370111

ADMINISTRATOR-HANDBUCH

Cisco
Gigabit-Dual-WAN-VPN-Router RV320/RV325

Inhalt

Inhalt

Inhalt

2

Erste Schritte

Die Standardeinstellungen sind für viele kleine Unternehmen ausreichend. Möglicherweise müssen Sie die Einstellungen aufgrund der Netzwerkanforderungen des Internetdienstanbieters (Internet Service Provider, ISP) ändern. Für die Verwendung der Weboberfläche benötigen Sie einen PC mit Internet Explorer (Version 6 und höher), Firefox oder Safari (für Mac).

So starten Sie die Weboberfläche:

SCHRITT 1 Schließen Sie einen PC an einen nummerierten LAN-Anschluss des Geräts an. Wenn der PC als DHCP-Client konfiguriert ist, wird ihm eine IP-Adresse im Bereich 192.168.1.x zugewiesen.

SCHRITT 2 Starten Sie einen Webbrowser.

SCHRITT 3 Geben Sie in der Adresszeile die Standard-IP-Adresse des Geräts ein: **192.168.1.1**. Möglicherweise wird im Browser eine Warnung angezeigt, aus der hervorgeht, dass die Website nicht vertrauenswürdig ist. Fahren Sie mit dem Laden der Website fort.

SCHRITT 4 Wenn die Anmeldeseite angezeigt wird, geben Sie den Standardbenutzernamen **cisco** und das Standardkennwort **cisco** (jeweils in Kleinbuchstaben) ein.

SCHRITT 5 Klicken Sie auf **Anmelden**. Die Seite **Systemübersicht** wird angezeigt. Überprüfen Sie unter **Anschlussaktivität**, ob eine WAN-Verbindung aktiviert ist. Wenn dies nicht der Fall ist, fahren Sie mit dem nächsten Schritt fort.

SCHRITT 6 Zum Konfigurieren der Internetverbindung mithilfe des Einrichtungsassistenten klicken Sie auf der Seite **Systemübersicht** auf **Einrichtungsassistent**. Klicken Sie alternativ im Navigationsbaum auf **Assistent** und dann im Abschnitt **Basiseinrichtung** auf **Jetzt starten**. Befolgen Sie die Anweisungen auf dem Bildschirm.

Wenn im Webbrowser eine Warnmeldung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 7 Über die Links im Navigationsbaum können Sie weitere Einstellungen konfigurieren.

Tipps zur Fehlerbehebung

Bei Problemen mit dem Herstellen der Verbindung mit dem Internet oder der Weboberfläche:

- Vergewissern Sie sich, dass im Webbrowser nicht der Offlinemodus festgelegt ist.
- Überprüfen Sie die LAN-Verbindungseinstellungen für den Ethernetadapter. Der PC sollte über DHCP eine IP-Adresse beziehen. Alternativ kann der PC eine statische IP-Adresse im Bereich 192.168.1.x haben und das Standardgateway auf 192.168.1.1 (die Standard-IP-Adresse des Geräts) festgelegt sein.
- Vergewissern Sie sich, dass Sie im Assistenten die richtigen Einstellungen zum Einrichten der Internetverbindung eingegeben haben.
- Setzen Sie das Modem und das Gerät zurück, indem Sie beide Geräte ausschalten. Schalten Sie das Modem ein, und lassen Sie es etwa zwei Minuten lang im Leerlauf. Schalten Sie dann das Gerät ein. Jetzt sollten Sie eine WAN-IP-Adresse erhalten.
- Wenn Sie ein DSL-Modem haben, bitten Sie den ISP, das DSL-Modem in den Bridge-Modus zu versetzen.

Funktionen der Benutzeroberfläche

Die Benutzeroberfläche soll das Einrichten und Verwalten des Geräts erleichtern.

Navigation

Die Hauptmodule der Weboberfläche werden links im Navigationsbereich durch Schaltflächen dargestellt. Klicken Sie auf eine Schaltfläche, um weitere Optionen anzuzeigen. Klicken Sie auf eine Option, um eine Seite zu öffnen.

Popup-Fenster

Über einige Links und Schaltflächen werden Popup-Fenster geöffnet, in denen weitere Informationen oder verwandte Konfigurationsseiten angezeigt werden. Wenn im Webbrowser eine Warnmeldung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

Hilfe

Zum Anzeigen von Informationen zur ausgewählten Konfigurationsseite klicken Sie in der rechten oberen Ecke der Weboberfläche auf **Hilfe**. Wenn im Webbrowser eine Warnmeldung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

Abmelden

Zum Verlassen der Weboberfläche klicken Sie in der rechten oberen Ecke der Weboberfläche auf **Abmeldung**. Die Seite **Anmelden** wird angezeigt.

3

Assistent

Auf der Seite **Assistent** können Sie den Einrichtungsassistenten für die Basiseinrichtung starten, der Sie durch die Erstkonfiguration des Geräts führt. Der Assistent für Zugriffsregeln führt Sie durch die Konfiguration der Sicherheitsrichtlinien für das Netzwerk.

Basiseinrichtung

Mit dem Einrichtungsassistenten für die Basiseinrichtung können Sie die Anzahl der WAN-Anschlüsse ändern oder die Internetverbindung konfigurieren.

Klicken Sie auf **Jetzt starten**, um den Einrichtungsassistenten für die Basiseinrichtung auszuführen. Folgen Sie den Anweisungen auf dem Bildschirm. Nehmen Sie beim Eingeben der erforderlichen Einstellungen für die Verbindung die Informationen vom ISP zu Hilfe.

Zugriffsregeln einrichten

Mit dem Einrichtungsassistenten für die Zugriffsregeln können Sie Firewallzugriffsregeln erstellen. Klicken Sie auf **Jetzt starten**, um den Einrichtungsassistenten für die Zugriffsregeln auszuführen. Der Assistent stellt Informationen zu den Standardregeln für das Gerät bereit. Folgen Sie den Anweisungen auf dem Bildschirm.

3

Assistent

4

Systemübersicht

In der Systemübersicht werden Informationen zum aktuellen Status der Verbindungen sowie zu Status, Einstellungen und Protokollen des Geräts angezeigt.

Systeminformationen

Beschreibungen der Systeminformationen:

- **Seriennummer**: Seriennummer des Geräts
- **Firmwareversion**: Versionsnummer der installierten Firmware
- **PID-VID**: Versionsnummer der Hardware
- **MD5-Prüfsumme**: Ein für die Überprüfung von Dateien verwendeter Wert
- **LAN IPv4/Subnetzmaske**: Verwaltungs-IP-Adresse für IPv4 und Subnetzmaske des Geräts
- **LAN IPv6/Präfix**: IPv6-Verwaltungs-IP-Adresse und -Präfix
- **Arbeitsmodus**: Steuert das Verhalten des Geräts im Zusammenhang mit der WAN-Verbindung. Den Gatewaymodus wählen Sie aus, wenn im Gerät eine Internet-WAN-Verbindung gehostet wird. Den Routermodus wählen Sie aus, wenn sich das Gerät in einem Netzwerk ohne WAN-Verbindung befindet oder die WAN-Verbindung über ein anderes Gerät hergestellt wird. Zum Ändern dieses Parameters klicken Sie auf **Arbeitsmodus**, um das Fenster **Erweitertes Routing** anzuzeigen.
- **Systembetriebszeit**: Gibt an, seit wie vielen Tagen, Stunden und Minuten das Gerät aktiv ist.

Konfiguration (Assistent)

Zum Zugreifen auf den Setup-Assistenten für Internetverbindungen und zum Durchlaufen des Vorgangs anhand von Eingabeaufforderungen klicken Sie auf **Einrichtungsassistent**, um den **Assistenten** zu starten.

Anschlussaktivität

Unter **Anschlussaktivität** werden die Anschlussschnittstellen identifiziert und die Status der einzelnen Anschlüsse angezeigt:

- **Anschluss-ID**: Beschriftung des Anschlusses.
- **Schnittstelle**: Schnittstellentyp, LAN, WAN oder DMZ. Mehrere WAN-Schnittstellen werden mit Nummern angegeben, beispielsweise WAN1 oder WAN2.
- **Status**: Status des Anschlusses, **Deaktiviert** (rot), **Aktiviert** (schwarz) oder **Verbunden** (grün). Bei dem Statuswert handelt es sich um einen Hyperlink. Klicken Sie auf den Hyperlink, um das Fenster **Anschlussinformationen** zu öffnen.

IPv4 und IPv6

Im Abschnitt **IPv4** oder **IPv6** finden Sie die Statistiken der einzelnen WAN-Anschlusses. (Die Registerkarte **IPv6** ist verfügbar, wenn auf der Seite **Einrichten des Netzwerks** die Option **Dual-Stack-IP** aktiviert ist.

WAN-Informationen

Die folgenden WAN-Informationen werden bereitgestellt:

- **IP-Adresse**: Öffentliche IP-Adresse für diese Schnittstelle
- **Standardgateway**: Standardgateway für diese Schnittstelle
- **DNS**: IP-Adresse des DNS-Servers für diese Schnittstelle
- **Dynamischer DNS**: DDNS-Einstellungen für diesen Anschluss: **Deaktiviert** oder **Aktiviert**.

Sicherheitsstatus

In diesem Abschnitt wird der Status der Sicherheitsfunktionen angezeigt:

- **SPI (Stateful Packet Inspection)**: Status der Firewall, **Ein** (grün) oder **Aus** (rot). Verfolgt den Status von Netzwerkverbindungen wie beispielsweise TCP-Streams und UDP-Kommunikation, die durch die Firewall weitergeleitet werden. Die Firewall unterscheidet zwischen legitimen Paketen für verschiedene Verbindungstypen. Nur Pakete, die mit einer bekannten aktiven Verbindung übereinstimmen, können die Firewall passieren. Andere Pakete werden abgelehnt.
- **DoS (Denial of Service)**: Status des DoS-Filters, **Ein** (grün) oder **Aus** (rot). Bei einer DoS-Attacke handelt es sich um den Versuch, einen Computer oder eine Netzwerkressource für die vorgesehenen Benutzer nicht verfügbar zu machen.
- **WAN-Anfrage sperren**: Erschwert externen Benutzern den Zugriff auf das Netzwerk, indem die Netzwerkports vor Netzwerkgeräten *verborgen* werden. Außerdem wird das Senden von Ping-Signalen an das Netzwerk und die Erkennung des Netzwerks durch andere Internetbenutzer verhindert. Der Status entspricht **Ein** (grün) oder **Aus** (rot). WAN-Anfrage sperren
- **Remoteverwaltung**: Gibt an, dass eine Remoteverbindung zum Verwalten des Geräts zulässig ist oder verweigert wird. **Ein** (grün) bedeutet, dass Remote-Management zulässig ist. **Aus** (rot) bedeutet, dass Remote-Management nicht zulässig ist.
- **Zugriffsregel**: Anzahl der festgelegten Zugriffsregeln

Zum Anzeigen detaillierter Informationen zur Sicherheitsfunktion klicken Sie auf die Bezeichnung der Funktion.

VPN-Einstellungsstatus

In diesem Abschnitt wird der Status der VPN-Tunnel angezeigt:

- **VPN-Tunnel belegt**: Verwendete VPN-Tunnel
- **VPN-Tunnel verfügbar**: Verfügbare VPN-Tunnel
- **Easy VPN-Tunnel belegt**: Verwendete Easy VPN-Tunnel

- **Easy VPN-Tunnel verfügbar**: Verfügbare Easy VPN-Tunnel
- **PPTP-Tunnel belegt**: Verwendete PPTP-Tunnel (Point-to-Point Tunneling Protocol). PPTP ist eine Methode zum Implementieren virtueller privater Netzwerke. Bei PPTP werden PPP-Pakete mithilfe eines Steuerungskanals über TCP und einen GRE-Tunnel (Generic Routing Encapsulation) gekapselt.
- **PPTP-Tunnel verfügbar**: Verfügbare PPTP-Tunnel

Protokolleinstellungsstatus

In diesem Abschnitt wird der Status der Protokolle angezeigt:

- **Syslog-Server**: Status von Syslog: **Ein** (grün) oder **Aus** (rot).
- **E-Mail-Protokoll**: Status des E-Mail-Protokolls: **Ein** (grün) oder **Aus** (rot).

5

Einrichten

Auf der Seite **Einrichten > Netzwerk** können Sie ein LAN, ein WAN (Internet), eine DMZ usw. einrichten.

Einrichten des Netzwerks

Bei manchen ISPs müssen Sie zur Identifizierung des Geräts einen Hostnamen und einen Domänennamen zuweisen. Es werden Standardwerte bereitgestellt, die Sie jedoch nach Bedarf ändern können:

- **Hostname**: Behalten Sie die Standardeinstellung bei, oder geben Sie einen vom ISP vorgegebenen Hostnamen ein.
- **Domänenname**: Behalten Sie die Standardeinstellung bei, oder geben Sie einen vom ISP vorgegebenen Domänennamen ein.

IP-Modus

Wählen Sie den Adressierungstyp aus, der in den Netzwerken verwendet werden soll:

- **Nur IPv4**: Nur IPv4-Adressierung
- **Dual-Stack-IP**: IPv4- und IPv6-Adressierung. Nach dem Speichern der Parameter können Sie IPv4- und IPv6-Adressen für die LAN-, WAN- und DMZ-Netzwerke konfigurieren.

Hinzufügen oder Bearbeiten eines IPv4-Netzwerks

Standardmäßig ist ein IPv4-LAN-Subnetz konfiguriert (192.168.1.1). Für die meisten kleinen Unternehmen reicht in der Regel ein einziges Subnetzwerk aus. Die Firewall verweigert den Zugriff, wenn die Quell-IP-Adresse eines LAN-Geräts zu einem nicht ausdrücklich zugelassenen Subnetz gehört. Sie können Verkehr aus anderen Subnetzen zulassen und dieses Gerät als Edge-Router verwenden, der Internetkonnektivität für ein Netzwerk bereitstellt.

SCHRITT 1 Klicken Sie auf die Registerkarte **IPv4**, um die Multi-Subnetztabelle anzuzeigen.

SCHRITT 2 Zum Hinzufügen eines Subnetzes klicken Sie auf **Hinzufügen**. In den Spalten werden die Felder **IP-Adresse** und **Subnetzmaske** angezeigt. Nach dem Klicken auf **Speichern** können Sie das Subnetz bearbeiten, um es als Teil eines VLANs festzulegen, die IP-Adressen über den DHCP-Server zu verwalten oder Parameter für TFTP-Server festzulegen.

SCHRITT 3 Geben Sie die **IP-Adresse** und die **Subnetzmaske** für das Gerät ein.

SCHRITT 4 Klicken Sie auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

Zum Bearbeiten eines Subnetzes wählen Sie das zu ändernde IPv4-Subnetz aus, und klicken Sie auf **Bearbeiten**. Im Abschnitt **DHCP-Einrichtung** wird beschrieben, wie Sie die Subnetzparameter ändern.

Bearbeiten des IPv6-Adresspräfixes

Wenn Sie Dual-Stack-IP für den IP-Modus aktiviert haben, können Sie das IPv6-Präfix konfigurieren.

Zum Konfigurieren des IPv6-Präfixes klicken Sie auf die Registerkarte **IPv6**, wählen Sie das IPv6-Präfix aus, und klicken Sie auf **Bearbeiten**. Die Standard-IP-Adresse lautet **fc00::1**, und die Standardpräfixlänge lautet **7**. Die Registerkarte **IPv6** ist nur verfügbar, wenn in der Tabelle **IP-Modus** die Option **Dual-Stack-IP** aktiviert ist. Das Fenster **DHCP-Einrichtung** wird angezeigt.

Anschlusseinstellungen für WAN1 oder WAN2

In der **WAN-Einstellungstabelle** werden die Schnittstelle (beispielsweise USB1, WAN1 oder WAN2) und der Verbindungstyp angezeigt. Die Einstellungen für die Schnittstellen können Sie ändern.

HINWEIS Wenn Sie IPv6 ausführen, wählen Sie die Registerkarte **IPv6** und dann die zu konfigurierende WAN-Schnittstelle aus. Anderenfalls werden die IPv6-Parameter im Fenster **WAN-Verbindungseinstellungen** nicht angezeigt.

Zum Konfigurieren der **WAN-Verbindungseinstellungen** wählen Sie eine WAN-Schnittstelle aus, und klicken Sie auf **Bearbeiten**. Das Fenster **WAN-Verbindungseinstellungen** wird angezeigt.

Wählen Sie im Menü den **WAN-Verbindungstyp** aus, und ändern Sie die zugehörigen Parameter wie in den folgenden Abschnitten beschrieben:

IP-Adresse automatisch beziehen

Wählen Sie diese Option aus, wenn der ISP dem Gerät dynamisch eine IP-Adresse zuweist. (Die meisten Kabelmodembenutzer verwenden diesen Verbindungstyp.) Der ISP weist dem Gerät eine IP-Adresse für diesen Anschluss zu (einschließlich der IP-Adressen von DNS-Servern).

Zum Angeben eines DNS-Servers aktivieren Sie das Kontrollkästchen **Folgende DNS-Server-Adressen verwenden**, und geben Sie die IP-Adresse von **DNS-Server 1** ein. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.

Wenn die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**) automatisch festgelegt werden soll, wählen Sie **Automatisch** aus. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

Zum Konfigurieren der IPv6-Parameter aktivieren Sie das Kontrollkästchen **Aktivieren**. Der DHCPv6-Clientprozess und Anfragen für die Präfix-Delegation durch die ausgewählte Schnittstelle werden aktiviert. Verwenden Sie diese Option, wenn der ISP LAN-Präfixe über DHCPv6 senden kann. Wenn der ISP diese Option nicht unterstützt, konfigurieren Sie manuell ein LAN-Präfix:

HINWEIS Wenn DHCP-PD aktiviert ist, ist die manuelle LAN-IPv6-Adressierung deaktiviert. Wenn DHCP-PD deaktiviert ist, ist die manuelle LAN-IPv6-Adressierung aktiviert.

- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge: Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**:
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

Statische IP-Adresse

Wählen Sie diese Option aus, wenn der ISP Ihrem Konto eine feste IP-Adresse zugewiesen hat. Geben Sie die vom ISP vorgegebenen Einstellungen ein:

- **WAN-IP-Adresse angeben**: Die IP-Adresse, die der ISP Ihrem Konto zugewiesen hat
- **Subnetzmaske (IPv4)**: Subnetzmaske
- **Standardgatewayadresse**: IP-Adresse des Standardgateways

Zum Angeben eines DNS-Servers geben Sie die IP-Adresse von **DNS-Server 1** ein. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.

Wenn die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**) automatisch festgelegt werden soll, wählen Sie **Automatisch** aus. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

So konfigurieren Sie die IPv6-Parameter:

- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge: Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

PPPoE

Wählen Sie diese Option aus, wenn der ISP zum Herstellen von Internetverbindungen PPPoE (Point-to-Point Protocol over Ethernet) verwendet (typisch bei DSL-Leitungen). Geben Sie dann die vom ISP vorgegebenen Einstellungen ein:

- **Benutzername** und **Kennwort**: Benutzername und Kennwort für das ISP-Konto. Hier können Sie jeweils maximal 255 Zeichen eingeben.
- **Servicename**: Eine Reihe vom ISP bereitgestellter Services, die anhand des Servicenamens identifiziert werden

- **Verbindungstimer**: Nach einer bestimmten Dauer der Inaktivität wird die Verbindung getrennt.
  - **Verbindung bei Bedarf**: Wenn diese Funktion aktiviert ist, wird die Verbindung vom Gerät automatisch hergestellt. Wenn Sie diese Funktion aktiviert haben, geben Sie in **Max. Leerlaufzeit** ein, nach wie vielen Minuten der Inaktivität die Verbindung getrennt wird. Der Standardwert für die maximale Leerlaufzeit beträgt **5 Minuten**.
  - **Keep-Alive**: Stellt sicher, dass der Router immer mit dem Internet verbunden ist. Wenn diese Funktion ausgewählt ist, hält der Router die Verbindung aufrecht, indem er in regelmäßigen Abständen einige Datenpakete sendet. Mit dieser Option bleibt die Verbindung auch dann unbegrenzt aktiv, wenn sich die Leitung längere Zeit im Leerlauf befindet. Wenn Sie diese Funktion aktivieren, geben Sie auch unter **Zeit bis Neueinwahl** an, wie oft der Router die Internetverbindung überprüft. Der Standardwert lautet **30 Sekunden**.
- **Folgende DNS-Server-Adressen verwenden**: Aktiviert das Beziehen von Verbindungsinformationen von DNS-Servern.
- **DNS-Server 1** und **DNS-Server 2**: IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **MTU**: Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**). Wählen Sie **Automatisch** aus, wenn die Größe automatisch festgelegt werden soll. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

Zum Konfigurieren der IPv6-Parameter aktivieren Sie das Kontrollkästchen **Aktivieren**. Der DHCPv6-Clientprozess und Anfragen für die Präfix-Delegation durch die ausgewählte Schnittstelle werden aktiviert. Verwenden Sie diese Option, wenn der ISP LAN-Präfixe über DHCPv6 senden kann. Wenn der ISP diese Option nicht unterstützt, konfigurieren Sie manuell ein LAN-Präfix:

HINWEIS Wenn DHCP-PD aktiviert ist, ist die manuelle LAN-IPv6-Adressierung deaktiviert. Wenn DHCP-PD deaktiviert ist, ist die manuelle LAN-IPv6-Adressierung aktiviert.

- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)

- **Präfixlänge**: IPv6-Präfixlänge. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**:
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

PPTP (IPv4)

Wählen Sie diese Option aus, wenn dies für den ISP erforderlich ist. PPTP (Point-to-Point Tunneling Protocol) ist ein in Europa und Israel verwendeter Dienst.

- **WAN-IP-Adresse angeben**: Die IP-Adresse, die der ISP Ihrem Konto zugewiesen hat
- **Subnetzmaske (IPv4)**: Dem Konto zugewiesene Subnetzmaske
- **Standardgatewayadresse**: IP-Adresse des Standardgateways
- **Benutzername** und **Kennwort**: Benutzername und Kennwort für das ISP-Konto. Es sind maximal 60 Zeichen zulässig.
- **Verbindungstimer**: Nach einer bestimmten Dauer der Inaktivität wird die Verbindung getrennt.
  - **Verbindung bei Bedarf**: Wenn diese Funktion aktiviert ist, wird die Verbindung vom Gerät automatisch hergestellt. Wenn Sie diese Funktion aktiviert haben, geben Sie in **Max. Leerlaufzeit** ein, nach wie vielen Minuten der Inaktivität die Verbindung getrennt wird. Der Standardwert für die maximale Leerlaufzeit beträgt **5 Minuten**.
  - **Keep-Alive**: Stellt sicher, dass der Router immer mit dem Internet verbunden ist. Wenn diese Funktion ausgewählt ist, hält der Router die Verbindung aufrecht, indem er in regelmäßigen Abständen einige Datenpakete sendet. Mit dieser Option bleibt die Verbindung auch dann

unbegrenzt aktiv, wenn sich die Leitung längere Zeit im Leerlauf befindet. Wenn Sie diese Funktion aktivieren, geben Sie auch unter **Zeit bis Neueinwahl** an, wie oft der Router die Internetverbindung überprüft. Der Standardwert lautet **30 Sekunden**.

- **MTU**: Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**). Wählen Sie **Automatisch** aus, wenn die Größe automatisch festgelegt werden soll. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

Transparente Bridge (IPv4)

Wählen Sie diese Option aus, wenn Sie den Router verwenden, um zwei Netzwerksegmente zu verbinden. Sie können nur jeweils eine WAN-Schnittstelle als transparente Bridge festlegen.

- **WAN-IP-Adresse angeben**: Externe IP-Adresse, die der ISP Ihrem Konto zugewiesen hat
- **Subnetzmaske**: Vom ISP vorgegebene Subnetzmaske
- **Standardgatewayadresse**: IP-Adresse des Standardgateways
- **DNS-Server 1** und **DNS-Server 2**: IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **Interner LAN-IP-Bereich**: Überbrückter interner LAN-IP-Bereich. Das WAN und das LAN der transparenten Bridge müssen sich im gleichen Subnetz befinden.
- **MTU**: Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**). Wählen Sie **Automatisch** aus, wenn die Größe automatisch festgelegt werden soll. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

Automatische Konfigurierung der statusfreien Adresse (IPv6)

Wählen Sie diese Option aus, wenn der ISP IPv6-Routeranfragen und -Routerankündigungen verwendet. Hosts im Netzwerk lernen, mit welchem Netzwerk sie verbunden sind, und können dann automatisch eine Host-ID im jeweiligen Netzwerk konfigurieren.

Zum Angeben eines DNS-Servers geben Sie die IP-Adresse von **DNS-Server 1** ein. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.

Wenn die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**) automatisch festgelegt werden soll, wählen Sie **Automatisch** aus. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

So konfigurieren Sie die IPv6-Parameter:

- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge: Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**:
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

IPv6 in IPv4-Tunnel (IPv6)

Wählen Sie diese Option aus, wenn der ISP zum Herstellen von Internetverbindungen IPv6 in IPv4-Tunnel verwendet.

Sie müssen eine **Statische IP-Adresse**-Adresse für IPv4 eingeben. Geben Sie dann die vom ISP vorgegebenen Einstellungen ein:

- **Lokale IPv6-Adresse**: Lokale IPv6-Adresse für das ISP-Konto
- **Remote IPv4 Address** (Remote-IPv4-Adresse): Remote-IPv4-Adresse für das ISP-Konto
- **Remote IPv6 Address** (Remote-IPv6-Adresse): Remote-IPv6-Adresse für das ISP-Konto
- **DNS-Server 1** und **DNS-Server 2**: IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge: Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

6to4-Tunnel (IPv6)

Wählen Sie diese Option aus, um zwischen zwei unabhängigen IPv6-Netzwerken einen automatischen Tunnel in einem IPv4-Netzwerk (oder eine echte IPv4-Internetverbindung) einzurichten. Geben Sie die folgenden Parameter ein:

Relay IPv4 Address (Relais-IPv4-Adresse): Ermöglicht einem 6to4-Host die Kommunikation mit dem nativen IPv6-Internet. Dafür muss ein IPv6-Standardgateway auf eine 6to4-Adresse festgelegt sein, in der die IPv4-Adresse eines 6to4-Relais-Routers enthalten ist. Damit die Benutzer dies nicht manuell einrichten müssen, ist die Anycast-Adresse `192.88.99.1` für das Senden von Paketen an einen 6to4-Relais-Router reserviert.

- **DNS-Server 1** und **DNS-Server 2**: IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

IPv6 Rapid Deployment-Tunnel (6rd-Tunnel)

Wählen Sie diese Option aus, wenn der ISP zum Herstellen von Internetverbindungen 6rd-Tunnel (IPv6 Rapid Deployment) verwendet. Geben Sie die vom ISP vorgegebenen Einstellungen ein.

- **6rd-Konfigurationsmodus**:
  - **Manuell**: Legen Sie das 6rd-Präfix, die Relais-IPv4-Adresse und die IPv4-Maskenlänge gemäß den Vorgaben des ISPs manuell fest.
  - **Automatisch (DHCP)**: Das 6rd-Präfix, die Relais-IPv4-Adresse und die IPv4-Maskenlänge werden über DHCP (Option 212) bezogen.
- **6rd-Präfix**: 6rd-Präfix für das ISP-Konto
- **Relay IPv4 Address** (Relais-IPv4-Adresse): Relais-IPv4-Adresse für das ISP-Konto
- **IPv4-Maskenlänge**: 6rd-IPv4-Subnetzmaskenlänge für das ISP-Konto. (Normalerweise lautet dieser Wert **0**.)
- **DNS-Server 1** und **DNS-Server 2**: IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **LAN-IPv6-Adresse**: Globales IPv6-Präfix, das gegebenenfalls vom ISP für die LAN-Geräte zugewiesen wurde. (Weitere Informationen erhalten Sie von Ihrem ISP.)
- **Präfixlänge**: IPv6-Präfixlänge. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Netzwerk haben identische erste Bits für ihre IPv6-Adresse. Geben Sie die Anzahl der ersten Bits in den Netzwerkadressen ein. Der Standardwert für die Präfixlänge lautet **64**.
- **LAN-Präfixzuweisung**
  - **Ohne Aktion**: Es werden keine statusfreien oder statusbehafteten IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA konfigurieren**: Es werden *statusfreie* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für DHCPv6 konfigurieren**: Es werden *statusbehaftete* IPv6-Adressen für PCs im LAN bereitgestellt.
  - **Automatisch für RA und DHCPv6 konfigurieren**: Es werden statusfreie und statusbehaftete IPv6-Adressen für PCs im LAN bereitgestellt.

Anschlusseinstellungen für USB1 oder USB2

Mit der USB-Anschlusskonfiguration verwalten Sie die Verbindung zwischen dem Gerät und dem USB-Modem. Außerdem verwalten Sie damit die redundante Ausfallsicherung für den WAN-Anschluss. Bei manchen USB-Dongles werden die Anmeldeinformationen automatisch konfiguriert. Andere, beispielsweise das Verizon UML290VW 4G-Dongle, müssen Sie manuell konfigurieren. Weitere Informationen finden Sie in der Dokumentation des Dongle-Herstellers.

3G/4G-Verbindung

Zum Herstellen einer 3G- oder 4G-Verbindung geben Sie Folgendes ein:

- **PIN-Code** und **PIN-Code bestätigen**: PIN-Code für die SIM-Karte. Dieses Feld wird nur für GSM-SIM-Karten angezeigt.
- **Name des Access Points**: Internetnetzwerk, mit dem das mobile Gerät eine Verbindung herstellt. Geben Sie den Namen des Access Points ein, den Sie vom Dienstanbieter für das mobile Netzwerk erhalten haben. Wenn Sie den Namen des Access Points nicht kennen, wenden Sie sich an den Dienstanbieter.
- **Einwählnummer**: Nummer, die Sie vom Dienstanbieter für das mobile Netzwerk für die Internetverbindung erhalten haben
- **Benutzername** und **Kennwort**: Benutzername und Kennwort, die Sie vom Dienstanbieter für das mobile Netzwerk erhalten haben
- **DNS aktivieren**: Aktivieren Sie das Kontrollkästchen, um DNS zu aktivieren.
- **DNS Server (Required)** (DNS-Server (erforderlich)) und **DNS Server (Optional)** (DNS-Server (optional): IP-Adressen der DNS-Server. Optional können Sie einen zweiten DNS-Server eingeben. Der erste verfügbare DNS-Server wird verwendet.
- **MTU**: Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, **MTU**). Wählen Sie **Automatisch** aus, wenn die Größe automatisch festgelegt werden soll. Wenn Sie alternativ die **MTU**-Größe manuell festlegen möchten, wählen Sie **Manuell** aus, und geben Sie die MTU-Größe ein. (Dabei handelt es sich um die Größe der größten Protokoll-Dateneinheit, die von der Schicht übergeben werden kann, in Byte.)

Einrichten von Failover und Wiederherstellung

Obwohl sowohl eine Ethernet- als auch eine mobile Netzwerkverbindung verfügbar sein können, kann immer nur eine Verbindung zum Aufbau einer WAN-Verbindung verwendet werden. Immer wenn eine WAN-Verbindung getrennt wird, versucht das Gerät, eine andere Verbindung an einer anderen Schnittstelle herzustellen. Diese Funktion wird als *Failover oder Ausfallsicherheit* bezeichnet. Wenn die primäre WAN-Verbindung wiederhergestellt ist, wird wieder diese Verbindung verwendet und die Sicherungsverbindung verworfen. Diese Funktionalität wird *Wiederherstellung* genannt.

SCHRITT 1 Zum Anzeigen des Fensters **Failover & Recovery** (Failover und Wiederherstellung) klicken Sie auf **Einrichten** > **Netzwerk**.

SCHRITT 2 Wählen Sie einen USB-Anschluss aus, und klicken Sie auf **Bearbeiten**. Das Fenster **Netzwerk** wird angezeigt.

SCHRITT 3 Klicken Sie auf die Registerkarte **USB Failover** (USB-Failover), und geben Sie Folgendes ein:

- **Betriebsmodus**: Wenn eine Ethernet-WAN-Verbindung getrennt wird, versucht das Gerät, die mobile Netzwerkverbindung an der USB-Schnittstelle zu aktivieren. Konfigurieren Sie das Failover-Verhalten:
  - **3G/4G-Failover (Hot-Standby)**: Wenn die Verbindung an einem Ethernet-WAN-Anschluss getrennt wird, wird der WAN-Verkehr über die 3G/4G-USB-Verbindung weitergeleitet. Das USB-Modem ist eingeschaltet und befindet sich im Standbymodus.
  - **3G/4G-Failover (Cold-Standby)**: Wenn die Verbindung an einem Ethernet-WAN-Anschluss getrennt wird, wird der WAN-Verkehr über die 3G/4G-USB-Verbindung weitergeleitet. Das USB-Modem ist im Standbymodus nicht aktiv.
  - **Primärmodus**: Die 3G/4G-Verbindung wird als primäre WAN-Verbindung verwendet.
- **Signalqualität**: Gibt die Signalstärke zwischen dem 3G/4G-USB-Dongle und dem Access Point an. Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren.

SCHRITT 4 Wählen Sie einen **Gebührenzähler** aus, um zu große Datenmengen zu vermeiden. Mit **Verkehr (KB)** wird die über die USB-Verbindung gesendete oder empfangene Datenmenge in Kilobyte verfolgt. Mit **Zeit (Minuten)** wird gezählt, wie viele Minuten lang die 3G/4G-Verbindung aktiv ist.

- Wenn Sie **Verkehr (KB)** auswählen, geben Sie Folgendes ein:
  - **Kosten**: Kosten in Dollar für eine bestimmte Datenmenge
  - **Zusatzgebühr**: Kosten für Daten in Dollar pro Kilobyte bei Überschreitung einer bestimmten Menge
  - **Verbindung beenden**: Aktivieren Sie diese Option, damit die Verbindung getrennt wird, wenn die vorgegebene Menge überschritten ist.
- Wenn Sie **Zeit (Minuten)** auswählen, geben Sie Folgendes ein:
  - **Kosten**: Kosten in Dollar für eine bestimmte Zeitdauer
  - **Zusatzgebühr**: Kosten in Dollar bei Überschreitung einer bestimmten Zeitdauer
  - **Verbindung beenden**: Aktivieren Sie diese Option, damit die Verbindung getrennt wird, wenn die vorgegebene Zeitdauer überschritten ist.

Das folgende Fenster wird angezeigt:

- **Vorherige Zeit (zusammengefasst)**: Gibt an, wie lange die 3G/4G-Verbindung seit dem Zurücksetzen aktiv war.
- **Aktuelle Zeit (zusammengefasst)**: Gibt an, wie viel Zeit verstrichen ist, seit die 3G/4G-Verbindung vom Gerät aktiviert wurde.
- **Gebühr**: Geschätzte Kosten für die Verbindung seit dem Zurücksetzen der Zähler

SCHRITT 5 Legen Sie das Verhalten für die **Diagnose** fest:

- **Zähler an Tag**: Aktivieren Sie das Kontrollkästchen, und geben Sie einen Tag im Monat ein, um das Zurücksetzen der Zähler an diesem Tag zu aktivieren. Wenn der Wert größer als die Anzahl der Tage des Monats ist (beispielsweise **31** für einen Monat mit 30 Tagen), werden die Zähler am letzten Tag des Monats neu gestartet.
- **Selbsttest täglich um**: Aktivieren Sie das Kontrollkästchen, und geben Sie die Uhrzeit (im 24-Stunden-Format) ein, zu der die Verbindung getestet werden soll. Ein Selbsttest gilt als erfolgreich, wenn das Gerät eine IP-Adresse vom Dienstanbieter beziehen kann. Fehler werden an das Protokoll gesendet.

- **Selbsttest protokollieren**: Aktivieren Sie das Kontrollkästchen, damit alle Selbsttestaktivitäten protokolliert werden. (Alle Testergebnisse werden an das Protokoll gesendet.)

SCHRITT 6 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

DMZ aktivieren

Bei einer DMZ handelt es sich um ein Subnetz, das öffentlich verfügbar ist, sich aber hinter der Firewall befindet. Mithilfe einer DMZ können Sie an die IP-Adresse des WAN-Anschlusses gerichtete Pakete an eine bestimmte IP-Adresse im LAN umleiten. Sie können Firewallregeln konfigurieren, um den Zugriff auf bestimmte Services und Ports in der DMZ über das LAN oder das WAN zuzulassen. Im Fall eines Angriffs auf einen der DMZ-Knoten ist das LAN nicht zwangsläufig ebenfalls verwundbar. Es wird empfohlen, Hosts, die für das WAN verfügbar gemacht werden müssen (beispielsweise Webserver oder E-Mail-Server), im DMZ-Netzwerk zu platzieren.

So konfigurieren Sie die DMZ:

SCHRITT 1 Wählen Sie **Einrichten** > **Netzwerk** aus, und aktivieren Sie das Kontrollkästchen **DMZ aktivieren**. Daraufhin wird eine Meldung angezeigt.

SCHRITT 2 Klicken Sie auf **Ja**, um die Änderung zu akzeptieren.

SCHRITT 3 Wählen Sie die DMZ-Schnittstelle in der Tabelle **DMZ-Einstellungen** aus, und klicken Sie auf **Bearbeiten**. Das Fenster **DMZ-Verbindung bearbeiten** wird angezeigt.

SCHRITT 4 Wählen Sie **Subnetz** aus, um ein Subnetz für DMZ-Services zu identifizieren, und geben Sie die **DMZ-IP-Adresse** und die **Subnetzmaske** ein. Wählen Sie alternativ **Bereich** aus, um eine Gruppe von IP-Adressen im gleichen Subnetz für DMZ-Services zu reservieren, und geben Sie den IP-Adressbereich ein.

SCHRITT 5 Klicken Sie auf **Speichern**.

Kennwort

Über den Benutzernamen und das Kennwort erhalten Sie Administratorzugriff auf das Gerät. Der Standardbenutzername lautet **cisco**. Das Standardkennwort lautet **cisco**. Sie können den Benutzernamen und das Kennwort ändern. Es wird dringend empfohlen, das Standardkennwort in ein starkes Kennwort zu ändern.

Wenn auf der Seite **Allgemein** (Firewall) die Remoteverwaltung aktiviert ist, *müssen* Sie das Kennwort ändern.

VORSICHT Wenn Sie das Kennwort verlieren oder vergessen, können Sie es nicht wiederherstellen. Wenn Sie das Kennwort verlieren oder vergessen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Dabei gehen alle Konfigurationsänderungen verloren. Wenn Sie remote auf das Gerät zugreifen und das Gerät auf die Werkseinstellungen zurücksetzen, können Sie sich erst wieder beim Gerät anmelden, wenn Sie eine lokale, drahtgebundene Verbindung im gleichen Subnetz hergestellt haben.

Nach dem Ändern des Benutzernamens oder Kennworts werden Sie abgemeldet. Melden Sie sich beim Gerät mit Ihren neuen Anmeldeinformationen an.

So ändern Sie den Benutzernamen oder das Kennwort:

SCHRITT 1 Wählen Sie **Einrichten** > **Kennwort**.

SCHRITT 2 Geben Sie in das Feld **Benutzername** den neuen Benutzernamen ein. Wenn Sie den aktuellen Benutzernamen beibehalten möchten, lassen Sie das Feld leer.

SCHRITT 3 Geben Sie in das Feld **Altes Kennwort** das aktuelle Kennwort ein. Dies ist erforderlich, wenn Sie den Benutzernamen ändern, aber das aktuelle Kennwort beibehalten.

HINWEIS Wenn Sie den Benutzernamen ändern und das aktuelle Kennwort beibehalten, lassen Sie die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** leer.

SCHRITT 4 Geben Sie in das Feld **Neues Kennwort** das neue Kennwort für das Gerät ein. Verwenden Sie eine Kombination aus alphanumerischen Zeichen und Symbolen. Das Kennwort darf keine Leerzeichen enthalten. Geben Sie in das Feld **Neues Kennwort bestätigen** erneut das neue Kennwort ein. Achten Sie darauf, dass die beiden Kennwörter übereinstimmen.

SCHRITT 5 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Kennwortkomplexitätseinstellung zu aktivieren.

So konfigurieren Sie die Einstellungen für Kennwortkomplexität:

SCHRITT 1 Aktivieren Sie im Feld **Einstellungen für Kennwortkomplexität** das Kontrollkästchen **Aktivieren**.

SCHRITT 2 Konfigurieren Sie die Einstellungen in den folgenden Feldern:

Kennwortmindestlänge	Geben Sie die Kennwortmindestlänge ein (0 - 64 Zeichen). Die Mindestlänge beträgt standardmäßig 8 Zeichen.
Mindestanzahl an Zeichenklassen	Geben Sie an, wie viele Klassen das Kennwort beinhalten muss. Das Kennwort muss standardmäßig Zeichen aus mindestens drei dieser Klassen enthalten: ▪ Großbuchstaben ▪ Kleinbuchstaben ▪ Ziffern ▪ Auf einer Standardtastatur verfügbare Sonderzeichen
Das neue Kennwort darf nicht mit dem aktuellen identisch sein	Aktivieren Sie das Kontrollkästchen **Aktivieren**, wenn das neue Kennwort sich von dem aktuellen Kennwort unterscheiden muss.
Kennwortfälligkeit	Die **Sicherheitsmessung** zeigt die Sicherheit des Kennworts basierend auf den Komplexitätsregeln. Die Skala reicht von Rot (nicht akzeptabel) über Gelb (akzeptabel) bis zu Grün (stark).
Kennwortfälligkeitszeit	Geben Sie ein, nach wie vielen Tagen das Kennwort abläuft (1 – 365). Die Fälligkeitszeit beträgt standardmäßig 180 Tage.

SCHRITT 3 Geben Sie in das Feld **Sitzungszeitüberschreitung** ein, nach wie vielen Minuten die Sitzung abläuft. Speichern Sie Ihre Änderungen

SCHRITT 4 Klicken Sie auf **Speichern**.

Uhrzeit

Die Uhrzeit spielt für Netzwerkgeräte eine wichtige Rolle, damit Systemprotokolle und Fehlermeldungen mit dem richtigen Zeitstempel versehen werden und Datenübertragungen mit anderen Netzwerkgeräten synchronisiert werden.

Sie können die Zeitzone konfigurieren, ob die Zeit an die Sommerzeit angepasst werden soll und mit welchem NTP-Server (Network Time Protocol) Datum und Uhrzeit synchronisiert werden sollen. Der Router erhält dann die Datums- und Uhrzeitinformationen vom NTP-Server.

Zum Konfigurieren von NTP und Zeiteinstellungen wählen Sie **Einrichten** > **Uhrzeit** aus.

- **Zeitzone**: Zur Greenwich Mean Time (GMT) relative Zeitzone
- **Sommerzeit**: Aktivieren oder deaktivieren Sie die Anpassung für die Sommerzeit. Geben Sie im Feld **Von** das Anfangsdatum und im Feld **Bis** das Enddatum ein.
- Mit **Datum und Uhrzeit festlegen – Automatisch** aktivieren Sie den NTP-Server. Wenn Sie **Automatisch** ausgewählt haben, geben Sie den vollständigen Namen oder die IP-Adresse für den **NTP-Server** ein. Mit **Manuell** können Sie Datum und Uhrzeit lokal festlegen. Die Zeit wird durch die Uhr des Geräts geregelt. Wenn Sie **Manuell** ausgewählt haben, geben Sie **Datum und Uhrzeit** ein.

DMZ-Host

Mit der Option **DMZ-Host** können Sie einen Host im LAN im Internet sichtbar machen, damit Services wie Internetspiele oder Videokonferenzen verwendet werden können. Den Zugriff auf den DMZ-Host über das Internet können Sie mit Firewallzugriffsregeln einschränken.

Zum Konfigurieren eines DMZ-Hosts geben Sie eine **Private DMZ-IP-Adresse** ein, und klicken Sie auf **Speichern**.

(Port)weiterleitung

Mit der Portweiterleitung können Sie den öffentlichen Zugriff auf Services von Netzwerkgeräten im LAN zulassen, indem Sie einen bestimmten Port oder Portbereich für einen Service wie beispielsweise FTP öffnen. Durch die Portauslösung wird ein Portbereich für Services wie Internetspiele geöffnet, bei denen für die Kommunikation zwischen dem Server und dem LAN-Host alternative Ports verwendet werden.

Konfigurieren von Forwarding

Wenn Benutzer Services im Netzwerk anfordern, leitet das Gerät diese Anfragen auf der Grundlage der Parameter für die Portweiterleitung an Ihre Server weiter. Nicht angegebenen Services wird der Zugriff verweigert. Wenn beispielsweise die Portnummer 80 (HTTP) an die IP-Adresse 192.168.1.2 weitergeleitet wird, werden alle HTTP-Anfragen an der Schnittstelle an 192.168.1.2 weitergeleitet. Der gesamte sonstige Verkehr wird verweigert, sofern er nicht durch einen anderen Eintrag ausdrücklich zugelassen wird.

Mit dieser Funktion können Sie einen Webserver oder FTP-Server einrichten. Achten Sie darauf, eine gültige IP-Adresse einzugeben. (Wenn Sie einen Internetserver ausführen möchten, müssen Sie möglicherweise eine statische IP-Adresse verwenden.) Die Sicherheit wird dadurch erhöht, dass externe Benutzer zwar mit dem Server kommunizieren, aber keine Verbindungen mit Netzwerkgeräten herstellen können.

So können Sie in der Tabelle einen Service hinzufügen oder bearbeiten:

SCHRITT 1 Zum Hinzufügen eines Services klicken Sie in der **Tabelle für Portbereichsweiterleitungsregeln** auf **Hinzufügen**.

Zum Bearbeiten eines Services wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.

Die Felder werden geöffnet und können bearbeitet werden.

SCHRITT 2 Konfigurieren Sie Folgendes:

- Wählen Sie im Dropdown-Menü **Service** einen Service aus. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste gemäß den Anweisungen im Abschnitt **Hinzufügen oder Bearbeiten eines Servicenamens** ändern.)
- Geben Sie die **IP-Adresse** des Servers ein.
- Wählen Sie die **Schnittstelle** aus.

- Wählen Sie den **Status** aus. Aktivieren Sie das Kontrollkästchen, um den Service zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um den Service zu deaktivieren.

SCHRITT 3 Klicken Sie auf **Speichern**.

Hinzufügen oder Bearbeiten eines Servicenamens

So können der Serviceliste einen Eintrag hinzufügen oder einen bestehenden Eintrag bearbeiten:

SCHRITT 1 Klicken Sie auf **Serviceverwaltung**. Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 2 Zum Hinzufügen eines Services klicken Sie in der **Serviceverwaltungstabelle** auf **Hinzufügen**.

Zum Bearbeiten eines Services wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**.

Die Felder werden geöffnet und können bearbeitet werden. Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 3 Die Liste kann max. 30 Services enthalten:

- **Servicename**: Kurze Beschreibung
- **Protokoll**: Benötigtes Protokoll. Weitere Informationen finden Sie in der Dokumentation für den zu hostenden Service.
- **Portbereich**: Bereich der für diesen Service reservierten Portnummern

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der Port-Auslösung

Mithilfe der Port-Auslösung kann das Gerät ausgehende Daten für bestimmte Portnummern überwachen. Die IP-Adresse des Clients, der die entsprechenden Daten gesendet hat, wird im Gerät gespeichert. Wenn die angeforderten Daten durch das Gerät zurückgegeben werden, werden sie mithilfe von IP-Adressierung und Portzuordnungsregeln an den richtigen Client gesendet.

Manche Internetanwendungen oder Spiele verwenden für die Kommunikation zwischen dem Server und dem LAN-Host atypische Ports. Geben Sie den auslösenden (ausgehenden) Port und den alternativen eingehenden Port in der **Tabelle für Portauslösungsstatus** ein, um diese Anwendungen zu verwenden.

So können Sie in der Tabelle einen Anwendungsnamen hinzufügen oder bearbeiten:

SCHRITT 1 Klicken Sie auf **Einrichten** > **Weiterleitung**.

SCHRITT 2 Zum Hinzufügen eines Anwendungsnamens klicken Sie in der **Tabelle für Portbereichsweiterleitungsregeln** auf **Hinzufügen**.

Zum Bearbeiten eines Anwendungsnamens wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Felder werden geöffnet und können bearbeitet werden.

Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 3 Konfigurieren Sie Folgendes:

- **Anwendungsname**: Name der Anwendung
- **Auslöser-Portbereich**: Erste und letzte Portnummer des Auslöser-Portbereichs. Weitere Informationen finden Sie in der Dokumentation für die Anwendung.
- **Portbreich eingehend**: Erste und letzte Portnummer des eingehenden Portbereichs. Weitere Informationen finden Sie in der Dokumentation für die Anwendung.

SCHRITT 4 Klicken Sie auf **Speichern**.

Löschen eines Tabelleneintrags

Zum Löschen eines Eintrags aus einer Tabelle klicken Sie auf die zu löschenden Einträge und dann auf **Entfernen**.

Port-Adressen-Übersetzung

Port-Adressen-Übersetzung (Port Address Translation, PAT) ist eine Erweiterung des NAT-Verfahrens (Network Address Translation), mit dem mehrere Geräte in einem LAN einer einzigen öffentlichen IP-Adresse zugeordnet werden können, um IP-Adressen zu sparen.

PAT ist mit Port Forwarding vergleichbar, jedoch wird ein eingehendes Paket mit Zielport (einem externen Port) in ein Paket mit einem anderen Zielport (einem internen Port) umgewandelt. Der Internetdienstanbieter (Internet Service Provider, ISP) weist dem Edge-Gerät eine einzige IP-Adresse zu. Wenn ein Computer im Internet angemeldet wird, weist das Gerät dem Client eine Portnummer zu, die der internen IP-Adresse angefügt wird. Dadurch erhält der Computer eine eindeutige IP-Adresse.

Wenn ein anderer Computer im Internet angemeldet wird, weist das Gerät dem Computer die gleiche öffentliche IP-Adresse zu, jedoch eine andere Portnummer. Obwohl beide Computer die gleiche öffentliche IP-Adresse haben, weiß das Gerät, an welchen Computer Pakete gesendet werden sollen, da das Gerät den Paketen anhand der Portnummern die eindeutigen internen IP-Adressen der Computer zuweist.

So können Sie Port-Adressen-Übersetzungen hinzufügen oder bearbeiten:

SCHRITT 1 Zum Hinzufügen eines Services klicken Sie in der Tabelle **Port-Adressen-Übersetzung** auf **Hinzufügen**.

Zum Bearbeiten eines Services wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Felder werden geöffnet und können bearbeitet werden.

Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Service** den Service aus. Es sind max. 30 Services möglich. (Wenn ein Service nicht aufgeführt ist, können Sie die Liste gemäß den Anweisungen im Abschnitt **Hinzufügen oder Bearbeiten eines Servicenamens** ändern.)

SCHRITT 3 Geben Sie die IP-Adresse oder den Namen des Netzwerkgeräts ein, in dem sich der Service befindet.

SCHRITT 4 Klicken Sie auf **Speichern**.

Hinzufügen oder Bearbeiten eines Servicenamens

So können der Serviceliste einen Eintrag hinzufügen oder einen bestehenden Eintrag bearbeiten:

SCHRITT 1 Klicken Sie auf **Serviceverwaltung**. Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 2 Zum Hinzufügen eines Services klicken Sie in der **Serviceverwaltungstabelle** auf **Hinzufügen**.

Zum Bearbeiten eines Services wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Felder werden geöffnet und können bearbeitet werden.

Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

SCHRITT 3 Die Liste kann max. 30 Services enthalten:

- **Servicename**: Kurze Beschreibung
- **Protokoll**: Benötigtes Protokoll. Weitere Informationen finden Sie in der Dokumentation für den zu hostenden Dienst.
- **Externer Port**: Externe Portnummer
- **Interner Port**: Interne Portnummer

SCHRITT 4 Klicken Sie auf **Speichern**.

Einrichten von One-to-One-NAT

One-to-One-NAT stellt eine Relation her, bei der einer gültigen WAN-IP-Adresse eine Menge von LAN-IP-Adressen zugeordnet werden, die durch NAT gegenüber dem WAN (Internet) verborgen werden. Dadurch sind die LAN-Geräte vor Erkennung und Angriffen geschützt.

Die besten Ergebnisse erzielen Sie, wenn Sie IP-Adressen für die internen Ressourcen reservieren, die über One-to-One-NAT erreichbar sein sollen.

Sie können eine einzelne LAN-IP-Adresse oder einen IP-Adressbereich einem externen Bereich aus WAN-IP-Adressen gleicher Länge zuordnen (beispielsweise drei interne Adressen und drei externe Adressen). Die erste interne Adresse wird der ersten externen Adresse zugeordnet, die zweite interne IP-Adresse wird der zweiten externen Adresse zugeordnet usw.

Zum Aktivieren der Funktion aktivieren Sie das Kontrollkästchen **Aktivieren**.

Zum Hinzufügen eines Eintrags zur Liste klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Informationen ein:

- **Anfang privater Bereich**: Erste IP-Adresse des internen IP-Adressbereichs, den Sie dem öffentlichen Bereich zuordnen möchten. Die IP-Adresse für die Routerverwaltung darf in diesem Bereich nicht enthalten sein.
- **Anfang öffentlicher Bereich**: Erste IP-Adresse des vom ISP bereitgestellten öffentlichen IP-Adressbereichs. Die WAN-IP-Adresse des Routers darf in diesem Bereich nicht enthalten sein.
- **Bereichslänge**: Anzahl der IP-Adressen im Bereich. Die Bereichslänge darf die Anzahl der gültigen IP-Adressen nicht überschreiten. Zum Zuordnen einer einzelnen Adresse geben Sie den Wert **1** ein.

Zum Ändern eines Eintrags aktivieren Sie das Kontrollkästchen des zu ändernden Eintrags, und klicken Sie auf **Bearbeiten**. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Klonen von MAC-Adressen

Bei manchen ISPs müssen Sie eine MAC-Adresse registrieren (den eindeutigen 12-stelligen Identifizierungscode, der jedem Netzwerkgerät zugewiesen ist). Wenn Sie bereits eine andere MAC-Adresse für das Gerät beim ISP registriert haben, können Sie diese Funktion auswählen, um die Adresse für das Gerät zu klonen. Anderenfalls müssen Sie den ISP bitten, die registrierte MAC-Adresse zu ändern.

HINWEIS Wenn die Option **MAC-Adressklon** aktiviert ist, kann die Anschlussspiegelung nicht verwendet werden.

So klonen Sie eine MAC-Adresse:

SCHRITT 1 Klicken Sie auf das Optionsfeld **Schnittstelle**.

SCHRITT 2 Klicken Sie auf **Bearbeiten**, um die Seite **MAC-Adressklon bearbeiten** anzuzeigen.

- **Benutzerdefinierte WAN-MAC-Adresse**: Klicken Sie auf das Optionsfeld, und geben Sie die 12 Stellen der beim ISP registrierten MAC-Adresse ein.
- **MAC-Adresse von diesem PC**: Klicken Sie auf diese Schaltfläche, um die MAC-Adresse des Computers als MAC-Adressklon für das Gerät zu verwenden.

SCHRITT 3 Klicken Sie auf **Speichern**.

Dynamischem DNS

Der DDNS-Dienst (Dynamic Domain Name System) weist einer dynamischen WAN-IP-Adresse einen festen Domänennamen zu, sodass Sie einen eigenen Webserver, FTP-Server oder eine andere Art von TCP/IP-Server im LAN hosten können. Wählen Sie diese Funktion aus, um die WAN-Schnittstellen mit den DDNS-Informationen zu konfigurieren.

Bevor Sie dynamisches DNS im Router konfigurieren, sollten Sie www.dyndns.org besuchen und einen Domänennamen registrieren. (Der Dienst wird von DynDNS.org bereitgestellt.) Benutzer in China nehmen die Registrierung unter www.3322.org vor.

Wenn Sie eine Schnittstelle ausgewählt und auf **Bearbeiten** geklickt haben, wird die Seite **Einrichtung des dynamischen DNS bearbeiten** angezeigt.

So bearbeiten Sie den DDNS-Dienst:

SCHRITT 1 Wählen Sie in der Liste **DDNS-Dienst** einen Dienst aus.

SCHRITT 2 Geben Sie die Informationen für das Konto ein:

- **Benutzername**: Benutzername für das DDNS-Konto. Wenn Sie keinen Hostnamen registriert haben, klicken Sie auf **Registrieren**, um zur Website DynDNS.com zu wechseln. Dort können Sie sich für den kostenlosen DDNS-Dienst anmelden.

- **Kennwort**: Kennwort für das DDNS-Konto
- **Hostname**: Hostname, den Sie beim DDNS-Anbieter registriert haben. Wenn der Hostname beispielsweise *MeinHaus.dyndns.org* lautet, geben Sie im ersten Feld *MeinHaus*, im zweiten Feld *dyndns* und im letzten Feld *org* ein.

Die folgenden schreibgeschützten Informationen werden angezeigt:

- **Internet-IP-Adresse**: WAN-IP-Adresse für die Schnittstelle
- **Status**: Status des DDNS Wenn aus den Statusinformationen ein Fehler hervorgeht, vergewissern Sie sich, dass Sie die Informationen für das Konto beim DDNS-Dienst richtig eingegeben haben.

SCHRITT 3 Klicken Sie auf **Speichern**.

Erweitertes Routing

Mit dieser Funktion aktivieren Sie dynamisches Routing und fügen der Routingtabelle für IPv4 und IPv6 statische Routen hinzu.

Zum Anzeigen der Routingtabelle klicken Sie auf **Routingtabelle anzeigen**. Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren. Klicken Sie auf **Schließen**, um das Popup-Fenster zu schließen.

Konfigurieren von dynamischem Routing

Beim dynamischen Routing werden automatisch Routingtabellen erstellt, die auf in den Routing-Protokollen enthaltenen Informationen basieren und es dem Netzwerk ermöglichen, nahezu autonom Netzwerkfehler und Blockierungen zu vermeiden.

Zum Konfigurieren von dynamischem Routing für IPv4 mithilfe des RIP-Protokolls (Routing Information Protocol) klicken Sie auf die Registerkarte **IPv4**.

Zum Konfigurieren von dynamischem Routing für IPv6 mithilfe des RIPng-Protokolls (Routing Information Protocol next generation) klicken Sie auf die Registerkarte **IPv6**.

Konfigurieren von dynamischem Routing für IPv4

SCHRITT 1 Wählen Sie den Arbeitsmodus aus:

- **Gateway**: Wählen Sie diesen Modus aus, wenn die Netzwerkverbindung mit dem Internet von diesem Gerät gehostet wird. Dies ist die Standardeinstellung.
- **Router**: Wählen Sie diesen Modus aus, wenn sich das Gerät in einem Netzwerk mit anderen Routern befindet und ein anderes Gerät als Netzwerk-Gateway zum Internet fungiert oder dieses Netzwerk nicht mit dem Internet verbunden ist. Im Routermodus ist die Internetkonnektivität nur dann für die Netzwerkgeräte verfügbar, wenn ein weiterer Router als Gateway fungiert. Da der Firewallschutz vom Gateway bereitgestellt wird, deaktivieren Sie die Firewall dieses Geräts.

SCHRITT 2 Aktivieren Sie **RIP**, damit das Gerät seine Routinginformationen automatisch mit anderen Routern austauscht und die Routingtabellen bei Netzwerkänderungen dynamisch angepasst werden. Die Standardeinstellung lautet **Deaktiviert**. Wenn Sie diese Funktion aktivieren, konfigurieren Sie auch die folgenden Einstellungen:

- **RIP-Versionen empfangen**: Wählen Sie das RIP-Protokoll für den Empfang von Netzwerkdaten aus: **Ohne**, **RIPv1**, **RIPv2** oder **RIPv1 und v2**.

  RIPv1 ist eine klassenbasierte Routingversion. Diese Version enthält keine Subnetzinformationen und unterstützt daher keine Subnetzmasken variabler Länge (Variable Length Subnet Mask, VLSM). RIPv1 enthält außerdem keine Unterstützung für Routerauthentifizierung und ist damit anfällig für Angriffe. **RIPv2** enthält eine Subnetzmaske und unterstützt Sicherheit durch Kennwortauthentifizierung.
- **RIP-Versionen übertragen**: Wählen Sie das RIP-Protokoll für das Senden von Netzwerkdaten aus: **Ohne**, **RIPv1**, **RIPv2 – Broadcast** oder **RIPv2 – Multicast**.

  Mit **RIPv2 – Broadcast** (empfohlen) werden Daten im gesamten Subnetz gesendet. Mit **RIPv2 – Multicast** werden Daten an Multicast-Adressen gesendet. Mit **RIPv2 - Multicast** können Sie darüber hinaus unnötige Lasten vermeiden, indem Routingtabellen per Multicast an benachbarte Router und nicht an das gesamte Netzwerk gesendet werden.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von dynamischem Routing für IPv6

Die Registerkarte **IPv6** ist nur verfügbar, wenn Sie auf der Seite **Einrichten** > **Netzwerk** die Option **Dual-Stack-IP** aktiviert haben.

Zum Aktivieren von RIPng aktivieren Sie das Kontrollkästchen **RIPng**.

Konfigurieren von statischem Routing

Sie können statisches Routing für IPv4 oder IPv6 konfigurieren. Diese Routen werden nicht aus der Routingtabelle entfernt, wenn sie veralten. Sie können max. 30 Routen eingeben.

Zum Konfigurieren einer statischen Route klicken Sie auf **Hinzufügen**, oder wählen Sie einen Eintrag aus, und klicken Sie auf **Bearbeiten**:

- **Ziel-IP**: Subnetzadresse des Remote-LAN-Segments. Bei einer IP-Domäne der Klasse C entspricht die Netzwerkadresse den ersten drei Feldern der Ziel-LAN-IP; das letzte Feld sollte **0** lauten.
- **Subnetzmaske** (nur IPv4): In der Ziel-LAN-IP-Domäne verwendete Subnetzmaske. Für IP-Domänen der Klasse C lautet die Subnetzmaske normalerweise **255.255.255.0**.
- **Präfixlänge (Nur IPv6)**: IPv6-Präfixlänge
- **Standardgateway**: IP-Adresse des als letzter Ausweg vorgesehenen Routers
- **Hop-Zählung**: Maximale Anzahl der Knoten oder Hops (maximal 15 Hops), die ein Paket durchläuft, bevor es verworfen wird. Ein Knoten ist ein beliebiges Gerät im Netzwerk, beispielsweise ein Switch oder Router.
- **Schnittstelle**: Schnittstelle, die für diese Route verwendet werden soll

Zum Löschen eines Eintrags aus der Liste klicken Sie auf den zu löschenden Eintrag und dann auf **Entfernen**.

Zum Anzeigen der aktuellen Daten klicken Sie auf **Routingtabelle anzeigen**. Die Liste für Routing-Tabelleneinträge wird angezeigt. Sie können auf **Aktualisieren** klicken, um die Daten zu aktualisieren, oder auf **Schließen**, um das Popup-Fenster zu schließen.

Lastenausgleich eingehend

Beim eingehenden Lastenausgleich wird der eingehende Verkehr gleichmäßig auf alle WAN-Anschlüsse verteilt, um die Bandbreite optimal zu nutzen. Außerdem können Sie eine ungleichmäßige Verteilung des Verkehrs und eine Überlastung des Netzwerks verhindern.

So aktivieren und konfigurieren Sie den eingehenden Lastenausgleich:

SCHRITT 1 Klicken Sie auf **"Lastenausgleich eingehend" aktivieren**.

SCHRITT 2 Geben Sie die Informationen für **Domänenname** ein:

- **Domänenname**: Vom DNS-Dienstanbieter zugewiesener Domänenname
- **TTL** (Time-to-Live): Zeitintervall für DNS-Anfragen (Sekunden, 0 - 65535). Ein langes Intervall wirkt sich auf die Dauer der Aktualisierung aus. Ein kürzeres Intervall erhöht die Systemlast, verbessert jedoch die Genauigkeit des eingehenden Lastenausgleichs. Sie können diesen Parameter anpassen, um die Leistung für das Netzwerk zu optimieren.
- **Administrator**: E-Mail-Adresse des Administrators

SCHRITT 3 Geben Sie die Parameter für den **DNS-Server** ein:

- **Nameserver**: DNS-Server, der den Domänennamen umwandelt
- **Schnittstelle**: Dem Nameserver entsprechende WAN-Schnittstelle. Das System zeigt die bezogenen aktivierten WAN-IP-Adressen an.

SCHRITT 4 Geben Sie im Feld **Host** (Datensatz) **Name** den Hostnamen ein, der Services bereitstellt, beispielsweise der Mailserver oder FTP-Server, und wählen Sie die **WAN-IP**-Schnittstelle aus, an die der eingehende Verkehr verteilt wird.

SCHRITT 5 Geben Sie den **Alias**, der einem möglicherweise Services bereitstellenden Computer mehrere Namen zuweist, und das **Ziel**, einen vorhandenen A-Eintrag-Domänennamen, ein.

SCHRITT 6 Klicken Sie auf **SPF-Einstellungen**, um SPF-Text hinzuzufügen. SPF (Sender Policy Framework) ist ein E-Mail-Überprüfungssystem, das E-Mail-Spam verhindert, indem E-Mail-Spoofing (eine allgemeine Schwachstelle) durch Überprüfung der IP-Adressen von Absendern erkannt wird. (Sie müssen dieses Feld nicht konfigurieren. Weitere Informationen finden Sie unter http://www.openspf.org/Tools#wizard?mydomain=&x=35&y=6.)

SCHRITT 7 Geben Sie die Parameter für den **Mailserver** ein:

- **Hostname**: Name des Mailhosts (ohne den Domänennamen)
- **Gewichtung**: Reihenfolge der Mail-Hosts. Die niedrigere Zahl hat die höchste Priorität.
- **Mailserver**: Name des im A-Eintrag gespeicherten Servers oder der Name eines externen Mailservers

SCHRITT 8 Klicken Sie auf **Speichern**.

USB-Geräteaktualisierung

Sie können mit diesem Netzwerk-Gerät die Firmware von USB-Geräten aktualisieren.

Zum Aktualisieren eines an einen USB-Anschluss angeschlossenen USB-Geräts suchen Sie die Datei, die Sie von einem PC in das USB-Gerät hochladen möchten, und klicken Sie auf **Upgrade**.

6

DHCP

DHCP (Dynamic Host Configuration Protocol) ist ein Netzwerkprotokoll, mit dem Sie Netzwerkgeräte für die Kommunikation in einem IP-Netzwerk konfigurieren können. Ein DHCP-Client verwendet das DHCP-Protokoll, um Konfigurationsinformationen wie beispielsweise eine IP-Adresse, eine Standardroute und mindestens einen DNS-Server von einem DHCP-Server zu beziehen. Anschließend konfiguriert der DHCP-Client mithilfe dieser Informationen seinen Host. Nach Abschluss des Konfigurationsprozesses kann der Host über das Internet kommunizieren.

Auf dem DHCP-Server wird eine Datenbank mit verfügbaren IP-Adressen und Konfigurationsinformationen verwaltet. Wenn der DHCP-Server eine Anfrage von einem Client empfängt, ermittelt er das Netzwerk, mit dem der DHCP-Client verbunden ist, und weist dem Client eine geeignete IP-Adresse oder ein geeignetes Präfix zu und sendet für den Client geeignete Konfigurationsinformationen.

Der DHCP-Server und der DHCP-Client müssen über die gleiche Netzwerkverbindung verbunden sein. In größeren Netzwerken enthält jede Netzwerkverbindung mindestens einen DHCP-Relais-Agent. Diese DHCP-Relais-Agents empfangen Nachrichten von DHCP-Clients und leiten diese an DHCP-Server weiter. DHCP-Server senden Antworten zurück an den Relay Agent, der diese Antworten an den DHCP-Client in der lokalen Netzwerkverbindung sendet.

DHCP-Server weisen Clients in der Regel IP-Adressen für einen begrenzten Zeitraum zu, der als *Lease* bezeichnet wird. Die DHCP-Clients müssen ihre IP-Adresse vor Ablauf des Intervalls erneuern und dürfen die Adresse nach Ablauf des Intervalls nicht mehr verwenden, wenn die Erneuerung nicht möglich war.

DHCP wird für IPv4 und IPv6 verwendet. Obwohl beide Versionen dem gleichen Zweck dienen, sind die Details des Protokolls für IPv4 und IPv6 so unterschiedlich, dass sie als getrennte Protokolle betrachtet werden können.

DHCP-Einrichtung

Bei der DHCP-Einrichtung wird DHCP für IPv4 oder IPv6 konfiguriert. Außerdem kann bei einigen Geräten die jeweilige Konfiguration von einem TFTP-Server heruntergeladen werden. Wenn ein Gerät ohne vorkonfigurierte IP-Adresse und IP-Adresse des TFTP-Servers gestartet wird, sendet das Gerät eine Anfrage mit den Optionen 66, 67 und 150 an den DHCP-Server, um diese Informationen abzurufen.

Bei der DHCP-Option 150 handelt es sich um eine proprietäre Option von Cisco. Der dieser Anforderung entsprechende IEEE-Standard ist Option 66. Wie Option 150 wird Option 66 verwendet, um den Namen des TFTP-Servers anzugeben. Mit Option 67 wird der Name der Bootdatei bereitgestellt.

Mit Option 82 (Option für Informationen zum DHCP-Relais-Agent) kann ein DHCP-Relais-Agent beim Weiterleiten der von Clients stammenden DHCP-Pakete an einen DHCP-Server eigene Informationen einschließen. Der DHCP-Server kann mithilfe dieser Informationen die IP-Adressierung oder andere Richtlinien für die Parameterzuweisung implementieren.

Zum Einrichten von DHCP für IPv4 klicken Sie auf die Registerkarte **IPv4**. Zum Einrichten von DHCP für IPv6 klicken Sie auf die Registerkarte **IPv6**.

Konfigurieren von DHCP für IPv4

So konfigurieren Sie DHCP für IPv4:

SCHRITT 1 Wählen Sie **VLAN** oder **Option 82** aus.

SCHRITT 2 Wenn Sie **Option 82** ausgewählt haben, fügen Sie mit **DHCP > Option 82** Leitungs-IDs hinzu. Diese Leitungs-IDs werden dann im Dropdown-Menü **Leitungs-ID** aufgeführt.

Wenn Sie **VLAN** ausgewählt haben, wählen Sie im Menü **VLAN-ID** das VLAN aus, und geben Sie Folgendes ein:

- **Geräte-IP-Adresse**: Verwaltungs-IP-Adresse
- **Subnetzmaske**: Verwaltungs-IP-Subnetzmaske

SCHRITT 3 Wählen Sie den **DHCP-Modus** aus:

- **Deaktivieren**: Deaktiviert DHCP für dieses Gerät. Sie müssen keine weiteren Parameter angeben.
- **DHCP-Server**: Übermittelt die DHCP-Anfragen von Clients an den DHCP-Server des Geräts.

- **DHCP-Relais**: Übergibt DHCP-Anfragen und -Antworten von einem anderen DHCP-Server über das Gerät. Wenn Sie **DHCP-Relais** ausgewählt haben, geben Sie die IP-Adresse für den **Remote-DHCP-Server** ein.
- **Client-Lease-Dauer**: Gibt an, wie viele Minuten einem Netzwerkbenutzer zur Verfügung stehen, um eine Verbindung mit dem Router mit der aktuellen IP-Adresse herzustellen. Gültig sind Werte von 5 bis 43200 Minuten. Die Standardeinstellung lautet **1440 Minuten** (entspricht 24 Stunden).
- **Bereichsanfang** und **Bereichsende**: Die erste und letzte IP-Adresse eines IP-Adressbereichs, der dynamisch zugewiesen werden kann. Der Bereich kann aus der maximalen Anzahl von IP-Adressen bestehen, die vom Server ohne Überlappung mit Funktionen wie PPTP und SSL-VPN zugewiesen werden können. Die LAN-IP-Adresse des Geräts darf in diesem dynamischen IP-Bereich nicht enthalten sein. Wenn der Router beispielsweise die vorgegebene LAN-IP-Adresse **192.168.1.1** verwendet, muss der Anfangswert mindestens 192.168.1.2 betragen.
- **DNS-Server**: Der Typ des DNS-Service; gibt an, wo die IP-Adresse des DNS-Servers bezogen wird.
- **Statisches DNS 1** und **Statisches DNS 2**: Statische IP-Adresse eines DNS-Servers. (Optional) Wenn Sie einen zweiten DNS-Server eingeben, verwendet das Gerät zur Beantwortung einer Anfrage den ersten DNS-Server.
- **WINS**: Optionale IP-Adresse eines WINS-Servers (Windows Internet Naming Service), der NetBIOS-Namen in IP-Adressen auflöst. Wenn Sie die IP-Adresse des WINS-Servers nicht kennen, verwenden Sie den Standardwert **0.0.0.0**.

SCHRITT 4 Geben Sie die Parameter für den TFTP-Server ein:

- **TFTP-Serverhostname**: Hostname des TFTP-Servers
- **TFTP-Server-IP**: IP-Adresse des TFTP-Servers
- **Konfigurationsdateiname**: Name der Konfigurationsdatei, die zum Aktualisieren eines Geräts verwendet wird

Konfigurieren von DHCP für IPv6

So konfigurieren Sie DHCP für IPv6:

SCHRITT 1 Geben Sie die **IPv6-Adresse** ein.

SCHRITT 2 Geben Sie die **Präfixlänge** ein.

SCHRITT 3 Wählen Sie den **DHCP-Modus** aus:

- **Deaktivieren**: Deaktiviert DHCP für dieses Gerät. Sie müssen keine weiteren Parameter angeben.
- **DHCP-Server**: Übermittelt die DHCP-Anfragen von Clients an den DHCP-Server des Geräts.
- **DHCP-Relais**: Übergibt DHCP-Anfragen und -Antworten von einem anderen DHCP-Server über das Gerät.
- **Client-Lease-Dauer**: Gibt an, wie viel Zeit einem Netzwerkbenutzer zur Verfügung steht, um eine Verbindung mit dem Router mit der aktuellen IP-Adresse herzustellen. Geben Sie den Zeitraum in Minuten ein. Gültig sind Werte von 5 bis 43200 Minuten. Die Standardeinstellung lautet **1440 Minuten** (entspricht 24 Stunden).
- **DNS-Server 1** und **DNS-Server 2**: (Optional) IP-Adresse eines DNS-Servers. Wenn Sie einen zweiten DNS-Server eingeben, verwendet das Gerät für Antworten den ersten DNS-Server. Durch Angeben eines DNS-Servers können Sie den Zugriff im Vergleich zur Verwendung eines dynamisch zugewiesenen DNS-Servers beschleunigen. Verwenden Sie die Standardeinstellung **0.0.0.0**, um einen dynamisch zugewiesenen DNS-Server zu verwenden.

SCHRITT 4 Geben Sie den IPv6-Adresspool ein:

- **Startadresse**: Erste Adresse des IPv6-Adresspools
- **Endadresse**: Letzte Adresse des IPv6-Adresspools
- **Präfixlänge**: Länge des IPv6-IP-Adresspräfixes

Anzeigen des DHCP-Status

Unter **DHCP-Status** wird der Status des DHCP-Servers und der Clients angezeigt.

Für den DHCP-Server werden die folgenden Informationen angezeigt:

- **DHCP-Server**: IP-Adresse des DHCP-Servers
- **Verwendete dynamische IP-Adresse**: Anzahl der verwendeten dynamischen IP-Adressen
- **Verwendete statische IP-Adresse** (nur IPv4): Anzahl der verwendeten statischen IP-Adressen
- **DHCP verfügbar**: Anzahl der verfügbaren dynamischen IP-Adressen
- **Gesamt**: Gesamtanzahl der vom DHCP-Server verwalteten dynamischen IP-Adressen

In der Clienttabelle werden die folgenden Informationen zum DHCP-Client angezeigt:

- **Client-Hostname**: Der einem Client-Host zugewiesene Name
- **IP-Adresse**: Die einem Client zugewiesene dynamische IP-Adresse
- **MAC-Adresse** (nur IPv4): MAC-Adresse eines Clients
- **Client-Lease-Dauer**: Gibt an, wie lange ein Netzwerkbenutzer über eine dynamische IP-Adresse mit dem Router verbunden sein kann.

Zum Freigeben der IPv4-IP-Adresse eines Clients wählen Sie die Option **Client-Hostname** aus, und klicken Sie auf **Entfernen**.

Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren.

Option 82

Mit Option 82 (Option für Informationen zum DHCP-Relais-Agent) kann ein DHCP-Relais-Agent beim Weiterleiten der von Clients stammenden DHCP-Pakete an einen DHCP-Server eigene Informationen einschließen. Der DHCP-Server kann mithilfe dieser Informationen die IP-Adressierung oder andere Richtlinien für die Parameterzuweisung implementieren.

Die über DHCP-Option 82 konfigurierbare Leitungs-ID erhöht die Überprüfungssicherheit, da Sie bestimmen können, welche Informationen in der Beschreibung der Leitungs-ID für Option 82 bereitgestellt werden.

Zum Hinzufügen einer **Leitungs-ID** klicken Sie auf **Hinzufügen**. Der Tabelle wird eine neue Zeile hinzugefügt, und die Leitungs-IDs werden im Fenster **DHCP-Einrichtung** im Dropdown-Menü **Leitungs-ID** aufgeführt.

Zum Bearbeiten einer **Leitungs-ID** wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**. Die Zeile wird geöffnet und kann geändert werden.

IP- und MAC-Bindung

Wenn das Gerät als DHCP-Server oder als DHCP-Relais konfiguriert ist, können Sie statische IP-Adressen an max. 80 Netzwerkgeräte (beispielsweise Webserver oder FTP-Server) binden. Durch die Bindung wird den Geräten keine IP-Adresse zugewiesen. Stellen Sie sicher, dass jedes Gerät in der IP- und MAC-Bindungstabelle an eine statische IP-Adresse gebunden und für die Verwendung einer statischen IP-Adresse konfiguriert ist.

Normalerweise finden Sie die MAC-Adresse eines Geräts auf einem Aufkleber auf der Unter- oder Rückseite des Geräts.

Binden von IP-Adressen durch Erkennung

So binden Sie bekannte IP-Adressen an MAC-Adressen und legen einen Namen für die Bindung fest:

SCHRITT 1 Klicken Sie auf **Unbekannte MAC-Adressen anzeigen**. Die IP- und MAC-Bindungstabelle wird angezeigt. Wenn im Webbrowser eine Meldung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

Die Geräte werden nach IP-Adresse und MAC-Adresse aufgeführt. Klicken Sie gegebenenfalls auf **Aktualisieren**, um die Daten zu aktualisieren.

SCHRITT 2 Geben Sie in **Name** einen aussagekräftigen Namen ein.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **Aktivieren**. Alternativ können Sie alle Geräte in der Liste auswählen, indem Sie auf das Kontrollkästchen oben in der Spalte **Aktivieren** klicken.

SCHRITT 4 Klicken Sie auf **Speichern**, um die Geräte der Liste **Statische IP-Adresse** hinzuzufügen, oder auf **Schließen**, um das Popup-Fenster ohne Hinzufügen der ausgewählten Geräte zu schließen.

Manuelles Binden von IP-Adressen

Zum Hinzufügen einer neuen Bindung zur Liste klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Informationen ein:

- **Statische IP-Adresse**: Statische IP-Adresse. Wenn der Router dem Gerät eine statische IP-Adresse zuweisen soll, können Sie **0.0.0.0** eingeben.
- **MAC-Adresse**: MAC-Adresse des Geräts. Geben Sie die Adresse ohne Satzzeichen ein.
- **Name**: Aussagekräftiger Name für das Gerät
- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um die statische IP-Adresse an das Gerät zu binden.

Bearbeiten oder Löschen von Bindungseinträgen

Zum **Bearbeiten** der Einstellungen wählen Sie in der Liste einen Eintrag aus, und klicken Sie auf **Bearbeiten**. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Zum **Entfernen** eines Eintrags aus der Liste wählen Sie den zu löschenden Eintrag aus, und klicken Sie auf **Entfernen**. Zum Auswählen eines Eintragsblocks klicken Sie auf den ersten Eintrag, halten Sie die Umschalttaste gedrückt, und klicken Sie auf den letzten Eintrag im Block. Zum Auswählen einzelner Einträge drücken Sie beim Klicken auf die einzelnen Einträge die Strg-Taste. Zum Aufheben der Auswahl eines Eintrags drücken Sie beim Klicken auf den Eintrag die Strg-Taste.

Verwenden der Liste "Statische IP-Adresse" zum Sperren von Geräten

Mithilfe der Liste **Statische IP-Adressen** können Sie den Zugriff auf das Netzwerk steuern.

So sperren Sie den Zugriff durch in der Liste nicht enthaltene Geräte oder Geräte ohne korrekte IP-Adresse:

- **In der Liste enthaltene MAC-Adressen mit falscher IP-Adresse sperren**: Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass ein Gerät mit geänderter IP-Adresse auf das Netzwerk zugreift. Wenn Sie beispielsweise die statische IP-Adresse 192.168.1.100 zugewiesen haben und ein Benutzer die Adresse 192.168.149 für das Gerät konfiguriert hat, kann das Gerät keine Verbindung mit dem Netzwerk herstellen. Auf diese Weise können Sie verhindern, dass Benutzer die IP-Adressen von Geräten ohne Ihre Genehmigung ändern. Deaktivieren Sie das Kontrollkästchen, um den Zugriff unabhängig von der zurzeit zugewiesenen IP-Adresse zuzulassen.
- **Nicht in der Liste enthaltene MAC-Adressen sperren**: Aktivieren Sie dieses Kontrollkästchen, um den Zugriff über nicht in der Liste **Statische IP-Adresse** enthaltene Geräte zu sperren. Dadurch verhindern Sie, dass unbekannte Geräte auf das Netzwerk zugreifen. Deaktivieren Sie das Kontrollkästchen, um den Zugriff durch alle Geräte zuzulassen, die mit einer IP-Adresse im richtigen Bereich konfiguriert sind.

Lokale DNS-Datenbank

Der DNS-Service (Domain Name Service) ordnet einem Domänennamen seine weiterleitbare IP-Adresse zu. Sie können eine lokale DNS-Datenbank einrichten, mit deren Hilfe das Gerät als lokaler DNS-Server für häufig verwendete Domänennamen fungieren kann. Durch die Verwendung einer lokalen Datenbank können Sie möglicherweise gegenüber der Verwendung eines externen DNS-Servers eine Beschleunigung erzielen. Wenn ein angeforderter Domänenname in der lokalen Datenbank nicht gefunden wurde, wird die Anfrage an den auf der Seite **Einrichten des Netzwerks** > WAN-Einstellung angegebenen DNS-Server weitergeleitet.

Wenn Sie diese Funktion aktivieren, müssen Sie auch die Clientgeräte so konfigurieren, dass das Gerät als DNS-Server verwendet wird. Windows-Computer sind standardmäßig so eingerichtet, dass die Adresse des DNS-Servers automatisch vom Standardgateway bezogen wird.

Zum Ändern der TCP/IP-Verbindungseinstellungen auf einem PC unter Windows beispielsweise wechseln Sie zum Fenster *Eigenschaften von LAN-Verbindung* > *Internetprotokoll* > *TCP/IP-Eigenschaften*. Wählen Sie **Folgende DNS-Server-Adresse verwenden** aus, und geben Sie unter **Bevorzugter DNS-Server** die LAN-IP-Adresse des Routers ein. Weitere Informationen finden Sie in der Dokumentation für den zu konfigurierenden Client.

Hinzufügen, Bearbeiten oder Löschen lokaler DNS-Einträge

Zum Hinzufügen eines neuen Eintrags klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Informationen ein:

- **Hostname**: Geben Sie den Domänennamen ein, beispielsweise *beispiel.com* oder *beispiel.org*. Wenn Sie die letzte Ebene des Domänennamens nicht angeben, wird bei Clients unter Microsoft Windows® dem Eintrag automatisch die Zeichenfolge *.com* angefügt.
- **IP-Adresse**: Geben Sie die IP-Adresse der Ressource ein.

Zum **Bearbeiten** der Einstellungen wählen Sie in der Liste einen Eintrag aus. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Zum **Entfernen** eines Eintrags aus der Liste wählen Sie den zu löschenden Eintrag aus, und klicken Sie auf **Entfernen**. Zum Auswählen eines Eintragsblocks klicken Sie auf den ersten Eintrag, halten Sie die Umschalttaste gedrückt, und klicken Sie auf den letzten Eintrag im Block. Zum Auswählen einzelner Einträge drücken Sie beim Klicken auf die einzelnen Einträge die Strg-Taste. Zum Aufheben der Auswahl eines Eintrags drücken Sie beim Klicken auf den Eintrag die Strg-Taste.

Routerankündigung (IPv6)

Der RADVD (Router Advertisement Daemon) wird für die automatische IPv6-Konfiguration und für Routing verwendet. Wenn die Funktion aktiviert ist, sendet der Router Nachrichten sowohl in regelmäßigen Abständen als auch direkt als Antwort auf Anfragen. Ein Host entnimmt den Informationen die Präfixe und Parameter für das lokale Netzwerk. Wenn Sie diese Funktion deaktivieren, deaktivieren Sie damit die automatische Konfiguration und müssen die IPv6-Adresse, das Subnetzpräfix und das Standardgateway für jedes Gerät manuell konfigurieren.

Diese Seite ist verfügbar, wenn Sie auf der Seite **Einrichten des Netzwerks** die Option **Dual-Stack-IP** aktiviert haben. Anderenfalls wird eine Meldung angezeigt, wenn Sie diese Seite zu öffnen versuchen.

Zum Aktivieren der Routerankündigung aktivieren Sie das Kontrollkästchen **Routerankündigung aktivieren**, und füllen Sie die übrigen Felder aus:

- **Anzeigemodus**: Wählen Sie eine der folgenden Optionen aus:
  - **Unaufgefordertes Multicast**: Routerankündigungsnachrichten werden an alle Schnittstellen in der Multicast-Gruppe gesendet. Dies ist die Standardeinstellung. Geben Sie außerdem das **Ankündigungsintervall** ein, das heißt das Intervall, in dem Routerankündigungsnachrichten gesendet werden. Geben Sie einen beliebigen Wert zwischen 10 und 1800 Sekunden ein. Der Standardwert lautet **30 Sekunden**.
  - **Nur Unicast**: Routerankündigungsnachrichten werden nur an allgemein bekannte IPv6-Adressen gesendet.
- **RA-Kennzeichen**: Bestimmt, ob Hosts IP-Adressen und zugehörige Informationen über DHCPv6 beziehen können. Folgende Optionen sind möglich:
  - **Verwaltet**: Hosts verwenden ein verwaltetes, statusbehaftetes Konfigurationsprotokoll (DHCPv6), um statusbehaftete Adressen und andere Informationen über DHCPv6 zu beziehen.
  - **Sonstige**: Andere nicht im Zusammenhang mit Adressen stehende Informationen wie beispielsweise Adressen von DNS-Servern werden über ein verwaltetes, statusbehaftetes Konfigurationsprotokoll (DHCPv6) bezogen.

- **Routerpriorität - Hoch, Mittel** oder **Niedrig**: Diese Prioritätsmetrik wird in Netzwerktopologien verwendet, in denen Multihome-Hosts auf mehrere Router zugreifen können. Anhand dieser Metrik kann ein Host einen geeigneten Router auswählen. Wenn zwei Router erreichbar sind, wird der mit der höheren Priorität ausgewählt. Diese Werte werden von Hosts ignoriert, die keine Routerpriorität implementieren. Die Standardeinstellung lautet **Hoch**.
- **MTU**: Die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Die MTU (Maximum Transmission Unit, maximale Übertragungseinheit) wird in Routerankündigungsnachrichten verwendet, um sicherzustellen, dass alle Knoten im Netzwerk den gleichen MTU-Wert verwenden, wenn die LAN-MTU-Größe nicht allgemein bekannt ist. Die Standardeinstellung lautet **1500 Byte**, was dem Standardwert für Ethernet-Netzwerke entspricht. Bei PPPoE-Verbindungen lautet der Standardwert **1492 Byte**. Sofern der ISP keine andere Einstellung vorgibt, sollten Sie diese Einstellung nicht ändern.
- **Routergültigkeitsdauer**: Gibt an, wie viele Sekunden lang die Routerankündigungsnachrichten in der Route vorhanden sind. Der Standardwert lautet **3600 Sekunden**.

Zum Hinzufügen eines neuen Subnetzes klicken Sie auf **Hinzufügen**, und geben Sie Werte für **IPv6-Adresse**, **Präfixlänge** und **Gültigkeitsdauer** ein.

7

Systemverwaltung

Unter **Systemverwaltung** konfigurieren Sie erweiterte Einstellungen wie beispielsweise Diagnosetools und führen Aufgaben wie beispielsweise Firmwareupgrades, Sicherungen und Neustarts des Geräts aus.

Dual-WAN-Verbindung

Wenn Sie mehrere WAN-Schnittstellen verwenden, konfigurieren Sie mit dieser Funktion die Einstellungen für Internetverbindungen.

Zum Konfigurieren des Lastenausgleichs wählen Sie für die Verwaltung der WAN-Verbindungen einen der folgenden Modi aus:

- **Smart Link-Sicherung**: Stellt konstante Konnektivität sicher. Wenn die primäre WAN-Verbindung nicht verfügbar ist, wird die WAN-Sicherungsverbindung verwendet. Wählen Sie im Dropdown-Menü die primäre WAN-Schnittstelle aus.
- **Lastenausgleich**: Verwenden Sie beide WAN-Verbindungen, um die verfügbare Bandbreite zu erhöhen. Der Router gleicht den Verkehr zwischen den beiden Schnittstellen mithilfe der gewichteten Round-Robin-Methode aus.

HINWEIS Auf DNS-Abfragen wird kein Lastenausgleich angewendet.

Zum Konfigurieren der Schnittstelleneinstellungen wählen Sie die **WAN-Schnittstelle** aus, und klicken Sie auf **Bearbeiten**. Das Fenster mit den Einstellungen für die Schnittstelle wird angezeigt. Geben Sie die folgenden Parameter ein:

Max. vom ISP bereitgestellte Bandbreite

Geben Sie die Einstellungen für die vom ISP vorgegebene maximale Bandbreite ein. Wenn die Bandbreite die angegebene Zahl überschreitet, verwendet der Router für die nächste Verbindung eine andere WAN-Schnittstelle.

- **Upstream**: Vom ISP bereitgestellte maximale Upstream-Bandbreite. Der Standardwert lautet **10000 KBit/s**. Maximal sind 1 000 000 KBit/s möglich.
- **Downstream**: Vom ISP bereitgestellte maximale Downstream-Bandbreite. Der Standardwert lautet **10000 KBit/s**.

Netzwerkserviceerkennung

Aktivieren Sie optional das Kontrollkästchen, damit das Gerät durch Senden eines Ping-Signals an bestimmte Geräte Netzwerkverbindungen erkennen kann, und geben Sie die Einstellungen wie hier beschrieben ein:

- **Wiederholungsanzahl**: Anzahl der an ein Gerät gesendeten Ping-Signale. Gültig sind Werte im Bereich von 1 bis 99999. Der Standardwert lautet **3**.
- **Wiederholungszeitüberschreitung**: Gibt an, wie viele Sekunden lang zwischen Ping-Signalen gewartet werden soll. Gültig sind Werte im Bereich von 1 bis 9999999. Der Standardwert lautet **10 Sekunden**.
- **Bei Fehlschlagen**: Aktion, die bei Fehlschlagen eines Ping-Tests ausgeführt werden soll:
  - **Generate the Error Condition in the System Log** (Fehlerzustand im Systemprotokoll generieren): Zeichnet den Fehler im Systemprotokoll auf. Ein Failover an die andere Schnittstelle findet nicht statt.
  - **Keep System Log and Remove the Connection** (Systemprotokoll beibehalten und Verbindung entfernen): Es findet ein Failover statt, und die Sicherungsschnittstelle wird verwendet. Wenn die Konnektivität des WAN-Anschlusses wiederhergestellt ist, wird der Verkehr an diesem Anschluss wiederhergestellt.
- **Standardgateway, ISP-Host, Remotehost** und **DNS-Abruf-Host**: Wählen Sie das Gerät aus, an das Sie ein Ping-Signal senden möchten, um die Netzwerkverbindungen zu ermitteln. Bei einem ISP-Host oder einem Remote-Host geben Sie die IP-Adresse ein. Bei einem DNS-Abruf-Host geben Sie einen Hostnamen oder einen Domänennamen ein. Deaktivieren Sie das entsprechende Kontrollkästchen, wenn Sie kein Ping-Signal zur Netzwerkserviceerkennung an dieses Gerät senden möchten.

Protokollbindung

Die Protokollbindung setzt voraus, dass diese Schnittstelle für bestimmte Protokolle sowie Quell- und Zieladressen verwendet wird. Ein Administrator kann bestimmten ausgehenden Verkehr an eine WAN-Schnittstelle binden. Diese Möglichkeit wird im Allgemeinen verwendet, wenn die beiden WAN-Schnittstellen unterschiedliche Merkmale haben oder wenn bestimmter Verkehr vom LAN zum WAN durch die gleiche WAN-Schnittstelle fließen muss.

Zum Hinzufügen oder Bearbeiten von Tabelleneinträgen klicken Sie auf **Hinzufügen** oder **Bearbeiten**, und geben Sie Folgendes ein:

- **Service**: Der Service (oder **Gesamter Datenverkehr**), der an diese WAN-Schnittstelle gebunden werden soll. Wenn ein Service nicht aufgeführt ist, können Sie ihn durch Klicken auf **Serviceverwaltung** hinzufügen. Weitere Informationen finden Sie unter **Hinzufügen oder Bearbeiten eines Services**.
- **Quell-IP** und **Ziel-IP**: Interne Quelle und externes Ziel für den Verkehr, der durch diesen WAN-Anschluss fließt. Geben Sie bei einem IP-Adressbereich im ersten Feld die erste Adresse und im Feld *Bis* die letzte Adresse ein. Bei einer einzelnen IP-Adresse geben Sie in beiden Feldern die gleiche Adresse ein.

Zum Aktivieren der Protokollbindung aktivieren Sie das Kontrollkästchen, um die Regel zu aktivieren, oder deaktivieren Sie es, um die Regel zu deaktivieren.

Zum **Bearbeiten** der Einstellungen wählen Sie in der Liste einen Eintrag aus. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Zum **Entfernen** eines Eintrags aus der Liste wählen Sie den zu löschenden Eintrag aus, und klicken Sie auf **Entfernen**. Zum Auswählen eines Eintragsblocks klicken Sie auf den ersten Eintrag, halten Sie die **Umschalttaste** gedrückt, und klicken Sie auf den letzten Eintrag im Block. Zum Auswählen einzelner Einträge drücken Sie beim Klicken auf die einzelnen Einträge die Strg-Taste. Zum Aufheben der Auswahl eines Eintrags drücken Sie beim Klicken auf den Eintrag die Strg-Taste.

Hinzufügen oder Bearbeiten eines Services

Zum Hinzufügen eines neuen Eintrags zur Serviceliste oder zum Ändern eines Eintrags klicken Sie auf **Serviceverwaltung**. Die Liste kann max. 30 Services enthalten. Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

Zum Hinzufügen eines Services zur Liste klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Informationen ein:

- **Servicename**: Kurze Beschreibung
- **Protokoll**: Benötigtes Protokoll. Weitere Informationen finden Sie in der Dokumentation für den zu hostenden Service.
- **Portbereich**: Erforderlicher Portbereich

Zum **Bearbeiten** der Einstellungen wählen Sie in der Liste einen Eintrag aus, und klicken Sie auf **Bearbeiten**. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Zum **Entfernen** eines Eintrags aus der Liste wählen Sie den zu löschenden Eintrag aus, und klicken Sie auf **Entfernen**. Zum Auswählen eines Eintragsblocks klicken Sie auf den ersten Eintrag, halten Sie die **Umschalttaste** gedrückt, und klicken Sie auf den letzten Eintrag im Block. Zum Auswählen einzelner Einträge drücken Sie beim Klicken auf die einzelnen Einträge die Strg-Taste. Zum Aufheben der Auswahl eines Eintrags drücken Sie beim Klicken auf den Eintrag die Strg-Taste.

Bandbreitenmanagement

Mit Bandbreitenmanagement können Sie die Bandbreiteneinstellungen für Upstream- und Downstream-Verkehr und die QoS-Einstellungen (Quality of Service) für verschiedene Verkehrstypen wie beispielsweise Sprachdienste anpassen.

Maximale vom ISP bereitgestellte Bandbreite

Geben Sie die Einstellungen für die vom ISP vorgegebene maximale Bandbreite ein:

- **Upstream**: Vom ISP bereitgestellte maximale Upstream-Bandbreite.
- **Downstream**: Vom ISP bereitgestellte maximale Downstream-Bandbreite.

Bandbreitenmanagementtyp

Wählen Sie eine der folgenden Verwaltungsoptionen aus:

- **Überwachung des Datendurchsatzes**: Minimale (garantierte) Bandbreite und maximale (begrenzte) Bandbreite für die einzelnen Services oder IP-Adressen. Sie können max. 100 Services hinzufügen.
- **Priorität**: Verwalten Sie die Bandbreite, indem Sie Services mit hoher Priorität und Services mit niedriger Priorität identifizieren.

Überwachung des Datendurchsatzes

Zum Hinzufügen einer Schnittstelle mit Bandbreitenmanagement klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Einstellungen ein:

- **Schnittstelle**: Schnittstelle, die den Service unterstützt
- **Service**: Zu verwaltender Service. Wenn ein Service nicht aufgeführt ist, klicken Sie auf **Serviceverwaltung**, um einen Service hinzuzufügen.
- **IP**: Zu steuernde IP-Adresse bzw. zu steuernder Bereich
- **Richtung**: Wählen Sie für ausgehenden Verkehr die Option **Upstream** aus. Wählen Sie für eingehenden Verkehr die Option **Downstream** aus.
- **Min. Rate**: Minimale Rate in KBit/s für die garantierte Bandbreite
- **Max. Rate**: Maximale Rate in KBit/s für die garantierte Bandbreite

Aktivieren Sie das Kontrollkästchen, um den Service zu aktivieren.

Konfigurieren der Priorität

Zum Hinzufügen einer Schnittstelle mit Bandbreitenmanagement klicken Sie auf **Hinzufügen**, und geben Sie die folgenden Einstellungen ein:

- **Schnittstelle: Schnittstelle, die den Service unterstützt**
- **Service**: Zu verwaltender Service. Wenn ein Service nicht aufgeführt ist, klicken Sie auf **Serviceverwaltung**, um einen Service hinzuzufügen.
- **Richtung**: Wählen Sie für ausgehenden Verkehr die Option **Upstream** aus. Wählen Sie für eingehenden Verkehr die Option **Downstream** aus.
- **Priorität**: Wählen Sie die Priorität für den Service aus, **Hoch** oder **Niedrig**. Die Standardprioritätsstufe lautet **Mittel**. Diese Stufe gilt implizit und wird auf der Weboberfläche nicht angezeigt.

Aktivieren Sie das Kontrollkästchen, um den Service zu aktivieren.

Zum **Bearbeiten** der Einstellungen wählen Sie in der Liste einen Eintrag aus, und klicken Sie auf **Bearbeiten**. Die Informationen werden in den Textfeldern angezeigt. Nehmen Sie die Änderungen vor, und klicken Sie auf **Speichern**.

Zum **Entfernen** eines Eintrags aus der Liste wählen Sie den zu löschenden Eintrag aus, und klicken Sie auf **Entfernen**. Zum Auswählen eines Eintragsblocks klicken Sie auf den ersten Eintrag, halten Sie die **Umschalttaste** gedrückt, und klicken Sie auf den letzten Eintrag im Block. Zum Auswählen einzelner Einträge drücken Sie beim Klicken auf die einzelnen Einträge die Strg-Taste. Zum Aufheben der Auswahl eines Eintrags drücken Sie beim Klicken auf den Eintrag die Strg-Taste.

SNMP

Mit dem SNMP-Protokoll (Simple Network Management Protocol) können Netzwerkadministratoren Benachrichtigungen über im Netzwerk auftretende kritische Ereignisse verwalten, überwachen und empfangen. Das Gerät unterstützt SNMPv1/v2c und SNMPv3. Das Gerät unterstützt Standard-MIBs (Managementinformationsbasen) wie beispielsweise MIBII sowie private MIBs.

Das Gerät fungiert als SNMP-Agent, der auf SNMP-Befehle von SNMP-Netzwerkmanagementsystemen (NMS) antwortet. Dabei werden die SNMP-Standardbefehle **get**, **next** und **set** unterstützt. Außerdem werden Trap-Nachrichten generiert, um den SNMP-Manager bei Auftreten von Alarmzuständen zu benachrichtigen. Dazu gehören beispielsweise Neustarts, Aus- und Einschalten sowie Ereignisse im Zusammenhang mit WAN-Verbindungen.

Konfigurieren von SNMP

- **Systemname**: Hostname für das Gerät
- **Systemkontakt**: Name des Netzwerkadministrators, der als Kontakt im Zusammenhang mit Updates für das Gerät zur Verfügung steht
- **Systemstandort**: Kontaktinformationen für den Netzwerkadministrator**,** E-Mail-Adresse, Telefonnummer oder Pager-Nummer
- **Trap Community Name** (Trap-Community-Name): Kennwort, das mit jedem Trap an den SNMP-Manager gesendet wird. Die Zeichenfolge kann aus bis zu 64 alphanumerischen Zeichen bestehen. Der Standardwert lautet **public**.

- **Enable SNMPv1/v2c** (SNMPv1/v2c aktivieren): Aktiviert SNMP v1/v2c.
  - **Community-Name abrufen**: Community String für die Authentifizierung von SNMP-GET-Befehlen. Sie können einen Namen mit maximal 64 alphanumerischen Zeichen eingeben. Der Standardwert lautet *public*.
  - **Community-Name festlegen**: Community String für die Authentifizierung von SNMP-SET-Befehlen. Sie können einen Namen mit maximal 64 alphanumerischen Zeichen eingeben. Der Standardwert lautet *private*.
  - **SNMPv1/v2c Trap Receiver IP Address** (IP-Adresse des SNMPv1/v2c-Trap-Empfängers): IP-Adresse oder Domänenname für den Server, auf dem Sie die SNMP-Verwaltungssoftware ausführen
- **Enable SNMPv3** (SNMPv3 aktivieren): Aktiviert SNMPv3. (Aktivieren Sie das Kontrollkästchen und klicken Sie auf **Speichern**, bevor Sie SNMP-Gruppen und -Benutzer erstellen.) Folgen Sie den Anweisungen unter **Konfigurieren von SNMPv3**.
  - **SNMPv3 Trap Receiver IP Address** (IP-Adresse des SNMPv3-Trap-Empfängers): IP-Adresse oder Domänenname für den Server, auf dem Sie die SNMP-Verwaltungssoftware ausführen
  - **SNMPv3 Trap Receiver User** (SNMPv3-Trap-Empfänger-Benutzer): Benutzername für den Server, auf dem Sie die SNMP-Verwaltungssoftware ausführen

Konfigurieren von SNMPv3

Sie können SNMPv3-Gruppen erstellen, um den SNMP-MIB-Zugriff zu verwalten und die Benutzer zu identifizieren, die auf die einzelnen Gruppen zugreifen können.

So können Sie eine Gruppe hinzufügen oder bearbeiten:

SCHRITT 1 Klicken Sie auf **Hinzufügen**, oder wählen Sie in der Gruppentabelle eine Gruppe aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie den Wert für **Gruppenname** ein.

SCHRITT 3 Wählen Sie im Dropdown-Menü die **Sicherheitsstufe** aus. Wenn Sie **Authentifizierung** oder **Datenschutz** auswählen, werden die Benutzer gezwungen, sich mit Kennwörtern zu authentifizieren. Wenn Sie **Keine Authentifizierung**, **Kein Datenschutz** ausgewählt haben, müssen die Benutzer in dieser Gruppe kein Authentifizierungskennwort oder Datenschutzkennwort

festlegen. Die Standardeinstellung lautet **Keine Authentifizierung, Kein Datenschutz**. Authentifizierungs- und Datenschutzkennwörter müssen aus mindestens acht Zeichen bestehen.

SCHRITT 4 Wählen Sie die **MIBs** aus, auf die die Mitglieder der Gruppe zugreifen können.

SCHRITT 5 Klicken Sie auf **Speichern**.

So können Sie einen Benutzer hinzufügen oder bearbeiten:

SCHRITT 1 Klicken Sie auf **Hinzufügen**, oder wählen Sie in der Benutzertabelle einen Benutzer aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Geben Sie den Wert für **Benutzername** ein.

SCHRITT 3 Wählen Sie im Dropdown-Menü die **Gruppe** aus.

SCHRITT 4 Wählen Sie das **Authentifizierungsverfahren** aus, und geben Sie das **Authentifizierungskennwort** ein.

SCHRITT 5 Wählen Sie die **Datenschutzmethode** aus, und geben Sie das **Datenschutzkennwort** ein.

SCHRITT 6 Klicken Sie auf **Speichern**.

SMTP

Benutzer die Konfiguration der SMTP-Einstellungen ermöglichen, mit denen das Protokoll oder die Konfigurationsdatei für OpenVPN gesendet werden.

Wählen Sie zum Öffnen dieser Seite im Navigationsverzeichnis **Systemverwaltung > SMTP** aus.

Zur Konfiguration von SMTP geben Sie die folgenden Einstellungen ein, und klicken Sie auf **Speichern**.

- **Absender**: E-Mail-Adresse des Absenders
- **Mailserver**: Name oder IP-Adresse des Mailservers
- **Authentifizierung**: Authentifizierungstyp für die Anmeldung beim Mailserver
  - **Ohne**: Ohne Authentifizierung

- **Unverschlüsselte Anmeldung**: Authentifizierung im unverschlüsselten Format
- **TLS**: Authentifizierungsprotokoll der sicheren Verbindung (Bei Gmail beispielsweise wird die TLS-Authentifizierungsoption an Port 587 verwendet.)
- **SSL**: Authentifizierungsprotokoll der sicheren Verbindung (Bei Gmail beispielsweise wird die SSL-Authentifizierungsoption an Port 465 verwendet.)

▪ **SMTP-Port**: Portnummer für das SMTP-Protokoll

▪ **Benutzername**: E-Mail-Benutzername Beispiel:
Mailserver: smtp.gmail.com
Authentifizierung: SSL
SMTP-PORT: 465
Benutzername: xxxxx@gmail.com
Kennwort: yyyyyy

Kennwort: E-Mail-Kennwort

Erkennung – Bonjour

Bonjour ist ein Serviceerkennungsprotokoll, das Netzwerkgeräte wie beispielsweise Computer und Server im LAN findet. Wenn die Funktion aktiviert ist, sendet das Gerät regelmäßig per Multicast Bonjour-Servicedatensätze an das LAN, um sein Vorhandensein anzukündigen.

HINWEIS Für die Erkennung von Cisco-Produkten stellt Cisco ein Dienstprogramm bereit, das über die einfache Symbolleiste mit dem Namen "FindIt" im Webbrowser verwendet wird. Mit diesem Dienstprogramm werden Cisco-Geräte im Netzwerk erkannt und grundlegende Informationen wie beispielsweise Seriennummern und IP-Adressen angezeigt. Weitere Informationen und das Dienstprogramm zum Herunterladen finden Sie auf der Website www.cisco.com/go/findit.

Zum globalen Aktivieren von Bonjour aktivieren Sie das Kontrollkästchen **Erkennung aktivieren**. Die Einstellung ist standardmäßig aktiviert.

Zum Aktivieren von Bonjour für ein VLAN aktivieren Sie das Kontrollkästchen in der Spalte **Bonjour aktivieren**. Die Einstellung ist standardmäßig aktiviert.

LLDP-Eigenschaften

LLDP (Link Layer Discovery Protocol) ist ein anbieterneutrales Protokoll aus der Internetprotokollsuite, das von Netzwerkgeräten zum Ankündigen ihrer Identität, ihrer Funktionen und ihrer Nachbarn in einem IEEE 802-LAN (hauptsächlich drahtgebundenes Ethernet) verwendet wird. LLDP-Informationen werden in festen Intervallen in Form eines Ethernet-Frames von Geräten über alle Schnittstellen gesendet. Jeder Frame enthält eine LLDP-Dateneinheit (LLDP Data Unit, LLDPDU). Jede LLDPDU entspricht einer Sequenz aus TLV-Strukturen (Type-Length-Value).

Zum Aktivieren von LLDP-Eigenschaften aktivieren Sie das Kontrollkästchen **Aktivieren**. (Das Kontrollkästchen ist standardmäßig aktiviert.)

Zum Aktivieren von LLDP-Eigenschaften für eine Schnittstelle aktivieren Sie das Kontrollkästchen **Aktivieren**, **WAN1** oder **WAN2**. (Die Kontrollkästchen sind standardmäßig aktiviert.)

In der LLDP-Nachbartabelle werden die folgenden Informationen angezeigt:

- **Lokaler Port**: Anschluss-ID
- **Geräte-ID-Subtyp**: Typ der Geräte-ID (beispielsweise MAC-Adresse)
- **Geräte-ID**: ID des Geräts. Wenn es sich beim Geräte-ID-Subtyp um eine MAC-Adresse handelt, wird die MAC-Adresse des Geräts angezeigt.
- **Anschluss-ID-Subtyp**: Typ der Anschluss-ID
- **Anschluss-ID**: Anschluss-ID
- **Systemname**: Name des Geräts
- **Time-to-Live**: Rate in Sekunden, mit der Updates von LLDP-Ankündigungen gesendet werden

Verwenden der Diagnose

Über die Seite **Diagnose** können Sie auf zwei integrierte Tools zugreifen, DNS-Namensabruf und Ping. Wenn Sie ein Konnektivitätsproblem vermuten, können Sie mit diesen Tools die Ursache ermitteln.

Zum Herausfinden einer IP-Adresse mithilfe von DNS wählen Sie **DNS-Abruf** aus, geben Sie den Wert für **Domänennamen abrufen** ein (beispielsweise www.cisco.com), und klicken Sie auf **Los**. Die IP-Adresse wird angezeigt.

Zum Testen der Konnektivität mit einem bestimmten Host wählen Sie **Ping** aus, geben Sie eine IP-Adresse oder einen Hostnamen ein, und klicken Sie auf **Los**. Wenn Sie die IP-Adresse nicht kennen, machen Sie sie mit dem DNS-Abruftool ausfindig. Mit Ping können Sie anzeigen, ob das Gerät ein Paket an einen Remote-Host senden und eine Antwort empfangen kann.

Wenn der Test erfolgreich verläuft, werden die folgenden Informationen angezeigt:

- **Status**: Status des Tests, **Test wird durchgeführt**, **Test erfolgreich** oder **Test fehlgeschlagen**
- **Pakete**: Anzahl der gesendeten Pakete, Anzahl der empfangenen Pakete und Prozentanteil der beim Ping-Test verlorenen Pakete
- **Umlaufzeit**: Minimale, maximale und durchschnittliche Umlaufzeiten für den Ping-Test

Werkseinstellungen

Zum Neustarten des Geräts und Zurücksetzen aller Parameter auf die Werkseinstellungen klicken Sie auf **Werkseinstellungen**.

Zum Wiederherstellen der Werkseinstellungen des Geräts einschließlich der Standardzertifikate klicken Sie auf **Werkseinstellungen inkl. Zertifikate**.

Firmware-Upgrade

Mit dieser Funktion können Sie die Firmware für das Gerät von einem PC oder USB-Flash-Laufwerk herunterladen und installieren. Im Fenster wird die **Firmwareversion** angezeigt, die zurzeit im Gerät ausgeführt wird.

HINWEIS Wenn Sie eine frühere Version der Firmware auswählen, wird das Gerät möglicherweise auf die Werkseinstellungen zurückgesetzt. Es wird empfohlen, vor dem Aktualisieren der Firmware die Konfiguration mit dem Verfahren unter **Sicherung und Wiederherstellung** zu sichern.

Das Aktualisieren der Firmware kann mehrere Minuten dauern.

Während dieses Vorgangs dürfen Sie weder das Gerät von der Stromversorgung trennen, noch die Reset-Taste drücken, den Browser schließen oder die Verbindung trennen.

Zum Hochladen der Firmware von einem PC wählen Sie **Firmware-Upgrade von PC** aus, und navigieren Sie zur Datei.

Zum Hochladen der Firmware von einem USB-Flash-Laufwerk wählen Sie **Firmware-Upgrade von USB** aus, und wählen Sie die Datei aus.

Sprachauswahl oder Spracheinrichtung

Auf der Seite **Sprachauswahl** oder **Spracheinrichtung** können Sie die Sprache für die Benutzeroberfläche und die Hilfe für Ihr Gerät ändern.

Bei Firmware-Versionen nach 1.0.2.03 wird die Sprache auf der Seite **Sprachauswahl** geändert.

SCHRITT 1 Navigieren Sie zu **Systemverwaltung** > **Sprachauswahl**.

SCHRITT 2 Wählen Sie aus der Dropdown-Liste **Sprache auswählen** eine Sprache aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Alternativ können Sie auch folgendermaßen eine Sprache auswählen:

- Wählen Sie auf der Anmeldeseite aus der Dropdown-Liste **Sprache** eine Sprache aus.
- Auf allen Konfigurationsseiten können Sie aus der Dropdown-Liste rechts oben eine Sprache auswählen.

Bei den Firmware-Versionen 1.0.2.03 oder älter können Sie auf der Seite **Spracheinrichtung** eine neue Sprache wählen, indem Sie ein Sprachpaket auf Ihr Gerät laden.

So fügen Sie ein Sprachpaket hinzu und wählen eine Sprache aus:

SCHRITT 1 Navigieren Sie zu **Systemverwaltung** > **Spracheinrichtung**.

SCHRITT 2 Wählen Sie in der Dropdown-Liste **Modus Hinzufügen**.

SCHRITT 3 Geben Sie den Wert für **Name der neuen Sprache** ein.

SCHRITT 4 Suchen Sie nach **Name der Sprachdatei**, um die neue Sprachdatei hochzuladen.

SCHRITT 5 Klicken Sie auf **Speichern**.

SCHRITT 6 Nachdem Sie das Sprachpaket hochgeladen haben, wählen Sie rechts oben auf der Seite **Spracheinrichtung** oder anderen Konfigurationsseiten aus der Dropdown-Liste eine Sprache aus.

Neustart

Wenn Sie über die Seite **Neustart** einen Neustart ausführen, sendet der Router die Protokolldatei (sofern die Protokollierung aktiviert ist), bevor das Gerät zurückgesetzt wird. Die Parameter für das Gerät bleiben erhalten.

Zum Neustarten des Geräts klicken Sie auf **Router neu starten**.

Sicherung und Wiederherstellung

Sie können Konfigurationsdateien importieren, exportieren und kopieren. Für den Router werden zwei Konfigurationsdateien verwaltet, die Startdatei und die Spiegeldatei. Das Gerät lädt die Startdatei beim Starten mit der aktuellen Konfiguration aus dem Arbeitsspeicher und kopiert die Startdatei in die Spiegeldatei. Daher enthält die Spiegeldatei die letzte als gültig bekannte Konfiguration.

Wenn die Startkonfigurationsdatei beschädigt ist oder aus irgendeinem Grund Fehler auftreten, wird die Spiegelkonfigurationsdatei verwendet. Der Router kopiert die Startkonfiguration automatisch nach 24 Betriebsstunden im stabilen Zustand (24 Stunden ohne Neustart oder Konfigurationsänderungen) in die Spiegelkonfiguration.

Wiederherstellen der Einstellungen aus einer Konfigurationsdatei

So stellen Sie die Startkonfiguration aus einer zuvor auf einem PC oder USB-Flash-Laufwerk gespeicherten Datei wieder her:

SCHRITT 1 Wählen Sie im Abschnitt **Startkonfigurationsdatei wiederherstellen** die Option **Startkonfigurationsdatei von PC wiederherstellen** aus, und klicken Sie auf **Durchsuchen**. Wählen Sie alternativ **Startkonfigurationsdatei von USB wiederherstellen** aus, und klicken Sie auf **Aktualisieren**.

SCHRITT 2 Wählen Sie eine Konfigurationsdatei (**.config**) aus.

SCHRITT 3 Klicken Sie auf **Wiederherstellen**. Dieser Vorgang kann bis zu einer Minute dauern. Wenn die Konfigurationsdatei ein anderes Kennwort als das aktuelle Verwaltungskennwort für das Gerät enthält, werden Sie zur Eingabe dieses Kennworts aufgefordert, bevor die Konfigurationsdatei wiederhergestellt wird.

SCHRITT 4 Klicken Sie im Navigationsbaum auf die Optionen **Systemverwaltung > Neustart**.

Die importierten Einstellungen werden erst angewendet, wenn Sie das Gerät über **Systemverwaltung > Neustart** neu starten.

Alternativ können Sie den Router neu starten, indem Sie die **Reset**-Taste am Gerät eine Sekunde lang drücken und dann loslassen.

Sichern von Konfigurationsdateien und Spiegeldateien

So speichern Sie die Start- und Spiegelkonfigurationsdateien auf dem Computer oder auf einem USB-Flash-Laufwerk:

SCHRITT 1 Wählen Sie **Konfigurationsdatei auf PC sichern** oder **Konfigurationsdatei auf USB sichern** aus.

SCHRITT 2 Klicken Sie auf **Startkonfiguration sichern** oder **Spiegelkonfiguration sichern**. Das Fenster zum Herunterladen der Datei wird angezeigt.

SCHRITT 3 Klicken Sie auf **Speichern**, und wählen Sie einen Dateispeicherort aus. Geben Sie optional einen Dateinamen ein, und klicken Sie auf **Speichern**.

TIPP Die Standarddateinamen lauten *Startup.config* und *Mirror.config*. Die Dateien müssen die Erweiterung *.config* haben. Zur leichteren Identifizierung können Sie einen Dateinamen eingeben, der das aktuelle Datum und die aktuelle Uhrzeit enthält.

Kopieren der Spiegeldatei in die Startdatei

Sie können die Startkonfigurationsdatei für das Gerät manuell in die Spiegelkonfigurationsdatei kopieren.

Auf diese Weise können Sie eine als gültig bekannte Konfiguration sichern, bevor Sie Änderungen an der Startkonfiguration vornehmen.

- Die Startkonfigurationsdatei wird automatisch alle 24 Stunden in die Spiegelkonfigurationsdatei kopiert.

- Wenn Sie Änderungen an den Parametern für das Gerät speichern, wird der Zeitzähler zurückgesetzt. Der nächste automatische Kopiervorgang findet 24 Stunden später statt, sofern Sie nicht manuell das Speichern der Startdatei als Spiegeldatei erzwingen.

Zum Kopieren der Startdatei in die Spiegeldatei klicken Sie auf **Spiegel nach Start kopieren**. Der Kopiervorgang wird sofort ausgeführt und kann nicht abgebrochen werden. Nach Abschluss des Vorgangs wird die Seite aktualisiert.

Bereinigen der Konfiguration

Beim Bereinigen der Konfiguration wird die Spiegeldatei und die Startkonfigurationsdatei gelöscht.

Klicken Sie auf **Konfiguration bereinigen**, um die Spiegeldatei und die Startkonfigurationsdatei zu löschen.

VORSICHT Die Spiegelkonfiguration wird sofort gelöscht, der Vorgang kann nicht abgebrochen werden. Das Gerät wird zurückgesetzt, um die Standardeinstellungen zu verwenden, und wird neu gestartet.

Sichern der Firmware auf einem USB-Flash-Laufwerk

Zum Sichern der Firmware auf einem Flash-Laufwerk am USB-Anschluss wählen Sie den Anschluss im Dropdown-Menü aus, und klicken Sie auf **Sicherung**. Das Gerät speichert das Firmware-Image unter **`image.bin`**.

8

Anschlussverwaltung

Unter **Anschlussverwaltung** können Sie Anschlusseinstellungen konfigurieren und den Status des Anschlusses anzeigen.

Sie können die Anschlusspiegelung aktivieren, einen Anschluss deaktivieren oder Priorität, Geschwindigkeit, Duplexmodus und automatische Aushandlung festlegen. Außerdem können Sie portbasierte VLANs aktivieren, um den Verkehr zwischen Geräten im Netzwerk zu steuern.

Konfigurieren der Anschlüsse

Sie können die Anschlusspiegelung festlegen und Anschlüsse verwalten (einschließlich der Priorität und des Modus). Bei der Anschlussspiegelung wird eine Kopie der an einem Anschluss erkannten Netzwerkpakete an eine Netzwerküberwachungsverbindung an einem anderen Anschluss gesendet. Diese Funktion wird normalerweise für Netzwerkgeräte verwendet, bei denen eine Überwachung des Netzwerkverkehrs erforderlich ist, beispielsweise für ein Intrusion Detection System. Bei einem Switch von Cisco Systems wird die Anschlusspiegelung im Allgemeinen als Switched Port Analyzer (SPAN) bezeichnet.

Netzwerktechniker oder Administratoren verwenden die Anschlussspiegelung zum Analysieren und Debuggen von Daten oder zum Diagnostizieren von Fehlern in einem Netzwerk. Sie können mit dieser Funktion die Netzwerkleistung überwachen und sich benachrichtigen lassen, wenn Probleme auftreten.

HINWEIS Wenn **Klonen von MAC-Adressen** aktiviert ist, kann die Anschlussspiegelung nicht verwendet werden.

Zum Aktivieren der Anschlussspiegelung für RV320 aktivieren Sie das Kontrollkästchen **Spiegelanschluss aktivieren**. An WAN- und LAN-Anschlüsse eingehende und ausgehende Pakete werden an LAN 1 kopiert.

Zum Aktivieren der Anschlussspiegelung für RV325 aktivieren Sie das Kontrollkästchen **Spiegelanschluss aktivieren**. An LAN-Anschlüssen eingehende und ausgehende Pakete werden an LAN 1 kopiert.

Für jeden Anschluss werden die folgenden schreibgeschützten Informationen angezeigt:

- **Anschluss-ID**: Anschlussnummer oder -name gemäß der Beschriftung am Gerät
- **Schnittstelle**: Schnittstellentyp: LAN, WAN oder DMZ

Geben Sie folgende Einstellungen ein:

- **Deaktivieren**: Aktivieren Sie dieses Kontrollkästchen, um einen Anschluss zu deaktivieren. Standardmäßig sind alle Anschlüsse aktiviert.
- **EEE**: Aktivieren Sie dieses Kontrollkästchen, um Energy Efficient Ethernet zur Reduzierung des Stromverbrauchs bei geringer Datenaktivität zu aktivieren.
- **Priorität**: Wählen Sie für die einzelnen Anschlüsse die gewünschte Prioritätsstufe aus (**Hoch** oder **Normal**). Damit stellen Sie die Quality of Service (QoS) sicher, da der Verkehr für Geräte an bestimmten Anschlüssen priorisiert wird. Beispielsweise können Sie einem für Spiele oder Videokonferenzen verwendeten Anschluss die Priorität **Hoch** zuweisen. Die Standardeinstellung lautet **Normal**.
- **Modus**: Anschlussgeschwindigkeit und Duplexmodus. Wenn **Automatisch aushandeln** ausgewählt ist, handelt das Gerät Verbindungsgeschwindigkeiten und den Duplexmodus automatisch mit dem verbundenen Gerät aus.

Anschlussstatus

Unter **Anschlussstatus** wird eine Übersicht über den Status der Anschlüsse angezeigt. Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren.

In der Ethernet-Tabelle wird Folgendes angezeigt:

- **Anschluss-ID**: Position des Anschlusses
- **Typ**: Anschlusstyp
- **Leitungsstatus**: Status der Verbindung

- **Anschlussaktivität**: Status des Anschlusses
- **Priorität**: Die im Fenster **Anschluss einrichten** festgelegte Anschlusspriorität
- **Geschwindigkeitsstatus**: Geschwindigkeit des Anschlusses (10 MBit/s, 100 MBit/s oder 1000 MBit/s)
- **Duplex-Status**: Duplexmodus (*Halb* oder *Voll*)
- **Automatisch aushandeln**: Status des Duplexmodus

Verkehrsstatistiken

In der Tabelle **Statistik** wird für den ausgewählten Anschluss Folgendes angezeigt:

- **Anschluss-ID**: Position des Anschlusses
- **Leitungsstatus**: Status der Verbindung
- **Empfangene Pakete**: Anzahl der am Anschluss empfangenen Pakete
- **Empfangene Pakete**: Anzahl der empfangenen Pakete in Bytes
- **Übertragene Pakete**: Anzahl der über den Anschluss gesendeten Pakete
- **Übertragene Pakete**: Anzahl der gesendeten Pakete in Bytes
- **Paketfehler**: Anzahl der Paketfehler

VLAN-Mitgliedschaft

Alle LAN-Anschlusses befinden sich standardmäßig in VLAN 1.

Zum Aktivieren von VLANs aktivieren Sie das Kontrollkästchen **VLAN aktivieren**.

So können Sie ein VLAN hinzufügen oder bearbeiten:

- **VLAN-ID**: ID für das VLAN
- **Beschreibung**: Beschreibung des VLANs

- **Inter-VLAN-Routing**: Ermöglicht die Übertragung von Paketen zwischen VLANs. Ein VLAN mit deaktiviertem Inter-VLAN-Routing ist von anderen VLANs isoliert. Sie können Firewallzugriffsregeln konfigurieren, um den Inter-VLAN-Verkehr weiter zu regeln (zulassen oder verweigern).
- **Bei RV320**, **LAN 1** bis **LAN 4**: Ein Anschluss kann getaggt, ungetaggt oder vom VLAN ausgeschlossen sein.
- **Bei RV325**, **LAN 1** bis **LAN 14**: Ein Anschluss kann getaggt, ungetaggt oder vom VLAN ausgeschlossen sein.

QoS: CoS/DSCP-Einstellung

Mit dieser Option gruppieren Sie Verkehr nach Serviceklassen (Classes of Service, CoS), um eine bestimmte Bandbreite und eine höhere Priorität für die angegebenen Services sicherzustellen. Für sämtlichen nicht der IP-Gruppe hinzugefügten Verkehr wird der intelligente Ausgleichsmodus verwendet.

Zum Konfigurieren der Servicewarteschlangen wählen Sie im Dropdown-Menü die Priorität der **Warteschlange** aus (4 ist die höchste und 1 die niedrigste Priorität).

Zum Festlegen des DSCP-Werts (Differential Services Code Point) wählen Sie in den Dropdown-Menüs die **Warteschlange** aus.

DSCP-Markierung

Mit Differentiated Services Code Point (DSCP) oder DiffServ geben Sie eine einfache, skalierbare Methode für die Klassifizierung und Verwaltung des Netzwerkverkehrs sowie für die Bereitstellung der Quality of Service (QoS) an. Sie können mithilfe von DiffServ eine niedrige Latenz für kritischen Netzwerkverkehr wie beispielsweise Sprache oder Streaming-Medien und gleichzeitig für nicht kritische Services wie Webverkehr oder Dateiübertragungen bestmöglichen Datenverkehr bereitstellen.

Zum Konfigurieren der Servicewarteschlangen klicken Sie auf **Bearbeiten**, legen Sie die CoS/802.1p-Werte fest und geben Sie den Status und die Priorität ein.

802.1X-Konfiguration

Eine portbasierte Netzwerkzugriffssteuerung ermöglicht mithilfe der physischen Zugriffsmerkmale von IEEE 802-LAN-Infrastrukturen die Authentifizierung und Autorisierung von Geräten, die an einen LAN-Anschluss mit Point-to-Point-Verbindungsmerkmalen angeschlossen sind. Außerdem wird bei nicht erfolgreicher Authentifizierung und Autorisierung der Zugriff auf diesen Anschluss verhindert. Ein Anschluss ist in diesem Kontext eine einzelne Anschlussstelle für die LAN-Infrastruktur.

So konfigurieren Sie die portbasierte Authentifizierung:

SCHRITT 1 Aktivieren Sie das Kontrollkästchen **Anschlussbasierte Authentifizierung**, um die Funktion zu aktivieren.

SCHRITT 2 Geben Sie die IP-Adresse des RADIUS-Servers ein.

SCHRITT 3 Geben Sie die Nummer für den **RADIUS-UDP-Port** ein.

SCHRITT 4 Geben Sie das **RADIUS-Secret** ein.

SCHRITT 5 Wählen Sie in der Anschlusstabelle im Dropdown-Menü den **Administrationsstatus** aus:

- **Autorisierung erzwingen**: Es ist keine Autorisierung erforderlich. Wenn die Autorisierung für einen LAN-Anschluss erzwungen wird, müssen die an diesen LAN-Anschluss angeschlossenen PCs über eine statische IP-Adresse verfügen. *Die Autorisierung muss für mindestens einen LAN-Anschluss erzwungen werden.*
- **"Nicht autorisiert" erzwingen**: Der Status des gesteuerten Anschlusses wird so festgelegt, dass der Verkehr verworfen wird und Pakete nicht passieren können.
- **Automatisch**: Aktiviert die portbasierte Authentifizierung. Die Schnittstelle wechselt basierend auf dem Authentifizierungsaustausch zwischen dem Gerät und dem Client zwischen einem autorisierten und einem nicht autorisierten Status.

SCHRITT 6 Klicken Sie auf **Speichern**.

9

Firewall

Der Hauptzweck einer Firewall besteht darin, den ein- und ausgehenden Netzwerkverkehr zu steuern. Dazu werden zunächst die Datenpakete analysiert, und anschließend wird auf der Grundlage eines Satzes zuvor festgelegter Regeln ermittelt, ob die Pakete passieren dürfen. Eine Netzwerkfirewall richtet eine Brücke zwischen einem als sicher und vertrauenswürdig geltenden Netzwerk und einem anderen Netzwerk ein. Bei dem anderen Netzwerk handelt es sich normalerweise um ein externes Netzwerk (Internetzwerk) wie beispielsweise das Internet, das als nicht sicher und nicht vertrauenswürdig gilt.

Allgemein

Mit allgemeinen Firewallsteuerelementen verwalten Sie die Funktionen, die in der Regel von Browsern und Anwendungen verwendet werden.

Aktivieren von Firewallfunktionen

Zum Aktivieren der **Firewall** aktivieren Sie das Kontrollkästchen **Aktivieren**. Die folgenden Firewallfunktionen können Sie nach Bedarf aktivieren oder deaktivieren:

- **SPI (Zustandsbehaftete Paketprüfung)**: Überwacht den Status von Netzwerkverbindungen (beispielsweise TCP-Streams, UDP-Kommunikation im Netzwerk). Die Firewall unterscheidet zwischen legitimen Paketen für verschiedene Verbindungstypen. Nur Pakete, die mit einer bekannten aktiven Verbindung übereinstimmen, werden von der Firewall zugelassen. Andere Pakete werden abgelehnt.
- **DoS (Denial of Service)**: Erkennt Versuche, eine Überlastung des Servers auszulösen. Allgemein ausgedrückt werden DoS-Angriffe implementiert, indem das Zurücksetzen der Zielcomputer erzwungen wird oder die Ressourcen der Zielcomputer verbraucht werden, damit diese nicht mehr die vorgesehenen Services bereitstellen können. Alternativ werden die Kommunikationswege zwischen den vorgesehenen Benutzern und dem Opfer blockiert, sodass diese nicht mehr angemessen kommunizieren können.

- **WAN-Anfrage sperren**: TCP-Anfragen und ICMP-Pakete werden verworfen.
- **Remoteverwaltung**: Wenn diese Funktion aktiviert ist, kann das Gerät remote verwaltet werden. Der Standardwert für den Port lautet **443**. Sie können den Wert in einen beliebigen benutzerdefinierten Port ändern.- Die Zeichenfolge lautet **https://<WAN-IP>:<Remoteverwaltungsport>**.
- **Multicast-Passthrough**: Lässt zu, dass Multicast-Nachrichten das Gerät passieren.
- **HTTPS**: HTTPS (Hypertext Transfer Protocol Secure) ist ein Kommunikationsprotokoll für sichere Kommunikation über ein Computernetzwerk und wird vor allem im Internet eingesetzt.
- **SSL VPN**: Ermöglicht SSL-VPN-Verbindungen.
- **SIP-ALG**: Anwendungsschicht-Gateway, das eine Firewall oder NAT verstärkt. Angepasste NAT-Traversal-Filter können in das Gateway integriert werden, um die Umwandlung von Ports und Adressen für SIP-Protokolle (*Steuerung/Daten*) zu unterstützen.
- **UPnP**: Bei Universal Plug and Play (UPnP) handelt es sich um einen Satz von Netzwerkprotokollen, die Netzwerkgeräten wie beispielsweise PCs, Druckern, Internet-Gateways, Wi-Fi-Access Points und mobilen Geräten die nahtlose Erkennung ihres gegenseitigen Vorhandenseins im Netzwerk und die Einrichtung funktionsfähiger Netzwerkservices für Datenfreigabe und Kommunikation ermöglichen.
- **SSH**: Secure Shell (SSH) ist ein Netzwerkprotokoll, das Administratoren eine sichere Möglichkeit für den Zugriff auf einen Remote-Computer bietet. SSH wird von Netzwerkadministratoren häufig für die Remote-Verwaltung von Systemen und Anwendungen verwendet und ermöglicht es ihnen, sich über ein Netzwerk auf einem anderen Computer anzumelden, Befehle auszuführen und Dateien von einem Computer auf einen anderen zu verschieben.
- **Remote SSH**: Remote Secure Shell ist eine Methode für die sichere Remote-Anmeldung von einem Computer auf einem anderen. Diese Methode bietet verschiedene Alternativoptionen für eine starke Authentifizierung und schützt die Sicherheit und Integrität der Kommunikation mit einer starken Verschlüsselung.

Einschränken von Webfunktionen

Zum Einschränken der Webfunktionen **Java**, **Cookies**, **ActiveX** oder **Zugriff auf HTTP-Proxyserver** aktivieren Sie das jeweilige Kontrollkästchen.

Wenn Sie *nur* die ausgewählten Funktionen (**Java**, **Cookies**, **ActiveX** oder **Zugriff auf HTTP-Proxyserver**) zulassen und alle anderen einschränken möchten, aktivieren Sie die Option **Ausnahme**.

Konfigurieren vertrauenswürdiger Domänennamen

Zum Hinzufügen vertrauenswürdiger Domänen klicken Sie auf **Hinzufügen**, und geben Sie in **Domänenname** den Domänennamen ein.

Zum Bearbeiten einer vertrauenswürdigen Domäne klicken Sie auf **Bearbeiten**, und ändern Sie in **Domänenname** den Domänennamen.

Zugriffsregeln

Zugriffsregeln begrenzen den Zugriff auf das Subnetz, indem sie den Zugriff durch bestimmte anhand der IP-Adresse identifizierte Services oder Geräte zulassen oder verweigern.

Zum Hinzufügen oder Bearbeiten eines Services klicken Sie auf **Serviceverwaltung**. Diese Funktion wird unter **Hinzufügen oder Bearbeiten eines Servicenamens** beschrieben.

Hinzufügen einer Zugriffsregel zur IPv4-Zugriffsregeltabelle

So können Sie eine IPv4-Zugriffsregel hinzufügen oder bearbeiten:

SCHRITT 1 Klicken Sie auf die Registerkarte **IPv4**.

SCHRITT 2 Klicken Sie auf **Hinzufügen** (oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**).

SCHRITT 3 Wählen Sie im Dropdown-Menü die Aktion **Zulassen** oder **Verweigern** für die Regel aus.

SCHRITT 4 Wählen Sie im Dropdown-Menü **Service** einen Service aus.

SCHRITT 5 Wählen Sie **Pakete protokollieren, die dieser Regel entsprechen** oder **Kein Protokoll** aus.

SCHRITT 6 Wählen Sie im Dropdown-Menü die **Quellschnittstelle** aus.

SCHRITT 7 Wählen Sie im Dropdown-Menü die **Quell-IP**-Adresse aus. Wenn Sie **Einzeln** ausgewählt haben, geben Sie die Quell-IP-Adresse ein. Wenn Sie **Bereich** ausgewählt haben, geben Sie den Bereich für die Quell-IP-Adressen ein.

SCHRITT 8 Wählen Sie im Dropdown-Menü **Ziel-IP** die Ziel-IP-Adresse aus. Wenn Sie **Einzeln** ausgewählt haben, geben Sie die Ziel-IP-Adresse ein. Wenn Sie **Bereich** ausgewählt haben, geben Sie den Bereich für die Ziel-IP-Adressen ein.

SCHRITT 9 Konfigurieren Sie die **Planung** für diese Zugriffsregel, indem Sie die Uhrzeit auswählen. Wählen Sie **Immer** aus, wenn die Zugriffsregel 24 Stunden am Tag gelten soll. Wählen Sie **Intervall** aus, um eine Uhrzeit festzulegen, und geben Sie in den Feldern **Von** und **Bis** die Stunden und Minuten für die Geltung der Zugriffsregel ein. Beispiel: *07:00* bis *20:00*. Die Zugriffsregel lässt nicht die Festlegung zweier Zeitintervalle zu.

SCHRITT 10 Wählen Sie unter **Gilt** die entsprechenden Wochentage aus.

SCHRITT 11 Klicken Sie auf **Speichern**.

Hinzufügen einer Zugriffsregel zur IPv6-Zugriffsregeltabelle

So können Sie eine IPv6-Zugriffsregel hinzufügen oder bearbeiten:

SCHRITT 1 Klicken Sie auf die Registerkarte **IPv6**.

SCHRITT 2 Klicken Sie auf **Hinzufügen** (oder wählen Sie die Zeile aus, und klicken Sie auf **Bearbeiten**).

SCHRITT 3 Wählen Sie im Dropdown-Menü die Aktion **Zulassen** oder **Verweigern** für die Regel aus.

SCHRITT 4 Wählen Sie im Dropdown-Menü **Service** den Service aus.

SCHRITT 5 Wählen Sie im Dropdown-Menü das **Protokoll** aus.

SCHRITT 6 Wählen Sie im Dropdown-Menü die **Quellschnittstelle** aus.

SCHRITT 7 Wählen Sie im Dropdown-Menü die **Länge des Quell-IP-Präfixes** aus. Wenn Sie **Einzeln** ausgewählt haben, geben Sie das Quell-IP-Präfix ein. Wenn Sie **Bereich** ausgewählt haben, geben Sie das erste IP-Präfix und die Präfixlänge ein.

SCHRITT 8 Wählen Sie im Dropdown-Menü die **Länge des Zielpräfixes** aus. Wenn Sie **Einzeln** ausgewählt haben, geben Sie das Ziel-IP-Präfix ein. Wenn Sie **Bereich** ausgewählt haben, geben Sie das erste IP-Präfix und die Präfixlänge ein.

SCHRITT 9 Klicken Sie auf **Speichern**.

Inhaltsfilter

Mit dem Inhaltsfilter können Sie den Zugriff auf bestimmte unerwünschte Websites einschränken. Damit kann der Zugriff auf Websites basierend auf Domänennamen und Schlüsselbegriffen gesperrt werden. Es kann auch geplant werden, wann der Inhaltsfilter aktiv sein soll. Befolgen Sie die folgenden Schritte, um den Inhaltsfilter zu konfigurieren und zu aktivieren.

SCHRITT 1 Klicken Sie auf Firewall > Inhaltsfilter.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Block Forbidden Domains** (Verbotene Domänen sperren), um bestimmte Webseiten zu sperren, oder aktivieren Sie das Kontrollkästchen **Accept Allowed Domains** (Erlaubte Domänen akzeptieren), um bestimmte Webseiten zu akzeptieren.

SCHRITT 3 Aktivieren Sie im Abschnitt „Forbidden Domains“ (Verbotene Domänen) das Kontrollkästchen **Aktivieren**, um die verbotenen Domänen zu aktivieren.

SCHRITT 4 Klicken Sie in der Tabelle der verbotenen Domänen auf **Hinzufügen**, um den Domänennamen hinzuzufügen, und geben Sie den Namen der Domäne ein. Klicken Sie auf **Bearbeiten** oder **Löschen**, um eine vorhandene Domäne in der Tabelle der verbotenen Domänen zu ändern.

SCHRITT 5 Aktivieren Sie im Abschnitt „Website Blocking by Keywords“ (Websites nach Schlüsselbegriffen sperren) das Kontrollkästchen **Aktivieren**, um die Sperrung von Websites zu aktivieren.

SCHRITT 6 Klicken Sie in der Tabelle für das Sperren von Websites nach Schlüsselbegriffen auf **Hinzufügen** und geben Sie die zu sperrenden Schlüsselbegriffe ein.

SCHRITT 7 Um festzulegen, wann die Regeln für den Inhaltsfilter aktiv sein sollen, konfigurieren Sie den Zeitplan, indem Sie die Zeit aus der Dropdown-Liste auswählen. Sie können die Felder „Von“ und „Bis“ anpassen sowie den Tag für die Aktivierung des Inhaltsfilters auswählen.

SCHRITT 8 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

10

VPN

Ein VPN ist eine Verbindung zwischen zwei Endpunkten in verschiedenen Netzwerken, die es ermöglicht, persönliche Daten sicher über ein freigegebenes oder öffentliches Netzwerk wie beispielsweise das Internet zu senden. Durch diesen Tunnel wird ein privates Netzwerk eingerichtet, in dem Daten sicher und geschützt durch Verschlüsselung und Authentifizierungsmethoden entsprechend dem Industriestandard gesendet werden können.

Zusammenfassung

Mit dieser Funktion können Sie allgemeine Informationen zu den VPN-Tunneleinstellungen anzeigen. Das Gerät unterstützt bis zu 100 Tunnel. Der Bereich für virtuelle IP-Adressen ist für EasyVPN-Benutzer oder VPN-Clients reserviert, die Verbindungen mit dem Gerät herstellen und für die die Option **Moduskonfiguration** aktiviert ist (siehe Beschreibung unter **Erweiterte Einstellungen für IKE mit Pre-Shared Key und IKE mit Zertifikat**).

Zum Festlegen eines IP-Adressbereichs, der für VPN-Tunnel verwendet werden kann, klicken Sie auf **Bearbeiten**, und geben Sie die folgenden Parameter ein:

- **Bereichsanfang** und **Bereichsende**: Anfang und Ende des für VPN-Tunnel verwendeten IP-Adressbereichs
- **DNS-Server 1** und **DNS-Server 2**: Optionale IP-Adresse eines DNS-Servers. Wenn Sie einen zweiten DNS-Server eingeben, verwendet das Gerät für Antworten den ersten DNS-Server. Durch Angeben eines DNS-Servers können Sie den Zugriff im Vergleich zur Verwendung eines dynamisch zugewiesenen DNS-Servers beschleunigen. Verwenden Sie die Standardeinstellung **0.0.0.0**, um einen dynamisch zugewiesenen DNS-Server zu verwenden.
- **WINS-Server 1** und **WINS-Server 2**: Optionale IP-Adresse eines WINS-Servers. Der Windows Internet Naming Service (WINS) löst NetBIOS-Namen in IP-Adressen auf. Wenn Sie die IP-Adresse des WINS-Servers nicht kennen, verwenden Sie den Standardwert **0.0.0.0**.

- **Domänenname 1** bis **4**: Wenn der Router über eine statische IP-Adresse und einen registrierten Domänennamen verfügt (beispielsweise *MeinServer.MeineDomäne.com*), geben Sie den für die Authentifizierung zu verwendenden Wert für **Domänenname** ein. Ein Domänenname kann nur für jeweils eine Tunnelverbindung verwendet werden.

Unter **VPN-Tunnel-Status** wird die Anzahl für **Tunnel belegt**, **Tunnel verfügbar**, **Tunnel aktiviert** und **Tunnel definiert** angezeigt.

Tunnelstatus-Verbindungstabelle

In der Verbindungstabelle werden die unter **VPN >** Gateway zu Gateway und **VPN >** Client zu Gateway erstellten Einträge angezeigt:

- (Tunnel) **Nr.**: Automatisch generierte Tunnel-ID-Nummer
- (Tunnel) **Name**: Name des VPN-Tunnels, beispielsweise **Büro Los Angeles**, **Zweigstelle Chicago** oder **Abteilung New York**. Diese Beschreibung dient zu Referenzzwecken und muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.
- **Status**: Status des VPN-Tunnels, *Verbunden* oder *Waiting for Connection* (Warten Verbindung auf)
- **Phase2 – Verschl/Auth/Grp**: Verschlüsselungstyp für Phase 2 (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentifizierungsverfahren (NULL/MD5/SHA1) und DH-Gruppennummer (1/2/5)
- **Lokale Gruppe**: IP-Adresse und Subnetzmaske der lokalen Gruppe
- **Remotegruppe**: IP-Adresse und Subnetzmaske der Remote-Gruppe
- **Remote-Gateway**: IP-Adresse des Remotegateways
- **Aktion**: Status des VPN-Tunnels

Status des FlexVPN-Tunnels

In der Verbindungstabelle werden die unter VPN > **FlexVPN (Spoke)** erstellten Einträge angezeigt. Zum Hinzufügen eines Tunnels klicken Sie auf **Hinzufügen**.

- **Tunnelname**: Name des FlexVPN-Tunnels. Diese Beschreibung dient zu Referenzzwecken und muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.
- **Status**: Status des FlexVPN, „Verbunden“ oder „Warten auf Verbindung“.
- **Spoke-Netzwerk**: Subnetz von Spoke.
- **Virtuelle IP-Adresse des Spoke**: Virtuelle IP-Adresse von Spoke.

- **Hub-IP-Adresse**: IP-Adresse des Hubs.
- **Aktion**: Tunnel verbinden bzw. trennen**Hub-IP-Adresse**: IP-Adresse des Hub.

Verbindungstabelle für Gruppen-VPN-Status

In der Verbindungstabelle werden die unter **VPN > Client zu Gateway** erstellten Einträge angezeigt:

- **Gruppenname**: Name des VPN-Tunnels. Diese Beschreibung dient zu Referenzzwecken und muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.
- **Tunnel**: Anzahl der beim Gruppen-VPN angemeldeten Benutzer
- **Phase2 – Verschl/Auth/Grp**: Verschlüsselungstyp für Phase 2 (NULL/DES/3DES/AES-128/AES-192/AES-256), Authentifizierungsverfahren (NULL/MD5/SHA1) und DH-Gruppennummer (1/2/5)
- **Lokale Gruppe**: IP-Adresse und Subnetzmaske der lokalen Gruppe
- **Remoteclient**: IP-Adresse und Subnetzmaske des Remoteclients
- **Details**: IP-Adresse des Remotegateways
- **Aktion**: Status des VPN-Tunnels

Gateway zu Gateway

Bei einem standortübergreifenden oder Gateway-übergreifenden VPN stellt der lokale Router in einer Niederlassung durch einen VPN-Tunnel eine Verbindung mit einem Remote-Router her. Clientgeräte können so auf die Netzwerkressourcen zugreifen, als befänden sie sich am gleichen Standort. Dieses Modell kann für mehrere Benutzer in einer Remote-Niederlassung verwendet werden.

Damit die Verbindung erfolgreich hergestellt wird, muss mindestens einer der Router durch eine statische IP-Adresse oder einen dynamischen DNS-Hostnamen identifizierbar sein. Wenn ein Router nur über eine dynamische IP-Adresse verfügt, können Sie alternativ eine beliebige E-Mail-Adresse als Authentifizierung zum Herstellen der Verbindung verwenden.

Die beiden Enden des Tunnels können sich nicht im gleichen Subnetz befinden. Wenn beispielsweise für das LAN an Standort A das Subnetz 192.168.1.x/24 verwendet wird, kann für Standort B 192.168.2.x/24 verwendet werden.

Zum Konfigurieren eines Tunnels geben Sie beim Konfigurieren der beiden Router die entsprechenden Einstellungen ein (dabei vertauschen Sie *lokal* und *remote*). Nehmen wir an, dieser Router wird als Router A identifiziert. Geben Sie die Einstellungen für diesen Router im Abschnitt *Einrichtung der lokalen Gruppe* und die Einstellungen für den anderen Router (Router B) im Abschnitt *Remotegruppeneinrichtung* ein. Geben Sie beim Konfigurieren des anderen Routers (Router B) die zugehörigen Einstellungen im Abschnitt *Einrichtung der lokalen Gruppe* und die Einstellungen für Router A im Abschnitt *Remotegruppeneinrichtung* ein.

Hinzufügen eines neuen Tunnels

Geben Sie die Einstellungen für einen Tunnel ein:

- **Tunnelnr.**: ID-Nummer des Tunnels
- **Tunnelname**: Name des VPN-Tunnels, beispielsweise **Büro Los Angeles**, **Zweigstelle Chicago** oder **Abteilung New York**. Diese Beschreibung dient zu Referenzzwecken. Sie muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.
- **Schnittstelle**: Der für diesen Tunnel zu verwendende WAN-Anschluss
- **Schlüsselmodus**: Identifiziert die Tunnelsicherheit, **Manuell**, **IKE mit Pre-Shared Key**, **IKE mit Zertifikat**.
- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um den VPN-Tunnel zu aktivieren, oder deaktivieren Sie es, um den Tunnel zu deaktivieren. Der Tunnel ist standardmäßig aktiviert.

Einrichtung der lokalen Gruppe

Geben Sie die Einstellungen für die Einrichtung der lokalen Gruppe für diesen Router ein. (Verwenden Sie diese Einstellungen beim Konfigurieren des VPN-Tunnels im anderen Router spiegelbildlich.)

HINWEIS Alle Optionen sind dokumentiert, angezeigt werden jedoch nur die Optionen, die sich auf den ausgewählten Parameter beziehen.

Schlüsselmodus = Manuell oder IKE mit Pre-Shared Key

- **Typ des lokalen Sicherheitsgateways**: Methode zum Identifizieren des Routers, mit dem der VPN-Tunnel aufgebaut werden soll. Das lokale Sicherheits-Gateway befindet sich auf diesem Router und das Remote-Sicherheits-Gateway auf dem anderen Router. Mindestens einer der Router muss eine statische IP-Adresse oder einen DNS-Hostnamen haben, damit eine Verbindung hergestellt werden kann.
  - **Nur IP**: Dieser Router hat eine statische WAN-IP-Adresse. Die WAN-IP-Adresse wird automatisch angezeigt.
  - **IP-Adresse + Zertifikat**: Dieser Router hat eine statische WAN-IP-Adresse, die automatisch angezeigt wird. Diese Option ist nur verfügbar, wenn **IKE mit Zertifikat** ausgewählt ist.
  - **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Dieses Gerät hat eine statische IP-Adresse und einen registrierten Domänennamen, beispielsweise *MeinServer.MeineDomäne.com*. Geben Sie außerdem in **Domänenname** den für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.
  - **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieses Gerät hat eine statische IP-Adresse, und für die Authentifizierung wird eine E-Mail-Adresse verwendet. Die WAN-IP-Adresse wird automatisch angezeigt. Geben Sie die **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.
  - **Authentifizierung mit dynamischer IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine dynamische IP-Adresse und einen registrierten dynamischen DNS-Hostnamen (bei Anbietern wie DynDNS.com verfügbar). Geben Sie in **Domänenname** einen für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.

- **Authentifizierung mit dynamischer IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine dynamische IP-Adresse, aber keinen dynamischen DNS-Hostnamen. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.

  Wenn beide Router dynamische IP-Adressen haben (wie bei PPPoE-Verbindungen), wählen Sie nicht für beide Gateways die Option **Authentifizierung mit dynamischer IP-Adresse und E-Mail-Adresse** aus. Wählen Sie für das Remotegateway die Optionen **IP-Adresse** und **IP nach DNS aufgelöst** aus.

- **Typ der lokalen Sicherheitsgruppe**: Hier können Sie eine einzelne **IP**-Adresse, ein **Subnetz** oder einen **IP-Bereich** (Adressbereich) in einem Subnetz auswählen.
  - **IP-Adresse**: Geben Sie ein Gerät an, das diesen Tunnel verwenden kann. Geben Sie die **IP-Adresse** des Geräts ein.
  - **Subnetz**: Mit dieser Option lassen Sie zu, dass alle Geräte in einem Subnetz den VPN-Tunnel verwenden. Geben Sie die **IP-Adresse** des Subnetzes und die **Subnetzmaske** ein.

Remotegruppeneinrichtung

Geben Sie die Einstellungen für die Einrichtung der Remotegruppe für diesen Router ein:

- **Typ des Remote-Sicherheits-Gateways**: Methode zum Identifizieren des Routers, mit dem der VPN-Tunnel aufgebaut werden soll. Das Remote-Sicherheits-Gateway ist der andere Router. Mindestens einer der Router muss eine statische IP-Adresse oder einen dynamischen DNS-Hostnamen haben, damit eine Verbindung hergestellt werden kann.
  - **Nur IP**: Statische WAN-IP-Adresse. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den Domänennamen des Routers ein. Ein Cisco-Router kann die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.

- **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine statische IP-Adresse und einen registrierten Domänennamen, beispielsweise *MeinServer.MeineDomäne.com*. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den Domänennamen des Routers ein. Cisco-Router können die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.
- **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine statische IP-Adresse, und Sie möchten für die Authentifizierung eine E-Mail-Adresse verwenden. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die IP-Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den tatsächlichen Domänennamen des Routers ein. Cisco-Router können die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.
- **Authentifizierung mit dynamischer IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine dynamische IP-Adresse und einen registrierten dynamischen DNS-Hostnamen (bei Anbietern wie DynDNS.com verfügbar). Geben Sie in **Domänenname** einen für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.
- **Authentifizierung mit dynamischer IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine dynamische IP-Adresse, aber keinen dynamischen DNS-Hostnamen. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.
  Wenn beide Router dynamische IP-Adressen haben (wie bei PPPoE-Verbindungen), wählen Sie *nicht* für beide Gateways die Option **Authentifizierung mit dynamischer IP-Adresse und E-Mail-Adresse** aus. Wählen Sie für das Remotegateway die Option **IP-Adresse** oder **IP nach DNS aufgelöst** aus.

- **Typ der lokalen Sicherheitsgruppe**: LAN-Ressourcen, die diesen Tunnel verwenden können. Die lokale Sicherheitsgruppe gilt für die LAN-Ressourcen dieses Routers und die Remote-Sicherheitsgruppe für die LAN-Ressourcen des anderen Routers.
  - **IP-Adresse**: Geben Sie ein Gerät an, das diesen Tunnel verwenden kann. Geben Sie die **IP-Adresse** des Geräts ein.

- **Subnetz**: Mit dieser Option lassen Sie zu, dass alle Geräte in einem Subnetz den VPN-Tunnel verwenden. Geben Sie die **IP-Adresse** des Subnetzes und die **Subnetzmaske** ein.

IPSec einrichten

Voraussetzung für die erfolgreiche Verschlüsselung ist, dass sich beide Enden eines VPN-Tunnels auf das Verschlüsselungs-, Entschlüsselungs- und Authentifizierungsverfahren einigen. Geben Sie für beide Router genau die gleichen Einstellungen ein.

Geben Sie die Einstellungen für Phase 1 und Phase 2 ein. In Phase 1 werden die Pre-Shared Keys für die Erstellung eines sicheren authentifizierten Kommunikationskanals festgelegt. In Phase 2 handeln die IKE-Peers über den sicheren Kanal Sicherheitsvereinbarungen im Namen anderer Services wie beispielsweise IPSec aus. Achten Sie darauf, beim Konfigurieren des anderen Routers für diesen Tunnel die gleichen Einstellungen einzugeben.

- **Phase 1/Phase 2 – DH-Gruppe**: DH (Diffie-Hellman) ist ein Protokoll für den Schlüsselaustausch. Es gibt drei Gruppen mit unterschiedlich langen Primärschlüsseln: Gruppe 1 – 768 Bit, Gruppe 2 – 1.024 Bit und Gruppe 5 – 1.536 Bit. Eine höhere Geschwindigkeit und niedrigere Sicherheit erhalten Sie, wenn Sie **Gruppe 1** auswählen. Eine niedrigere Geschwindigkeit und höhere Sicherheit erhalten Sie, wenn Sie **Gruppe 5** auswählen. Standardmäßig ist Gruppe 1 ausgewählt.
- **Phase 1/Phase 2 – Verschlüsselung**: Verschlüsselungsmethode für diese Phase: DES, 3DES, AES-128, AES-192 oder AES-256. Von der Methode hängt die Länge des Schlüssels ab, der zum Verschlüsseln oder Entschlüsseln von ESP-Paketen verwendet wird. Aufgrund der höheren Sicherheit wird AES-256 empfohlen.
- **Phase 1/Phase 2 – Authentifizierung**: Authentifizierungsverfahren für diese Phase: MD5 oder SHA1. Vom Authentifizierungsverfahren hängt ab, wie die ESP-Header-Pakete (Encapsulating Security Payload Protocol) überprüft werden. MD5 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 128-Bit-Digest erzeugt wird. SHA1 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 160-Bit-Digest erzeugt wird. Aufgrund der höheren Sicherheit wird SHA1 empfohlen. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels das gleiche Authentifizierungsverfahren verwendet wird.
- **Phase 1/Phase 2 – SA-Gültigkeitsdauer**: Gibt an, wie lange ein VPN-Tunnel in dieser Phase aktiv ist. Der Standardwert für Phase 1 lautet **28800 Sekunden**. Der Standardwert für Phase 2 lautet **3600 Sekunden**.

- **PFS (Perfect Forward Secrecy)**: Wenn PFS (Perfect Forward Secrecy) aktiviert ist, wird bei der IKE-Aushandlung in Phase 2 neues Schlüsselmaterial für die Verschlüsselung des IP-Verkehrs generiert. Auf diese Weise können sich Hacker, die Verschlüsselungsschlüssel mit Brute-Force-Angriffen zu knacken versuchen, keine zukünftigen IPSec-Schlüssel verschaffen. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, oder deaktivieren Sie es, um die Funktion zu deaktivieren. Diese Funktion wird empfohlen.
- **Preshared Key**: Pre-Shared Key, der zum Authentifizieren des Remote-IKE-Peers verwendet werden soll. Sie können max. 30 Tastaturzeichen oder Hexadezimalwerte eingeben, beispielsweise **Mein_@123** oder **4d795f40313233** (die Zeichen ' ' " \ werden nicht unterstützt). An beiden Enden des VPN-Tunnels muss der gleiche Preshared Key verwendet werden. Es wird dringend empfohlen, den Preshared Key in regelmäßigen Abständen zu ändern, um die VPN-Sicherheit zu maximieren.
- **Minimale Preshared Key-Komplexität**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Preshared Key-Sicherheitsmessung zu aktivieren.
- **Preshared Key-Sicherheitsmessung**: Wenn Sie die Option **Minimale Preshared Key-Komplexität** aktivieren, gibt diese Messung die Sicherheit des Preshared Keys an. Beim Eingeben eines Preshared Keys werden farbige Balken angezeigt. Die Skala reicht von Rot (unsicher) über Gelb (akzeptabel) bis zu Grün (sicher).

TIPP Geben Sie einen komplexen Preshared Key ein, der mehr als acht Zeichen enthält (Groß- und Kleinbuchstaben, Ziffern und Symbole wie -*^+=).

Erweiterte Einstellungen für IKE mit Pre-Shared Key und IKE mit Zertifikat

Für die meisten Benutzer sollten die Basiseinstellungen ausreichen. Fortgeschrittene Benutzer können auf **Erweitert** klicken, um die erweiterten Einstellungen anzuzeigen. Wenn Sie die erweiterten Einstellungen in einem Router ändern, geben Sie die Einstellungen auch im anderen Router ein.

- **Aggressiver Modus**: Für die IKE-SA-Aushandlung sind zwei Modi möglich, Hauptmodus und aggressiver Modus. Wenn Sie größeren Wert auf die Netzwerksicherheit legen, wird der Hauptmodus empfohlen. Wenn Sie größeren Wert auf die Netzwerkgeschwindigkeit legen, wird der aggressive Modus empfohlen. Aktivieren Sie dieses Kontrollkästchen, um den aggressiven Modus zu aktivieren, oder deaktivieren Sie es, um den Hauptmodus zu verwenden.

  Wenn als Typ des Remote-Sicherheits-Gateways einer der Typen mit *dynamischer IP-Adresse* festgelegt ist, müssen Sie den aggressiven Modus verwenden. Das Kontrollkästchen wird automatisch aktiviert, und Sie können die Einstellung nicht ändern.

- **IP Comp-Unterstützung**: IP Comp (IP Payload Compression Protocol) ist ein Protokoll zum Reduzieren der Größe von IP-Datagrammen. Aktivieren Sie das Kontrollkästchen, damit der Router beim Initiieren einer Verbindung Kompression vorschlagen kann. Wenn der Vorschlag von der Antwortstelle verworfen wird, implementiert der Router keine Kompression. Wenn der Router die Antwortstelle ist, akzeptiert er die Kompression, auch wenn diese nicht aktiviert ist. Wenn Sie die Funktion für diesen Router aktivieren, müssen Sie sie auch für den Router am anderen Ende des Tunnels aktivieren.

- **Keep-Alive**: Es wird versucht, eine getrennte VPN-Verbindung wiederherzustellen.

- **AH-Hash-Algorithmus**: Im AH-Protokoll (Authentication Header) werden das Paketformat und die Standards für die Paketstruktur beschrieben. Wenn AH als Sicherheitsprotokoll festgelegt ist, wird der Schutz auf den IP-Header ausgeweitet, um die Integrität des gesamten Pakets zu überprüfen. Aktivieren Sie das Kontrollkästchen, um diese Funktion zu verwenden, und wählen Sie ein Authentifizierungsverfahren aus: MD5 oder SHA1. Mit MD5 wird ein 128-Bit-Digest für die Authentifizierung von Paketdaten erzeugt. Mit SHA1 wird ein 160-Bit-Digest für die Authentifizierung von Paketdaten erzeugt. Auf beiden Seiten des Tunnels muss der gleiche Algorithmus verwendet werden.

- **NetBIOS-Broadcast**: Broadcast-Nachrichten, die für die Namensauflösung in Windows-Netzwerken verwendet werden, um Ressourcen wie Computer, Drucker und Dateiserver zu identifizieren. Diese Nachrichten werden von einigen Softwareanwendungen und von Windows-Funktionen wie beispielsweise **Netzwerkumgebung** verwendet. LAN-Broadcast-Verkehr wird normalerweise nicht über einen VPN-Tunnel weitergeleitet. Sie können dieses Kontrollkästchen jedoch aktivieren, damit NetBIOS-Broadcasts von einem Ende des Tunnels an das andere Ende weitergesendet werden können.
- **NAT-Traversal**: Mithilfe des NAT-Verfahrens (Network Address Translation) können Benutzer mit privaten LAN-Adressen auf Internetressourcen zugreifen, indem sie eine öffentlich weiterleitbare IP-Adresse als Quelladresse verwenden. Für eingehenden Verkehr verfügt das NAT-Gateway jedoch über keine automatische Methode zur Umwandlung der öffentlichen IP-Adresse in ein bestimmtes Ziel im privaten LAN. Dieses Problem verhindert den erfolgreichen IPSec-Austausch. Wenn sich der VPN-Router hinter einem NAT-Gateway befindet, aktivieren Sie dieses Kontrollkästchen, um NAT-Traversal zu aktivieren. An beiden Enden des Tunnels muss die gleiche Einstellung verwendet werden.
- **Dead Peer Detection (DPD)**: Sendet in regelmäßigen Abständen HELLO-/ACK-Nachrichten, um den Status des VPN-Tunnels zu überprüfen. Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert sein. Geben Sie im Feld **Intervall** das Intervall zwischen HELLO-/ACK-Nachrichten ein.
- **Erweiterte Authentifizierung**: Zum Authentifizieren der VPN-Clients werden ein IPSec-Hostbenutzername und ein entsprechendes Kennwort oder die Benutzerdatenbanken unter **Benutzerverwaltung** verwendet. Sowohl für den IPSec-Host als auch für das Edge-Gerät muss die erweiterte Authentifizierung aktiviert sein. Wenn Sie den **IPSec-Host** verwenden möchten, klicken Sie auf das Optionsfeld, und geben Sie die Werte für **Benutzername** und **Kennwort** ein. Wenn Sie das **Edge-Gerät** verwenden möchten, klicken Sie auf das Optionsfeld, und wählen Sie im Dropdown-Menü die Datenbank aus. Zum Hinzufügen oder Bearbeiten der Datenbank klicken Sie auf **Hinzufügen/Bearbeiten**, um das Fenster **Benutzerverwaltung** anzuzeigen.

- **Tunnel-Backup**: Wenn DPD feststellt, dass der Remote-Peer nicht verfügbar ist, aktivieren Sie mit dieser Funktion, dass der Router den VPN-Tunnel mit einer alternativen IP-Adresse für den Remote-Peer oder einer alternativen WAN-Schnittstelle erneut aufbaut. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, und geben Sie die folgenden Einstellungen ein. Diese Funktion ist nur verfügbar, wenn Dead Peer Detection aktiviert ist.
  - **Remote-Sicherungs-IP-Adresse**: Geben Sie eine alternative IP-Adresse für den Remote-Peer oder erneut die bereits für das Remotegateway festgelegte WAN-IP-Adresse ein.
  - **Lokale Schnittstelle**: WAN-Schnittstelle, die zum erneuten Herstellen der Verbindung verwendet werden soll
  - **VPN-Tunnel-Backup-Leerlaufzeit**: Wenn beim Starten des Routers die Verbindung mit dem primären Tunnel nicht im angegebenen Zeitraum hergestellt wird, wird der Backup-Tunnel verwendet. Die standardmäßige Leerlaufzeit beträgt 30 Sekunden.
- **Split-DNS**: Sendet auf der Grundlage angegebener Domänennamen einen Teil der DNS-Anfragen an einen DNS-Server und andere DNS-Anfragen an einen anderen DNS-Server. Wenn der Router eine Adressauflösungsanfrage vom Client empfängt, untersucht er den Domänennamen. Wenn dieser einem der Domänennamen in den Split-DNS-Einstellungen entspricht, wird die Anfrage dem angegebenen DNS-Server übergeben. Anderenfalls wird die Anfrage dem DNS-Server übergeben, der in den WAN-Schnittstelleneinstellungen angegeben ist.

  DNS-Server 1 und **DNS-Server 2**: IP-Adresse des DNS-Servers, der für die angegebenen Domänen verwendet werden soll. Optional können Sie im Feld **DNS-Server 2** einen sekundären DNS-Server angeben.

  Domänenname 1 bis **Domänenname 4**: Geben Sie die Domänennamen für die DNS-Server an. Anfragen für diese Domänen werden den angegebenen DNS-Servern übergeben.

Client zu Gateway

Mit dieser Funktion können Sie einen neuen VPN-Tunnel erstellen, damit Telemitarbeiter und Geschäftsreisende über VPN-Clientsoftware von Drittanbietern wie beispielsweise TheGreenBow auf das Netzwerk zugreifen können.

Konfigurieren Sie einen VPN-Tunnel für einen Remote-Benutzer, ein Gruppen-VPN für mehrere Remote-Benutzer oder Easy VPN:

- **Tunnel**: Erstellt einen Tunnel für einen einzelnen Remote-Benutzer. Die Tunnelnummer wird automatisch generiert.
- **Gruppen-VPN**: Erstellt einen Tunnel für eine Gruppe von Benutzern. Das Konfigurieren einzelner Benutzer entfällt. Alle Remote-Benutzer können mit dem gleichen Preshared Key eine Verbindung mit dem Gerät herstellen (bis zur maximalen Anzahl der unterstützten Tunnel). Der Router unterstützt maximal zwei VPN-Gruppen. Die Gruppennummer wird automatisch generiert.
- **Easy VPN**: Ermöglicht Remote-Benutzern das Herstellen einer Verbindung mit diesem Gerät über das auf der Produkt-CD verfügbare Dienstprogramm Cisco VPN Client (auch unter dem Namen *Cisco Easy VPN Client* bekannt):
  - Version 5.0.07 unterstützt Windows 7 (32-Bit und 64-Bit), Windows Vista (32-Bit und 64-Bit) und Windows XP (32-Bit).
  - Version 4.9 unterstützt Mac OS X 10.4 und 10.5.
  - Version 4.8 unterstützt Linux auf Intel-Basis.

  Zum Einrichten von Easy VPN konfigurieren Sie auf dieser Seite ein Gruppenkennwort, und fügen Sie für jeden Cisco VPN Client-Benutzer in der Benutzerverwaltungstabelle im Abschnitt **Benutzerverwaltung** einen Benutzernamen und ein Kennwort hinzu. Wählen Sie beim Hinzufügen eines Benutzers die Gruppe **Unassigned** (Nicht zugewiesen) aus. Die anderen Gruppen werden für SSL-VPN verwendet.

Konfigurieren eines Tunnels oder eines Gruppen-VPNs

Geben Sie die folgenden Informationen ein:

- **Tunnelname**: Name zur Beschreibung des Tunnels. Bei einem einzelnen Benutzer können Sie den Benutzernamen oder den Standort eingeben. Bei einem Gruppen-VPN können Sie die geschäftliche Rolle der Gruppe oder den Standort angeben. Diese Beschreibung dient zu Referenzzwecken und muss nicht mit dem Namen übereinstimmen, der am anderen Ende des Tunnels verwendet wird.
- **Schnittstelle**: WAN-Anschluss
- **Schlüsselmodus**: Wählen Sie die Schlüsselverwaltungsmethode aus:
  - **Manuell**: Sie generieren den Schlüssel selbst, ohne die Schlüsselaushandlung zu aktivieren. Die manuelle Schlüsselverwaltung wird in kleinen, statischen Umgebungen oder für die Fehlerbehebung verwendet. Geben Sie die erforderlichen Einstellungen ein.
  - **IKE** (Internet Key Exchange) **mit Preshared Key**: Dieses Protokoll wird verwendet, um eine Sicherheitsvereinbarung (Security Association, SA) für den Tunnel einzurichten. (Diese Einstellung wird empfohlen.) Wenn Sie **Gruppen-VPN** ausgewählt haben, ist dies die einzige verfügbare Option.
  - **IKE mit Zertifikat**: Verwenden Sie ein Zertifikat, um einen Remote-IKE-Peer zu authentifizieren.
- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um das VPN zu aktivieren.

Einrichtung der lokalen Gruppe

Geben Sie die folgenden Informationen ein:

- **Typ des lokalen Sicherheitsgateways**: Methode zum Identifizieren des Routers, mit dem der VPN-Tunnel aufgebaut werden soll. Das Remote-Sicherheits-Gateway ist der andere Router. Mindestens einer der Router muss eine statische IP-Adresse oder einen dynamischen DNS-Hostnamen haben, damit eine Verbindung hergestellt werden kann.
  - **Nur IP**: Statische WAN-IP-Adresse. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den Domänennamen des Routers ein. Ein Cisco-Router kann die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.

- **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Dieses Gerät hat eine statische IP-Adresse und einen registrierten Domänennamen, beispielsweise *MeinServer.MeineDomäne.com*. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den Domänennamen des Routers ein. Cisco-Router können die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.
- **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieses Gerät hat eine statische IP-Adresse, und für die Authentifizierung wird eine E-Mail-Adresse verwendet. Wenn Sie die IP-Adresse des Remote-VPN-Routers kennen, wählen Sie **IP-Adresse** aus, und geben Sie die IP-Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Routers nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den tatsächlichen Domänennamen des Routers ein. Cisco-Router können die IP-Adresse eines Remote-VPN-Geräts nach der DNS-Auflösung abrufen.
- **Authentifizierung mit dynamischer IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine dynamische IP-Adresse und einen registrierten dynamischen DNS-Hostnamen (bei Anbietern wie DynDNS.com verfügbar). Geben Sie in **Domänenname** einen für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.
- **Authentifizierung mit dynamischer IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine dynamische IP-Adresse, aber keinen dynamischen DNS-Hostnamen. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.

  Wenn beide Router dynamische IP-Adressen haben (wie bei PPPoE-Verbindungen), wählen Sie nicht für beide Gateways die Option **Authentifizierung mit dynamischer IP-Adresse und E-Mail-Adresse** aus. Wählen Sie für das Remotegateway die Optionen **IP-Adresse** und **IP nach DNS aufgelöst** aus.

- **Typ der lokalen Sicherheitsgruppe** : Geben Sie die LAN-Ressourcen an, die auf diesen Tunnel zugreifen können.
  - **IP-Adresse**: Wählen Sie diese Option aus, damit nur ein einziges LAN-Gerät auf den VPN-Tunnel zugreifen kann. Geben Sie dann die IP-Adresse des Computers ein. Nur dieses Gerät kann den VPN-Tunnel verwenden.
  - **Subnetz**: Wählen Sie diese Option (die Standardoption) aus, damit alle Geräte in einem Subnetz auf den VPN-Tunnel zugreifen können. Geben Sie dann die IP-Adresse des Subnetzes und die Subnetzmaske ein.

Remoteclienteinrichtung für einen einzelnen Benutzer

Geben Sie die Methode an, mit der der Client beim Aufbauen des VPN-Tunnels identifiziert werden soll. Die folgenden Optionen stehen für einen einzelnen Benutzer oder *Tunnel*typ oder ein VPN zur Verfügung:

- **Nur IP**: Der Remote-VPN-Client hat eine statische WAN-IP-Adresse. Wenn Sie die IP-Adresse des Clients kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Clients nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den Domänennamen des Clients im Internet ein. Der Router ruft die IP-Adresse des Remote-VPN-Clients nach DNS aufgelöst ab, und diese IP-Adresse wird auf der Seite **Zusammenfassung** im Abschnitt **VPN-Status** angezeigt.
- **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Der Client hat eine statische IP-Adresse und einen registrierten Domänennamen. Geben Sie außerdem in **Domänenname** einen für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzige Tunnelverbindung verwendet werden.

  Wenn Sie die IP-Adresse des Remote-VPN-Clients kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Clients nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den tatsächlichen Domänennamen des Clients im Internet ein. Der Router ruft die IP-Adresse des Remote-VPN-Clients nach DNS aufgelöst ab, und diese IP-Adresse wird auf der Seite **Zusammenfassung** im Abschnitt **VPN-Status** angezeigt.
- **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Der Client hat eine statische IP-Adresse, und Sie möchten für die Authentifizierung eine E-Mail-Adresse verwenden. Die aktuelle WAN-IP-Adresse wird automatisch angezeigt. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.

Wenn Sie die IP-Adresse des Remote-VPN-Clients kennen, wählen Sie **IP-Adresse** aus, und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Remote-VPN-Clients nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus, und geben Sie den tatsächlichen Domänennamen des Clients im Internet ein. Das Gerät ruft die IP-Adresse eines Remote-VPN-Clients nach DNS aufgelöst ab, und die IP-Adresse des Remote-VPN-Geräts wird auf der Seite **Zusammenfassung** im Abschnitt **VPN-Status** angezeigt.

- **Authentifizierung mit dynamischer IP-Adresse + Domänenname (FQDN)**: Der Client hat eine dynamische IP-Adresse und einen registrierten dynamischen DNS-Hostnamen (bei Anbietern wie DynDNS.com verfügbar). Geben Sie in **Domänenname** den für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.
- **Authentifizierung mit dynamischer IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Der Client hat eine dynamische IP-Adresse, aber keinen dynamischen DNS-Hostnamen. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.

Remoteclienteinrichtung für eine Gruppe

Geben Sie die Methode an, mit der die Clients beim Aufbauen des VPN-Tunnels identifiziert werden sollen. Die folgenden Optionen stehen für ein Gruppen-VPN zur Verfügung:

- **Authentifizierung mit Domänenname (FQDN)**: Identifiziert den Client anhand eines registrierten Domänennamens. Geben Sie in **Domänenname** einen für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzige Tunnelverbindung verwendet werden.
- **Authentifizierung mit E-Mail-Adresse (USER-FQDN)**: Identifiziert den Client anhand einer E-Mail-Adresse für die Authentifizierung. Geben Sie die Adresse in die angezeigten Felder ein.
- **Microsoft XP-/2000-VPN-Client**: Als Clientsoftware wird der integrierte VPN-Client für Microsoft XP/2000 verwendet.

IPSec-Einrichtung

Voraussetzung für die erfolgreiche Verschlüsselung ist, dass sich beide Enden eines VPN-Tunnels auf das Verschlüsselungs-, Entschlüsselungs- und Authentifizierungsverfahren einigen. Geben Sie für beide Router genau die gleichen Einstellungen ein.

Geben Sie die Einstellungen für Phase 1 und Phase 2 ein. In Phase 1 werden die Pre-Shared Keys für die Erstellung eines sicheren authentifizierten Kommunikationskanals festgelegt. In Phase 2 verwenden die IKE-Peers den sicheren Kanal zum Aushandeln von Sicherheitsvereinbarungen für andere Services wie beispielsweise IPSec. Achten Sie darauf, beim Konfigurieren anderer Router für diesen Tunnel die gleichen Einstellungen einzugeben.

- **Phase 1/Phase 2 – DH-Gruppe**: DH (Diffie-Hellman) ist ein Protokoll für den Schlüsselaustausch. Es gibt drei Gruppen mit unterschiedlich langen Primärschlüsseln: Gruppe 1 – 768 Bit, Gruppe 2 – 1.024 Bit und Gruppe 5 – 1.536 Bit. Eine höhere Geschwindigkeit und niedrigere Sicherheit erhalten Sie, wenn Sie **Gruppe 1** auswählen. Eine niedrigere Geschwindigkeit und höhere Sicherheit erhalten Sie, wenn Sie **Gruppe 5** auswählen. Standardmäßig ist Gruppe 1 ausgewählt.
- **Phase 1/Phase 2 – Verschlüsselung**: Verschlüsselungsmethode für diese Phase: DES, 3DES, AES-128, AES-192 oder AES-256. Von der Methode hängt die Länge des Schlüssels ab, der zum Verschlüsseln oder Entschlüsseln von ESP-Paketen verwendet wird. Aufgrund der höheren Sicherheit wird AES-256 empfohlen.
- **Phase 1/Phase 2 – Authentifizierung**: Authentifizierungsverfahren für diese Phase: MD5 oder SHA1. Vom Authentifizierungsverfahren hängt ab, wie die ESP-Header-Pakete (Encapsulating Security Payload Protocol) überprüft werden. MD5 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 128-Bit-Digest erzeugt wird. SHA1 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 160-Bit-Digest erzeugt wird. Aufgrund der höheren Sicherheit wird SHA1 empfohlen. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels das gleiche Authentifizierungsverfahren verwendet wird.
- **Phase 1/Phase 2 – SA-Gültigkeitsdauer**: Gibt an, wie lange ein VPN-Tunnel in dieser Phase aktiv ist. Der Standardwert für Phase 1 lautet **28800 Sekunden**. Der Standardwert für Phase 2 lautet **3600 Sekunden**.

- **PFS (Perfect Forward Secrecy)**: Wenn PFS (Perfect Forward Secrecy) aktiviert ist, wird bei der IKE-Aushandlung in Phase 2 neues Schlüsselmaterial für die Verschlüsselung des IP-Verkehrs generiert. Auf diese Weise können sich Hacker, die Verschlüsselungsschlüssel mit Brute-Force-Angriffen zu knacken versuchen, keine zukünftigen IPSec-Schlüssel verschaffen. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, oder deaktivieren Sie es, um die Funktion zu deaktivieren. Diese Funktion wird empfohlen.
- **Minimale Preshared Key-Komplexität**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Preshared Key-Sicherheitsmessung zu aktivieren.
- **Preshared Key**: Pre-Shared Key, der zum Authentifizieren des Remote-IKE-Peers verwendet werden soll. Sie können max. 30 Tastaturzeichen oder Hexadezimalwerte eingeben, beispielsweise **Mein_@123** oder **4d795f40313233**. An beiden Enden des VPN-Tunnels muss der gleiche Preshared Key verwendet werden. Es wird empfohlen, den Preshared Key in regelmäßigen Abständen zu ändern, um die VPN-Sicherheit zu maximieren.
- **Preshared Key-Sicherheitsmessung**: Wenn Sie die Option **Minimale Preshared Key-Komplexität** aktivieren, gibt diese Messung die Sicherheit des Preshared Keys an. Beim Eingeben eines Preshared Keys werden farbige Balken angezeigt. Die Skala reicht von Rot (unsicher) über Gelb (akzeptabel) bis zu Grün (sicher).

TIPP Geben Sie einen komplexen Preshared Key ein, der mehr als acht Zeichen enthält (Groß- und Kleinbuchstaben, Ziffern und Symbole wie -*^+=, die Zeichen ' ' " \ werden nicht unterstützt).

Erweiterte Einstellungen für IKE mit Pre-Shared Key und IKE mit Zertifikat

Für die meisten Benutzer sollten die Basiseinstellungen ausreichen. Fortgeschrittene Benutzer können auf **Erweitert** klicken, um die erweiterten Einstellungen anzuzeigen. Wenn Sie die erweiterten Einstellungen in einem Router ändern, geben Sie die Einstellungen auch im anderen Router ein.

- **Aggressiver Modus**: Für die IKE-SA-Aushandlung sind zwei Modi möglich: Hauptmodus und aggressiver Modus. Wenn Sie größeren Wert auf die Netzwerksicherheit legen, wird der Hauptmodus empfohlen. Wenn Sie größeren Wert auf die Netzwerkgeschwindigkeit legen, wird der aggressive Modus empfohlen. Aktivieren Sie dieses Kontrollkästchen, um den aggressiven Modus zu aktivieren, oder deaktivieren Sie es, um den Hauptmodus zu verwenden.
  Wenn als **Typ des Remote-Sicherheits-Gateways** einer der Typen mit *dynamischer IP-Adresse* festgelegt ist, müssen Sie den aggressiven Modus verwenden. Das Kontrollkästchen wird automatisch aktiviert, und Sie können die Einstellung nicht ändern.

- **Komprimieren (IPComp, IP Payload Compression Protocol, unterstützen)**: Ein Protokoll zum Reduzieren der Größe von IP-Datagrammen. Aktivieren Sie das Kontrollkästchen, damit der Router beim Initiieren einer Verbindung Kompression vorschlagen kann. Wenn der Vorschlag von der Antwortstelle verworfen wird, implementiert der Router keine Kompression. Wenn der Router die Antwortstelle ist, akzeptiert er die Kompression, auch wenn diese nicht aktiviert ist. Wenn Sie die Funktion für diesen Router aktivieren, müssen Sie sie auch für den Router am anderen Ende des Tunnels aktivieren.

- **Keep-Alive**: Es wird versucht, eine getrennte VPN-Verbindung wiederherzustellen.

- **AH-Hash-Algorithmus**: Im AH-Protokoll (Authentication Header) werden das Paketformat und die Standards für die Paketstruktur beschrieben. Wenn AH als Sicherheitsprotokoll festgelegt ist, wird der Schutz auf den IP-Header ausgeweitet, um die Integrität des gesamten Pakets zu überprüfen. Aktivieren Sie das Kontrollkästchen, um diese Funktion zu verwenden, und wählen Sie ein Authentifizierungsverfahren aus: MD5 oder SHA1. Mit MD5 wird ein 128-Bit-Digest für die Authentifizierung von Paketdaten erzeugt. Mit SHA1 wird ein 160-Bit-Digest für die Authentifizierung von Paketdaten erzeugt. Auf beiden Seiten des Tunnels muss der gleiche Algorithmus verwendet werden.

- **NetBIOS-Broadcast**: Broadcast-Nachrichten, die für die Namensauflösung in Windows-Netzwerken verwendet werden, um Ressourcen wie Computer, Drucker und Dateiserver zu identifizieren. Diese Nachrichten werden von einigen Softwareanwendungen und von Windows-Funktionen wie beispielsweise **Netzwerkumgebung** verwendet. LAN-Broadcast-Verkehr wird normalerweise nicht über einen VPN-Tunnel weitergeleitet. Sie können dieses Kontrollkästchen jedoch aktivieren, damit NetBIOS-Broadcasts von einem Ende des Tunnels an das andere Ende weitergesendet werden können.
- **NAT-Traversal**: Mithilfe des NAT-Verfahrens (Network Address Translation) können Benutzer mit privaten LAN-Adressen auf Internetressourcen zugreifen, indem sie eine öffentlich weiterleitbare IP-Adresse als Quelladresse verwenden. Für eingehenden Verkehr verfügt das NAT-Gateway jedoch über keine automatische Methode zur Umwandlung der öffentlichen IP-Adresse in ein bestimmtes Ziel im privaten LAN. Dieses Problem verhindert den erfolgreichen IPSec-Austausch. Wenn sich der VPN-Router hinter einem NAT-Gateway befindet, aktivieren Sie dieses Kontrollkästchen, um NAT-Traversal zu aktivieren. An beiden Enden des Tunnels muss die gleiche Einstellung verwendet werden.
- **Dead Peer Detection Interval** (Intervall für Dead Peer Detection): eine Methode zum Erkennen inaktiver Internet Key Exchange (IKE-)Peers. Diese Methode nutzt IPsec-Datenverkehrsmuster, um die Zahl der Nachrichten zu minimieren. Das Mindest-Prüfintervall der VPN Dead Peer Detection beträgt 10 Sekunden.
- **Erweiterte Authentifizierung**: Hier können Sie zusätzlich zu einem Preshared Key oder Zertifikat einen Benutzernamen und ein Kennwort für die Authentifizierung eingehender IPSec-Tunnelanfragen angeben.
  - **IPSec-Host**: Gibt an, dass ein **IPSec-Host** für die erweiterte Authentifizierung verwendet wird.
    Benutzername: Benutzername für die Authentifizierung
    Kennwort: Authentifizierungskennwort
  - **Edge-Gerät**: Stellt dem eingehenden Tunnelanfrager (nach der Authentifizierung) eine IP-Adresse aus dem im Fenster **Zusammenfassung** konfigurierten virtuellen IP-Bereich. Wählen Sie im Dropdown-Menü das Gerät aus. Zum Hinzufügen oder Bearbeiten der Domäne des Geräts klicken Sie auf **Hinzufügen/Bearbeiten**, um das Fenster **Benutzerverwaltung** anzuzeigen.
- **Moduskonfiguration**: Stellt dem eingehenden Tunnelanfrager (nach der Authentifizierung) eine IP-Adresse aus dem im Fenster **VPN > Zusammenfassung** konfigurierten virtuellen IP-Bereich.

FlexVPN (Spoke)

FlexVPN nutzt die auf offenen Standards basierende Sicherheitstechnologie IKEv2 und bietet ein hohes Sicherheitsniveau. FlexVPN wurde zur Vereinfachung der Bereitstellung von VPNs und zur Behebung der Komplexität von verschiedenen Lösungen entwickelt. Als einheitliches Partnernetzwerk deckt es alle Arten von VPN ab: Remote-Zugriff, Telearbeiter, Site-to-Site, Mobilität, Managed Security Services und weitere.

Hinzufügen eines neuen FlexVPN-TunnelsReferenzzwecken.

Konfigurieren Sie Folgendes, um einen neuen Tunnel hinzuzufügen:

- **Tunnelname**: Geben Sie einen Namen für den FlexVPN-Tunnel ein.
- **Schnittstelle**: Wählen Sie aus der Dropdown-Liste den WAN-Port aus, der für diesen Tunnel verwendet werden soll.
- **Aktivieren**: Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, um den Tunnel zu aktivieren bzw. zu deaktivieren. Der FlexVPN-Tunnel ist standardmäßig aktiviert

Einrichten von Spoke

Geben Sie die Einstellungen für die Einrichtung von Spoke für diesen Router ein:

- **Typ des Spoke-Sicherheits-Gateways**: Wählen Sie aus der Dropdown-Liste eine Option zum Identifizieren des Routers aus, mit dem der FlexVPN-Tunnel aufgebaut werden soll.
  - **Nur IP**: Dieser Router hat eine statische WAN-IP-Adresse. Die WAN-IP-Adresse wird automatisch angezeigt.
  - **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Dieses Gerät hat eine statische IP-Adresse und einen registrierten Domänennamen, beispielsweise MeinServer.MeineDomäne.com. Geben Sie außerdem in **Domänenname** den für die Authentifizierung zu verwendenden Domänennamen ein. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.
  - **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER FQDN)**: Dieses Gerät hat eine statische IP-Adresse und für die Authentifizierung wird eine E-Mail-Adresse verwendet. Die WAN-IP-Adresse wird automatisch angezeigt. Geben Sie die **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.

- **Authentifizierung mit dynamischer IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine dynamische IP-Adresse und einen registrierten dynamischen DNS-Hostnamen (bei Anbietern wie DynDNS.com verfügbar). Geben Sie unter **Domänenname** einen Domänennamen ein, der für die Authentifizierung verwendet werden soll. Der Domänenname kann nur für eine einzelne Tunnelverbindung verwendet werden.

- **Authentifizierung mit dynamischer IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine dynamische IP-Adresse, aber keinen dynamischen DNS-Hostnamen. Geben Sie eine **E-Mail-Adresse** ein, die für die Authentifizierung verwendet werden soll.
- **Domänenname**: Geben Sie einen Domänennamen ein.
- **GRE-IP-Adresse**: IP-Adresse der virtuellen Schnittstelle (GRE).
- **Vom Hub beziehen**: Vom Hub zugewiesene IP-Adresse der GRE.
- **Statisch konfigurieren**: Die IP-Adresse der GRE ist manuell konfiguriert.
- **Minimale Preshared Key-Komplexität**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Preshared Key-Sicherheitsmessung zu aktivieren.
- **Preshared Key**: Preshared Key, der zum Authentifizieren des Spoke-IKE verwendet werden soll. Sie können max. 30 Tastaturzeichen oder Hexadezimalwerte eingeben, beispielsweise „Mein_@123“ oder „4d795f40313233“ (die Zeichen ' ' " \ werden nicht unterstützt). An beiden Enden des FlexVPN-Tunnels muss der gleiche Preshared Key verwendet werden. Es wird dringend empfohlen, den Preshared Key in regelmäßigen Abständen zu ändern, um die FlexVPN-Sicherheit zu maximieren.
- **Preshared Key-Sicherheitsmessung**: Wenn Sie die Option „Minimale Preshared Key-Komplexität“ aktivieren, gibt diese Messung die Sicherheit des Preshared Keys an. Beim Eingeben eines Preshared Keys werden farbige Balken angezeigt. Die Skala reicht von Rot (unsicher) über Gelb (akzeptabel) bis zu Grün (sicher).

Spoke-Netzwerk

Das Spoke-Netzwerk erlaubt allen Geräten im Spoke-Netzwerk die Nutzung des FlexVPN-Tunnels. Um ein neues Spoke-Netzwerk hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie die IP-Adresse des Subnetzwerks und die Subnetzmaske ein.

Einrichtung des Hubs

Geben Sie die Einstellungen für die Einrichtung des Hubs für diesen Router ein:

- **Typ des Hub-Sicherheits-Gateways**: Methode zum Identifizieren des Routers, mit dem das FlexVPN aufgebaut werden soll. Wählen Sie eine der folgenden Optionen aus:
  - **Nur IP**: Statische WAN-IP-Adresse. Wenn Sie die IP-Adresse des Hubs kennen, wählen Sie **IP-Adresse** aus und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Hubs nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus und geben Sie den Domänennamen des Routers ein. Ein Cisco Router kann die IP-Adresse des Hubs nach der DNS-Auflösung abrufen. Einrichtung des Hub.
  - **Authentifizierung mit IP-Adresse + Domänenname (FQDN)**: Dieser Router hat eine statische IP-Adresse und einen registrierten Domänennamen, beispielsweise MeinServer. MeineDomäne.com. Wenn Sie die IP-Adresse des Hubs kennen, wählen Sie **IP-Adresse** aus und geben Sie die Adresse ein. Wenn Sie die IP-Adresse des Hubs nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus und geben Sie den Domänennamen des Routers ein. Cisco Router können die IP-Adresse des Hubs nach der DNS-Auflösung abrufen.
  - **Authentifizierung mit IP-Adresse + E-Mail-Adresse (USER-FQDN)**: Dieser Router hat eine statische IP-Adresse und Sie möchten für die Authentifizierung eine E-Mail-Adresse verwenden. Wenn Sie die IP-Adresse des Hubs kennen, wählen Sie **IP-Adresse** aus und geben Sie die IP-Adresse ein. Wenn Sie die IP-Adresse des Hubs nicht kennen, wählen Sie **IP nach DNS aufgelöst** aus und geben Sie den echten Domänennamen des Routers ein. Cisco Router können die IP-Adresse des Hubs nach der DNS-Auflösung abrufen.
- **Minimale Preshared Key-Komplexität**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Preshared Key-Sicherheitsmessung zu aktivieren.
- **Preshared Key**: Preshared Key, der zum Authentifizieren des Hub-IKE verwendet werden soll. Sie können max. 30 Tastaturzeichen oder Hexadezimalwerte eingeben, beispielsweise „Mein_@123“ oder „4d795f40313233“ (die Zeichen ' ' " \ werden nicht unterstützt). An beiden Enden des FlexVPN-Tunnels muss der gleiche Preshared Key verwendet werden. Es wird ausdrücklich empfohlen, den Preshared Key in regelmäßigen Abständen zu ändern, um die FlexVPN-Sicherheit zu maximieren.
- **Preshared Key-Sicherheitsmessung**: Wenn die Option „Minimale Preshared Key-Komplexität“ aktiviert ist, gibt diese Messung die Sicherheit des Preshared Keys an. Beim Eingeben eines Preshared Keys werden farbige Balken angezeigt. Die Skala reicht von Rot (unsicher) über Gelb (akzeptabel) bis zu Grün (sicher).

IPSec einrichten

Voraussetzung für die erfolgreiche Verschlüsselung ist, dass sich beide Enden eines FlexVPN-Tunnels auf das Verschlüsselungs-, Entschlüsselungs- und Authentifizierungsverfahren einigen. Geben Sie für beide Router genau die gleichen Einstellungen ein.

Geben Sie die Einstellungen für Phase 1 und Phase 2 ein. In Phase 1 werden die Preshared Keys für den Aufbau eines sicheren authentifizierten Kommunikationskanals festgelegt. In Phase 2 verhandeln die IKE-Peers über den sicheren Kanal Sicherheitsvereinbarungen im Namen anderer Services wie beispielsweise IPSec. Achten Sie darauf, beim Konfigurieren des anderen Routers für diesen Tunnel die gleichen Einstellungen einzugeben.

- **Phase 1/Phase 2 – DH-Gruppe**: DH (Diffie-Hellman) ist ein Protokoll für den Schlüsselaustausch. Es gibt drei Gruppen mit unterschiedlich langen Primärschlüsseln: Gruppe 1 – 768 Bit, Gruppe 2 – 1.024 Bit und Gruppe 5 – 1.536 Bit. Eine höhere Geschwindigkeit und niedrigere Sicherheit erhalten Sie, wenn Sie **Gruppe 1** auswählen. Eine niedrigere Geschwindigkeit und höhere Sicherheit erhalten Sie, wenn Sie Gruppe 5 auswählen. Standardmäßig ist Gruppe 2 ausgewählt.

FlexVPN (Spoke)

- **Phase 1/Phase 2 – Verschlüsselung**: Verschlüsselungsmethode für diese Phase: DES, 3DES, AES-128, AES-192 oder AES-256. Mit der Methode wird die Länge des Schlüssels zum Verschlüsseln/Entschlüsseln von ESP-Paketen bestimmt. Aufgrund der höheren Sicherheit wird AES-256 empfohlen.
- **Phase 1/Phase 2 – Authentifizierung**: Authentifizierungsverfahren für diese Phase: MD5 oder SHA1. Vom Authentifizierungsverfahren hängt ab, wie die ESP-Header-Pakete (Encapsulating Security Payload Protocol) überprüft werden. MD5 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 128-Bit-Digest erzeugt wird. SHA1 ist ein unidirektionaler Hash-Algorithmus, mit dem ein 160-Bit-Digest erzeugt wird. Aufgrund der höheren Sicherheit wird SHA1 empfohlen. Stellen Sie sicher, dass an beiden Enden des VPN-Tunnels das gleiche Authentifizierungs-verfahren verwendet wird.
- **Phase 1/Phase 2 – SA-Gültigkeitsdauer**: Gibt an, wie lange ein VPN-Tunnel in dieser Phase aktiv ist. Der Standardwert für Phase 1 lautet „28800 Sekunden“. Der Standardwert für Phase 2 lautet „3600 Sekunden“.

Erweiterte Einrichtung

Für die meisten Benutzer reichen die Standardeinstellungen aus. Wenn Sie die erweiterten Einstellungen in einem Router ändern, nehmen Sie dieselben Änderungen auch im anderen Router vor.

- **Keep-Alive**: Es wird versucht, eine getrennte VPN-Verbindung wiederherzustellen.
- **Dead Peer Detection (DPD)**: Sendet in regelmäßigen Abständen HELLO-/ACK-Nachrichten, um den Status des FlexVPN-Tunnels zu überprüfen. Geben Sie in das Feld **Intervall** das Intervall zwischen HELLO-/ACK-Nachrichten ein.
- **Tunnel-Backup**: Wenn DPD feststellt, dass der Remote-Peer nicht verfügbar ist, aktivieren Sie mit dieser Funktion, dass der Router den FlexVPN-Tunnel mit einer alternativen IP-Adresse für den Remote-Peer oder einer alternativen WAN-Schnittstelle erneut aufbaut. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, und geben Sie die folgenden Einstellungen ein. Diese Funktion ist nur verfügbar, wenn Dead Peer Detection aktiviert ist.
  - **Hub-IP-Adresse**: Alternative IP-Adresse für den Remote-Peer. Alternativ können Sie die WAN-IP-Adresse, die bereits für das Remote-Gateway festgelegt wurde, erneut eingeben.
  - **Spoke-Schnittstelle**: WAN-Schnittstelle, die zum erneuten Herstellen der Verbindung verwendet werden soll.
  - **VPN-Tunnel-Backup-Leerlaufzeit**: Wenn beim Starten des Routers die Verbindung mit dem primären Tunnel nicht im angegebenen Zeitraum hergestellt wird, wird der Backup-Tunnel verwendet. Die standardmäßige Leerlaufzeit beträgt 30 Sekunden.
- **PFS (Perfect Forward Secrecy)**: Wenn PFS (Perfect Forward Secrecy) aktiviert ist, wird bei der IKE-Aushandlung in Phase 2 neues Schlüsselmaterial für die Verschlüsselung des IP-Verkehrs generiert. Auf diese Weise können sich Hacker, die Verschlüsselungsschlüssel mit Brute-Force-Angriffen zu knacken versuchen, keine zukünftigen IPSec-Schlüssel verschaffen. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren, oder deaktivieren Sie es, um die Funktion zu deaktivieren. Diese Funktion wird empfohlen.

VPN-Passthrough

Mit VPN-Passthrough können VPN-Clients den Router passieren und eine Verbindung mit einem VPN-Endpunkt herstellen. Die Funktion ist standardmäßig aktiviert.

Zum Aktivieren von VPN-Passthrough aktivieren Sie das Kontrollkästchen **Aktivieren** für die zulässigen Protokolle:

- **IPSec-Passthrough**: IPSec (Internet Protocol Security) ist eine Protokollsuite zur Implementierung des sicheren Austauschs in der IP-Schicht.
- **PPTP-Passthrough**: PPTP (Point-to-Point Tunneling Protocol) ermöglicht das Tunneln des Point-to-Point-Protokolls (PPP) durch ein IP-Netzwerk.
- **L2TP-Passthrough**: Das Layer 2 Tunneling-Protokoll wird als Methode zum Aktivieren von Point-to-Point-Sitzungen über das Internet in Layer 2 verwendet.

PPTP-Server

Sie können für Benutzer, die PPTP-Clientsoftware ausführen, max. zehn PPTP-VPN-Tunnel (Point-to-Point Tunneling-Protokoll) aktivieren. Beispiel: Ein Benutzer öffnet in Windows XP oder Windows 2000 die Systemsteuerungsoption **Netzwerkverbindungen** und erstellt eine neue Verbindung. Der Benutzer wählt im Assistenten die Option zum Erstellen einer Verbindung mit dem Arbeitsplatz aus und verwendet eine VPN-Verbindung. Der Benutzer muss die WAN-IP-Adresse dieses Geräts kennen. Weitere Informationen finden Sie in der Dokumentation oder den Hilfedateien des Betriebssystems.

Zum Aktivieren des PPTP-Servers und zum Zulassen von VPN-Tunneln aktivieren Sie das Kontrollkästchen **Aktivieren**, und geben Sie den Bereich ein:

Bereichsanfang und **Bereichsende**: LAN-Adressbereich, der den PPTP-VPN-Clients zugewiesen werden soll. Der LAN-IP-Adressbereich für PPTP-VPN-Clients sollte außerhalb des normalen DHCP-Bereichs des Routers liegen.

Der **Status des PPTP-Tunnels** zeigt die Menge der **belegten Tunnel** und die Menge der **verfügbaren Tunnel.**

In der **Verbindungstabelle** werden die verwendeten Tunnel angezeigt.

11

OpenVPN

OpenVPN ist eine VPN-Technologie (Virtual Private Network) für den Aufbau sicherer Point-to-Point- oder Site-to-Site-Verbindungen in Konfigurationen mit Routern oder Bridges und Einrichtungen mit Remote-Zugriff. Sie verwendet ein benutzerdefiniertes Sicherheitsprotokoll, das SSL/TLS für den Schlüsselaustausch einsetzt.

OpenVPN ermöglicht den Peers, sich gegenseitig mithilfe von Benutzername und Kennwort oder von Zertifikaten zu authentifizieren. Bei Verwendung in einer Multiclient-Serverkonfiguration kann der Server damit ein Authentifizierungszertifikat für jeden Client mit Signatur und Zertifizierungsstelle ausgebenu.

Zusammenfassung

Mit dieser Funktion können Sie allgemeine Informationen zu den OpenVPN-Tunneleinstellungen anzeigen. Das Gerät unterstützt bis zu 50 OpenVPN-Konten.

Unter **OpenVPN-Tunnelnummer** wird die Anzahl der **belegten Tunnel**, **verfügbaren Tunnel**, **aktivierten Tunnel** und **definierten Tunnel** angezeigt.

Servereinstellungstabelle

In der Servereinstellungstabelle werden die unter **OpenVPN** > **OpenVPN** erstellten Einträge angezeigt. **Server**

- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um den OpenVPN-Server zu aktivieren, oder deaktivieren Sie es, um den OpenVPN-Server zu deaktivieren.
- **Authentifizierung**: Kennwort oder Kennwort + Zertifikat.
- **Protokoll**: Benötigtes Protokoll und Port-Nummer.

- **Verschlüsselung**: Verschlüsselungsmethode für diese Phase: NULL, DES, 3DES, AES128, AES-192 oder AES-256. Mit der Methode wird die Länge des Schlüssels zum Verschlüsseln/Entschlüsseln von Paketen bestimmt.
- **Client-Adresspool**: Stellt die IP-Adresse des Clients aus diesem Pool bereit.

OpenVPN-Server

Status der OpenVPN-Konto-ID

In der Konto-ID-Einstellungstabelle werden die unter **OpenVPN > OpenVPN-Konto** erstellten Einträge angezeigt. Klicken Sie auf **Hinzufügen**, um ein OpenVPN-Konto hinzuzufügen.

- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um ein bestehendes OpenVPN-Konto zu aktivieren, oder deaktivieren Sie es, um das OpenVPN-Konto zu deaktivieren.

Ermöglicht Managern, die Einstellungen des OpenVPN-Servers hinzuzufügen oder zu ändern.

Zum Hinzufügen eines OpenVPN-Servers geben Sie die folgenden Einstellungen ein und klicken Sie auf **Speichern**.

Basiseinrichtung

- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um den OpenVPN-Server zu aktivieren, oder deaktivieren Sie es, um den OpenVPN-Server zu deaktivieren.

OpenVPN-Konto

Ermöglicht Managern, die Benutzer des OpenVPN-Servers hinzuzufügen oder zu ändern.

Zum Hinzufügen eines OpenVPN-Kontos geben Sie die folgenden Einstellungen ein und klicken Sie auf **Speichern**.

- **Aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um das OpenVPN-Konto zu aktivieren, oder deaktivieren Sie es, um das OpenVPN-Konto zu deaktivieren.
- **Authentifizierung**: Kennwort.
  - **OpenVPN-Server**: Name oder IP-Adresse des OpenVPN-Servers.

- **Benutzername**: Benutzername des OpenVPN-Client.
- **Kennwort**: Kennwort des OpenVPN-Client.

12

Zertifikatverwaltung

Ein digitales Zertifikat bestätigt, dass der im Zertifikat genannte Inhaber Besitzer eines bestimmten öffentlichen Schlüssels ist. Auf diese Weise können andere (vertrauende Parteien) den Signaturen oder Behauptungen des privaten Schlüssels vertrauen, der dem zertifizierten öffentlichen Schlüssel entspricht. In diesem Vertrauensstellungsmodell ist eine Zertifizierungsstelle (Certification Authority, CA) eine vertrauenswürdige dritte Partei, der sowohl der Inhaber (Besitzer) des Zertifikats als auch die auf das Zertifikat vertrauende Partei vertrauen. Zertifizierungsstellen sind charakteristische Merkmale vieler öffentlicher PKI-Schemas (Public Key Infrastructure).

Mithilfe der Zertifikatverwaltung können Sie SSL-Zertifikate generieren und installieren.

Mein Zertifikat

Sie können max. 50 selbstsignierte oder durch einen Drittanbieter autorisierte Zertifikate hinzufügen. Außerdem können Sie mit dem **Zertifikatgenerator** Zertifikate erstellen oder Zertifikate von einem PC oder USB-Gerät importieren.

Selbstsignierte SSL-Zertifikate sind für Browser nicht zwangsläufig vertrauenswürdig. Sie können zwar zur Verschlüsselung verwendet werden, führen jedoch dazu, dass im Browser Warnmeldungen angezeigt werden. In diesen werden die Benutzer informiert, dass das Zertifikat nicht von einer Entität ausgestellt wurde, die der Benutzer als vertrauenswürdig eingestuft hat.

Benutzer können auch Verbindungen herstellen, ohne dass auf dem PC ein Zertifikat installiert ist. Beim Herstellen der Verbindung mit dem VPN-Tunnel wird den Benutzern eine Sicherheitswarnung angezeigt. Der Vorgang kann jedoch ohne diese zusätzliche Sicherheit fortgesetzt werden.

Zum Identifizieren eines Zertifikats als primäres Zertifikat klicken Sie auf das Optionsfeld des gewünschten Zertifikats, und klicken Sie dann auf **Als primäres Zertifikat auswählen**.

Zum Anzeigen von Zertifikatinformationen klicken Sie auf das Symbol **Details**.

Exportieren oder Anzeigen eines Zertifikats oder eines privaten Schlüssels

Mithilfe des Clientzertifikats kann der Client eine Verbindung mit dem VPN herstellen. So können Sie ein Zertifikat oder einen privaten Schlüssel exportieren oder anzeigen:

SCHRITT 1 Klicken Sie auf das zugehörige Symbol **Zertifikat für Client exportieren**, **Zertifikat für Administrator exportieren** oder **Privaten Schlüssel exportieren**. Das Fenster zum Herunterladen der Datei wird angezeigt.

Zertifikat für Client exportieren: Clientzertifikat, mit dessen Hilfe der Client eine Verbindung mit dem VPN herstellen kann

Zertifikat für Administrator exportieren: Enthält den privaten Schlüssel. Sie können eine Kopie als Sicherungsdatei exportieren. Beispielsweise können Sie das Zertifikat exportieren, bevor Sie das Gerät auf die Werkseinstellungen zurücksetzen. Nach dem Neustarten des Geräts importieren Sie diese Datei, um das Zertifikat wiederherzustellen.

Privaten Schlüssel exportieren: Bei manchen VPN-Clientsoftwareprodukten sind Anmeldeinformationen mit einem privaten Schlüssel und einem getrennten Zertifikat erforderlich.

SCHRITT 2 Klicken Sie auf **Öffnen**, um den Schlüssel anzuzeigen. Klicken Sie auf **Speichern**, um den Schlüssel zu speichern.

Importieren eines Zertifikats eines Drittanbieters oder eines selbstsignierten Zertifikats

Eine extern generierte Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) kann nicht autorisiert oder signiert sein. Sie müssen mithilfe der **CSR-Autorisierung** eine externe CSR hinzufügen.

So importieren Sie ein Zertifikat:

SCHRITT 1 Klicken Sie auf **Hinzufügen**.

SCHRITT 2 Wählen Sie **Von Drittanbieter autorisiert** oder **Selbstsigniert** aus.

SCHRITT 3 Wählen Sie **Von PC importieren** oder **Von USB-Gerät importieren** aus.

SCHRITT 4 Durchsuchen Sie **Zertifizierungsstellenzertifikat**. (Nur Drittanbieter)

SCHRITT 5 Durchsuchen Sie **Zertifikat und öffentlicher Schlüssel** (Drittanbieter oder selbstsigniert).

SCHRITT 6 Klicken Sie auf **Speichern**.

Vertrauenswürdiges IPSec-Zertifikat

IPSec wird beim Austausch von Generierungs- und Authentifizierungsdaten für Schlüssel, als Protokoll für das Festlegen von Schlüsseln, als Verschlüsselungsalgorithmus oder als Authentifizierungsmechanismus für die sichere Authentifizierung und Überprüfung von Onlinetransaktionen mit SSL-Zertifikaten verwendet.

Zum Anzeigen von Zertifikatinformationen klicken Sie auf das Symbol **Details**.

Zum Exportieren und Anzeigen eines Zertifikats klicken Sie auf das Symbol **Zertifikat exportieren**. Daraufhin wird ein Popup-Fenster angezeigt, in dem Sie auf **Öffnen** klicken können, um das Zertifikat zur Überprüfung zu öffnen, oder auf **Speichern**, um das Zertifikat auf einem PC zu speichern.

Zum Importieren eines Zertifikats eines Drittanbieters klicken Sie auf **Hinzufügen**, und importieren Sie das Zertifikat:

SCHRITT 1 Wählen Sie das **Zertifizierungsstellenzertifikat** aus.

SCHRITT 2 Wählen Sie **Von PC importieren** oder **Von USB-Gerät importieren** aus.

SCHRITT 3 Durchsuchen Sie **Zertifikat** (Drittanbieter oder selbstsigniert).

SCHRITT 4 Klicken Sie auf **Speichern**.

OpenVPN-Zertifikat

Unterstützt OpenVPN-Authentifizierungsmethoden auf Grundlage von Zertifikaten.

Um diese Seite zu öffnen, wählen Sie im Navigationsbaum die Optionen **Zertifikatverwaltung > OpenVPN-Zertifikat** aus.

Zum Anzeigen von Zertifikatinformationen klicken Sie auf das Symbol **Details**.

Zum Erstellen des neuen Zertifikats für den OpenVPN-Server oder OpenVPN-Client klicken Sie auf **Hinzufügen** und wechseln Sie zur Seite **Zertifikatverwaltung > Zertifikatgenerator**.

Zertifikatgenerator

Der Zertifikatanforderungsgenerator sammelt Informationen und generiert eine private Schlüsseldatei und eine Zertifikatanforderung. Sie können auswählen, ob Sie ein selbstsigniertes Zertifikat oder eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) generieren möchten, die von einer externen Zertifizierungsstelle signiert werden soll. Sie können zudem auswählen, dass ein Zertifikat für den OpenVPN-Server oder OpenVPN-Client erstellt werden soll. Nach dem Speichern der Konfiguration wird die generierte CSR bzw. das selbstsignierte Zertifikat unter **Mein Zertifikat** angezeigt. Das Zertifikat für den OpenVPN-Server oder OpenVPN-Client wird unter „OpenVPN-Zertifikat“ angezeigt.

So generieren Sie ein Zertifikat:

SCHRITT 1 Geben Sie die folgenden Parameter ein:

- **Typ**: Typ der Zertifikatanforderung.
- **Name des Lands**: Ursprungsland.
- **Name des Bundeslands oder der Region**: Bundesland oder Region (optional).
- **Name des Standorts**: Stadt (optional).
- **Name der Organisation**: Organisation (optional).
- **Name der Organisationseinheit**: Teilmenge der Organisation.
- **Allgemeiner Name**: Allgemeiner Name der Organisation.
- **E-Mail-Adresse**: E-Mail-Adresse eines Kontakts (optional).
- **Schlüsselverschlüsselungslänge**: Länge des Schlüssels.
- **Gültigkeitsdauer**: Anzahl der Tage, an denen das Zertifikat gültig ist.

- **Root-Zertifizierungsstelle**: Wählen Sie eine der Root-Zertifizierungsstellen aus, um das Zertifikat für den OpenVPN-Server oder OpenVPN-Client zu erstellen.

SCHRITT 2 Klicken Sie auf **Speichern**. Das Fenster **Mein Zertifikat** oder „OpenVPN-Zertifikat“ wird angezeigt.

CSR-Autorisierung

Eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) ist ein von einem Zertifikatgenerator generiertes digitales Identitätszertifikat. Das Zertifikat ist erst vollständig, wenn es von einer Zertifizierungsstelle (Certificate Authority, CA) signiert wurde. Das Gerät kann als Zertifizierungsstelle fungieren und eine CSR signieren bzw. autorisieren, die extern unter **Zertifikatverwaltung > CSR-Autorisierung** generiert wurde. Eine von diesem Gerät signierte extern generierte CSR wird zu einem vertrauenswürdigen Zertifikat und wird in das Fenster **Vertrauenswürdiges IPSec-Zertifikat** verschoben. (Zum Zurücksetzen der Gerätekonfiguration auf die Werkseinstellungen, einschließlich der Standardzertifikate, verwenden Sie das Fenster **Werkseinstellungen**.)

So signieren Sie ein Zertifikat:

SCHRITT 1 Klicken Sie auf **Durchsuchen**, um die Zertifikatsignierungsanforderung zu identifizieren.

SCHRITT 2 Zum Auswählen des entsprechenden privaten Schlüssels für das Autorisieren und Signieren der CSR wählen Sie im Dropdown-Menü **Mein Zertifikat** das Zertifikat aus, das Sie der Anforderung zuordnen möchten.

SCHRITT 3 Klicken Sie auf **Speichern**.

13

Protokoll

In Protokollen wird mithilfe von Traps oder in regelmäßigen Abständen der Status des Systems dokumentiert.

Systemprotokoll

Konfigurieren Sie SMS-Protokolle und Benachrichtigungen.

Konfigurieren des Systemprotokolls und Senden von SMS-Nachrichten

Zum Konfigurieren der Leitung für das Protokoll führen Sie die folgenden Schritte aus:

SCHRITT 1 Klicken Sie auf **Aktivieren**.

SCHRITT 2 Wählen Sie **USB1** oder **USB2** aus, um das Protokoll über die USB-Anschlüsse zu senden.

SCHRITT 3 Aktivieren Sie **Einwählnummer 1** und/oder **Einwählnummer 2**, und geben Sie die gewünschte Telefonnummer ein.

SCHRITT 4 Klicken Sie auf **Testen**, um die Verbindung zu testen.

SCHRITT 5 Wählen Sie aus, wann das Protokoll gesendet wird:

- Beim Aktivieren einer Verbindung
- Beim Deaktivieren einer Verbindung
- Bei Authentifizierungsfehlern
- Beim Starten des Systems

SCHRITT 6 Klicken Sie auf **Speichern**.

Konfigurieren der Systemprotokollserver

Zum Aktivieren eines Servers klicken Sie auf **Aktivieren**, und geben Sie in **Syslog-Server** den Namen des Syslog-Servers ein.

Konfigurieren von E-Mail-Benachrichtigungen

Zum Konfigurieren von E-Mail-Benachrichtigungen aktivieren Sie das Kontrollkästchen **Aktivieren**, und füllen Sie die folgenden Felder aus:

- **Mailserver**: Name oder IP-Adresse des Mailservers
- **Authentifizierung**: Authentifizierungstyp für die Anmeldung beim Mailserver
  - **Ohne**: Ohne Authentifizierung
  - **Unverschlüsselte Anmeldung**: Authentifizierung im unverschlüsselten Format
  - **TLS**: Authentifizierungsprotokoll der sicheren Verbindung (Bei Gmail beispielsweise wird die TLS-Authentifizierungsoption an Port 587 verwendet.)
  - **SSL**: Authentifizierungsprotokoll der sicheren Verbindung (Bei Gmail beispielsweise wird die SSL-Authentifizierungsoption an Port 465 verwendet.)
- **SMTP-Port**: Portnummer für das SMTP-Protokoll
- **Benutzername**: E-Mail-Benutzername. Beispiel:
  Mailserver: smtp.gmail.com
  Authentifizierung: SSL
  SMTP-PORT: 465
  Benutzername: xxxxx@gmail.com
  Kennwort: yyyyyy
- **Kennwort**: E-Mail-Kennwort
- **E-Mail senden an 1** und (optional) **2**: E-Mail-Adresse. Beispiel: E-Mail senden an: `zzz@Unternehmen.com`.
- **Protokollwarteschlangenlänge**: Anzahl der Einträge, die protokolliert werden, bis die Benachrichtigung gesendet wird. Beispiel: *10* Einträge.
- **Protokollzeitschwelle**: Zeitabstand zwischen Protokollbenachrichtigungen. Beispiel: *10* Minuten.

- **Benachrichtigung in Echtzeit**: Ereignis, das eine sofortige Benachrichtigung auslöst
- **Benachrichtigung per E-Mail, wenn auf gesperrte/gefilterte Inhalte zugegriffen wird**: Bei Zugriffsversuchen über ein gesperrtes oder gefiltertes Gerät wird eine Benachrichtigungs-E-Mail gesendet.
- **E-Mail-Benachrichtigung bei Hackerangriff**: Eine Benachrichtigungs-E-Mail wird gesendet, wenn ein Hacker mithilfe einer DoS-Attacke (Denial of Service) zuzugreifen versucht.

Wenn das Protokoll sofort per E-Mail gesendet werden soll, klicken Sie auf **Protokoll jetzt per E-Mail versenden**.

Konfigurieren der Protokolle

Wählen Sie die Ereignisse aus, die Protokolleinträge auslösen sollen:

- **SYN-Flooding**: TCP-Verbindungsanfragen werden schneller empfangen, als sie vom Gerät verarbeitet werden können.
- **IP-Spoofing**: IP-Pakete mit anscheinend gefälschten Quell-IP-Adressen, die gesendet werden, um die Identität des Absenders zu verbergen oder die Identität eines anderen Computersystems anzunehmen
- **Nicht autorisierter Anmeldeversuch**: Abgelehnter Anmeldeversuch beim Netzwerk
- **Ping of Death**: Erkennung eines an den Computer gesendeten Pings mit inkorrekter Form oder eines anderweitig bösartigen Pings. Ein Ping ist normalerweise 32 Byte groß (oder 84 Byte, wenn der IP-Header (Internetprotokoll) berücksichtigt wird). In der Vergangenheit konnten viele Computersysteme Ping-Pakete, bei denen die maximale IPv4-Paketgröße von 65.535 Byte überschritten wurde, nicht verarbeiten. Durch das Senden eines zu großen Pings kann der Zielcomputer zum Absturz gebracht werden.
- **WinNuke**: Ein remote ausgeführter DoS-Angriff (Denial of Service), der die Computerbetriebssysteme Microsoft Windows 95, Microsoft Windows NT und Microsoft Windows 3.1x betrifft
- **"Verweigern"-Richtlinien**: Der Zugriff wurde auf der Grundlage konfigurierter Richtlinien verweigert.
- **Autorisierte Anmeldung**: Ein autorisierter Benutzer hat sich beim Netzwerk angemeldet.

- **Meldungen zu Systemfehlern**: Meldungen zu Systemfehlern werden protokolliert.
- **"Zulassen"-Richtlinien**: Ein autorisierter Benutzer hat sich über die konfigurierten Richtlinien beim Netzwerk angemeldet.
- **Kernel**: Alle Meldungen zum System-Kernel
- **Konfigurationsänderungen**: Vorgenommene Änderungen an der Konfiguration des Geräts
- **IPSec und PPTP-VPN**: Status von VPN-Tunnel-Aushandlungen, Verbindungen und Trennungen von Verbindungen
- **SSL-VPN**: Status von SSL VPN-Tunnel-Aushandlungen, Verbindungen und Trennungen von Verbindungen
- **Netzwerk**: Die WAN/DMZ-Schnittstelle ist verbunden oder getrennt.

Zusätzliche Informationen (Protokollschaltflächen)

Wenn im Webbrowser eine Warnung zu dem Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu. Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren.

Klicken Sie auf die folgenden Schaltflächen, um zusätzliche Informationen anzuzeigen:

- **Systemprotokoll anzeigen**: Zeigt das **Systemprotokoll** an. Zum Angeben eines Protokolls wählen Sie im Dropdown-Menü den Filter aus.

  Protokolleinträge enthalten Datum und Uhrzeit des Ereignisses, den Ereignistyp und eine Meldung. Aus der Meldung gehen der Richtlinientyp (beispielsweise Zugriffsregel), die LAN-IP-Adresse der Quelle (SRC) und die MAC-Adresse hervor.
- **Protokolltabelle ausgehend**: Informationen zu ausgehenden Paketen
- **Protokolltabelle eingehend**: Informationen zu eingehenden Paketen
- **Protokoll jetzt löschen**: Klicken Sie auf diese Schaltfläche, um das Protokoll zu löschen, ohne es per E-Mail zu senden (nur wenn Sie die Informationen nicht zu einem späteren Zeitpunkt anzeigen möchten).

Systemstatistik

Hier werden detaillierte Informationen zu den Anschlüssen und den an die Anschlüsse angeschlossenen Geräten angezeigt.

Prozesse

Hier werden detaillierte Informationen zu den ausgeführten Prozessen angezeigt.

14

Benutzerverwaltung

Mit der Benutzerverwaltung können Sie den Zugriff für Benutzer und Domänen steuern. Diese Möglichkeit wird in erster Linie für PPTP und Cisco VPN Client (auch unter dem Namen EasyVPN bekannt) verwendet.

So können Sie eine Domäne hinzufügen oder ändern:

SCHRITT 1 Klicken Sie auf **Hinzufügen** oder wählen Sie einen Eintrag aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 2 Wählen Sie den **Authentifizierungstyp** aus, und geben Sie die erforderlichen Informationen ein:

- **Lokale Datenbank**: Die Authentifizierung erfolgt anhand einer lokalen Datenbank.
  - **Domäne**: Zur Anmeldung wählen Benutzer den Namen der Domain.
- **RADIUS (PAP, CHAP, MSCHAP, MSCHAPv2)**: Die Authentifizierung erfolgt über einen RADIUS-Server mit den Protokollen PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP (Microsoft Challenge Handshake Authentication Protocol) oder MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2) ausgeführt.
  - **Domäne**: Zur Anmeldung wählen Benutzer den Namen der Domain.
  - **RADIUS-Server**: IP-Adresse des RADIUS-Servers
  - **RADIUS-Kennwort**: *Geheimer Schlüssel* für die Authentifizierung
- **Active Directory**: Authentifizierung über Windows Active Directory. Beachten Sie, dass die Active Directory-Authentifizierung am fehleranfälligsten ist. Wenn die Authentifizierung mit Active Directory nicht möglich ist, lesen Sie die Informationen zur Fehlerbehebung am Ende dieses Abschnitts.
  - **Domäne**: Zur Anmeldung wählen Benutzer den Namen der Domain.

- **AD-Serveradresse**: IPv4-Adresse des Active Directory-Servers
- **AD-Domänenname**: Domänenname des Active Directory-Servers

- **LDAP**: Lightweight Directory Access Protocol
  - **Domäne**: Domänenname, den Benutzer auswählen, um sich beim SSL-VPN-Portal anzumelden.
  - **LDAP-Serveradresse**: IPv4-Adresse des LDAP-Servers
  - **LDAP-Basis-DN**: Suchbasis für LDAP-Abfragen. Beispiel für eine Suchbasisabfrage: `CN=Users,DC=IhreDomäne,DC=com`.

SCHRITT 3 Klicken Sie auf **OK**.

Zum Hinzufügen bzw. Ändern eines Benutzers klicken Sie auf **Hinzufügen** – oder wählen Sie einen Eintrag aus, und klicken Sie auf **Bearbeiten** – und geben Sie die folgenden Informationen ein:

- **Benutzername**: Name, den der Benutzer eingibt, um sich beim SSL-VPN-Portal anzumelden.
- **Kennwort**: Für die Authentifizierung verwendetes Kennwort
- **Gruppe**: Die Gruppe **Nicht zugewiesen** enthält PPTP-VPN-Benutzer und EasyVPN-Benutzer. Die Gruppe **Administrator** enthält nur einen Benutzer. Der Standardbenutzername der Gruppe **Administrator** lautet **cisco**.
- **Domäne**: In der Domänenverwaltungstabelle aufgeführter Name der Domäne

15

Webfilter

Webfilter schützen Sie mithilfe des folgenden Mechanismus vor dem Zugriff auf unerwünschte Websites. Diese Funktion ist nur in den Modellen RV320-WB und RV325-WB verfügbar.

SCHRITT 1 Wenn die eingehende URL in der **Ausschlussliste** aufgeführt ist und ihr Indexwert für die **Webreputation** nicht niedriger als 40 ist, gilt die URL als sicher und wird zugelassen. Dies gilt auch im umgekehrten Fall.

SCHRITT 2 Wenn die eingehende URL nicht in der **Ausschlussliste** aufgeführt ist, überprüfen Sie, ob sie in der **Schwarzen Liste** aufgeführt ist. Sollte sie auf der **Schwarzen Liste** stehen, wird die URL blockiert. Wenn die eingehende URL nicht in der **Schwarzen Liste** aufgeführt ist, überprüfen Sie, ob sie in der **Weißen Liste** aufgeführt ist.

SCHRITT 3 Sollte sie auf der **Weißen Liste** stehen, wird die URL zugelassen. Sollte dies nicht der Fall sein, überprüfen Sie die Webkategorie.

SCHRITT 4 Wenn die URL zu den ausgewählten Elementen der Kategorie gehört, ist sie blockiert. Sollte dies nicht der Fall sein, überprüfen Sie die **Webreputation**.

SCHRITT 5 Liegt der Reputations-Indexwert nicht unter 40, wird die URL zugelassen. Dies gilt auch im umgekehrten Fall.

Webfilter – Wenn Sie die Webfilter immer anwenden möchten, klicken Sie auf **Immer an**. Um die Webfilter nach Zeitplänen anzuwenden, klicken Sie auf **Geplant**. Zum Deaktivieren der Webfilter klicken Sie auf **Immer aus** und dann auf **Speichern**.

Webreputation – Aktivieren Sie die **Webreputation**, um die Analyse der Webreputation zu starten.

Kategorien – Klicken Sie auf **Kategorien**. Die Seite mit der Webfilterkategorie wird geöffnet. Wählen Sie Hoch, Mittel, Niedrig oder Benutzdefiniert aus, um den Umfang des Filters festzulegen. Sie können auch die Elemente aus den Kategorien Erotische Inhalte/Inhalte für Erwachsene, Business/Investment, Unterhaltung, Illegale/Fragwürdige Inhalte, IT-Ressourcen, Lifestyle/Kultur, Sonstiges und Sicherheit wählen. Eingehende URLs, die zu den ausgewählten Elementen gehören, werden blockiert. Klicken Sie auf **Speichern** und **Zurück**, um zur Seite mit den Webfiltern zurückzukehren.

Ausnahmen – Klicken Sie auf **Ausnahmen**. Die Seiten **Weiße Liste** und **Schwarze Liste** sowie die **Ausschlussliste** werden angezeigt. Wählen Sie unter jedem Listenfeld den **Typ** für den Filtermechanismus aus dem Dropdown-Menü aus, und geben Sie den Wert ein, um ein Element hinzuzufügen oder zu bearbeiten. Klicken Sie auf **Speichern** und **Zurück**, um zur Seite mit den Webfiltern zurückzukehren.

- Klicken Sie auf **Hinzufügen**, und geben Sie die Werte für die Felder an.
  - **Name**: der Name des Zeitplans
  - **Beschreibung**: Erläuterung des Zeitplans
  - Überprüfen Sie die Daten für die Implementierung des Zeitplans.
  - **Start**: die Startzeit des Zeitplans
  - **Ende**: die Endzeit des Zeitplans
  - **Aktiv**: Aktivieren Sie diese Option, um den Zeitplan zu starten.
  - Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Cisco Web Filtering Service Supplemental End User License Agreement

This Supplemental End User License Agreement (“SEULA”) contains additional terms and conditions that grant the right to use the Cisco Small Business Web Filtering Service and its associated software (collectively, the “Service”) under the End User License Agreement (“EULA”) between you and Cisco (collectively, the “Terms”). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Service, you agree to comply at all times with the terms and conditions provided in this SEULA. ACCESSING AND USING THE SERVICE CONSTITUTES ACCEPTANCE OF THE TERMS, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "END USER") TO THE TERMS. END USER MUST CAREFULLY READ AND ACCEPT ALL OF THE TERMS BEFORE CISCO WILL PROVIDE YOU ACCESS TO THE SERVICE. IF YOU DO NOT AGREE TO ALL OF THE TERMS, YOU SHOULD CLICK THE "DECLINE" BUTTON WHERE PROMPTED AND DO NOT ACCESS OR USE THE SERVICE. IF YOU AGREE TO ALL OF THE TERMS YOU SHOULD CLICK THE "ACCEPT" BUTTON WHERE PROMPTED.

These Terms are effective on the date of End User's acceptance. Upon termination of these Terms, End User shall no longer be eligible to use the Service.

1. SCOPE OF THE SERVICE

1.1 These Terms describe the terms and conditions of your use of the Service.

1.2 Service Changes. Cisco reserves the right, at its sole discretion and from time to time, to modify the Service, or parts thereof, including, but not limited to, terminating the availability of a given feature or functionality. Some material Service changes may include a requirement that End User agree to the changed Terms. If End User does not agree with a change in the Service, or a modification of the Terms reflecting such change to the Services, either party may terminate these Terms pursuant to Section 3 (Term and Termination) and End User will no longer have access to the Service.

1.3 Third Party Service. End User understands and agrees that the Service is being provided by one or more third parties on behalf of Cisco (collectively, "Service Provider"), and that if Service Provider stops providing the Service for any reason, End User will no longer have access to the Service. End User may contact Cisco for more information in such event.

2. THE SERVICE

2.1 Service. Subject to End User's compliance with the Terms, Cisco shall provide End User the Service for use on your Cisco device in accordance with the Service datasheet(s) available at: http://www.cisco.com/c/en/us/products/routers/smallbusiness-rv-series-routers/datasheet-listing.html

3. TERM AND TERMINATION

3.1 Cisco may terminate these Terms immediately upon notice: (i) if End User breaches any provision of these Terms and fails to remedy such breach within thirty (30) days after written notification by Cisco to End User of such breach; or (ii) in the event that Cisco determines, at its sole discretion, to discontinue the Service. Upon termination as specified in these Terms, (a) all rights and licenses of End User hereunder shall terminate, and (b) End User access to the Service shall terminate.

3.2 Cisco may at any time terminate these Terms for convenience, for any reason, or for no reason at all, by providing End User with thirty (30) days prior notice of termination via posting an end of sale notice at: http://www.cisco.com/c/en/us/products/routers/small-business-rv-series-routers/eos-eol-notice-listing.html

3.3 End User may terminate these Terms upon thirty (30) days prior written notice to Cisco if End User does not agree to a change of scope or content made by Cisco in accordance with Section 1.

4. OWNERSHIP AND LICENSE

4.1 Ownership. End User agrees that Cisco and/or Service Provider own all right, title and interest, including intellectual property rights in and to the Service.

4.2 License. Subject to the terms and conditions of these Terms, Cisco grants to End User a limited, non-exclusive, non-transferable license to use the Service on the Cisco device.

5. DATA USAGE AND PROTECTION

5.1 Collection. The Service may collect and send to the Cisco and/or Service Provider the following data: (a) your IP address; (b) your Cisco device model and serial numbers and (c) your Internet search requests (including, but not limited to, full URLs, Internet domains and destination web server IP addresses) (collectively, “Your Data”). End User represents and warrants that End User owns or has all necessary rights to Your Data, and acknowledges that Cisco and Service Provider do not test or screen Your Data, other than what is necessary to provide the Service. Cisco and Service Provider take no responsibility and assumes no liability for Your Data. End User shall be solely responsible and liable for Your Data.

5.2 Transfer. By using the Service, End User agrees and consents to the collection, use, processing and storage of Your Data and any other personal data according to the Terms and the Cisco Privacy Statement (available at: http://www.cisco.com/web/siteassets/legal/privacy.html). To the extent that there is a conflict between the terms and conditions of the Cisco Privacy Statement and the Terms, the terms and conditions of the Terms will take precedence. In performance of the Services, Cisco and/or Service Provider may transfer Your Data to its locations in the United States and/or other jurisdictions. By agreeing to the Terms or using the Service,

End User agrees to such transfer of Your Data. Please note that Your Data may not be subject to the same controls as Your current location. End User consents to the uses described above, including but not limited to having Your Data transferred to and processed in the United States and other jurisdictions.

5.3 End User further agrees and consents that Cisco and/or Service Provider may use Your Data to improve the Services and related services from Cisco and/or Service Provider, and may aggregate Your Data in a manner which does not identify End User. Cisco and/or Service Provider may share such aggregate information with third parties.

6. LIMITED WARRANTY AND DISCLAIMER

NOTHING IN THESE TERMS SHALL AFFECT THE WARRANTIES PROVIDED WITH ANY HARDWARE PURCHASED OR SOFTWARE LICENSED FROM CISCO BY END USER. ANY AND ALL SERVICES PROVIDED HEREUNDER ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (EVEN IF THE PURPOSE IS KNOWN TO CISCO), SATISFACTORY QUALITY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED

TO THE GREATEST EXTENT ALLOWED BY APPLICABLE LAW. END USER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY SHALL BE, AT CISCO'S OPTION, RE-PERFORMANCE OF THE SERVICE; OR TERMINATION OF THE SERVICE.

IN NO EVENT DOES CISCO OR SERVICE PROVIDER WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, SECURE OR ERROR FREE.

NEITHER CISCO NOR SERVICE PROVIDER SHALL BE LIABLE FOR ANY FAILURE TO ACHIEVE ANY SERVICE LEVEL AGREEMENT FOR THE SERVICE.

END USER EXPRESSLY ACKNOWLEDGES AND AGREES THAT IT IS SOLELY RESPONSIBLE FOR YOUR DATA AND ANY OTHER DATA UPLOADED TO OR DOWNLOADED USING THE SERVICE. IN NO EVENT SHALL CISCO OR SERVICE PROVIDER BE LIABLE FOR THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN CONNECTION WITH THE SERVICE.

CISCO'S (AND SERVICE PROVIDER'S) TOTAL LIABILITY TO END USER IN CONNECTION WITH CLAIMS ARISING UNDER THESE TERMS SHALL BE LIMITED TO THE MONEY, IF ANY, PAID BY END USER FOR THE SERVICE. THIS LIMITATION OF LIABILITY IS CUMULATIVE AND NOT PER INCIDENT (I.E., THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

EXCEPT FOR END USER'S BREACH OF SECTION 4 (OWNERSHIP AND LICENSE), IN NO EVENT SHALL EITHER PARTY, ITS RESPECTIVE AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS OR SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR LOST REVENUE, LOST PROFITS, OR LOST OR DAMAGED DATA, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY THEREOF.

7. GENERAL

7.1 Indemnification. End User hereby indemnifies and holds Cisco harmless from any claim, loss, damage, liability and expense, including reasonable court costs and attorney's fees, resulting from any claim (i) arising out of the acts of End User, its employees or its agents or (ii) arising in connection with Your Data. This shall not limit Cisco's obligations, subject to these Terms, to provide the Service. All financial obligations associated with End User's business are the sole responsibility of End User.

7.2 Third Party Services. Cisco reserves the right to subcontract the provision of all or part of the Service to a third party.

7.3 Force Majeure. Cisco shall not be liable for any delay or failure in performance whatsoever resulting from acts beyond its reasonable control. Such acts shall include, but not be limited to delays attributed to delays of common carriers, acts of God, earthquakes, labor disputes, shortages of supplies, actions of governmental entities, riots, war, acts or threatened acts of terrorism, fire, epidemics and similar occurrences.

7.4 No Waiver. No waiver of rights under these Terms by either party shall constitute a subsequent waiver of this or any other right under these Terms.

7.5 Survival. The following sections shall survive the termination of these Terms: Sections 3 (Term and Termination), 4 (Ownership and License), 5 (Data Usage and Protection), 6 (Limited Warranty and Disclaimer) and 7 (General).

16

Weitere Informationen

Support	
Cisco Support-Community	www.cisco.com/go/smallbizsupport
Cisco Support und Ressourcen	www.cisco.com/go/smallbizhelp
Telefonischer Kundensupport	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware-Downloads	www.cisco.com/cisco/software/navigator.html?i=!ch Klicken Sie auf einen Link, um Firmware für Cisco Produkte herunterzuladen. Eine Anmeldung ist nicht erforderlich.
Cisco Open-Source-Anfrage	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (Partner-Anmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Produktdokumentation	
Router und Firewalls von Cisco	www.cisco.com/go/smallbizrouters

Ergebnisse im Zusammenhang mit EU-Lot 26 finden Sie unter www.cisco.com/go/eu-lot26-results.

Cisco und das Cisco-Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den USA und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter folgender URL: **www.cisco.com/go/trademarks**. Hier genannte Marken Dritter sind Eigentum ihrer jeweiligen Inhaber. Die Verwendung des Worts "Partner" impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und einem anderen Unternehmen. (1110R)

Copyright © 2014

Überarbeitung: 9. Sep 2014 78-21282-01B0