachrichtigungen

    Normaler, jedoch außergewöhnlicher Zustand
  - 6 - Informationen

    Nur Informationsmeldungen
  - 7- Debugging

    Debugging-Meldungen
- Spalte **Uhrzeit**

  Zeigt die Uhrzeit des Protokollereignisses an.
- Spalte Beschreibung

  Zeigt eine Beschreibung des Protokollereignisses an.

Schaltfläche Aktualisieren

Aktualisiert das Fenster mit aktuellen Angaben zur Protokollierung und mit den aktuellen Protokolleinträgen.

Schaltfläche Protokoll löschen

Löscht alle Meldungen aus dem Logging-Puffer des Routers.

Schaltfläche Suchen

Öffnet ein Suchfenster. In das Suchfenster können Sie in das Feld **Suchen** einen Text eingeben. Wenn Sie auf die Schaltfläche **Suchen** klicken, werden alle Einträge angezeigt, die den gesuchten Text enthalten. Bei Suchbefehlen wird zwischen Groß- und Kleinschreibung *nicht* unterschieden.

Firewall-Protokoll

Die in diesem Fenster im oberen Teil angezeigten Protokolleinträge stammen von den Protokollmeldungen, die die Firewall generiert hat. Damit die Firewall Protokolleinträge generieren kann, müssen Sie individuelle Zugriffs-Regeln festlegen, um Protokollmeldungen zu generieren, wenn sie aufgerufen werden. Eine Anleitung zum Konfigurieren von Zugriffsregeln für die Generierung von Protokollmeldungen finden Sie im Hilfethema Wie zeige ich Aktivitäten auf meiner Firewall an?

Damit Firewall-Protokolleinträge gesammelt werden können, müssen Sie die Protokollierung im Router konfigurieren. Klicken Sie dazu auf **Zusätzliche Aufgaben > Routereigenschaften > Logging**. Klicken Sie dann auf **Bearbeiten**, um die Protokollierung zu konfigurieren. Um Firewall-Protokollmeldungen zu erhalten, müssen Sie als Protokollierungsniveau die Option Debugging (7) einstellen.

Firewall-Protokoll

Das Firewall-Protokoll wird angezeigt, wenn der Router für die Verwaltung eines Protokolls über die Verbindungsversuche konfiguriert ist, die von der Firewall akzeptiert und abgelehnt werden.

Anzahl an Versuchen, die von der Firewall verweigert wurden

Zeigt die Anzahl der Verbindungsversuche an, die von der Firewall verweigert wurden.

Tabelle der Anzahl an Versuchen, die von der Firewall verweigert wurden

Zeigt eine Liste der Verbindungsversuche an, die von der Firewall verweigert wurden. Diese Tabelle enthält die folgenden Spalten:

- Spalte **Uhrzeit**

  Zeigt die Uhrzeit an, zu der ein Verbindungsversuch verweigert wurde.

- Spalte **Beschreibung**

  Enthält die folgenden Informationen über den verweigerten Verbindungsversuch: Protokollname, Name oder Nummer der Zugriffsregel, Dienstangaben, Absenderadresse, Zieladresse und Anzahl der Pakete. Es folgt ein Beispiel:

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

Schaltfläche Aktualisieren

Ruft aktuelle Informationen vom Router ab und aktualisiert die auf dem Bildschirm angezeigten Informationen.

Schaltfläche Suchen

Öffnet ein Suchfenster. Wählen Sie im Menü **Suche** eine Suchalternative aus, und geben Sie den jeweiligen Text in das Feld **Suchen** ein. Klicken Sie anschließend auf die Schaltfläche **Suchen**, um die entsprechenden Protokolleinträge anzuzeigen.

Folgende Suchalternativen werden angeboten:

- IP-Quell-Adresse - Die IP-Adresse des Datenursprungs, von dem der Angriff ausging.

  Ein Teil der IP-Adresse kann eingegeben werden.

- IP-Ziel-Adresse - Die IP-Adresse des Angriffsziels.

  Ein Teil der IP-Adresse kann eingegeben werden.

- Protokoll - Das Netzwerkprotokoll, das für den Angriff verwendet wurde.
- Text - Ein beliebiger Text aus dem Protokolleintrag.

Bei Suchbefehlen wird zwischen Groß- und Kleinschreibung *nicht* unterschieden.

Anzeige der häufigsten Angriffe

Wählen Sie aus dem Dropdown-Menü **Ansicht** eine der folgenden Optionen für die Anzeige von Informationen über die häufigsten Angriffe aus:

- Häufigste Angriffsports - Die häufigsten Angriffe nach Ziel-Ports sortiert.
- Häufigste Hacker - sortiert nach IP-Adressen der Angreifer.

Die Tabelle mit den häufigsten Angriffen unterhalb des Dropdown-Menüs **Ansicht** enhält die Einträge zu den häufigsten Angriffen. Wenn Sie aus dem Dropdown-Menü **Ansicht** die Option **Häufigste Angriffsports** auswählen, enthält die Tabelle mit den häufigsten Angriffen Einträge in den folgenden Spalten:

- Portnummer - Der Zielport.
- Anzahl der Attacken - Die Anzahl der Angriffe auf den Zielport.
- Anzahl der abgelehnten Pakete - Die Anzahl der Pakete, denen der Zugang zum Zielport verweigert wurde.
- Details anzeigen - Ein Link, über den ein neues Fenster mit dem vollständigen Protokoll über die Angriffe auf den gewählten Port geöffnet wird.

Wenn Sie aus dem Dropdown-Menü **Ansicht** die Option **Häufigste Hacker** auswählen, enthält die Tabelle mit den häufigsten Angriffen Einträge in den folgenden Spalten:

- IP-Adresse der Hacker - Die IP-Adresse, von der die Angriffe ausgegangen sind.
- Anzahl der Attacken - Die Anzahl der Angriffe, die von der jeweiligen IP-Adresse stammen.
- Anzahl der abgelehnten Pakete - Die Anzahl der Pakete, die von der jeweiligen IP-Adresse ausgegangen sind und abgelehnt wurden.
- Details anzeigen - Ein Link, über den ein neues Fenster mit dem vollständigen Protokoll über die Angriffe von der gewählten IP-Adresse geöffnet wird.

Überwachen der Firewall über ein anderes Benutzerkonto ohne Administratorbefugnisse

Für die Überwachung der Firewall muss im Router die Funktion **Logging an Puffer** aktiviert sein. Wenn **Logging an Puffer** nicht aktiviert ist, müssen Sie sich über ein Administratoransicht-Konto oder über ein Benutzerkonto ohne Sichtbefugnis mit Berechtigungsstufe 15 bei Cisco SDM anmelden und die Protokollfunktion wunschgemäß einstellen.

Wenn Sie die Protokollierung in Cisco SDM konfigurieren möchten, wechseln Sie zu **Zusätzliche Aufgaben > Routereigenschaften > Logging**.

Anwendungssicherheitslog

Wenn die Protokollierung aktiviert ist und Sie angegeben haben, dass Alarme erzeugt werden, wenn der Router Datenverkehr von Anwendungen oder Protokollen antrifft, die Sie angegeben haben, werden diese Alarme in einem Protokoll gesammelt, das Sie in diesem Fenster ansehen können.

Um die Einträge im Anwendungssicherheit-Protokoll zu sammeln, müssen Sie im Router die Protokollfunktion entsprechend konfigurieren. Klicken Sie dazu auf **Zusätzliche Aufgaben > Routereigenschaften > Logging**. Klicken Sie dann auf **Bearbeiten**, um die Protokollierung zu konfigurieren. Um Firewall-Protokollmeldungen zu erhalten, müssen Sie als Protokollniveau **Informationsbezogen**:**(6)** oder höher einstellen. Wenn Sie als Protokollniveau bereits **Debugging (7)** eingestellt haben, sind die Anwendungssicherheitsmeldungen im Protokoll enthalten.

Folgendes ist ein Beispiel für einen Protokolltext:

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
```

```
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

Schaltfläche Aktualisieren

Aktualisiert den Bildschirm mit aktuellen Informationen zu Protokolldetails und den aktuellen Protokolleinträgen.

Schaltfläche Suchen

Öffnet ein Suchfenster. In das Suchfenster können Sie in das Feld **Suchen** einen Text eingeben. Wenn Sie auf die Schaltfläche **Suchen** klicken, werden alle Einträge angezeigt, die den gesuchten Text enthalten. Bei Suchbefehlen wird zwischen Groß- und Kleinschreibung *nicht* unterschieden.

SDEE-Meldungsbericht

Dieses Fenster listet die vom Router empfangenen SDEE-Meldungen auf. SDEE-Meldungen werden bei Änderungen an der IPS-Konfiguration erstellt.

SDEE Messages

Auswahl des anzuzeigenden SDEE-Meldungstyps:

- Alle- SDEE Fehlermeldungen, Statusmeldungen und Warnungen werden gezeigt.
- **Fehler** – Nur die SDEE-Fehlermeldungen werden angezeigt.
- **Status** – Nur die SDEE-Statusmeldungen werden angezeigt.
- Warnungen- Nur Warnungen werden gezeigt.

Schaltfläche Aktualisieren

Klicken Sie auf die Schaltfläche, um neue SDEE-Meldungen zu sehen.

Schaltfläche Suchen

Öffnet ein Suchfenster. Wählen Sie im Menü **Suche** eine Suchalternative aus, und geben Sie den jeweiligen Text in das Feld **Suchen** ein. Klicken Sie anschließend auf die Schaltfläche **Suchen**, um die entsprechenden Protokolleinträge anzuzeigen.

Folgende Suchalternativen werden angeboten:

- IP-Quell-Adresse
- IP-Ziel-Adresse
- Text

Bei Suchbefehlen wird zwischen Groß- und Kleinschreibung *nicht* unterschieden.

Zeit

Die Uhrzeit, zu der die Meldung eingegangen ist.

Typ

Dazu gehören Fehler-, Status- und Warnmeldungen. Klicken Sie auf SDEE-Meldungstext, um mögliche SDEE-Meldungen anzuzeigen.

Beschreibung

Verfügbare Beschreibung.

IPS-Status

Dieses Fenster wird angezeigt, wenn der Router ein Cisco IOS-Abbild ausführt, das IPS-Version 4.x oder früher unterstützt. In diesem Fenster wird eine Tabelle mit IPS-Signaturstatistiken angezeigt, die nach Signaturtyp gegliedert sind. Folgende statistische Angaben werden dort ausgegeben:

- **Signatur-ID** - Die Kennzahl der Signatur.
- **Beschreibung** - Beschreibung der Signatur.
- **Risikobewertung** – Ein Wert zwischen 0 und 100, der eine numerische Quantifizierung des mit einem bestimmten Ereignis im Netzwerk verbundenen Risikos darstellt.
- **Aktion** – Die auszuführende Aktion, wenn ein Paket mit einer Signatur übereinstimmt.
- **IP-Quell-Adresse** - Die IP-Adresse des Hosts, von dem das Paket ursprünglich ausgegeben wurde.
- **IP-Ziel-Adresse** - Die IP-Adresse des Zielhosts für das Paket.
- **Treffer** - Die Anzahl übereinstimmender Pakete.
- **Anzahl Abbrüche** - Die Anzahl übereinstimmender Pakete, die ignoriert wurden.

Zum Sortieren der Signaturen klicken Sie auf die Spaltenüberschrift mit dem Namen der Signaturstatistik, nach der sortiert werden soll.

Hinweis Wenn Sie nach Signaturen sortieren, geht jedoch die Sortierung nach Signaturtyp dabei verloren. Um die Gruppierung nach Signaturtyp wiederherzustellen, klicken Sie auf die Schaltfläche **Aktualisieren**.

Gesamtzahl aktiver Signaturen

Zeigt die Summe der verfügbaren Signaturen an, die im Router aktiv sind.

Gesamtzahl inaktiver Signaturen

Zeigt die Summe der verfügbaren Signaturen an, die im Router nicht aktiv sind.

Schaltfläche Aktualisieren

Klicken Sie darauf, um die neuesten Signaturstatistiken abzurufen und zu übernehmen.

Schaltfläche Löschen

Klicken Sie hierauf, um alle statistischen Zählerwerte wieder auf 0 zu stellen.

SDEE-Meldebericht

Klicken Sie hier, um SDEE-Meldungen anzuzeigen. Sie können diese Meldungen auch durch Klicken auf **Monitor > Logging > SDEE-Meldungsbericht** anzeigen.

IPS-Signaturstatistiken

Dieses Fenster wird angezeigt, wenn der Router eine IOS IPS 5.x-Konfiguration verwendet. Es werden Statistiken für jede aktivierte Signatur in der IOS IPS-Konfiguration angezeigt. Oben im Fenster werden die Gesamtzahlen der Signaturen angezeigt, um einen Überblick über die Signaturkonfiguration zu liefern. Es werden folgende Summen angegeben:

- Summe der Signaturen
- Summe der aktivierten Signaturen
- Summe der ausgeschiedenen Signaturen
- Summe der kompilierten Signaturen

Schaltflächen Aktualisieren und Löschen

Klicken Sie auf **Aktualisieren**, um die neuesten Signaturstatistiken abzurufen und zu übernehmen. Klicken Sie auf **Löschen**, um alle statistischen Zählerwerte wieder auf 0 zu stellen.

SDEE-Meldebericht

Klicken Sie hier, um SDEE-Meldungen anzuzeigen. Sie können diese Meldungen auch durch Klicken auf **Monitor > Logging > SDEE-Meldungsbericht** anzeigen.

Bereich Signaturliste

Für alle Signaturen wird die Signatur-ID, Beschreibung, Anzahl der Treffer und die Anzahl der Abbrüche dargestellt. Wenn ein Paket mit einer Signatur übereinstimmt, werden auch die Quell- und Ziel-IP-Adresse aufgelistet.

Statistiken zur IPS-Warnung

Im Fenster **Statistiken zur IPS-Warnung** werden Warnungsstatistiken zur einfachen Identifizierung mit Farbkodierungen angezeigt. Im oberen Teil des Bildschirms befindet sich eine Legende, in der die Bedeutung der Farben erläutert wird.

Farbe	Erläuterung
ROT	Das Ereignis hat eine Warnung mit einer hohen Risikobewertung (RR) zwischen 70 und 100 erzeugt.
MAGENTA	Das Ereignis hat eine Warnung mit einer mittleren Risikobewertung (RR) zwischen 40 und 69 erzeugt.
BLAU	Das Ereignis hat eine Warnung mit einer niedrigen Risikobewertung (RR) zwischen 0 und 39 erzeugt.

Durch Klicken auf die Spaltenüberschrift wird die Anzeige nach den Werten dieses Parameters sortiert. Beispiel: Wenn Sie auf die Überschrift **Signatur- ID** klicken, wird die Anzeige in auf- oder absteigender numerischer Reihenfolge nach den Signatur-IDs sortiert. Jede Spalte wird in der folgenden Liste beschrieben:

- **Signatur-ID** - Die Kennzahl der Signatur.
- **Beschreibung** - Beschreibung der Signatur.
- Risikobewertung – Ein Wert zwischen 0 und 100, der eine numerische Quantifizierung des mit einem bestimmten Ereignis im Netzwerk verbundenen Risikos darstellt.

- Ereignisaktion – Die von IOS IPS auszuführende Aktion, wenn ein Ereignis mit einer Signatur übereinstimmt.
- Quell-IP-Adresse – Die IP-Adresse, von der das Paket ursprünglich ausgegeben wurde.
- Ziel-IP-Adresse – Die IP-Adresse, an die das Paket adressiert war. Wenn das Paket in böser Absicht erstellt wurde, wird die Ziel-IP-Adresse als Ziel angesehen.
- Treffer - Die Anzahl übereinstimmender Pakete.
- Anzahl Abbrüche – Die Anzahl übereinstimmender Pakete, die ignoriert wurden.
- Engine – Die Signatur-Engine, die mit der Signatur verknüpft ist.

802.1x-Authentifizierungsstatus

802.1x-Authentifizierung im Schnittstellenbereich

Schnittstelle

802.1x-Authentifizierung

Erneute Authentifizierung

802.1x-Clients-Bereich

Client-MAC-Adresse

Authentifizierungsstatus

Schnittstelle

KAPITEL 40

Befehle im Menü Datei

Die folgenden Optionen sind über das Menü **Datei** von Cisco Router and Security Device Manager (Cisco SDM) verfügbar.

Aktive Konfiguration auf PC speichern

Speichert die aktive Konfigurationsdatei des Routers in einer Textdatei auf dem PC.

Konfiguration an Router senden

In diesem Fenster können Sie alle Konfigurationsänderungen, die Sie mit Cisco SDM vorgenommen haben, an den Router weiterleiten. Beachten Sie, dass sich mit Cisco SDM vorgenommene Konfigurationsänderungen erst auf den Router auswirken, wenn Sie die Konfiguration senden.

Speichern Sie die aktive Konfiguration in der Startkonfiguration des Routers

Aktivieren Sie dieses Kontrollkästchen, damit Cisco SDM die im Fenster angezeigte Konfiguration sowohl in der aktiven Konfigurationsdatei als auch in der Startdatei des Routers speichert. Die aktive Konfigurationsdatei ist temporär – sie wird bei einem Neustart des Routers gelöscht. Wenn die Konfiguration in der Startkonfiguration des Routers gespeichert wird, werden die Konfigurationsänderungen nach einem Neustart beibehalten.

Wenn Cisco SDM für die Konfiguration eines Cisco 7000-Routers verwendet wird, ist das Kontrollkästchen **Speichern Sie die aktive Konfiguration in der Startkonfiguration des Routers** deaktiviert, wenn die aktive Konfiguration **boot network**- oder **boot host**-Befehle mit **service config**-Befehlen enthält.

Abbrechen

Klicken Sie auf diese Schaltfläche, um die Konfigurationsänderungen zu verwerfen, und schließen Sie das Dialogfeld **Cisco SDM an Router liefern**.

In Datei speichern

Klicken Sie auf diese Schaltfläche, um die im Fenster angezeigten Konfigurationsänderungen in einer Textdatei zu speichern.

In Startkonfiguration schreiben

Schreibt die aktive Konfigurationsdatei des Routers in die Startkonfiguration des Routers.

Wird Cisco SDM für die Konfiguration eines Cisco 7000-Routers verwendet, ist dieser Menübefehl deaktiviert, wenn die aktive Konfiguration **boot network**- oder **boot host**-Befehle mit **service config**-Befehlen enthält.

Auf werksseitige Einstellungen zurücksetzen

Siehe Auf werksseitige Einstellungen zurücksetzen.

Dateiverwaltung

In diesem Fenster können Sie das Dateisystem auf Ihrem Cisco Router Flash-Speicher und den USB-Flashgeräten, die an diesen Router angeschlossen sind, ansehen und verwalten. Nur DOSFS-Dateisystem können in diesem Fenster angesehen und verwaltet werden.

Auf der linken Seite des Fensters sehen Sie den erweiterbaren Baum, der das Verzeichnissystem auf Ihrem Cisco Router Flash-Speicher und den USB-Flashes, die an diesen Router angeschlossen sind, darstellt.

Die rechte Seite des Fensters zeigt eine Liste der Datei- und Verzeichnisnamen, die in dem Verzeichnis gefunden wurden, das Sie auf der linken Seite des Fensters ausgewählt haben. Es zeigt auch die Größe jeder Datei in Bytes und Datum und Zeit der letzten Änderung an den Dateien und Verzeichnissen.

Sie können eine Datei oder ein Verzeichnis aus der Liste auf der rechten Seite des Fensters auswählen, und dann einen der Befehle aus der Liste oben auswählen.

Verzeichnisse (Ordner) können umbenannt oder gelöscht werden. Einzelne oder mehrere Dateien können kopiert, eingefügt oder gelöscht und einzelne Dateien umbenannt werden. Es gelten jedoch folgende Beschränkungen:

- Dateien können nicht in das Verzeichnis kopiert werden, aus dem sie herauskopiert wurden.
- Wenn Cisco SDM von Ihrem Router-Flash gestartet wird, können Cisco SDM-Dateien nicht gelöscht werden.

  Sie können Cisco SDM-Dateien löschen, die Kopien anderer Dateien sind, oder wenn Cisco SDM von einem PC gestartet wird.
- Wenn Cisco SDM von Ihrem Router-Flash gestartet wird, können Cisco SDM-Dateien nicht umbenannt werden.

  Sie können Cisco SDM-Dateien umbenennen, die Kopien anderer Dateien sind, oder wenn Cisco SDM von einem PC gestartet wird.
- Wenn Cisco SDM von Ihrem Router-Flash gestartet wird, können Sie eine Cisco SDM-Datei nicht ersetzen (eine Datei mit demselben Namen darüber kopieren).

  Sie können Cisco SDM-Dateien ersetzen, die Kopien anderer Dateien sind, oder wenn Cisco SDM von einem PC gestartet wird.

- Cisco IOS-Softwaredateien können nicht umbenannt werden.
- Verzeichnisse (Ordner) können nicht kopiert werden.

Wenn Ihr Router von einem tftp-Server gestartet wird, gelten keine Beschränkungen beim Handhaben der Dateien.

Schaltfläche Aktualisieren

Klicken Sie auf die Schaltfläche **Aktualisieren**, um ein neues Abbild der Verzeichnisse und Dateien aus dem Flash-Speicher des Cisco-Routers und den USB-Flash-Geräten abzurufen, die an diesen Router angeschlossen sind.

Schaltfläche Format

Klicken Sie auf die Schaltfläche **Format**, um Ihren Cisco Router-Flashspeicher oder ein USB-Flash-Gerät, das an diesen Router angeschlossen ist, neu zu formatieren. Die Schaltfläche **Format** ist nur dann verfügbar, wenn links im Fenster ein Symbol für den Flash-Speicher Ihres Cisco-Routers oder ein USB-Flash-Gerät ausgewählt wurde.

Vorsicht Wenn Sie den Flash-Speicher Ihres Cisco-Routers oder ein USB-Flash-Gerät, das an diesen Router angeschlossen ist, neu formatieren, *löscht* der Router alle Dateien aus dem Dateisystem.

Die Schaltfläche Neuer Ordner

Klicken Sie auf **Neuer Ordner**, um ein neues Verzeichnis in dem Verzeichnis zu erstellen, das Sie auf der linken Seite des Fensters ausgewählt haben. Ordnernamen dürfen keine Leerstellen oder Fragezeichen (?) enthalten.

Schaltfläche Datei vom PC laden

Klicken Sie auf **Datei vom PC laden**, um ein Dateiauswahlfenster auf dem lokalen PC zu öffnen. Wählen Sie eine Datei, um das gewählte Verzeichnis auf Ihren Cisco Router-Flashspeicher oder den USB-Flash zu speichern, der an diesem Router angeschlossen ist. Cisco SDM-Dateien und Dateien mit Namen, die Leerstellen enthalten, können nicht mit der Option **Datei vom PC laden** geladen werden.

Cisco SDM-Dateien, wie z. B. Cisco SDM.tar, können nicht mit der Option **Datei vom PC laden** geladen werden. Cisco SDM-Dateien sollten mit der Option **Extras > SDM aktualisieren** geladen werden.

Wenn Sie Datei vom PC laden zum Laden einer Boot-Image-Datei verwenden, kann sie nicht ins aktuelle Boot-Imagedateiverzeichnis gespeichert werden.

Die Schaltfläche Kopieren

Wählen Sie auf der rechten Seite des Fensters eine Datei aus, und klicken Sie auf die Schaltfläche **Kopieren**, um die Datei zu kopieren.

Die Schaltfläche Einfügen

Nachdem Sie auf die Schaltfläche **Kopieren** geklickt haben, um eine Datei zu kopieren, klicken Sie auf die Schaltfläche **Einfügen**, um die Kopie der Datei in ein anderes Verzeichnis zu kopieren. Wählen Sie ein Zielverzeichnis auf der linken Seite des Fensters. Es ist nicht möglich, eine Kopie der Datei im demselben Verzeichnis wie die Originaldatei abzulegen.

Die Schaltfläche Umbenennen

Wählen Sie auf der rechten Seite des Fensters eine Datei oder ein Verzeichnis aus, und klicken Sie auf die Schaltfläche **Umbenennen**, um den Namen zu ändern. Namen dürfen keine Leerstellen oder Fragezeichen („?“) enthalten.

Die Schaltfläche Löschen

Wählen Sie auf der rechten Seite des Fensters eine Datei oder ein Verzeichnis aus, und klicken Sie auf die Schaltfläche **Löschen**, um sie bzw. es zu löschen. Eine Datei mit einem Schreibschutzsymbol neben dem Namen kann nicht gelöscht werden.

Name

Klicken Sie auf **Name**, um die Dateien und Verzeichnisse alphabetisch nach Namen zu sortieren. Wenn Sie erneut auf **Name** klicken, wird die Reihenfolge umgekehrt.

Größe

Klicken Sie auf **Größe**, um die Dateien und Verzeichnisse nach ihrer Größe zu sortieren. Verzeichnisse haben immer eine Größe von 0 Bytes, auch wenn sie nicht leer sind. Wenn Sie erneut auf **Größe** klicken, wird die Reihenfolge umgekehrt.

Zeit geändert

Klicken Sie auf **Zeit der Änderung**, um die Dateien und Verzeichnisse nach Datum und Uhrzeit der Änderung zu sortieren. Wenn Sie nochmals auf **Zeit der Änderung** klicken, wird die Reihenfolge umgekehrt.

Rename

In diesem Fenster können Sie eine Datei auf Ihrem Cisco Router Flash-Speicher und den USB-Flashgeräten, die an diesen Router angeschlossen sind, umbenennen.

Geben Sie den neuen Dateinamen im Feld Neuer Name ein. Der Pfad zum Speicherort der Datei wird oben im Feld Neuer Name angegeben.

New Folder

In diesem Fenster können Sie einen neuen Ordner im Verzeichnissystem auf Ihrem Cisco Router Flash-Speicher und den USB-Flashgeräten, die an diesen Router angeschlossen sind, benennen und erstellen.

Geben Sie den Namen des neuen Ordners im Feld Ordnername ein. Der Pfad zum Speicherort des neuen Ordners wird oben im Feld Ordnername angegeben.

SDF auf PC speichern

Wenn Sie in IPS arbeiten, können Sie die Signatur-Definitionsdatei (SDF), mit der Sie arbeiten, auf Ihren PC speichern. Navigieren Sie zu dem Verzeichnis, in dem Sie die Datei speichern möchten, und klicken Sie auf **Speichern**.

Beenden

Beendet Cisco Router and Security Device Manager.

Squeeze flash kann nicht durchgeführt werden

Dieses Fenster wird angezeigt, wenn der Router keine **squeeze flash**-Operation durchführen kann, weil für den Router nie eine **erase flash**-Operation durchgeführt wurde. In diesem Hilfethema wird erläutert, wie Sie die Dateien herunterladen, die Sie vor dem Durchführen der **erase flash**-Operation benötigen, wie Sie **erase flash** durchführen und wie Sie danach die Dateien wieder auf den Router laden und wieder eine Verbindung zu Cisco SDM herstellen.

Mit der Ausführung des **erase flash**-Befehls werden Cisco SDM und das Cisco IOS-Abbild aus dem Flash-Speicher des Routers entfernt, und Ihre Verbindung zum Router wird getrennt. Drucken Sie dieses Hilfethema aus, damit Sie anhand der Anweisung ein Cisco IOS-Abbild und SDM.tar von Cisco.com abrufen und auf dem Router installieren können.

Schritt 1 Stellen Sie sicher, dass die Stromversorgung des Routers nicht ausfällt. Wenn die Stromversorgung des Routers nach einer **erase flash:**-Operation ausfällt, enthält der Speicher kein Cisco IOS-Abbild.

Hinweis Wenn der Router nach dem erase flash-Vorgang Leistung verliert, können Sie die Vorgehensweise unter dem folgenden Link verwenden, um die Leistung wiederherzustellen: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3700/sw_conf/37_swcf/appendc.htm#xtocid11

Schritt 2 Speichern Sie die aktive Konfiguration des Routers in einer Datei auf dem PC. Klicken Sie dazu auf **Datei -> Aktive Konfiguration auf PC speichern**, und geben Sie einen Dateinamen ein.

Schritt 3 Bereiten Sie einen TFTP-Server vor, auf den Sie Dateien speichern und von dem aus Sie diese auf den Router kopieren können. Sie müssen Schreibzugriff auf den TFTP-Server besitzen. Sie können Ihren PC zu diesem Zweck benutzen, wenn er über ein TFTP-Serverprogramm verfügt.

Schritt 4 Verwenden Sie den **tftpcopy**-Befehl, um das Cisco IOS-Abbild, die Datei SDM.tar und die Datei SDM.shtml vom Flash-Speicher auf einen TFTP-Server zu kopieren:

copy flash: tftp://*Adresse des tftp-Servers***/***Dateiname*

Beispiel:

```
copy flash: tftp://10.10.10.3/SDM.tar
```

Hinweis Wenn Sie es vorziehen, ein Cisco IOS-Abbild und die Dateien SDM.tar und SDM.shtml herunterzuladen, gehen Sie nach diesen Anweisungen vor, um über eine Internetverbindung ein von Cisco SDM unterstütztes Cisco IOS-Abbild und die Dateien SDM.tar und SDM.shtml herunterzuladen. Legen Sie diese Dateien dann auf einem TFTP-Server ab.

a. Klicken Sie auf den folgenden Link, um ein Cisco IOS-Abbild vom Cisco Software Center abzurufen:

http://www.cisco.com/kobayashi/sw-center/

b. Rufen Sie ein Abbild ab, das die von Ihnen gewünschten Funktionen in der Version 12.2(11)T oder höher unterstützt. Speichern Sie die Datei auf dem TFTP-Server, auf den vom Router zugegriffen werden kann.

c. Verwenden Sie den folgenden Link, um die Dateien SDM.tar und SDM.shtml abzurufen. Speichern Sie dann SDM.tar und SDM.shtml auf dem TFTP-Server.

http://www.cisco.com/go/sdm

Schritt 5 Melden Sie sich vom PC aus mit Telnet beim Router an, und wechseln Sie in den Aktivierungsmodus.

Schritt 6 Geben Sie den Befehl **erase flash:** ein, und bestätigen Sie ihn. Das IOS-Abbild, die Konfigurationsdatei und die Dateien SDM.tar und SDM.shtml des Routers werden aus dem NVRAM entfernt.

Schritt 7 Verwenden Sie den **tftpcopy**-Befehl, um zunächst das IOS-Abbild und dann SDM.tar vom TFTP-Server auf den Router zu kopieren:

copy tftp://*TFTP-Serveradresse***/***Dateiname* **flash:**

Beispiel:

```
copy tftp://10.10.10.3/Name_des_IOS_Abbilds flash:
! Ersetzen Sie Name_des_IOS_Abbilds durch den tatsächlichen Namen des
Abbilds
copy tftp://10.10.10.3/SDM.tar flash:
```

Schritt 8 Starten Sie den Webbrowser, und bauen Sie eine neue Verbindung zu Cisco SDM auf. Verwenden Sie dazu die IP-Adresse, die Sie beim Starten der Cisco SDM-Sitzung verwendet haben.

Nachdem nun eine **erase flash**-Operation auf dem Router ausgeführt wurde, können Sie bei Bedarf den **squeeze flash**-Befehl ausführen.

Squeeze flash kann nicht durchgeführt werden

KAPITEL 41

Befehle im Menü Bearbeiten

Die folgenden Optionen sind über das Menü **Bearbeiten** von Cisco Router and Security Device Manager (Cisco SDM) verfügbar.

Einstellungen

In diesem Bildschirm können Sie die folgenden Optionen von Cisco Router and Security Device Manager konfigurieren:

Zeigen Sie die Befehle in der Vorschau an, bevor Sie diese an den Router senden

Wählen Sie diese Option, wenn Sie möchten, dass Cisco SDM eine Liste der Cisco IOS-Konfigurationsbefehle anzeigt, die erstellt wurde, bevor die Befehle zum Router gesendet wurden.

Signaturdatei auf Flash speichern

Wählen Sie diese Option, wenn Sie möchten, dass die Signaturdefinitionsdatei (SDF), an der Sie arbeiten, auf dem Router-Flash gespeichert wird, wenn Sie auf **Änderungen übernehmen** klicken.

Bestätigen Sie, bevor Sie Cisco SDM schließen

Dies ist das Standardverhalten von Cisco SDM. Wählen Sie diese Option aus, wenn Cisco SDM ein Bestätigungsdialogfeld anzeigen soll, wenn Sie Cisco SDM beenden.

Überwachungsschnittstellenstatus fortsetzen bei Wechseln zwischen Modus/Aufgaben

Das ist das Standardverhalten von Cisco SDM. Cisco SDM beginnt mit der Überwachung des Schnittstellenstatus, wenn Sie auf **Überwachen** klicken und dann **Schnittstellenstatus** auswählen. Damit Cisco SDM mit der Überwachung der Schnittstelle auch dann fortfährt, wenn Sie den Überwachungsmodus verlassen und andere Aufgaben in Cisco SDM ausführen, aktivieren Sie dieses Kontrollkästchen, und geben Sie die maximale Anzahl von Schnittstellen an, die Cisco SDM überwachen soll. Der Standardwert für die maximale Anzahl der zu überwachenden Schnittstellen ist 4.

KAPITEL 42

Befehle im Menü Ansicht

Die folgenden Optionen sind über das Menü **Ansicht** von Cisco Router and Security Device Manager (Cisco SDM) verfügbar.

Startseite

Zeigt die Startseite von Cisco SDM mit Informationen zur Hardware und Software des Routers sowie zu LAN-, WAN-, Firewall- und VPN-Konfigurationen an.

Konfigurieren

Zeigt die Cisco SDM-Taskleiste an, mit der Sie geleitete und manuelle Konfigurationen für Schnittstellen und Verbindungen, Firewalls und ACLs, VPN-Routing und weitere Aufgaben durchführen können.

Monitor

Zeigt das Cisco SDM-Monitor-Fenster an, in dem Sie Statistiken zu Ihrem Router und Ihrem Netzwerk anzeigen können.

Aktive Konfiguration

Zeigt die aktive Konfiguration des Routers an.

Show-Befehle

Zeigt das Dialogfeld **Show-Befehle** an, in dem Sie Cisco IOS-**Show**-Befehle an den Router senden, die Ausgabe anzeigen und auf Ihrem PC speichern können. Die Ausgabedatei wird unter dem Standardnamen show_<*command*>[*router_ip_adresse*] gespeichert.

Mit dem Dialogfeld **Show-Befehle** können Sie die Ausgabe der folgenden **Show**-Befehle anzeigen:

- **show flash** – Zeigt den Inhalt des Flash-Speichers des Routers an.
- **show startup-config** – Zeigt die Startkonfigurationsdatei des Routers an.
- **show access-lists** – Zeigt alle Zugriffssteuerungslisten (ACL)-Befehle an, die momentan auf dem Router konfiguriert sind.
- **show diag** – Zeigt Informationen zu der auf dem Router installierten Hardware an.
- **show interfaces** – Zeigt Informationen zur Konfiguration der einzelnen Schnittstellen und zu den Paketen an, die über die Schnittstelle übertragen werden.
- **show protocols** – Zeigt Informationen zu den Netzwerkprotokollen an, die auf den einzelnen Schnittstellen konfiguriert sind.
- **show version** – Zeigt Informationen zu der Cisco IOS-Softwareversion an, die auf dem Router ausgeführt wird.
- **show tech-support** – Zeigt die Ausgabe von allen anderen **show**-Befehlen an.
- **show environment** – Zeigt Informationen zu der auf dem Router installierten Stromversorgung an. Wenn Ihr Router diesen Befehl nicht unterstützt, wird er möglicherweise nicht in der Dropdown-Liste **Show-Befehle** angezeigt.

Cisco SDM-Standardregeln

Auf dem Standardregelbildschirm von Cisco SDM wird eine Liste aller Standardregeln angezeigt, die von Cisco SDM konfiguriert wurden. Auf der linken Seite des Bildschirms befindet sich eine Struktur, in der Optionen für Zugriffsregeln, Firewall, VPN - IKE-Richtlinien und VPN - Transformationssätze angezeigt werden. Wenn Sie die Standardregeln für diese Optionen anzeigen möchten, klicken Sie in der Struktur auf die Option. Daraufhin werden die Standardregeln für diese Option auf der rechten Seite angezeigt. Weitere Informationen zu den Regeln finden Sie in den nachfolgenden Optionsbeschreibungen.

Zugriffsregeln

Zeigt alle Standardregeln der Zugriffssteuerungsliste (ACL) und je eine kurze Beschreibung an.

Firewall

Zeigt die Standardrichtlinien der Cisco SDM-Anwendungssicherheit an. Wählen sie eine Sicherheitsrichtlinie, die Sie in der Liste oben rechts im Fenster ansehen möchten.

- SDM_HIGH—Diese Richtlinie verhindert die Verwendung von Instant Messaging und Point-to-Point Anwendungen auf dem Netzwerk. Sie überwacht den HTTP und E-Mail-Datenverkehr und lehnt Verkehr ab, der nicht mit ihrem Protokoll übereinstimmt. Sie sendet anderen TCP- und UPD-Verkehr zurück, für Sitzungen, die in der Firewall gestartet wurden.
- SDM_MEDIUM—Diese Richtlinie überwacht die Verwendung von Instant Messaging und Point-to-Point Anwendungen, sowie HTTP und E-Mail-Datenverkehr. Sie sendet anderen TCP- und UPD-Verkehr zurück, für Sitzungen, die in der Firewall gestartet wurden.
- SDM_LOW—Diese Richtlinie überwacht keinen Anwendungsverkehr. Sie sendet anderen TCP- und UPD-Verkehr zurück, für Sitzungen, die in der Firewall gestartet wurden.

VPN - IKE-Richtlinie

Zeigt die Standardrichtlinien für Internet Key Exchange (IKE) an.

VPN - Transformationssätze

Zeigt die Standard-Transformationssätze für IP Security (IPSec) an.

Aktualisieren

Lädt die Konfigurationsinformationen vom Router neu. Wenn nicht gesendete Befehle vorhanden sind, zeigt Cisco SDM ein Meldungsfenster an, in dem Sie darüber informiert werden, dass bei der Aktualisierung nicht gesendete Befehle verloren gehen. Wenn Sie die Befehle senden möchten, klicken Sie in diesem Fenster auf **Nein** und dann in der Cisco SDM-Symbolleiste auf **Senden**.

KAPITEL 43

Befehle im Menü Extras

Die folgenden Optionen sind über das Menü **Extras** von Cisco Router and Security Device Manager (Cisco SDM) verfügbar.

Ping

Öffnet das Dialogfeld **Ping**, mit dem Sie eine Ping-Meldung an ein anderes Gerät im Netzwerk senden können. Informationen zur Verwendung des Fensters **Ping** finden Sie unter Spiegel generieren....

Telnet

Zeigt das Windows Telnet-Dialogfeld an, mit dem Sie über das Telnet-Protokoll eine Verbindung zu Ihrem Router herstellen und auf die Cisco IOS-Befehlszeilenschnittstelle (Command-Line Interface, CLI) zugreifen können.

Sicherheitsprüfung

Zeigt den Cisco SDM-Bildschirm für die Sicherheitsprüfung an. Weitere Informationen finden Sie unter Sicherheitsprüfung.

USB-Token-PIN-Einstellungen

Mit dem Dialogfeld USB-Token PIN-Einstellungen können Sie PINs für USB-Tokens einstellen, die an Ihren Router angeschlossen sind.

Wählen Sie eine PIN-Art aus

Wählen Sie **Benutzer-PIN**, um eine Benutzer-PIN oder **Admin-PIN**, um eine Administrator-PIN einzustellen.

Eine Benutzer-PIN wird zur Anmeldung beim Router verwendet. Wenn Sie ein USB-Token an einen Router anschließen und der Name des Tokens sowie die Benutzer-PIN mit einem Eintrag unter **Konfigurieren > VPN > VPN-Komponenten > Public-Key-Infrastruktur > USB-Token** übereinstimmen, werden Sie automatisch beim Router angemeldet.

Eine Adminstrator-PIN wird verwendet, um mit der Herstellersoftware die USB-Tokeneinstellungen zu verwalten. Mit Cisco SDM können Sie die Administrator-PIN für ein USB-Token ändern, wenn Sie die aktuelle Administrator-PIN bereitstellen können.

Token Name

Geben Sie den Namen USB-Tokens an.

Ein Tokenname wird vom Hersteller eingestellt. USB-Token, die von Aladdin Knowledge Systems hergestellt wurden, heißen beispielsweise eToken.

Sie können auch den Namen **usbtoken*x*** eingeben, wobei *x* die Nummer auf dem USB-Port ist, an den das USB-Token angeschlossen ist. Ist das USB-Token z. B. an USB-Port 0 angemeldet, lautet der Name usbtoken0.

Aktuelle PIN

Geben Sie die bestehende Benutzer- oder Administrator-PIN ein. Wenn Sie die aktuelle PIN nicht kennen, müssen Sie die Herstellersoftware des USB-Token verwenden, um sie zu finden.

Neue PIN

Geben Sie eine neue PIN für das USB-Token ein. Die aktuelle PIN wird durch die neue PIN ersetzt. Die neue PIN muss mindestens 4 Ziffern lang sein.

PIN bestätigen

Geben Sie die neue PIN nochmals ein, um sie zu bestätigen.

Neue PIN auf den Router speichern

Aktivieren Sie das Kontrollkästchen **Neue PIN auf Router speichern**, um die neue PIN als Eintrag unter **Konfigurieren > VPN > VPN-Komponenten > Public-Key-Infrastruktur > USB-Token** zu speichern. Wenn ein Eintrag mit demselben Namen bereits unter **Konfigurieren > VPN > VPN Komponenten > Public-Key-Infrastruktur > USB-Token** vorhanden ist, wird er durch den neuen Eintrag ersetzt.

Das Kontrollkästchen **Neue PIN auf Router speichern** ist nur für Benutzer-PINs verfügbar.

Wireless-Anwendung

Wenn der Router mit Funkschnittstellen ausgestattet ist, können Sie die Wireless-Anwendung starten, um diese Schnittstellen zu konfigurieren und zu überwachen. Cisco SDM kann Sie bei der Konfiguration und Anzeige der IP-Adressen oder Bridging-Details zu einer Wireless-Schnittstelle unterstützen, andere Konfigurationsparameter müssen Sie allerdings über die Wireless-Anwendung festlegen.

Aktualisieren von Cisco SDM

Sie können festlegen, dass Cisco SDM automatisch ein Update herunterlädt und installiert.

Aktualisieren von Cisco SDM über Cisco.com

Sie können Cisco SDM direkt über Cisco.com aktualisieren. Cisco SDM überprüft die unter Cisco.com verfügbaren Versionen und informiert Sie, wenn eine neuere Version als die Version vorhanden ist, die derzeit auf dem Router ausgeführt wird. Sie können Cisco SDM dann mit dem Aktualisierungsassistenten aktualisieren.

So aktualisieren Sie Cisco SDM über Cisco.com:

Schritt 1 Wählen Sie im Menü **Extras** die Option **Aktualisieren von Cisco SDM über Cisco.com**. Wenn Sie diese Option auswählen, wird der Aktualisierungsassistent gestartet.

Schritt 2 Verwenden Sie den Aktualisierungsassistenten, um die Cisco SDM-Dateien zu ermitteln und auf Ihren Router zu kopieren.

Aktualisieren von Cisco SDM über den lokalen PC

Sie können die Aktualisierung von Cisco SDM unter Verwendung einer ZIP-Datei für SDM durchführen, die Sie von Cisco.com heruntergeladen haben. Cisco SDM stellt einen Aktualisierungsassistenten bereit, der die erforderlichen Dateien auf Ihren Router kopiert.

Gehen Sie folgendermaßen vor, um Cisco SDM über den PC zu aktualisieren, auf dem Sie Cisco SDM ausführen:

Schritt 1 Laden Sie die Datei sdm-v*nn*.zip unter dem folgenden URL herunter:

`http://www.cisco.com/cgi-bin/tablebuild.pl/sdm`

Wenn mehrere ZIP-Dateien für Cisco SDM vorhanden sind, wählen Sie die Kopie mit der höchsten Versionsnummer aus.

Schritt 2 Verwenden Sie den Aktualisierungsassistenten, um die Cisco SDM-Dateien von Ihrem PC auf den Router zu kopieren.

Aktualisieren von Cisco SDM von der CD

Wenn Sie über die Cisco SDM-CD verfügen, können Sie diese zur Aktualisierung von Cisco SDM auf Ihrem Router verwenden. Gehen Sie dazu wie folgt vor:

Schritt 1 Legen Sie die Cisco SDM-CD in das CD-Laufwerk Ihres Computers ein.

Schritt 2 Wählen Sie **Cisco SDM aktualisieren von CD**, und klicken Sie im Fenster **Allgemeine Anleitung** auf **Cisco SDM aktualisieren**, nachdem Sie die Informationen gelesen haben.

Schritt 3 Cisco SDM ermöglicht es Ihnen, die Datei SDM-Updates.xml auf der CD zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf **Öffnen**.

Schritt 4 Befolgen Sie die Anweisungen des Installationsassistenten.

CCO-Anmeldung

Sie müssen für den Zugriff auf diese Webseite einen CCO-Anmeldenamen und ein Kennwort eingeben. Geben Sie einen Benutzernamen und ein Kennwort ein, und klicken Sie dann auf **OK**.

Wenn Sie nicht über einen CCO-Anmeldenamen und ein Kennwort verfügen, können Sie eines erhalten, indem Sie einen Webbrowser öffnen und zur Cisco-Website unter folgendem Link wechseln:

http://www.cisco.com

Wenn die Webseite geöffnet wird, klicken Sie auf **Registrieren**, und geben Sie die erforderlichen Informationen für die Zuteilung eines Benutzernamens und Kennworts ein. Versuchen Sie diesen Vorgang dann erneut.

KAPITEL 44

Befehle im Menü „Hilfe“

Die folgenden Optionen sind über das Hilfe-Menü von Cisco Router and Security Device Manager (Cisco SDM) verfügbar.

Hilfethemen

Zeigt die Cisco SDM-Online-Hilfe an. Im linken Bereich der Cisco SDM-Online-Hilfe wird das Inhaltsverzeichnis angezeigt.

Cisco SDM auf CCO

Öffnet einen Browser und zeigt die Cisco SDM-Seite auf der Cisco.com-Website an.

Hardware-/Softwarematrix

Öffnet einen Browser und zeigt eine Tabelle mit Cisco Routermodellen und Cisco IOS-Abbildversionen an, um Hilfestellung bei der Auswahl einer kompatiblen Cisco IOS-Abbildsoftware zu leisten. Für den Zugriff auf die Matrix sind ein Cisco Connection Online-Benutzername und ein Kennwort erforderlich.

Über diesen Router...

Zeigt Informationen zur Hardware und Software des Routers an, auf dem Cisco SDM ausgeführt wird.

Über Cisco SDM

Zeigt Informationen zur Cisco SDM-Version an.

GLOSSAR

Symbole und Zahlen

3DES Engl.: „triple DES“. Ein Verschlüsselungsalgorithmus, der in schneller Folge drei 56-Bit-DES-Verschlüsselungsschlüssel (also 168 Bit) verwendet. Eine Alternativversion von 3DES verwendet lediglich zwei 56-Bit-DES-Schlüssel, aber einen davon zweimal (was also zu einer Schlüssellänge von 112 Bit führt). Verwendung nur in den Vereinigten Staaten gesetzlich zulässig. Siehe DES.

802.1x 802.1x ist ein IEEE-Standard für die Zugriffssteuerung auf Medienebene und bietet die Möglichkeit, Netzwerkverbindungen zuzulassen oder zu verweigern, den VLAN-Zugang zu steuern und basierend auf der Benutzer- oder Computeridentität Datenverkehrsrichtlinien anzuwenden.

A

AAA Authentifizierung, Autorisierung und Accounting. „Triple-A“ genannt.

AAL5-MUX ATM Adaptation Layer 5, Multiplexing – ATM-Anpassung Schicht 5, Multiplexing

AAL5-SNAP ATM Adaptation Layer 5, Subnetwork Access Protocol – ATM-Anpassung Schicht 5, Subnetz-Zugriffsprotokoll

Ablaufdatum Das Ablaufdatum eines Zertifikats oder Schlüssels gibt das Ende seiner beschränkten Gültigkeitsdauer an. Das Zertifikat oder der Schlüssel ist nach dem Ablaufdatum nicht mehr vertrauenswürdig.

Abstreiten In kryptografischen Systemen bezeichnet Abstreiten den Vorgang, bei dem eine der an einer Kommunikation beteiligten Instanzen bestreitet, an der gesamten oder einem Teil der Kommunikation beteiligt gewesen zu sein.

ACE Access Control Entry – Zugriffssteuerungseintrag. Ein Eintrag in einer ACL, die einen Quellhost oder ein Quellnetzwerk angibt sowie ob Datenverkehr von diesem Host zugelassen oder abgelehnt wird. Ein ACE kann auch einen Zielhost oder ein Zielnetzwerk sowie den Datenverkehrstyp angeben.

ACL Access Control List – Zugriffssteuerungsliste. Informationen auf einem Gerät, die angeben, welchen Ressourcengruppen Zugriff auf dieses Gerät oder die Netzwerke hinter diesem Gerät gewährt wird. Zugriffssteuerungslisten bestehen aus einem oder mehreren Zugriffssteuerungseinträgen (ACE, Access Control Entry).

ACS Cisco Secure Access Control Server. Cisco-Software, die einen RADIUS-Server oder einen TACACS+-Server implementieren kann. Der ACS wird zur Speicherung von Regeldatenbanken verwendet, die von Easy VPN, NAC und anderen Funktionen verwendet werden, um den Zugriff auf das Netzwerk zu regulieren.

Adressenübersetzung Die Übersetzung einer Netzwerkadresse und/oder eines Ports in eine andere Netzwerkadresse und/oder einen anderen Port. Siehe auch IP-Adresse, NAT, PAT, Static PAT.

ADSL Asymmetric Digital Subscriber Line.

Aggressive-Modus Ein Modus für die Festlegung von ISAKMP-SAs, der die IKE-Authentifizierungsaushandlung (Phase 1) zwischen zwei oder mehreren IPSec-Peers vereinfacht. Der Aggressive-Modus ist schneller als der Main-Modus, aber nicht so sicher. Siehe Main-Modus, Quick-Modus.

AH Authentication Header. Dies ist ein älteres IPSec-Protokoll, das in den meisten Netzwerken eine geringere Bedeutung als ESP hat. AH bietet Authentifizierungsdienste, aber keine Verschlüsselungsdienste. Es wird bereitgestellt, um die Kompatibilität mit IPSec-Peers zu gewährleisten, die nicht ESP unterstützen (das sowohl Authentifizierung als auch Verschlüsselung bietet).

AH-MD5-HMAC Authentication Header mit dem MD5-Hash-Algorithmus (HMAC-Variante).

AHP Authentication Header Protocol. Ein Protokoll, das die Authentifizierung des Quellhosts und die Datenintegrität gewährleistet. AHP stellt keine Geheimhaltung sicher.

AH-SHA-HMAC Authentication Header mit dem SHA-Hash-Algorithmus (HMAC-Variante).

Algorithmus Eine logische Schrittfolge für die Lösung eines Problems. Sicherheitsalgorithmen betreffen entweder Datenverschlüsselung oder Authentifizierung.

DES und 3DES sind zwei Beispiele für Datenverschlüsselungsalgorithmen.

Beispiele für Algorithmen für Verschlüsselung und Entschlüsselung sind Blockchiffre, CBC, Nullchiffre und Stromchiffre.

Zu den Authentifizierungsalgorithmen gehören Hash-Algorithmen wie MD5 und SHA.

AMI Alternate Mark Inversion.

ARP Address Resolution Protocol – Ein hardwarenahes TCP/IP-Protokoll, das eine Hardwareadresse eines Knotens (als *MAC-Adresse* bezeichnet) ihrer IP-Adresse zuordnet.

ASA Adaptive Security Algorithm. Ermöglicht in einer Richtung (von innen nach außen) verlaufende Verbindungen ohne eine explizite Konfiguration für die einzelnen internen Systeme und Anwendungen.

asymmetrische Schlüssel Ein Paar von Kryptografieschlüsseln, zwischen denen eine mathematische Beziehung besteht. Der öffentliche Schlüssel verschlüsselt Informationen, die nur der private Schlüssel entschlüsseln kann (und umgekehrt). Darüber hinaus signiert der private Schlüssel Daten, die nur der öffentliche Schlüssel authentifizieren kann.

asymmetrische Verschlüsselung Dieser auch als *Public-Key-System* bezeichnete Ansatz erlaubt jedem, Zugriff auf den öffentlichen Schlüssel eines anderen zu erlangen und mit dem öffentlichen Schlüssel eine verschlüsselte Nachricht an diese Person zu senden.

ATM Asynchronous Transfer Mode. Internationaler Standard für Cell-Relay, bei dem mehrere Diensttypen (z. B. Sprache, Video und Daten) in Zellen mit fester Länge (53 Byte) übertragen werden. Zellen mit fester Länge ermöglichen die Verarbeitung der Zellen in der Hardware und verringern dadurch Transitverzögerungen.

Ausnahmeliste Bei einer NAC-Implementierung eine Liste von Hosts mit statischen Adressen, denen die Umgehung des NAC-Prozesses gestattet ist. Die Hosts sind wahrscheinlich in dieser Ausnahmeliste eingetragen, weil sie keine Posture-Agents installiert haben, oder weil es sich um andere Hosts wie z.B. Drucker oder Cisco IP-Telefone handelt.

äußere globale Die IP-Adresse, die einem Host im äußeren Netzwerk durch den Eigentümer des Hosts zugeordnet wurde. Die Adresse wurde aus einem Adress- oder Netzwerkraum zugeordnet, für den globales Routing möglich ist.

äußere lokale Die IP-Adresse eines äußeren Hosts, wie sie für das innere Netzwerk angezeigt wird. Die Adresse, die nicht unbedingt eine legitime Adresse ist, wurde aus einem Adressraum zugeordnet, für den innen Routing möglich ist.

authentifizieren Die Richtigkeit einer Identität feststellen.

Authentifizierung Im Zusammenhang mit der Sicherheit die Verifizierung der Identität einer Person oder eines Prozesses. Mit der Authentifizierung wird die Integrität eines Datenstroms festgestellt und so gewährleistet, dass er bei der Übertragung nicht verfälscht wurde. Außerdem wird die Herkunft des Datenstroms bestätigt.

B

Block Eine Bitsequenz mit fester Länge.

Blockchiffre Ein Verschlüsselungsalgorithmus, der Datenblöcke fester Größe mit einer symmetrischen 64-Bit-Chiffre verarbeitet. Siehe Chiffre.

BOOTP Bootstrap Protocol. Das Protokoll, das von einem Netzwerkknoten verwendet wird, um die IP-Adressen seiner Ethernet-Schnittstellen mit dem Ziel zu bestimmen, das Booten im Netzwerk zu beeinflussen.

Burst-Rate Die Anzahl der Bytes, die ein Datenverkehrsbündel nicht überschreiten darf.

C

C3PL Cisco Common Classification Policy Language. C3PL ist ein strukturierter Platzhalter für funktionsspezifische Konfigurationsbefehle und sorgt dafür, dass konfigurierbare Funktionalitäten in Form von Ereignissen, Bedingungen und Aktionen ausgedrückt werden können.

CA Certification Authority – Zertifizierungsstelle. Eine vertrauenswürdige dritte Instanz, die digitale Zertifikate ausgibt oder sperrt. Sie wird manchmal als *Notar* oder *zertifizierende Stelle* bezeichnet. Innerhalb der Domäne einer bestimmten CA benötigt jedes Gerät nur sein eigenes Zertifikat und den öffentlichen Schlüssel der CA, um jedes andere Gerät in dieser Domäne zu authentifizieren.

Cache Eine temporäre Ablage für Daten, die bei der Ausführung von Aufgaben in früheren Durchgängen gesammelt wurden, erneut verwendet werden können und auf diese Weise den Zeitbedarf für die Ausführung der Aufgaben verringern.

CA-Server Certification Authority-Server. Ein Netzwerkhost, der digitale Zertifikate ausstellt und/oder sperrt.

CA-Zertifikat Ein digitales Zertifikat, das einer Zertifizierungsstelle (CA) von einer anderen Zertifizierungsstelle erteilt wird.

CBAC Context-based Access Control. Protokoll, das internen Benutzern sichere Zugriffssteuerung für jede Anwendung und für den gesamten Datenverkehr über Netzwerkgrenzen hinweg bietet. CBAC führt eine genaue Prüfung von Quell- und Zieladressen durch und verfolgt den Verbindungsstatus der einzelnen Anwendungen.

CDP Cisco Discovery Protocol. Ein medien- und protokollunabhängiges Protokoll für die Suche nach Geräten, das auf allen von Cisco hergestellten Geräten eingesetzt wird. Dazu gehören Router, Zugriffsserver, Brücken und Switches. Mit CDP kann ein Gerät andere Geräte über seine Existenz informieren und Informationen über andere Geräte im selben LAN oder auf der Remote-Seite eines WANs empfangen.

CDP Certificate Revocation List Distribution Point – CRL-Verteilungspunkt, Sperrlistenverteilungspunkt. Ein Ort, von dem eine Sperrliste (CRL) abgerufen werden kann. Ein CDP ist in der Regel eine HTTP- oder LDAP-URL.

CEP Certificate Enrollment Protocol. Ein Protokoll für die Zertifikatsverwaltung. CEP ist eine frühere Implementierung der CRS (Certificate Request Syntax), eines Standards, der der IETF (Internet Engineering Task Force) vorgeschlagen wurde. CEP gibt an, wie ein Gerät mit einer CA kommuniziert. Hierzu gehören der Abruf des öffentlichen Schlüssels der CA, die Registrierung eines Geräts bei der CA und der Abruf einer CRL (Certificate Revocation List – Sperrliste). CEP verwendet PKCS (Public Key Cryptography Standards) 7 und 10 als Schlüsselkomponententechnologien. Die Public Key Infrastructure Working Group (PKIX) der IETF arbeitet an der Standardisierung eines Protokolls für diese Funktionen, entweder CRS oder ein Äquivalent. Wenn ein IETF-Standard sicher ist, wird er von Cisco unterstützt werden. CEP wurde gemeinsam von Cisco Systems und VeriSign, Inc. entwickelt.

CET Cisco Encryption Technology. Eine proprietäre Netzwerkschicht-Verschlüsselung, die in Cisco IOS 11.2. eingeführt wurde. CET bietet Netzwerkdatenverschlüsselung auf der Ebene von IP-Paketen und implementiert die folgenden Standards: DH, DSS und 40- und 56-Bit-DES.

CHAP Challenge Handshake Authentication Protocol. Eine Sicherheitsfunktion, die auf Leitungen mit PPP-Kapselung unterstützt wird und nicht autorisierten Zugriff verhindert. CHAP verhindert nicht selbst den nicht autorisierten Zugriff, sondern identifiziert lediglich das Remote-Ende. Der Router oder Zugriffsserver legt dann fest, ob der betreffende Benutzer Zugriff erhält. Siehe auch PAP.

chargen Character Generation. Über TCP ein Dienst, der einen kontinuierlichen Zeichenstrom sendet, bis er vom Client gestoppt wird. Über UDP sendet der Server immer dann, wenn der Client ein Datagramm sendet, eine zufallsmäßige Anzahl von Zeichen.

Chiffre Ein Algorithmus für Verschlüsselung und Entschlüsselung.

Chiffretext Verschlüsselte, nicht lesbare Daten vor ihrer Entschlüsselung.

Cisco SDM Cisco Router and Security Device Manager. Cisco SDM ist ein Internet-Browser-basiertes Software-Tool, das für die Konfiguration von LAN-, WAN- und Sicherheitsfunktionen auf einem Router konzipiert wurde. Weitere Informationen finden Sie unter Erste Schritte.

Clear Channel Ein Clear Channel ist ein Kanal, durch den unverschlüsselter Datenverkehr fließen kann. In diesen Kanälen gelten für übertragene Daten keine Sicherheitsbeschränkungen.

CLI Command Line Interface – Befehlszeilenschnittstelle. Die primäre Schnittstelle für die Eingabe von Konfigurations- und Überwachungsbefehlen auf dem Router. Informationen darüber, welche Befehle Sie über die CLI eingeben können, finden Sie in dem Konfigurationshandbuch für den Router, den Sie konfigurieren.

Client/Server-Computing Begriff, mit dem verteilte Computing-(Verarbeitungs-)Netzwerksysteme beschrieben werden, in denen die Aufgaben im Zusammenhang mit Transaktionen auf zwei Seiten verteilt sind: Client (Front End) und Server (Back End). Auch als Distributed Computing bezeichnet. Siehe auch RPC.

CNS Cisco Networking Services. Ein Satz von Diensten, die skalierbare Netzwerkbereitstellung, Konfiguration, Überwachung der Gewährleistung von Diensten und Bereitstellung von Diensten unterstützen.

comp-lzs Ein Algorithmus für die IP-Kompression.

Cookie Ein Cookie ist eine Webbrowser-Funktion, bei der Informationen, z. B. Benutzereinstellungen, dauerhaft gespeichert oder Informationen abgerufen werden. In Netscape und Internet Explorer werden Cookies durch die Speicherung kleiner Textdateien auf der lokalen Festplatte implementiert. Diese Datei kann bei der nächsten Ausführung eines Java Applets oder beim nächsten Besuch einer Website geladen werden. Auf diese Weise können Informationen, die nur für Sie als Benutzer gelten, zwischen Sitzungen gespeichert werden. Die maximale Größe für ein Cookie liegt bei rund 4 KB.

CPE Customer Premises Equipment – Teilnehmer-Endgerät.

CRL Certificate Revocation List – Sperrliste. Eine von einer Zertifizierungsstelle (CA) verwaltete und signierte Liste mit allen noch nicht abgelaufenen, aber gesperrten digitalen Zertifikaten.

Crypto Map In Cisco SDM geben Crypto Maps an, welcher Datenverkehr von IPSec geschützt werden soll, wohin durch IPSec geschützter Datenverkehr gesendet werden soll und welche IPSec-Transformationssätze auf diesen Datenverkehr angewendet werden sollen.

D

Datenintegrität Die angenommene Genauigkeit von übertragenen Daten – die die Authentizität des Absenders und die Unverfälschtheit der Daten angibt.

Datenursprungs-authentifizierung Eine Funktion eines Dienstes für die Nicht-Abstreitbarkeit (Non-Repudiation).

Datenvertraulichkeit Das Ergebnis der Datenverschlüsselung, das die Offenlegung von Informationen gegenüber nicht autorisierten Einzelpersonen, Instanzen oder Prozessen verhindert. Bei diesen Informationen kann es sich um Daten auf der Anwendungsebene oder Kommunikationsparameter handeln. Siehe Verkehrsflussvertrau- lichkeit oder Datenverkehranalyse.

Delta-Datei Eine Datei, die Cisco IOS IPS erstellt, um an Signaturen vorgenommene Änderungen zu speichern.

DES Data Encryption Standard. Ein Standardkryptografiealgorithmus, der vom US-amerikanischen NIST (National Institute of Standards and Technology) entwickelt und standardisiert wurde. Er verwendet einen geheimen 56-Bit-Verschlüsselungsschlüssel. Der DES-Algorithmus ist in zahlreichen Verschlüsselungsstandards enthalten.

DH, Diffie-Hellman Ein kryptografisches Public-Key-Protokoll, mit dem zwei Parteien gemeinsam genutzte, vertrauliche Informationen über einen nicht sicheren Kommunikationskanal austauschen können. Diffie-Hellman wird in IKE (Internet Key Exchange) zum Festlegen von Sitzungsschlüsseln verwendet. Diffie-Hellman ist eine Komponente des Oakley-Schlüsselaustauschs.

DHCP Dynamic Host Configuration Protocol. Dieses Protokoll bietet einen Mechanismus für die dynamische Zuordnung von IP-Adressen zu Hosts, damit Adressen erneut verwendet werden können, wenn Hosts sie nicht mehr benötigen.

Diffie-Hellman-Schlüsselaustausch Ein kryptografisches Public-Key-Protokoll, mit dem zwei Parteien gemeinsam genutzte, vertrauliche Informationen über einen nicht sicheren Kommunikationskanal austauschen können. Diffie-Hellman wird in IKE (Internet Key Exchange) zum Festlegen von Sitzungsschlüsseln verwendet. Diffie-Hellman ist eine Komponente des Oakley-Schlüsselaustauschs. Cisco IOS-Software unterstützt 768-Bit- und 1024-Bit-Diffie-Hellman-Gruppen.

Digest Die Ausgabe einer Hash-Funktion.

digitale Signatur Eine Authentifizierungsmethode, mit der gefälschte Daten einfach entdeckt werden können und das Abstreiten verhindert wird. Darüber hinaus kann mit der Verwendung von digitalen Signaturen verifiziert werden, dass eine Übertragung vollständig und unverändert empfangen wurde. In der Regel ist ein Übertragungszeitstempel enthalten.

digitales Zertifikat Eine kryptografisch signierte digitale Darstellung von Benutzer- oder Geräteattributen, die einen Schlüssel an eine Identität bindet. Ein eindeutiges Zertifikat, das mit einem öffentlichen Schlüssel verbunden ist, beweist, dass der Schlüssel nicht kompromittiert wurde. Ein Zertifikat wird von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben und signiert und bindet einen öffentlichen Schlüssel an seinen Besitzer. Zertifikate umfassen in der Regel den Namen und den öffentlichen Schlüssel des Besitzers sowie die Seriennummer und das Ablaufdatum des Zertifikats. Es können auch weitere Informationen vorhanden sein. Siehe X.509.

DLCI Data Link Connection Identifier. In Frame Relay-Verbindungen der Identifier für eine bestimmte Datenverbindung zwischen zwei Endpunkten.

DMVPN Dynamic Multipoint Virtual Private Network. Ein virtuelles privates Netzwerk, in dem Router in einer logischen Hub-und-Spoke-Topologie angeordnet sind und in dem die Spokes über Point-to-Point-Verbindungen mit GRE over IPSec mit dem Hub verbunden sind. DMVPN verwendet GRE und NHRP, um den Fluss von Paketen zu Zielen im Netzwerk zu ermöglichen.

DMZ Demilitarized Zone. Eine DMZ ist eine Pufferzone zwischen dem Internet und Ihren privaten Netzwerken. Es kann sich um ein öffentliches Netzwerk handeln, das in der Regel für Web-, FTP- und E-Mail-Server verwendet wird, auf die externe Clients im Internet zugreifen. Wenn Sie diese Server mit öffentlichem Zugriff in ein getrenntes isoliertes Netzwerk platzieren, erzielen Sie ein zusätzliches Maß an Sicherheit für Ihr internes Netzwerk.

DN Distinguished Name. Ein eindeutiger Identifier für einen Kunden einer Zertifizierungsstelle, der in jedem der Zertifikate enthalten ist, die der Kunde von dieser Zertifizierungsstelle erhält. Der DN enthält in der Regel den allgemeinen Namen des Benutzers, den Namen des Unternehmens oder der Organisation des Benutzers, den aus zwei Buchstaben bestehenden Ländercode des Benutzers, eine E-Mail-Adresse für die Kontaktaufnahme mit dem Benutzer, die Telefonnummer und die Abteilungsnummer des Benutzers und den Ort, in dem der Benutzer seinen Wohnsitz hat.

DNS Domain Name System (oder Service). Ein Internetdienst, der Domänennamen, die aus Buchstaben bestehen, in IP-Adressen übersetzt, die aus Zahlen bestehen.

Domänenname Der vertraute, einprägsame Name eines Hosts im Internet, der seiner IP-Adresse entspricht.

DPD Dead-Peer-Erkennung. DPD ermittelt, ob ein Peer noch aktiv ist, indem periodische Keepalive-Meldungen gesendet werden, auf die der Peer antworten sollte. Tut er dies nicht innerhalb einer vorgegebenen Zeitspanne, wird die Verbindung beendet.

DRAM Dynamic Random Access Memory. RAM, der Informationen in Kondensatoren speichert, die regelmäßig aufgeladen werden müssen.

DSCP Differentiated Services Code Point. DSCP-Markierungen können verwendet werden, um Datenverkehr für QoS zu klassifizieren. Siehe auch NBAR.

DSLAM Digital Subscriber Line Access Multiplexer.

DSS Digital Signature Standard. Der DSS-Algorithmus, der auch als *Digital Signature Algorithm* (DSA) bezeichnet wird, ist Teil von zahlreichen Public-Key-Standards für kryptografische Signaturen.

Dynamisches Routing Routing, das sich automatisch an Änderungen in der Netzwerktopologie oder im Datenverkehr anpasst. Auch als adaptives Routing bezeichnet.

E

EAPoUDP Extensible Authentication Protocol over User Datagram Protocol. Manchmal kurz EOU genannt. Das von einem Client und NAD verwendete Protokoll für die Posture-Validierung.

Easy VPN Eine zentralisierte VPN-Verwaltungslösung, die auf dem Cisco Unified Client Framework basiert. Ein Easy VPN von Cisco besteht aus zwei Komponenten: einem Cisco Easy VPN Remote-Client und einem Cisco Easy VPN-Server.

ECHO Siehe Ping, ICMP.

eDonkey Auch eDonkey 2000 oder ED2K genannt. Hierbei handelt es sich um ein äußerst großes Peer-to-Peer-Netzwerk. eDonkey implementiert das Multisource File Transmission Protocol (MFTP).

EIGRP Enhanced Interior Gateway Routing Protocol. Erweiterte, von Cisco Systems entwickelte Version von IGRP. Sie bietet hervorragende Konvergenzeigenschaften und Betriebseffizienz und kombiniert die Vorteile von Link-State-Protokollen mit denen von Distanzvektorprotokollen.

Einzel-DMVPN Ein Router mit einer Einzel-DMVPN-Konfiguration besitzt eine Verbindung zu einem DMVPN-Hub und einem konfigurierten GRE-Tunnel für die DMVPN-Kommunikation. Die GRE-Tunneladressen für den Hub und die Spokes müssen sich im selben Subnetz befinden.

Entschlüsselung Die umgekehrte Anwendung eines Verschlüsselungsalgorithmus auf verschlüsselte Daten, wodurch diese Daten in ihrem ursprünglichen, unverschlüsselten Zustand wiederhergestellt werden.

ERR Event Risk Rating – Ereignisrisikobewertung. ERR wird verwendet, um die Ebene zu steuern, auf der ein Benutzer Maßnahmen ergreift, um falschpositive Bewertungen zu minimieren.

erweiterte Regeln Ein Typ einer Zugriffsregel. Erweiterte Regeln können eine größere Bandbreite an Paketfeldern untersuchen, um eine Übereinstimmung zu ermitteln. Erweiterte Regeln können sowohl die Quell- als auch die Ziel-IP-Adressen, den Protokolltyp, die Quell- und Zielports und weitere Paketfelder untersuchen.

ESP Encapsulating Security Payload. Ein IPSec-Protokoll, das sowohl Datenintegrität als auch Vertraulichkeit bietet. ESP bietet Vertraulichkeit, Datenursprungsauthentifizierung, Replay-Erkennung, verbindungslose Integrität, Teilsequenz-Integrität und Verkehrsflussvertraulichkeit.

ESP_SEAL ESP mit dem SEAL-(Software Encryption Algorithm-)Verschlüsselungsalgorithmus mit 160-Bit-Schlüssel. Diese Funktion wurde mit 12.3(7)T eingeführt. Für die Verwendung dieser Funktion muss auf dem Router nicht die Hardware-IPSec-Verschlüsselung aktiviert sein.

esp-3des ESP-(Encapsulating Security Payload-)Transformation mit dem 168-Bit-DES-Verschlüsselungsalgorithmus (3DES oder Triple DES).

esp-des ESP-(Encapsulating Security Payload-)Transformation mit dem 56-Bit-DES-Verschlüsselungsalgorithmus.

ESP-MD5-HMAC ESP-(Encapsulating Security Payload-)Transformation mit dem SHA-Authentifizierungsalgorithmus, Variante MD5.

esp-null ESP-(Encapsulating Security Payload-)Transformation, die keine Verschlüsselung und keine Vertraulichkeit bietet.

ESP-SHA-HMAC ESP-(Encapsulating Security Payload-)Transformation mit dem SHA-Authentifizierungsalgorithmus, Variante HMAC

Ethernet Ein weit verbreitetes LAN-Protokoll, das von der Xerox Corporation erfunden und von Xerox, Intel und Digital Equipment Corporation entwickelt wurde. Ethernet-Netzwerke verwenden CSMA/CD und übertragen Daten mit einer Vielzahl von Kabeltypen mit 10 Mbps oder 100 Mbps. Ethernet ähnelt den Standards der IEEE 802.3-Reihe.

Event Action Override – Ereignisaktions-Override Ereignisaktions-Overrides werden in IOS IPS 5.x verwendet. Sie ermöglichen es Ihnen, auf der Basis des RR eines Ereignisses die mit dem Ereignis verknüpften Aktionen zu ändern.

F

Fasttrack Ein Netzwerk, in dem die Indizierungsfunktionen den verbundenen Peers, sog. Supernodes, dynamisch zugewiesen werden.

Finger Ein Software-Tool, mit dem festgestellt werden kann, ob eine Person ein Konto auf einer bestimmten Internetsite besitzt. Zahlreiche Sites lassen keine eingehenden Finger-Anfragen zu.

Fingerabdruck Der Fingerabdruck eines CA-Zertifikats ist der String alphanumerischer Zeichen, der sich aus einem MD5-Hash des gesamten CA-Zertifikats ergibt. Instanzen, die ein CA-Zertifikat erhalten, können seine Authentizität verifizieren, indem sie es mit seinem bekannten Fingerabdruck vergleichen. Diese Authentifizierung soll die Integrität von Kommunikationssitzungen sicherstellen, indem Man-In-The-Middle-Angriffe verhindert werden.

Firewall Ein Router oder Zugriffsserver, oder mehrere Router oder Zugriffsserver, mit der Funktion eines Puffers zwischen einem beliebigen öffentlichen Netzwerk, zu dem eine Verbindung besteht, und einem privaten Netzwerk. Ein Firewall-Router verwendet Zugriffslisten und andere Methoden, um die Sicherheit eines privaten Netzwerks sicherzustellen.

Flash

Flash-Speicher Ein Speicherchip, der Daten ohne Versorgungsspannung speichert. Softwareabbilder können nach Bedarf im Flash gespeichert, aus dem Flash gebootet und in den Flash geschrieben werden.

Frame Relay Ein Data Link Layer-Vermittlungsprotokoll nach Industriestandard, das mehrere virtuelle Verbindungen mit HDLC-Kapselung zwischen verbundenen Geräten verwaltet. Frame Relay ist effizienter als X.25, das Protokoll, das es nach allgemeiner Auffassung ersetzt.

FTP File Transfer Protocol. Teil des TCP/IP-Protokollstapels, für die Übertragung von Dateien zwischen Hosts verwendet.

G

G.SHDSL G.SHDSL, auch bekannt als G.991.2, ist ein internationaler Standard für symmetrisches DSL, der von der International Telecommunications Union entwickelt wurde. Mit G.SHDSL können symmetrische Datenströme mit hoher Geschwindigkeit über ein einzelnes Kupferdrahtpaar mit Raten zwischen 192 kbps und 2,31 Mbps gesendet und empfangen werden.

geheimer Schlüssel Siehe symmetrischer Schlüssel.

gemeinsamer Schlüssel Der geheime Schlüssel, den alle Benutzer in einer symmetrischen, auf Schlüsseln basierenden Kommunikationssitzung gemeinsam verwenden.

globale IKE-Richtlinie Eine IKE-Richtlinie, die global für ein Gerät gilt anstatt nur für eine einzelne Schnittstelle auf diesem Gerät.

Gnutella Ein dezentrales P2P-Protokoll für den gemeinsamen Dateizugriff. Bei Verwendung eines installierten Gnutella-Clients können Benutzer im Internet Dateien suchen, herunterladen und hochladen.

GRE Generic Routing Encapsulation. Ein Tunneling-Protokoll von Cisco, mit dem eine Vielzahl von Protokollpakettypen in IP-Tunneln gekapselt werden kann. Auf diese Weise wird über ein IP-Verbundnetzwerk eine virtuelle Point-to-Point-Verbindung zu Cisco-Routern an Remote-Punkten erstellt. Durch die Verbindung von Subnetzwerken mit mehreren Protokollen in einer Backbone-Umgebung mit einem einzelnen Protokoll ermöglicht IP-Tunneling mit GRE die Netzwerkerweiterung in einer solchen Umgebung.

GRE over IPSec Diese Technologie verwendet IPSec zur Verschlüsselung von GRE-Paketen.

Gültigkeitsdauer Siehe Ablaufdatum.

H

H.323 Ein Standard, der Videokonferenzen über LANs und andere paketvermittelte Netzwerke sowie Video über das Internet ermöglicht.

Hash Ein in einer Richtung ablaufender Prozess, mit dem eine Eingabe beliebiger Größe in eine Prüfsummenausgabe konvertiert wird, die als *Message Digest* oder nur als *Digest* bezeichnet wird. Dieser Prozess ist unumkehrbar, und es ist nicht möglich, Daten so zu erstellen oder zu ändern, dass sie einen bestimmten Digest ergeben.

Hash-Algorithmus Mit einem Hash-Algorithmus wird ein auch als Message Digest bekannter Hash-Wert generiert, der gewährleistet, dass der Inhalt von Nachrichten während der Übertragung nicht geändert wird. Die beiden am häufigsten verwendeten Typen von Hash-Algorithmen sind Secure Hash Algorithm (SHA) und MD5.

HDLC High-Level Data Link Control. Ein bitorientiertes synchrones Data Link Layer-Protokoll, das von der International Standards Organization (ISO) entwickelt wurde. HDLC gibt eine Datenkapselungsmethode auf synchronen seriellen Verbindungen an, bei der Frame-Zeichen und Prüfsummen verwendet werden.

Headend Das Upstream-Übertragungsende eines Tunnels.

HMAC Hash-based Message Authentication Code. HMAC ist ein Mechanismus für die Nachrichtenauthentifizierung unter Verwendung von kryptografischen Hash-Funktionen. HMAC kann mit verschiedenen iterativen kryptografischen Hash-Funktionen wie MD5 und SHA-1 in Verbindung mit einem gemeinsam verwendeten geheimen Schlüssel verwendet werden. Die kryptografische Stärke von HMAC hängt von den Eigenschaften der zugrunde liegenden Hash-Funktion ab.

HMAC-MD5 Hashed Message Authentication Codes mit MD5 (RFC 2104). Eine MD5-Version mit Schlüssel, die zwei Parteien die Validierung übertragener Informationen unter Verwendung eines geteilten Geheimnisses ermöglicht.

Host Ein Computer, z. B. ein PC, oder ein anderes Datenverarbeitungsgerät, z. B. ein Server, das mit einer einzelnen IP-Adresse und optional einem Namen verknüpft ist. Der Name für ein Gerät in einem TCP/IP-Netzwerk, das eine IP-Adresse besitzt. Außerdem jedes Gerät in einem Netzwerk, das eine Netzwerkadresse erhalten kann. Der Begriff *Knoten* umfasst Geräte wie Router und Drucker, die normalerweise nicht als *Hosts* bezeichnet werden.

HTTP

HTTPS Hypertext Transfer Protocol, Hypertext Transfer Protocol, Secure. Das Protokoll, das von Webbrowsern und Webservern für die Übertragung von Dateien, z. B. Texten und Grafikdateien, verwendet wird.

Hub In einem DMVPN-Netzwerk ist ein Hub ein Router mit einer Point-to-Point-IPSec-Verbindung zu allen Spoke-Routern im Netzwerk. Der Hub ist der logische Mittelpunkt eines DMVPN-Netzwerks.

I

ICMP Internet Control Message Protocol. Netzwerkschicht-Internetprotokoll, das Fehler meldet und andere für die Verarbeitung von IP-Paketen relevante Informationen bereitstellt.

IDM IDS Device Manager. IDM ist Software, die für die Verwaltung eines IDS-Sensors verwendet wird.

IDS Intrusion Detection System. Das Cisco IPS analysiert den Netzwerkdatenverkehr in Echtzeit, um Anomalien und Missbrauch zu ermitteln. Hierzu verwendet es eine Bibliothek mit Signaturen, mit denen es den Datenverkehr vergleichen kann. Wenn es nicht autorisierte Aktivitäten oder Anomalien ermittelt, kann es die Bedingung beenden, Datenverkehr von angreifenden Hosts blockieren und Alarmmeldungen an IDM senden.

IDS-Sensor Ein IDS-Sensor ist Hardware, auf der das Cisco IDS ausgeführt wird. Bei IDS-Sensoren kann es sich um eigenständige Geräte oder um Netzwerkmodule handeln, die in Router eingebaut sind.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

IGMP Internet Group Management Protocol. IGMP ist ein Protokoll, das von IPv4-Systemen verwendet wird, um IP-Multicast-Mitgliedschaften an benachbarte Multicast-Router zu melden.

IKE Internet Key Exchange. IKE ist ein KMP-Standard (Key Management-Protokoll), der zusammen mit IPSec und anderen Standards verwendet wird. IPSec kann ohne IKE konfiguriert werden, aber IKE erweitert IPSec, indem er zusätzliche Funktionen, Flexibilität und eine einfache Konfiguration für den IPSec-Standard bietet. IKE bietet Authentifizierung der IPSec-Peers und handelt IPSec-Schlüssel und IPSec Security Associations aus.

Bevor IPSec-Datenverkehr übertragen werden kann, muss jeder Router, jede Firewall und jeder Host in der Lage sein, die Identität des Peers zu verifizieren. Dies kann manuell durch die Eingabe von Pre-Shared Keys auf beiden Hosts oder durch einen CA-Dienst geschehen. IKE ist ein Hybridprotokoll, dass den Oakley- und den Skeme-Schlüsselaustausch im ISAKMP-Framework (Internet Security Association and Key Management Protocol) implementiert. (ISAKMP, Oakley und Skeme sind von IKE implementierte Sicherheitsprotokolle.)

IKE-Aushandlung Eine Methode für den sicheren Austausch von privaten Schlüsseln über nicht gesicherte Netzwerke.

IKE-Profil Eine Gruppe von ISAKMP-Parametern, die verschiedenen IP Security-Tunneln zugeordnet werden können.

IM Instant Messaging. Ein Echtzeit-Kommunikationsdienst, bei dem beide Parteien zur gleichen Zeit online sind. Zu beliebten IM-Diensten zählen Yahoo! Messenger (YM), Microsoft Networks Messenger und AOL Instant Messenger (AIM).

IMAP Internet Message Access Protocol. Ein von Clients verwendetes Protokoll für die Kommunikation mit einem E-Mail-Server. Das in RFC 2060 definierte IMAP ermöglicht es Clients, Nachrichten auf dem E-Mail-Server zu löschen, ihren Status zu ändern oder anderweitig zu beeinflussen sowie von diesem abzurufen.

implizite Regel Eine Zugriffsregel, die vom Router automatisch auf der Grundlage von Standardregeln oder als Ergebnis benutzerdefinierter Regeln erstellt wird.

innere globale Die IP-Adresse eines Hosts in einem Netzwerk, wie sie für Geräte außerhalb des Netzwerks angezeigt wird.

innere lokale Die konfigurierte IP-Adresse, die einem Host in einem Netzwerk zugeordnet ist.

Internet Das globale Netzwerk, das IP, Internetprotokolle, einsetzt. Es ist kein LAN. Siehe auch Intranet.

Intranet Intranetzwerk. Ein LAN, das IP und Internet-Protokolle, wie SNMP, FTP und UDP, einsetzt. Siehe auch Netzwerk, Internet.

IOS Cisco IOS-Software. Cisco-Systemsoftware, die allgemeine Funktionen, Skalierbarkeit und Sicherheit für alle Produkte bereitstellt, die unter die CiscoFusion-Architektur fallen. Cisco IOS ermöglicht die zentralisierte, integrierte und automatisierte Installation und Verwaltung von Verbundnetzwerken und gewährleistet die Unterstützung einer Vielzahl von Protokollen, Medien, Diensten und Plattformen.

IOS IPS

IPS Cisco IOS Intrusion Prevention System. IOS IPS vergleicht den Datenverkehr mit einer umfangreichen Datenbank mit Angriffssignaturen und kann eindringende Pakete entfernen und auf Grundlage der Konfiguration andere Maßnahmen ergreifen. Signaturen sind in IOS-Abbilder integriert, die diese Funktion unterstützen, und weitere Signaturen können in lokalen oder Remote-Signaturdateien gespeichert werden.

IP Internet Protocol. IP-Protokolle sind die weltweit am häufigsten genutzten „Open-System“-Protokolle (nicht proprietär), da diese zur Kommunikation über beliebige miteinander verbundene Netzwerke verwendet werden können und sich zugleich für den Einsatz in der LAN- und WAN-Kommunikation eignen.

IP-Adresse IP-Adressen der Version 4 weisen eine Länge von 32 Bits bzw. 4 Bytes auf. Dieser „Adressraum“ wird zum Zuweisen der Netzwerknummer, der optionalen Subnetzwerknummer und einer Hostnummer verwendet. Die 32 Bits sind in vier Oktette angeordnet (8 binäre Bits), die durch 4 Dezimalzahlen dargestellt und durch Punkte oder „Dots“ voneinander getrennt werden. Der Teil der Adresse, aus dem die Netzwerknummer, die Subnetzwerknummer und die Hostnummer hervorgehen, wird durch die Subnetzmaske angegeben.

IPSec Ein Framework offener Standards, das Datenvertraulichkeit, Datenintegrität und Datenauthentifizierung zwischen teilnehmenden Peers bietet. IPSec stellt diese Sicherheitsdienste in der IP-Schicht bereit. IPSec setzt IKE ein, um auf der Grundlage der lokalen Richtlinie Protokolle und Algorithmen auszuhandeln und um die von IPSec zu verwendenden Verschlüsselungs- und Authentifizierungsschlüssel zu generieren. IPSec kann eingesetzt werden, um einen oder mehrere Datenflüsse zwischen zwei Hosts, zwei Sicherheits-Gateways oder zwischen einem Sicherheits-Gateway und einem Host zu schützen.

IPSec-Regel Eine Regel, mit der angegeben wird, welcher Datenverkehr von IPSec geschützt wird.

IPSec-Richtlinie In Cisco SDM ist eine IPSec-Richtlinie ein benannter Satz von Crypto Maps, die mit einer VPN-Verbindung verknüpft sind.

IRB Integriertes Routing und Bridging. Mit IRB können Sie ein bestimmtes Protokoll über Weiterleitungsschnittstellen transportieren und an einem Switching-Router eine Kommunikationsbrücke zwischen Gruppen schaffen.

ISAKMP Das Internet Security Association Key Management Protocol ist die Grundlage für IKE. ISAKMP authentifiziert kommunizierende Peers, erstellt und verwaltet Security Associations und definiert Methoden für die Schlüsselgenerierung.

K

Kapselung Einschließen von Daten in einen bestimmten Protokoll-Header. So werden z. B. Ethernet-Daten vor der Übertragung im Netzwerk in einen bestimmten Ethernet-Header eingeschlossen. Bei der Überbrückung unterschiedlicher Netzwerke wird außerdem der gesamte Frame von einem Netzwerk einfach in den Header platziert, der vom Data Link Layer-Protokoll des anderen Netzwerks verwendet wird.

Kazaa2 Ein Peer-to-Peer-Dienst für die gemeinsame Dateinutzung.

Kennwort Eine geschützte und geheime Zeichenfolge (oder andere Datenquelle), die mit der Identität eines bestimmten Benutzers oder einer bestimmten Instanz verknüpft ist.

Key Escrow Eine vertrauenswürdige dritte Stelle, bei der die kryptografischen Schlüssel hinterlegt sind.

Key Recovery Eine vertrauenswürdige Methode, mit der verschlüsselte Informationen entschlüsselt werden können, wenn der Entschlüsselungsschlüssel verloren gegangen ist oder zerstört wurde.

Klartext Entschlüsselter Text. Auch *Klartext* genannt.

Klartext Gewöhnliche, unverschlüsselte Daten.

Klassenzuordnung

Konfiguration, Konfigurationsdatei Die Datei auf dem Router, die die Einstellungen und Eigenschaften enthält, die Sie mit Cisco SDM verwalten können.

Kryptografie Mathematische und wissenschaftliche Methoden, um Daten privat, authentisch und unverändert zu lassen und dafür zu sorgen, dass sie nicht abgestritten werden können.

L

L2F-Protokoll Layer 2 Forwarding Protocol. Protokoll, das die Erstellung von sicheren virtuellen privaten DFÜ-Netzwerken über das Internet unterstützt.

L2TP Layer 2 Tunneling Protocol. Ein in RFC 2661 definiertes IETF-Standards Track-Protokoll (Internet Engineering Task Force), das PPP-Tunneling bietet. L2TP basiert auf den besten Funktionen von L2F und PPTP und bietet eine branchenweit vollständig kompatible Methode für die Implementierung von VPDN. L2TP wird als Alternative zu IPSec vorgeschlagen, wird aber manchmal parallel zu IPSec für die Bereitstellung von Authentifizierungsdiensten verwendet.

LAC L2TP-Zugriffskonzentrator. Gerät, das Aufrufe für Remote-Systeme beendet und Tunneling für PPP-Sitzungen zwischen Remote-Systemen und dem LNS bietet.

LAN Local Area Network – lokales Netzwerk. Ein Netzwerk, das sich an einem Standort befindet oder zu einer Organisation gehört. Es verwendet in der Regel, aber nicht unbedingt, IP und andere Internetprotokolle. Nicht das globale Internet. *Siehe auch* Intranet, Netzwerk, Internet.

LAPB Link Access Procedure, Balanced.

Layer 3-Schnittstelle Layer 3-Schnittstellen unterstützen Routing in Verbundnetzwerken. Ein VLAN ist ein Beispiel für eine logische Layer 3-Schnittstelle. Ein Ethernet-Port ist ein Beispiel für eine physische Layer 3-Schnittstelle.

LBO Line Build Out.

LEFS Low-End File System.

LLQ Low Latency Queuing.

LNS L2TP-Netzwerkserver. Gerät, das L2TP-Tunnel von einem LAC und PPP-Sitzungen zu Remote-Systemen über L2TP-Datensitzungen terminieren kann.

logische Schnittstelle Eine Schnittstelle, die allein durch Konfiguration erstellt wurde und bei der es sich nicht um eine physikalische Schnittstelle auf dem Router handelt. Dialer- und Tunnelschnittstellen sind Beispiele für logische Schnittstellen.

lokales Subnetz Subnetzwerke sind IP-Netzwerke, die von einem Netzwerkadministrator (unter Verwendung einer Subnetzmaske) beliebig segmentiert werden, um eine mehrere Ebenen umfassende hierarchische Routing-Struktur zu bieten und das Subnetzwerk gleichzeitig vor der Komplexität der Adressierung verknüpfter Netzwerke abzuschirmen. Das lokale Subnetz ist das Subnetz, das mit Ihrem Ende einer Übertragung verknüpft ist.

Loopback In einem Loopback-Test werden Signale gesendet und dann von einem Punkt des Kommunikationspfads zurück zu ihrer Quelle geleitet. Loopback-Tests werden oft verwendet, um die Verwendbarkeit von Netzwerkschnittstellen zu bestimmen.

M

MAC Message Authentication Code. Die kryptografische Prüfsumme einer Nachricht, mit der ihre Authentizität verifiziert wird. Siehe Hash.

MD5 Message Digest 5. Eine in einer Richtung ausgeführte Hash-Funktion, die einen 128-Bit-Hash erzeugt. Sowohl MD5 als auch SHA (Secure Hashing Algorithm) sind Variationen von MD4 und wurden mit dem Ziel konzipiert, die Sicherheit des MD4-Hash-Algorithmus zu stärken. Cisco verwendet Hashes für die Authentifizierung im IPSec-Framework. MD5 verifiziert die Integrität und authentifiziert den Ursprung einer Kommunikation.

MD5 Message Digest 5. Ein in einer Richtung eingesetzter Hash-Algorithmus, der einen 128-Bit-Hash erzeugt. Sowohl MD5 als auch SHA (Secure Hash Algorithm) sind Variationen von MD4 und wurden mit dem Ziel konzipiert, die Sicherheit des MD4-Hash-Algorithmus zu stärken. Cisco verwendet Hashes für die Authentifizierung im IPSec-Framework. MD5 wird auch für die Nachrichtenauthentifizierung in SNMP 2 verwendet, verifiziert die Integrität der Kommunikation, authentifiziert den Ursprung und überprüft die Rechtzeitigkeit.

Message Digest Ein Bit-String, der einen größeren Datenblock darstellt. Dieser String definiert einen Datenblock auf Grundlage der Verarbeitung seines genauen Inhalts mit einer 128-Bit-Hash-Funktion. Message Digests werden bei der Generierung von digitalen Signaturen verwendet. Siehe Hash.

mGRE multipoint GRE.

MTU

Maximum Transmission Unit. Die maximale Paketgröße in Byte, die eine Schnittstelle übertragen oder empfangen kann.

Maske

Subnetzmaske

Netzmaske

Netzwerkmaske

Eine 32-Bit-Maske, die angibt, wie eine Internetadresse in die Teile für Netzwerk, Subnetz und Host aufzuteilen ist. Die Netzmaske hat Einsen (1) in den Bit-Positionen in der 32-Bit-Adresse, die für den Netzwerk- und den Subnetzteil zu verwenden sind, und Nullen (0) für den Hostteil. Die Maske sollte mindestens den standardmäßigen (durch die Adressklasse bestimmten) Netzwerkabschnitt enthalten, und das Subnetzfeld sollte an den Netzwerkabschnitt grenzen. Die Maske wird mit dem Dezimaläquivalent des Binärwerts konfiguriert.

Beispiele:

Dezimal: 255.255.255.0
Binär: 11111111 11111111 11111111 00000000
Die ersten 24 Bits liefern die Netzwerk- und die Subnetzwerkadresse, die letzten 8 die Hostadresse.

Dezimal: 255.255.255.248
Binär: 11111111 11111111 11111111 11111000
Die ersten 29 Bits liefern die Netzwerk- und die Subnetzwerkadresse, die letzten 3 die Hostadresse.

Siehe auch IP-Adresse, TCP/IP, Host, Host/Netzwerk.

N

NAC

Network Admission Control. Ein Verfahren, mit dem der Zugang zu einem Netzwerk unter Kontrolle gehalten wird, um ein Eindringen von Computerviren zu verhindern. Durch den Einsatz unterschiedlicher Protokolle und Softwareprodukte ruft NAC den Zustand der Hosts ab, sobald diese auf das Netzwerk zugreifen, und arbeitet den übergebenen Befehl abhängig vom jeweiligen Hostzustand ab, der als *Posture* (auf Deutsch Haltung) bezeichnet wird. Infizierte Hosts können unter Quarantäne gestellt werden; Hosts mit veraltetem Stand der Virenschutzsoftware können zum Abruf von Updates veranlasst werden, und nicht infizierten Hosts mit aktuellem Virenschutz kann der Zugang zum Netzwerk gestattet werden. Siehe auch ACL, Posture und EAPoUDP.

NAD

Netzwerkzugriffsgerät. Innerhalb einer NAC-Implementierung das Gerät, das die Aufforderung eines Hosts zur Anmeldung beim Netzwerk entgegennimmt. Ein NAD (meistens ein Router) arbeitet mit Posture-Agent-Software, die auf dem Host läuft, Virenschutz-Software und ACS- sowie Posture-/Wiederherstellungsservern im Netzwerk zusammen, um den Netzwerkzugang zu reglementieren und einen Befall durch Computerviren auszuschließen.

NAS

Netzwerkzugriffsserver. Plattform, die die Schnittstelle zwischen dem Internet und dem öffentlichen Telefonnetz bildet.

Gateway, das asynchrone Geräte über Netzwerk- und Terminalemulationssoftware mit einem LAN oder WAN verbindet. Führt sowohl synchrones als auch asynchrones Routing für unterstützte Protokolle aus.

NAT

Network Address Translation

Netzwerkadressenübersetzung. Mechanismus, der die Notwendigkeit von global eindeutigen IP-Adressen reduziert. NAT ermöglicht es einer Organisation mit Adressen, die nicht global eindeutig sind, eine Verbindung zum Internet herzustellen, indem es diese Adressen in Adressräume übersetzt, für die globales Routing möglich ist.

NBAR

Network-Based Application Recognition (NBAR). Eine Methode zur Klassifizierung des Datenverkehrs für QoS.

NetFlow Eine Funktion einiger Router, die es ihnen ermöglicht, eingehende Pakete in Flüssen zu kategorisieren. Da Pakete in einem Fluss oft auf dieselbe Weise behandelt werden können, kann mit dieser Klassifikation ein Teil der Arbeit des Routers umgangen und sein Switching beschleunigt werden.

Netzwerk Ein Netzwerk ist eine Gruppe von Datenverarbeitungsgeräten, die einen Teil eines IP-Adressraums gemeinsam verwenden (kein einzelner Host). Ein Netzwerk besteht aus mehreren „Knoten“ oder Geräten mit einer IP-Adresse, die alle als *Hosts* bezeichnet werden können. Siehe auch Internet, Intranet, IP, LAN.

Netzwerkbits Die Anzahl der Bits in einer Subnetzmaske, die auf binär 1 gesetzt sind. Die Subnetzmaske 255.255.255.0 besitzt 24 Netzwerkbits, da 24 Bits in der Maske auf 1 gesetzt sind. Die Subnetzmaske 255.255.248 besitzt 17 Netzwerkbits.

Netzwerkmodul Eine Netzwerkschnittstellenkarte, die in das Chassis des Routers eingebaut ist, um den Funktionsumfang des Routers zu erweitern. Beispiele sind Ethernet-Netzwerkmodule und IDS-Netzwerkmodule.

NHRP Next Hop Resolution Protocol. Ein Client/Server-Protokoll, das in DMVPN-Netzwerken verwendet wird und bei dem der Hub-Router der Server ist und die Spokes die Clients darstellen. Der Hub verwaltet eine NHRP-Datenbank mit den Adressen der öffentlichen Schnittstellen der einzelnen Spokes. Jeder Spoke registriert seine reale Adresse beim Booten und fragt die realen Adressen der Ziel-Spokes in der NHRP-Datenbank ab, um direkte Tunnel zu ihnen aufzubauen.

Nicht-Abstreitbarkeit, Dienst für Ein Sicherheitsdienst einer dritten Stelle, mit dem Belege zu Ursprung und Ziel aller in einer Kommunikation enthaltenen Daten für einen möglichen späteren Abruf gespeichert werden – ohne die eigentlichen Daten zu speichern. Mit diesen Belegen können alle Teilnehmer dieser Kommunikation davor geschützt werden, dass Teilnehmer fälschlicherweise abstreiten, Informationen gesendet bzw. empfangen zu haben.

NTP Network Time Protocol. Ein Protokoll für die Synchronisierung der Systemuhren auf Netzwerkgeräten. NTP ist ein UDP-Protokoll.

NVRAM Non-Volatile Random Access Memory – Nichtflüchtiger Arbeitsspeicher.

O

Oakley Ein Protokoll zum Festlegen von geheimen Schlüsseln für die Verwendung durch authentifizierte Parteien. Es basiert auf Diffie-Hellman und ist als kompatible Komponente von ISAKMP konzipiert.

OFB Output Feedback. Eine IPSec-Funktion, mit der verschlüsselte Ausgabe (im Allgemeinen, aber nicht unbedingt mit DES verschlüsselt) wieder in die ursprüngliche Eingabe übertragen wird. Klartext wird direkt mit dem symmetrischen Schlüssel verschlüsselt. Dies erzeugt einen pseudozufälligen Zahlenstrom.

OSPF Open Shortest Path First. Ein hierarchischer IGP-Link-State-Routing-Algorithmus, der in der Internet-Community als Nachfolger von RIP vorgeschlagen wurde. Zu den Funktionen von OSPF gehören Least-Cost Routing, Multipath Routing und Lastausgleich.

P

P2P Siehe Peer-to-Peer.

PAD Packet Assembler/Disassembler. Gerät, mit dem einfache Geräte (wie Textmodus-Terminals), die nicht den gesamten Funktionsumfang eines bestimmten Protokolls unterstützen, mit einem Netzwerk verbunden werden. PADs puffern Daten, setzen Pakete zusammen und zerlegen Pakete, die an diese Endgeräte gesendet werden.

Padding In Kryptosystemen bezieht sich *Padding* auf Zufallszeichen, Leerzeichen, Nullen und Nullwerte, die zum Anfang oder Ende von Nachrichten hinzugefügt werden, um ihre tatsächliche Länge zu verbergen oder die Anforderungen einiger Chiffren an die Datenblockgröße zu erfüllen. Padding verbirgt außerdem die Position, an der die kryptografische Codierung tatsächlich beginnt.

PAM Port-to-Application Mapping. PAM ermöglicht Ihnen die Anpassung von TCP- oder UDP-Portnummern für Netzwerkdienste oder –anwendungen. PAM benutzt diese Informationen, um Netzwerkumgebungen zu unterstützen, auf denen Dienste laufen, die Ports benutzen, welche sich von den registrierten oder gut bekannten Ports unterscheiden, die mit einer Anwendung verknüpft sind.

PAP Password Authentication Protocol. Ein Authentifizierungsprotokoll, das Peers die gegenseitige Authentifizierung ermöglicht. PAP überträgt das Kennwort und den Host- oder Benutzernamen in unverschlüsselter Form. Siehe auch CHAP.

Parameterzuordnung Parameterzuordnungen geben das Prüfverhalten für zonenbasierte Richtlinienfirewalls, für Parameter wie Denial-of-Service (DoS)-Schutz, Sitzungs- und Verbindungstimer und Protokollierungseinstellungen an. Parameterzuordnungen werden auch mit Layer 7-Klassen- und Richtlinienzuordnungen, wie HTTP-Objekten, POP3- und IMAP-Authentifizierungsanforderungen und anderen anwendungsspezifischen Informationen, angewandt, um anwendungsspezifisches Verhalten zu definieren.

PAT

Dynamische PAT Port Address Translation. Dynamic PAT bewirkt, dass mehrere ausgehende Sitzungen scheinbar von einer einzelnen IP-Adresse stammen. Wenn PAT aktiviert ist, wählt der Router eine eindeutige Portnummer von der PAT-IP-Adresse für jeden ausgehenden Translation Slot (xlate) . Diese Funktion ist wertvoll, wenn ein Internet-Service-Provider nicht genügend eindeutige IP-Adressen für Ihre ausgehenden Verbindungen vergeben kann. Die Adressen im globalen Pool werden immer zuerst verwendet, bevor eine PAT-Adresse verwendet wird.

Peer In IKE sind Peers Router, die als Proxy für die Teilnehmer in einem IKE-Tunnel fungieren. In IPSec sind Peers Geräte oder Instanzen, die über den Austausch von Schlüsseln oder digitalen Zertifikaten sicher miteinander kommunizieren.

Peer-to-Peer Ein Netzwerktyp, bei dem alle Hosts in etwa dieselben Funktionen haben. Auch P2P genannt. Die Peer-to-Peer-Vernetzung wird von vielen Netzwerken für gemeinsame Dateinutzung verwendet.

PEM Privacy Enhanced Mail-Format. Ein Format für das Speichern digitaler Zertifikate.

PFS Perfect Forward Secrecy. Ein Merkmal einiger Protokolle für die Vereinbarung asymmetrischer Schlüssel, das die Verwendung verschiedener Schlüssel in verschiedenen Phasen einer Sitzung zulässt, um sicherzustellen, dass durch die Kompromittierung eines einzelnen Schlüssels nicht die Sitzung als Ganzes kompromittiert wird.

physikalische Schnittstelle Eine Routerschnittstelle, die von einem Netzwerkmodul unterstützt wird, das in das Chassis des Routers eingebaut oder Teil der grundlegenden Hardware des Routers ist.

Ping Eine zwischen Hosts gesendete ICMP-Anforderung, um festzustellen, ob der Zugriff auf einen Host im Netzwerk möglich ist.

PKCS12 Public Key Cryptography Standard Nr. 12. Ein Format für das Speichern von Informationen digitaler Zertifikate. Siehe auch PEM.

PKCS7 Public Key Cryptography Standard Nr. 7.

PKI Public-Key-Infrastruktur. Ein System von Zertifizierungsstellen (CAs) und Registrierungsstellen (RAs), das die Verwendung von Kryptografie mit asymmetrischen Schlüsseln in der Datenkommunikation unterstützt. Dies geschieht mit Funktionen wie Zertifikatsverwaltung, Archivierung, Schlüssel- und Token-Verwaltung.

Oder auch jeder Standard für den Austausch asymmetrischer Schlüssel.

Diese Art von Austausch ermöglicht es dem Empfänger einer Nachricht, der Signatur in dieser Nachricht zu vertrauen, und der Absender einer Nachricht kann sie entsprechend für den vorgesehenen Empfänger verschlüsseln. Siehe Schlüsselverwaltung.

Platzhaltermaske Eine Bitmaske, die in Zugriffsregeln, IPSec-Regeln und NAT-Regeln verwendet wird, um anzugeben, welche Teile der IP-Adresse des Pakets mit der in der Regel angegebenen IP-Adresse übereinstimmen müssen. Eine Platzhaltermaske umfasst 32 Bits, dies entspricht der Anzahl der Bits einer IP-Adresse. Der Platzhalter-Bitwert 0 gibt an, dass das Bit an derselben Position der IP-Adresse des Pakets mit dem Bit in der IP-Adresse in der Regel übereinstimmen muss. Der Wert 1 gibt an, dass das entsprechende Bit der IP-Adresse des Pakets entweder 0 oder 1 sein kann, dass es also für die Regel keine Rolle spielt, welchen Wert das Bit angenommen hat. Eine Platzhaltermaske von 0.0.0.0 gibt an, dass alle 32 Bits der IP-Adresse des Pakets mit der IP-Adresse in der Regel übereinstimmen müssen. Eine Platzhaltermaske von 0.0.225.0 gibt an, dass für die ersten 16 Bits und die letzten 8 Bits eine Übereinstimmung vorhanden sein muss, während das dritte Oktett jeden Wert annehmen kann. Wenn die IP-Adresse in einer Regel 10.28.15.0 und die Maske 0.0.255.0 lautet, stimmt die IP-Adresse 10.28.88.0 mit der IP-Adresse in der Regel überein, während für die IP-Adresse 10.28.15.55 keine Übereinstimmung vorliegt.

POP3 Post Office Protocol Version 3. Ein Protokoll, das zum Abrufen von E-Mails von einem E-Mail-Server verwendet wird.

Posture Innerhalb einer NAC-Implementierung der Zustand eines Hosts, der einen Zugriffsversuch auf das Netzwerk unternimmt. Die auf einem Host ausgeführte Posture-Agent-Software tauscht Daten mit dem NAD aus, um die Einhaltung der Netzwerk-Sicherheitsregeln durch den Host mitzuteilen.

PPP Point-to-Point Protocol. Ein Protokoll, das Router-Router- und Host-Netzwerk-Verbindungen über synchrone und asynchrone Leitungen bietet. PPP besitzt integrierte Sicherheitsmechanismen wie CHAP und PAP.

PPPoA Point-to-Point Protocol over Asynchronous Transfer Mode (ATM). Wird hauptsächlich als Teil von ADSL implementiert. PPPoA nutzt RFC1483 und arbeitet entweder im LLC-SNAP-Modus (Logical Link Control, Subnetwork Access Protocol) oder im VC-Mux-Modus.

PPPoE Point-to-Point Protocol over Ethernet. In Ethernet-Frames gekapseltes PPP. Mit PPPoE können Hosts in einem Ethernet-Netzwerk über ein Breitbandmodem Verbindungen zu Remote-Hosts aufbauen.

PPTP

Point-to-Point Tunneling Protocol. Erstellt von Clients initiierte Tunnel durch Kapselung von Paketen in IP-Datagramme für die Übertragung in TCP/IP-basierten Netzwerken. Kann als Alternative für die Tunneling-Protokolle L2F und L2TP verwendet werden. Firmenspezifisches Protokoll von Microsoft.

Pre-Shared Key

Eine von drei in IPSec angebotenen Authentifizierungsmethoden (die beiden anderen Methoden sind mit RSA verschlüsselte zufällige Werte und RSA-Signaturen). Mit Pre-Shared Keys können ein oder mehrere Clients einzelne geteilte Geheimnisse verwenden, um verschlüsselte Tunnel für ein Gateway mit IKE zu authentifizieren. Pre-Shared Keys werden gemeinhin in kleinen Netzwerken mit bis zu 10 Clients verwendet. Mit Pre-Shared Keys ist es nicht erforderlich, zur Gewährleistung der Sicherheit eine CA einzubeziehen.

Der Diffie-Hellman-Schlüsselaustausch kombiniert öffentliche und private Schlüssel, um ein geteiltes Geheimnis für die Authentifizierung zwischen IPSec-Peers zu erstellen. Das Geheimnis kann zwischen zwei oder mehr Peers geteilt werden. Auf jedem teilnehmenden Peer geben Sie ein geteiltes Geheimnis als Teil einer IKE-Richtlinie an. Die Verteilung des Pre-Shared Keys findet in der Regel über einen sicheren Out-of-Band-Kanal statt. Wenn bei der Verwendung eines Pre-Shared Keys einer der teilnehmenden Peers nicht mit demselben Pre-Shared Key konfiguriert ist, kann die IKE SA nicht festgelegt werden. Eine IKE SA ist eine Voraussetzung für eine IPSec SA. Sie müssen den Pre-Shared Key auf allen Peers konfigurieren.

Digitale Zertifizierung und Wildcard Pre-Shared Keys (die einem oder mehreren Clients die Verwendung eines geteilten Geheimnisses für die Authentifizierung verschlüsselter Tunnel für ein Gateway ermöglichen) sind Alternativen zu Pre-Shared Keys. Sowohl die digitale Zertifizierung als auch Wildcard Pre-Shared Keys sind skalierbarer als Pre-Shared Keys.

privater Schlüssel

Siehe Public-Key-Verschlüs-selung.

Prüfregel

Eine CBAC-Prüfregel ermöglicht dem Router, bestimmten ausgehenden Datenverkehr zu prüfen, damit er zurücklaufenden Datenverkehr desselben Typs, der mit einer im LAN gestarteten Sitzung verknüpft ist, zulassen kann. Wenn eine Firewall eingerichtet ist, wird eingehender Datenverkehr, der mit einer innerhalb der Firewall gestarteten Sitzung verknüpft ist, möglicherweise entfernt, wenn keine Prüfregel konfiguriert wurde.

Prüfsumme Berechnungsmethode für die Überprüfung der Integrität von übertragenen Daten, berechnet aus einer Sequenz von Oktetten, die eine Reihe von arithmetischen Operationen durchlaufen. Der Empfänger berechnet den Wert erneut und vergleicht ihn zur Überprüfung.

pseudozufällig Eine geordnete Bitsequenz, die, oberflächlich gesehen, einer wirklich zufälligen Sequenz derselben Bits zu ähneln scheint. Ein Schlüssel, der aus einer Pseudozufallszahl generiert wurde, wird als zufälliger Wert (engl.: „Nonce“) bezeichnet.

Public-Key-Ver-schlüs-selung In Public-Key-Verschlüsselungssystemen besitzt jeder Benutzer einen öffentlichen und einen privaten Schlüssel. Jeder private Schlüssel wird von einem einzelnen Benutzer verwaltet und mit niemandem geteilt. Der private Schlüssel wird verwendet, um eine eindeutige digitale Signatur zu generieren und um Informationen zu entschlüsseln, die mit dem öffentlichen Schlüssel verschlüsselt wurden. Im Gegensatz dazu steht der öffentliche Schlüssel eines Benutzers jedem zur Verfügung, um für diesen Benutzer vorgesehene Informationen zu verschlüsseln oder um die digitale Signatur des Benutzers zu überprüfen. Manchmal auch als Public-Key-Kryptografie bezeichnet.

PVC Permanent Virtual Circuit/Connection. Virtuelle Verbindung, die kontinuierlich aktiv ist. PVCs sparen Bandbreite ein im Zusammenhang mit dem Auf- und Abbau von Verbindungen in Situationen, in denen bestimmte Verbindungen durchgehend vorhanden sein müssen. In ATM-Terminologie wird die Bezeichnung Permanent Virtual Connection verwendet.

Q

QoS Quality of Service. – Dienstgüte. Eine Methode, mit der Bandbreite für angegebene Typen von Datenverkehr garantiert wird.

Quick-Modus Der Name des Mechanismus in Oakley, der nach dem Festlegen einer Security Association verwendet wird, um Änderungen bei den Sicherheitsdiensten, z. B. neue Schlüssel, auszuhandeln.

R

RA Registration Authority – Registrierungsstelle. Eine Instanz, die als optionale Komponente in PKI-Systemen dient, um einige der Informationen aufzuzeichnen oder zu verifizieren, die Zertifizierungsstellen (CAs) nutzen, wenn sie Zertifikate ausstellen oder andere Aufgaben für die Verwaltung von Zertifikaten ausführen. Die CA selbst könnte alle RA-Aufgaben ausführen, aber sie werden im Allgemeinen getrennt gehalten. RA-Pflichten variieren erheblich, können aber die Zuordnung von Distinguished Names, die Verteilung von Tokens und die Ausführung von Aufgaben für die persönliche Authentifizierung umfassen.

RADIUS Abkürzung für Remote Authentication Dial-In User Service. Ein Protokoll zur Authentifizierung und Kontoführung des Serverzugriffs, das als Transportprotokoll UDP verwendet. Siehe auch TACACS+.

RCP Remote Copy Protocol. Protokoll, mit dem Benutzer Dateien in ein oder aus einem Dateisystem kopieren können, das sich auf einem Remote-Host oder -Server im Netzwerk befindet. Das RCP-Protokoll verwendet TCP, um die verlässliche Übertragung von Daten zu gewährleisten.

Regel Zur Konfiguration hinzugefügte Informationen, um eine Sicherheitsrichtlinie in der Form von Bedingungsanweisungen zu definieren, die den Router anweisen, wie auf eine bestimmte Situation reagiert werden soll.

Registrierungs-Proxy-Host Der Proxy-Server für einen Server für die Registrierung von Zertifikaten.

Registrierungs-URL Der Registrierungs-URL ist der HTTP-Pfad zu einer Zertifizierungsstelle (CA), der vom Cisco IOS-Router beim Senden von Zertifikatsanforderungen verwendet werden soll. Der URL enthält entweder einen DNS-Namen oder eine IP-Adresse, und darauf kann der vollständige Pfad zu den CA-Skripts folgen.

Remote-Subnetz Subnetzwerke sind IP-Netzwerke, die von einem Netzwerkadministrator (unter Verwendung einer Subnetzmaske) beliebig segmentiert werden, um eine mehrere Ebenen umfassende hierarchische Routing-Struktur zu bieten und das Subnetzwerk gleichzeitig vor der Komplexität der Adressierung verknüpfter Netzwerke abzuschirmen. Ein Remote-Subnetz ist das Subnetz, das *nicht* mit Ihrem Ende einer Übertragung verknüpft ist.

Replay-Erkennung Eine standardmäßige IPSec-Sicherheitsfunktion, die Sequenznummern mit Authentifizierung kombiniert. So kann der Empfänger in einer Kommunikation alte oder doppelte Pakete zurückweisen, um Replay-Angriffe zu verhindern.

RFC 1483-Routing RFC 1483 beschreibt zwei verschiedene Methoden für den Transport eines verbindungslosen Netzwerk-Datenverkehrs über ein ATM-Netzwerk: über Router übertragene PDUs (Protocol Data Units) und über Brücken übertragene PDUs. Cisco SDM unterstützt die Konfiguration von RFC 1483-Routing und ermöglicht Ihnen die Konfiguration von zwei Kapselungstypen: AAL5MUX und AAL5SNAP.

AAL5MUX: AAL5MUX-Kapselung unterstützt nur ein einzelnes Protokoll (IP oder IPX) pro PVC.

AAL5SNAP: AAL5 LLC/SNAP-Kapselung (Logical Link Control/Subnetwork Access Protocol) unterstützt Inverse ARP und integriert das LLC/SNAP, das dem Protokoll-Datagramm vorausgeht. Dadurch können mehrere Protokolle dieselbe PVC-Verbindung durchlaufen.

Richtlinienzuordnung Eine Richtlinienzuordnung besteht aus konfigurierten Aktionen, die auf den Datenverkehr angewandt werden. Datenverkehr wird in verknüpften Klassenzuordnungen definiert.

RIP Routing Information Protocol. Ein Routing-Protokoll, das die Anzahl der Router, die ein Paket zum Erreichen des Ziels durchlaufen muss, als Routing-Metrik verwendet.

Root CA Oberste Zertifizierungsstelle (CA), die die Zertifikate der ihr untergeordneten CAs signiert. Die Root CA besitzt ein selbstsigniertes Zertifikat, das ihren eigenen öffentlichen Schlüssel enthält.

Route Ein Pfad durch ein Verbundnetzwerk.

Routenzuordnung Mit Routenzuordnungen können Sie die Informationen kontrollieren, die zur Routing-Tabelle hinzugefügt werden. Cisco SDM erstellt automatisch Routenzuordnungen, um die Übersetzung bestimmter Quelladressen durch NAT zu verhindern, wenn eine Übersetzung dazu führen würde, dass Pakete Kriterien in einer IPSec-Regel nicht erfüllen.

RPC Remote Prodedure Call. RPCs sind Prozeduraufrufe, die von Clients erstellt oder angegeben und auf Servern ausgeführt werden. Die Ergebnisse werden über das Netzwerk an die Clients zurückgegeben. Siehe auch Client/Server-Computing.

RR Risk Rating – Risikobewertung. Ein RR ist ein Wert zwischen 0 und 100, der eine numerische Quantifizierung des mit einem bestimmten Ereignis im Netzwerk verbundenen Risikos darstellt.

RSA Eine nach den Erfindern Rivest, Shamir und Adelman bezeichnete kryptografische Schlüsselaustauschmethode, die auf der Faktorierung großer Zahlen basiert. RSA ist auch der Name der Technik selbst. RSA kann für Verschlüsselung und Authentifizierung verwendet werden und ist in viele Sicherheitsprotokolle integriert.

RSA-Schlüssel Ein asymmetrisches RSA-Schlüsselpaar besteht aus einem öffentlichen und einem entsprechenden privaten Schlüssel.

RSA-Signaturen Eine von drei in IPSec angebotenen Authentifizierungsmethoden (die beiden anderen Methoden sind mit RSA verschlüsselte zufällige Werte und Pre-Shared Keys). Auch einer der drei FIPS (Federal Information Processing Standards – US-amerikanische Bundesstandards für Informationsverarbeitung) – genehmigter Algorithmen für die Generierung und Verifizierung von digitalen Signaturen. Die beiden anderen genehmigten Algorithmen sind DSA und Elliptic Curve DSA.

S

SA Security Association. Eine von zwei Peers vereinbarte Gruppe von Sicherheitsparametern zum Schutz einer bestimmten Sitzung in einem bestimmten Tunnel. Sowohl IKE als auch IPSec verwenden SAs, auch wenn SAs unabhängig voneinander sind.

IPSec-SAs sind unidirektional und in jedem Sicherheitsprotokoll eindeutig. Eine IKE-SA wird nur von IKE verwendet, und im Gegensatz zur IPSec-SA ist sie bidirektional. IKE handelt für IPSec SAs aus und erzeugt sie. IPSec SAs können von Benutzern auch manuell erzeugt werden.

Für eine geschützte Daten-Pipe wird eine Gruppe von SAs benötigt, eine pro Richtung und Protokoll. Beispiel: Wenn Sie eine Pipe haben, die ESP (Encapsulating Security Protocol) zwischen Peers unterstützt, ist für jede Richtung eine ESP-SA erforderlich. SAs werden durch Zieladresse (IPSec-Endpunkt), Sicherheitsprotokoll (AH oder ESP) und Sicherheitsparameterindex (SPI) eindeutig identifiziert.

SAID Security Association-ID. Numerischer Identifier für die SA einer angegebenen Verbindung.

Salt Ein String mit pseudozufälligen Zeichen, der zur Erhöhung der kryptografischen Komplexität verwendet wird.

Schlüssel Ein Bit-String, der zum Verschlüsseln oder Entschlüsseln von Daten oder zum Berechnen von Message Digests verwendet wird.

Schlüsselaustausch Die Methode, mit der zwei oder mehr Parteien Verschlüsselungsschlüssel austauschen. Das IKE-Protokoll bietet eine solche Methode.

Schlüsselgültigkeits-dauer Ein Attribut eines Schlüsselpaars, das eine Zeitspanne angibt, in der das Zertifikat mit der öffentlichen Komponente dieses Schlüsselpaars als gültig angesehen wird.

Schlüsselpaar Siehe Public-Key-Verschlüs-selung.

Schlüsselvereinba-rung Der Prozess, mit dem zwei oder mehr Parteien vereinbaren, denselben geheimen symmetrischen Schlüssel zu verwenden.

Schlüsselverwaltung Die Erstellung, Verteilung, Authentifizierung und Speicherung von Verschlüsselungsschlüsseln.

Schnittstelle Die physikalische Verbindung zwischen einem bestimmten Netzwerk und dem Router. Die LAN-Schnittstelle des Routers ist mit dem lokalen Netzwerk verbunden, für das der Router betrieben wird. Der Router besitzt eine oder mehrere WAN-Schnittstellen, die mit dem Internet verbunden sind.

SDEE Security Device Event Exchange. Ein Mitteilungsprotokoll, das für den Bericht von Sicherheitsereignissen verwendet werden kann, wie für Alarmmeldungen, die generiert werden, wenn ein Paket mit den Merkmalen einer Signatur übereinstimmt.

SDF Signature Definition File. Eine Datei, meist im XML-Format, die Signaturdefinitionen enthält, die zum Laden von Signaturen in ein Sicherheitsgerät verwendet werden können.

SDP Secure Device Provisioning. SDP verwendet TTI (Trusted Transitive Introduction) für die einfache Bereitstellung einer Public-Key-Infrastruktur (PKI) zwischen zwei Endgeräten, z. B. einem Cisco IOS-Client und einem Cisco IOS-Zertifizierungsserver.

SEAF Signature Event Action Filter – Signaturereignis-Aktionsfilter. Ein Filter, der es Ihnen erlaubt, Aktionen von einem Ereignis abzuziehen, dessen Parameter in den definierten Bereich fallen. So kann beispielsweise ein SEAF erstellt werden, um die Aktion „TCP-Verbindung zurücksetzen“ von einem Ereignis abzuziehen, das mit einer bestimmten Hacker-Adresse verknüpft ist.

SEAO Signature Event Action Override – Signaturereignis-Aktions-Override. Ein SEAO erlaubt es Ihnen, einen Risikobewertungs-Bereich (RR-Bereich) für einen IPS-Ereignisaktionstyp wie beispielsweise einen Alarm festzulegen. Wenn ein Ereignis eintritt, dessen RR innerhalb des Bereichs liegt, den Sie dem Aktionstyp zugeordnet haben, wird diese Aktion zum Ereignis hinzugefügt. In diesem Fall würde dem Ereignis ein Alarm hinzugefügt werden.

SEAP Signature Event Action Processor – Signaturereignis-Aktionsprozessor. SEAP erlaubt das Filtern und Übergehen auf der Grundlage von Ereignisrisikobewertungs-Rückmeldungen (Event Risk Rating, ERR).

Security Association-Gültigkeitsdauer Der vorab festgelegte Zeitraum, in dem eine SA wirksam ist.

SFR Signature Fidelity Rating – Signatur-Vertrauenswürdigkeitsbewertung. Eine Gewichtung darüber, wie gut sich diese Signatur verhalten könnte, wenn bestimmte Angaben zum Ziel fehlen.

SHA In einigen Verschlüsselungssystemen wird der Secure Hashing Algorithm als Alternative zu MD5 zur Generierung von digitalen Signaturen verwendet.

SHA-1 Secure Hashing Algorithm 1. Algorithmus, der anhand einer Nachricht mit einer Länge unter 264 Bit einen 160-Bit-Message Digest erzeugt. Der große Message Digest bietet Sicherheit gegen Brute-Force-Kollisions- und Inversionsangriffe. SHA-1 [NIS94c] ist eine überarbeitete Version des 1994 veröffentlichten SHA.

Shared-Secret Ein kryptografischer Schlüssel.

Sicherheitszone Eine Gruppe von Schnittstellen, auf die eine Richtlinie angewandt werden kann. Sicherheitszonen sollten aus Schnittstellen bestehen, die ähnliche Funktionen oder Funktionalitäten haben. So können beispielsweise auf einem Router die Schnittstellen Ethernet 0/0 und Ethernet 0/1 mit dem lokalen LAN verbunden sein. Diese zwei Schnittstellen sind ähnlich, da sie das interne Netzwerk repräsentieren, sodass sie für Firewall-Konfigurationen in eine Zone gruppiert werden können.

Signatur Ein Datenelement in IOS IPS, das ein bestimmtes Muster oder einen Missbrauch des Netzwerks erkennt.

Signatur-Engine Eine Signatur-Engine ist eine Komponente von IOS IPS, die darauf ausgerichtet ist, viele Signaturen in einer bestimmten Kategorie zu unterstützen. Eine Engine besteht aus einem Parser und einem Inspector. Jede Engine verfügt über eine Gruppe legaler Parameter, die zulässige Bereiche oder Wertgruppen haben.

Signaturzertifikat Wird verwendet, um Ihre digitale Signatur mit Ihren Nachrichten oder Dokumenten zu verknüpfen und um sicherzustellen, dass Ihre Nachrichten oder Dateien unverändert übermittelt werden.

SIP Session Initiation Protocol. Ermöglicht Anrufverarbeitungssitzungen, insbesondere Zweier-Audiokonferenzen, oder „Anrufe“. SIP arbeitet für den Verbindungsaufbau mit SDP (Session Description Protocol). SDP gibt die Ports für den Medienstrom an. Mit SIP kann der Router beliebige SIP VoIP-Gateways (Voice over IP) und VoIP-Proxy-Server unterstützen.

Site-to-Site-VPN Ein typisches Site-to-Site-VPN ist ein Netzwerk, das zwei Netzwerke oder Subnetzwerke verbindet und einige andere spezifische Kriterien erfüllt. Hierzu gehören die Verwendung von statischen IP-Adressen auf beiden Seiten des Tunnels, das Fehlen von VPN-Clientsoftware auf den Stationen der Benutzer und das Fehlen eines zentralen VPN-Hubs (wie es ihn in Hub-und-Spoke-VPN-Konfigurationen gibt). Site-to-Site-VPNs sind nicht dazu vorgesehen, den Einwählzugriff durch Remote-Benutzer oder mobile Benutzer zu ersetzen.

Sitzungsschlüssel Ein Schlüssel, der nur einmal verwendet wird.

SMTP Simple Mail Transfer Protocol. Internetprotokoll, das E-Mail-Dienste bereitstellt.

SNMP Simple Network Management Protocol. Netzwerkverwaltungsprotokoll, das nahezu ausschließlich in TCP/IP-Netzwerken verwendet wird. SNMP bietet Möglichkeiten zur Überwachung und Steuerung von Netzwerkgeräten und zur Verwaltung von Konfigurationen, der Erfassung statistischer Daten, der Leistung und der Sicherheit.

SPD Selective Packet Discard. Wenn die Warteschlange überlastet ist, erhalten Routing-Protokollpakete und andere wichtige Keepalives der Schicht 2 für die Steuerung des Datenverkehrs durch SPD Priorität.

Sperrkennwort Das Kennwort, das Sie der CA mitteilen, wenn Sie bei ihr die Sperrung des digitalen Zertifikats eines Routers beantragen. Wird manchmal als *Anforderungskennwort* bezeichnet.

Spoke In einem DMVPN-Netzwerk ist ein Spoke-Router ein logischer Endpunkt im Netzwerk und ist über eine Point-to-Point-IPSec-Verbindung mit einem DMVPN-Hub-Router verbunden.

Spoofing

spoofen

Vorgang, bei dem in einem Paket unrechtmäßig behauptet wird, es sei von einer Adresse, von der es in Wahrheit nicht gesendet wurde. Spoofing verfolgt das Ziel, Netzwerksicherheitsmechanismen wie Filter und Zugriffslisten zu konterkarieren.

SRB

Source-Route Bridging. Von IBM entwickelte Briding-Methode, die häufig in Token Ring-Netzwerken eingesetzt wird. In einem SRB-Netzwerk wird die gesamte Route zu einem Ziel vor dem Senden von Daten an das Ziel vorab in Echtzeit bestimmt.

SSH

Secure Shell. Eine Anwendung, die auf einer verlässlichen Transportschicht wie TCP/IP ausgeführt wird und leistungsstarke Authentifizierungs- und Verschlüsselungsfunktionen bietet. Es können bis zu fünf SSH-Clients gleichzeitig auf die Routerkonsole zugreifen.

SSL

Secure Socket Layer. Eine Web-Verschlüsselungstechnologie, die für sichere Transaktionen eingesetzt wird, z. B. die Übertragung von Kreditkartennummern im E-Commerce.

SSL VPN

Secure Socket Layer Virtual Private Networks. SSL VPN ist eine Funktion, die es einem unterstützten Cisco-Router ermöglicht, Remote-Clients einen sicheren Zugang zu Netzwerkressourcen zu bieten, indem über die vom Client verwendete Breitband- oder ISP-Wählverbindung ein verschlüsselter Tunnel durch das Internet geschaffen wird.

SSL VPN-Gateway

Ein WebVPN-Gateway stellt einem WebVPN-Kontext eine IP-Adresse und ein Zertifikat zur Verfügung.

SSL VPN-Gruppenrichtlinie

Mit WebVPN-Gruppenrichtlinien werden die Portalseite und die Links für die Benutzer definiert, die von den jeweiligen Richtlinien betroffen sind. Eine WebVPN-Gruppenrichtlinie wird in einem WebVPN-Kontext konfiguriert.

SSL VPN-Kontext

Ein WebVPN-Kontext stellt die Ressourcen zur Verfügung, die zum Konfigurieren eines sicheren Zugangs zum firmeneigenen Intranet und zu sonstigen privaten Netzwerken benötigt werden. Zu einem WebVPN-Kontext gehört ein entsprechendes WebVPN-Gateway. Ein WebVPN-Kontext kann eine oder mehrere WebVPN-Gruppenrichtlinien bereitstellen.

Standard-Gateway

Das letztmögliche Gateway. Zu diesem Gateway wird ein Paket geleitet, wenn dessen Zieladresse keinem Eintrag in der Routingtabelle entspricht.

Standardregel Ein Typ einer Zugriffsregel oder NAT-Regel in Cisco SDM. Standardregeln vergleichen die Quell-IP-Adresse eines Pakets mit den zugehörigen Kriterien der IP-Adresse und ermitteln eine Übereinstimmung. Standardregeln verwenden eine Platzhaltermaske, um die Teile der IP-Adresse zu ermitteln, für die eine Übereinstimmung erforderlich ist.

Static PAT Static Port Address Translation. Eine statische Adresse ordnet eine lokale IP-Adresse einer globalen IP-Adresse zu. Bei Static PAT handelt es sich um eine statische Adresse, die auch einen lokalen Port einem globalen Port zuordnet. Siehe auch PAT.

statische Route Route, die explizit konfiguriert und in die Routing-Tabelle eingetragen wurde. Statische Routen haben Vorrang vor Routen, die von Protokollen für dynamisches Routing ausgewählt werden.

Subnetz, Subnetzwerk Ein Netzwerk in IP-Netzwerken mit einer bestimmten gemeinsam verwendeten Subnetzadresse. Subnetzwerke sind Netzwerke, die vom Netzwerkadministrator beliebig segmentiert werden, um eine mehrere Ebenen umfassende hierarchische Routing-Struktur zu bieten und das Subnetzwerk gleichzeitig vor der Komplexität der Adressierung verknüpfter Netzwerke abzuschirmen. Siehe auch IP-Adresse, Subnetz-Bits und Subnetzmaske.

Subnetz-Bits

Subnetzmaske 32-Bit-Adressenmasken, die im IP verwendet werden, um die Bits einer IP-Adresse anzugeben, die für das Netzwerk und die optionale Subnetzadresse verwendet werden. Subnetzmasken werden in Dezimalziffern ausgedrückt. Die Maske 255.255.255.0 gibt an, dass die ersten 24 Bits der Adresse ... Wird manchmal einfach als Maske bezeichnet. Siehe auch Adressenmaske und IP-Adresse.

SUNRPC SUN-Remote-Verfahrensaufruf (SUN Remote Procedure Call). RPC ist ein Protokoll, das es Clients erlaubt, Programme oder Routinen auf Remote-Servern auszuführen. SUNRPC ist die RPC-Version, die ursprünglich in der SUN Open Network Computing (ONC)-Bibliothek verteilt wurde.

symmetrischer Schlüssel Ein symmetrischer Schlüssel wird zum Entschlüsseln von zuvor verschlüsselten Informationen verwendet.

T

T1 Eine T1-Verbindung ist eine Datenverbindung, mit der Daten mit einer Rate von 1,5 Mbit/s übertragen werden können.

TACACS+ Terminal Access Controller Access Control System plus – Terminalzugriffs-Controller-Zugriffssteuerungssystem Plus. Ein Protokoll zur Authentifizierung und Kontoführung des Serverzugriffs, das als Transportprotokoll TCP verwendet.

Tail-End Der Daten empfangende Downstream-Endpunkt eines Tunnels.

TCP Transmission Control Protocol. Verbindungsorientiertes Transportschichtprotokoll, das zuverlässige Vollduplex-Datenübertragung bietet.

TCP Syn-Flood-Attacke Eine SYN-Flooding-Attacke findet statt, wenn ein Hacker einen Server mit unaufhörlich eingehenden Verbindungsanforderungen flutet. Da diese Nachrichten nicht erreichbare Rücksprungadressen haben, können die Verbindungen nicht aufgebaut werden. Das daraus resultierende Volumen nicht aufgelöster offener Verbindungen überflutet schließlich den Server und kann dazu führen, dass er gültigen Anforderungen nicht mehr entspricht. Dadurch können rechtmäßige Benutzer keine Websites mehr aufrufen, nicht mehr auf E-Mails zugreifen, nicht mehr den FTP-Dienst benutzen usw.

Telnet Ein Terminalemulationsprotokoll für TCP/IP-Netzwerke wie z. B. das Internet. Telnet wird allgemein für die Remote-Steuerung von Webservern eingesetzt.

TFTP Trivial File Transfer Protocol. TFTP ist ein einfaches Protokoll für die Übertragung von Dateien. Es wird auf UDP ausgeführt und ist in RFC (Request For Comments) 1350 detailliert erläutert.

Transformation Beschreibung eines Sicherheitsprotokolls und seiner entsprechenden Algorithmen.

Transformationssatz Ein Transformationssatz ist eine zulässige Kombination aus Sicherheitsprotokollen, Algorithmen und anderen Einstellungen, die für durch IPSec geschützten Datenverkehr angewendet werden. Während der IPSec Security Association-Aushandlung vereinbaren die Peers, einen bestimmten Transformationssatz beim Schutz eines bestimmten Datenflusses zu verwenden.

Tunnel Ein virtueller Kanal durch ein gemeinsam verwendetes Medium, z. B. das Internet. Er wird für den Austausch gekapselter Datenpakete verwendet.

Tunneling Der Prozess, bei dem der Strom eines Protokolls in einer Pipe durch ein anderes Protokoll geleitet wird.

TVR Target Value Rating – Zielwertbewertung. TVR ist ein benutzerdefinierter Wert, der den vom Benutzer wahrgenommenen Wert des Zielhosts repräsentiert. Dies ermöglicht es dem Benutzer, das Risiko eines Ereignisses zu erhöhen, das mit einem wichtigen System verbunden ist und das Risiko eines Ereignisses auf einem Ziel niedrigen Werts zu vermindern.

U

Überwachungsrate Die Rate der Bits pro Sekunde, die der Datenverkehr nicht überschreiten darf.

UDP User Datagram Protocol. Verbindungsloses Transportschichtprotokoll im TCP/IP-Protokoll, das zur Internetprotokollfamilie gehört.

Unity-Client Ein Client eines Unity Easy VPN-Servers.

unverschlüsselt Nicht verschlüsselt.

URI Uniform Resource Identifier. Typ eines formatierten Identifiers, der den Namen eines Internetobjekts enthält und mit einer Kennung des Namespace benennt, sodass ein Mitglied der universellen Namensgruppe in registrierten Namespaces und von Adressen erzeugt wird, die auf registrierte Protokolle oder Namespaces verweisen. [RFC 1630]

URL Universal Resource Locator. Ein standardisiertes Adressierungsschema für den Zugriff auf Hypertextdokumente und andere Dienste mit einem Browser. Es folgen zwei Beispiele:

http://www.cisco.com.

ftp://10.10.5.1/netupdates/sig.xml

V

VCI Virtual Channel Identifier. Ein virtueller Pfad kann mehrere virtuelle Kanäle aufnehmen, die einzelnen Verbindungen entsprechen. Der VCI identifiziert den Kanal, der verwendet wird. Die Kombination aus VPI und VCI identifiziert eine ATM-Verbindung.

Verifizierung Die Bestätigung der Identität einer Person oder eines Prozesses.

Verkehrsflussvertraulichkeit oder Datenverkehranalyse Sicherheitskonzept, das die nicht autorisierte Offenlegung von Kommunikationsparametern verhindert. Mit der erfolgreichen Implementierung dieses Konzepts werden Quell- und Ziel-IP-Adressen, Nachrichtenlänge und die Häufigkeit der Kommunikation vor nicht autorisierten Parteien verborgen.

verschlüsseln Aus Klartext mit kryptografischen Mitteln Chiffretext erzeugen.

Verschlüsselung Anwendung eines bestimmten Algorithmus auf Daten, um das Darstellungsbild von Daten so zu ändern, dass sie von Personen, die nicht zur Anzeige der Informationen berechtigt sind, nicht verstanden werden.

verteilter Schlüssel Ein gemeinsamer kryptografischer Schlüssel, der in Teile aufgeteilt ist, wobei jedes Teil an einen anderen Teilnehmer geht.

Vertrauenswürdigkeitsbewertung Eine Zahl von 1 bis 100, die angibt, wie viel Vertrauen ein Bewerter hat, dass eine Signatur eine korrekte Warnung erzeugt.

VFR Virtual Fragment Reassembly. VFR ermöglicht der IOS-Firewall die dynamische Erstellung von ACLs, um IP-Fragmente zu blockieren. IP-Fragmente enthalten häufig genügend Informationen, um von statischen ACLs gefiltert zu werden.

VPDN Virtual Private Dial-up Network. Ein System, in dem Einwahlnetzwerke als Remote-Netzwerke von Home-Netzwerken existieren können und den Anschein erwecken, dass sie direkt verbunden wären. VPDNs verwenden nicht den NAS (Network Access Server), sondern L2TP und L2F zur Terminierung der auf Schicht 2 und höher angesiedelten Komponenten der Netzwerkverbindung auf dem Home-Gateway.

VPI Virtual Path Identifier. Identifiziert den virtuellen Pfad, der von einer ATM-Verbindung verwendet wird.

VPN Virtual Private Network. Bietet Benutzern über eine öffentliche Infrastruktur dieselbe Netzwerkkonnektivität wie über ein privates Netzwerk. VPNs ermöglichen sicheren IP-Datenverkehr über ein öffentliches TCP/IP-Netzwerk durch Verschlüsselung des gesamten Datenverkehrs von einem Netzwerk in ein anderes. Ein VPN verwendet Tunneling zur Verschlüsselung aller Informationen auf der IP-Ebene.

VPN-Spiegelrichtlinie Eine VPN-Richtlinie auf einem Remote-System, die Werte enthält, die mit einer lokalen Richtlinie kompatibel sind und es dem Remote-System ermöglichen, eine VPN-Verbindung mit dem lokalen System aufzubauen. Einige Werte in einer Spiegelrichtlinie müssen mit den Werten in einer lokalen Richtlinie übereinstimmen. Andere Werte, z. B. die IP-Adresse des Peers, müssen der umgekehrte Wert des entsprechenden Wertes in der lokalen Richtlinie sein.

Sie können bei der Konfiguration von Site-to-Site-VPN-Verbindungen Spiegelrichtlinien erstellen, die Remote-Administratoren verwenden sollen. Informationen zum Generieren einer Spiegelrichtlinie finden Sie unter Spiegel generieren....

VPN-Verbindung Ein Site-to-Site-VPN. Ein Site-to-Site-VPN besteht aus einer Gruppe von VPN-Verbindungen zwischen Peers, wobei die definierenden Attribute der einzelnen Verbindungen die folgenden Gerätekonfigurationsdaten umfassen:

- Einen Verbindungsnamen
- Optional eine IKE-Richtlinie und einen Pre-Shared Key
- Einen IPSec-Peer
- Eine Liste mit einem oder mehreren Remote-Subnetzen oder -Hosts, die durch die Verbindung geschützt werden
- Eine IPSec-Regel, die definiert, welcher Datenverkehr zu verschlüsseln ist
- Eine Liste mit Transformationssätzen, die definieren, wie geschützter Datenverkehr zu verschlüsseln ist
- Eine Liste der Gerätenetzwerkschnittstellen, denen die Verbindung zugeordnet ist

VTI Virtual Template Interface – Virtuelle Vorlagenschnittstelle.

VTY Virtual Type Terminal. Allgemein als Virtual Terminal-Zeilen verwendet.

W

WAN Local Area Network – lokales Netzwerk. Ein Netzwerk für Benutzer, die über einen großen geografischen Bereich verteilt sind. In ihm werden oft Übertragungsgeräte von Telekommunikationsunternehmen verwendet. Siehe auch LAN.

WINS Windows Internet Naming Service. Ein Windows-System, das die IP-Adresse bestimmt, die mit einem bestimmten Netzwerkcomputer verknüpft ist.

X

X.509 Ein Standard für digitale Zertifikate, der die Zertifikatstruktur angibt. Die Hauptfelder sind ID, Inhaberfeld, Gültigkeitsdatumsangaben, öffentlicher Schlüssel und CA-Signatur.

X.509-Sperrliste (CRL) Eine Liste mit Nummern von Zertifikaten, die gesperrt wurden. Eine X.509-CRL ist eine Liste, die einer der beiden CRL-Formatierungsdefinitionen in X.509 entspricht.

X.509-Zertifikat Ein digitales Zertifikat, das nach den X.509-Richtlinien strukturiert ist.

XAuth IKE Extended Authentication. XAuth ermöglicht es allen AAA-Authentifizierungsmethoden der Cisco IOS-Software, die Benutzerauthentifizierung in einer eigenen Phase nach dem Austausch in der ersten IKE-Authentifizierungsphase durchzuführen. Der AAA-Konfigurationslistenname muss dem XAuth-Konfigurationslistennamen entsprechen, damit die Benutzerauthentifizierung stattfindet.

XAuth ist eine Erweiterung von IKE und ersetzt nicht die IKE-Authentifizierung.

Z

Zertifikat Siehe digitales Zertifikat.

Zertifikatsidentität Ein X.509-Zertifikat enthält Informationen zur Identität des Geräts oder der Instanz, die das Zertifikat besitzt. Die Informationen für die Identifizierung werden dann bei jeder nachfolgenden Peer-Verifizierung und -Authentifizierung untersucht. Zertifikatsidentitäten können aber für Spoofing-Angriffe anfällig sein.

Zone In einer zonenbasierten Richtlinienfirewall ist eine Zone eine Gruppe von Schnittstellen, die ähnliche Funktionen oder Funktionalitäten haben. Wenn beispielsweise die Schnittstellen FastEthernet 0/0 und FastEthernet 0/1 beide mit dem LAN verbunden sind, können Sie in eine einzelne Zone für das LAN gruppiert werden.

Zonenpaar Ein Zonenpaar erlaubt Ihnen, einen unidirektionalen Datenverkehrsstrom zwischen zwei Sicherheitszonen anzugeben. Siehe auch Sicherheitszone.

ZPF Zone-Based Policy Firewall – zonenbasierte Richtlinienfirewall. In einer ZPF-Konfiguration werden Schnittstellen Zonen zugeordnet, und es wird eine Prüfrichtlinie auf Datenverkehr zwischen zwei Zonen angewandt.

Zugriffssteuerung, Zugriffssteuerungsregel In die Konfiguration eingegebene Informationen, mit denen Sie angeben können, welcher Datenverkehrstyp für eine Schnittstelle zugelassen oder abgelehnt werden soll. Standardmäßig wird Datenverkehr, der nicht ausdrücklich zugelassen ist, abgelehnt. Zugriffssteuerungsregeln bestehen aus ACEs (Access Control Entry – Zugriffssteuerungseintrag).

Zustand, stateful, Stateful Inspection

Netzwerkprotokolle verwalten an jedem Ende einer Netzwerkverbindung zwischen zwei Hosts bestimmte Daten, die als Zustandsinformationen bezeichnet werden. Zustandsinformationen sind notwendig, um die Funktionen eines Protokolls zu implementieren, z. B. garantierte Paketübergabe, Datensequenzierung, Flusskontrolle und Transaktions- oder Sitzungs-IDs. Einige der Protokollzustandsinformationen werden in jedem Paket gesendet, während die einzelnen Protokolle verwendet werden. Ein mit einem Webserver verbundener Webbrowser verwendet z. B. HTTP und unterstützende TCP/IP-Protokolle. Jede Protokollschicht verwaltet Zustandsinformationen in den Paketen, die sie sendet und empfängt. Router prüfen die Zustandsinformationen in jedem Paket, um zu verifizieren, dass sie aktuell und gültig für jedes Protokoll sind, das sie enthalten. Dies wird als Stateful Inspection bezeichnet und dient dazu, eine starke Barriere gegen bestimmte Arten von Bedrohungen für die Sicherheit von Computern zu schaffen.

INDEX

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z