LAN-to-LAN IPsec-Tunnel zwischen einem Cisco VPN 3000-Concentrator und Router mit AES-Konfigurationsbeispiel

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm **Konfigurationen** Konfigurieren des VPN-Concentrators Überprüfen Überprüfen der Router-Konfiguration Überprüfen der Konfiguration des VPN Concentrators Fehlerbehebung Fehlerbehebung beim Router Fehlerbehebung beim VPN Concentrator Zugehörige Informationen

Einführung

In diesem Dokument wird die Konfiguration eines IPsec-Tunnels zwischen einem Cisco VPN 3000-Concentrator und einem Cisco Router mit Advanced Encryption Standard (AES) als Verschlüsselungsalgorithmus erläutert.

AES ist eine neue Publikation des Federal Information Processing Standard (FIPS), die vom National Institute of Standards and Technology (NIST) erstellt wurde und als Verschlüsselungsmethode verwendet wird. Dieser Standard legt einen symmetrischen AES-Verschlüsselungsalgorithmus fest, der den DES (Data Encryption Standard) als Datenschutztransformation sowohl für IPsec als auch für Internet Key Exchange (IKE) ersetzt. AES verfügt über drei verschiedene Schlüssellängen, eine 128-Bit-Taste (Standard), eine 192-Bit-Taste und eine 256-Bit-Taste. Die AES-Funktion in Cisco IOS® bietet IPsec Unterstützung für den neuen Verschlüsselungsstandard AES, mit dem Cipher Block Chaining (CBC) Mode.

Weitere Informationen zu AES finden Sie auf der <u>NIST Computer Security Resource Center-</u> <u>Website</u>.

Weitere Informationen zur Konfiguration des LAN-to-LAN-Tunnels zwischen dem Cisco VPN

<u>3000-Konzentrator und der PIX-Firewall finden Sie im Konfigurationsbeispiel</u> für den <u>LAN-to-LAN-</u> <u>Tunnel</u> zwischen einem VPN 3000-Concentrator und der PIX-Firewall.

Weitere Informationen zu PIX-Softwareversion 7.1 finden Sie unter Konfigurationsbeispiel des IPsec-Tunnels zwischen PIX 7.x und VPN 3000 Concentrator.

Voraussetzungen

<u>Anforderungen</u>

Dieses Dokument erfordert ein grundlegendes Verständnis des IPsec-Protokolls. Weitere Informationen zu IPsec finden Sie unter <u>Einführung in die IPSec-Verschlüsselung</u>.

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Routeranforderungen Die AES-Funktion wurde in Version 12.2(13)T der Cisco IOS-Software eingeführt. Um AES zu aktivieren, muss der Router IPsec unterstützen und ein IOS-Image mit langen Tasten "k9" (Subsystem "k9") ausführen. Hinweis: Hardware-Unterstützung für AES ist auch auf Cisco 2600XM-, 2691-, 3725- und 3745 AES-Acceleration-VPN-Modulen verfügbar. Diese Funktion hat keine Auswirkungen auf die Konfiguration, und das Hardwaremodul wird automatisch ausgewählt, wenn beide verfügbar sind.
- VPN Concentrator-Anforderungen Die Softwareunterstützung für die AES-Funktion wurde in Version 3.6 eingeführt. Der neue erweiterte, skalierbare Verschlüsselungsprozessor (SEP-E) bietet Hardwareunterstützung. Diese Funktion hat keine Auswirkungen auf die Konfiguration.Hinweis: In Cisco VPN 300 Concentrator Version 3.6.3 verhandeln Tunnel aufgrund der Cisco Bug-ID <u>CSCdy88797</u> nicht mit AES (<u>nur registrierte</u> Kunden). Dies wurde in Version 3.6.4 behoben.Hinweis: Der Cisco VPN 3000 Concentrator verwendet entweder SEP- oder SEP-E-Module, nicht beide. Installieren Sie nicht beide auf demselben Gerät. Wenn Sie ein SEP-E-Modul auf einem VPN Concentrator installieren, der bereits ein SEP-Modul enthält, deaktiviert der VPN Concentrator das SEP-Modul und verwendet nur das SEP-E-Modul.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Versionen Software und Hardware:

- Cisco Router der Serie 3600 mit Cisco IOS Software, Version 12.3(5)
- Cisco VPN 3060 Concentrator mit Softwareversion 4.0.3

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- IPsec-Router
- VPN-Konzentrator

Konfiguration des ipsec_Routers				
version 12.3				
service timestamps debug uptime				
service timestamps log datetime msec				
no service password-encryption				
!				
hostname ipsec_router				
!				
memory-size iomem 10				

no aaa new-model ip subnet-zero !--- Configuration for IKE policies. crypto isakmp policy 1 !--- Enables the IKE policy configuration (configisakmp) command mode, !--- where you can specify the parameters to be used during !--- an IKE negotiation. encryption aes 256 !--- Specifies the encryption algorithm as AES with a 256 !--- bit key within an IKE policy. authentication pre-share group 2 crypto isakmp key cisco123 address 20.20.20.1 !--- Specifies the preshared key "cisco123" which !--should be identical at both peers. ! !--- Configuration for IPsec policies. crypto ipsec security-association lifetime seconds 28800 !--- Specifies the lifetime of the IPsec security association (SA). ! crypto ipsec transform-set vpn espaes 256 esp-md5-hmac !--- Enables the crypto transform configuration mode, where you can !--- specify the transform sets to be used during an IPsec negotiation. ! crypto map vpn 10 ipsecisakmp !--- Indicates that IKE is used to establish the IPsec SA for protecting !--- the traffic specified by this crypto map entry. set peer 20.20.20.1 !--- Sets the IP address of the remote end (VPN *Concentrator*). set transform-set vpn !--- Configures IPsec to use the transform-set "vpn" defined earlier. ! !--- Specifies the traffic to be encrypted. match address 110 . interface Ethernet1/0 ip address 30.30.30.1 255.255.255.0 ip nat outside half-duplex crypto map vpn !--- Configures the interface to use the crypto map "vpn" for IPsec. ! interface FastEthernet2/0 ip address 192.168.20.1 255.255.255.0 ip nat inside duplex auto speed auto ip nat pool mypool 30.30.30.3 30.30.30.3 netmask 255.255.255.0 ip nat inside source route-map nonat pool mypool overload ip http server no ip http secure-server ip classless ip route 0.0.0.0 0.0.0.0 30.30.30.2 ! access-list 110 permit ip 192.168.20.0 0.0.0.255 172.16.0.0 0.0.255.255 !--- This crypto ACL-permit identifies the matching traffic !--- flows to be protected via encryption. !---Specifies the traffic not to be encrypted. access-list 120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0 0.0.255.255 !--- This crypto ACL-deny identifies the matching

traffic flows not to be encrypted. !			
access-list 120 permit ip 192.168.20.0 0.0.0.255 any			
! The access control list (ACL) used in the NAT			
configuration exempts ! the LAN-to-LAN traffic from			
the NAT process, ! but allows all traffic going to			
the Internet to be translated. !			
route-map nonat permit 10			
<pre>! The traffic flows not encrypted from the ! peer</pre>			
network are allowed. match ip address 120			
1			
line con O			
line aux 0			
line vty 0 4			
login			
!			
end			

Hinweis: Obwohl die ACL-Syntax unverändert ist, unterscheiden sich die Bedeutungen für Krypto-ACLs geringfügig. Bei Krypto-ACLs gibt **permit** an, dass übereinstimmende Pakete verschlüsselt werden sollen, während **deny** angibt, dass übereinstimmende Pakete nicht verschlüsselt werden müssen.

Konfigurieren des VPN-Concentrators

VPN Concentrators sind in den Werkseinstellungen nicht vorprogrammiert und verfügen nicht über IP-Adressen. Sie müssen den Konsolenport verwenden, um die Erstkonfigurationen zu konfigurieren, bei denen es sich um eine menübasierte Befehlszeilenschnittstelle (CLI) handelt. Informationen zur Konfiguration über die Konsole finden Sie unter Konfigurieren von VPN-Concentrators über die Konsole.

Nachdem die IP-Adresse der Ethernet 1-Schnittstelle (privat) konfiguriert wurde, kann der Rest entweder über die CLI oder die Browserschnittstelle konfiguriert werden. Die Browserschnittstelle unterstützt sowohl HTTP als auch HTTP über Secure Socket Layer (SSL).

Diese Parameter werden über die Konsole konfiguriert:

- Uhrzeit/Datum Die korrekte Uhrzeit und das richtige Datum sind sehr wichtig. Sie stellen sicher, dass Protokollierungs- und Abrechnungseinträge korrekt sind und dass das System ein gültiges Sicherheitszertifikat erstellen kann.
- Ethernet 1 (private) Schnittstelle Die IP-Adresse und -Maske (aus unserer Netzwerktopologie 172.16.1.1/24).

Der Zugriff auf den VPN Concentrator erfolgt über einen HTML-Browser aus dem internen Netzwerk. Informationen zur Konfiguration des VPN Concentrator im CLI-Modus finden Sie unter <u>Schnellkonfiguration mit CLI</u>.

 Geben Sie die IP-Adresse der privaten Schnittstelle im Webbrowser ein, um die GUI-Schnittstelle zu aktivieren.Klicken Sie auf das Symbol zum Speichern der Änderungen im Speicher. Der werksseitig voreingestellte Benutzername und das werkseitige Kennwort sind "admin". Groß- und Kleinschreibung ist zu beachten.



2. Wenn Sie die Benutzeroberfläche aufgerufen haben, wählen Sie **Configuration > Interfaces > Ethernet 2 (Public)** aus, um die Ethernet 2-Schnittstelle zu

	C		
kO	ntia	urie	ren
		0110	

Configuration Interfaces Stores	Configuration Interfaces Ethernet 2						
EUser Management	Configuring Ethernet Interface 2 (Public).						
	Gene	ral RIP OSPF B	andwidth				
			Gen	ieral Parameters			
	Sel	Attribute	Value		Description		
	0	Disabled			Select to disable this interface.		
	0	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Getevory via DHCP.		
	C.	Static IP Addressing					
		IP Address	20.20.20.1]	Enter the IP Address and Subnet Mask.		
		Subnet Mask	255.255.255.0		mentace.		
		Public Interface	A		Check to make this interface a "public" interface.		
		MAC Address	00.90 A4.00.4L F9		The MAC address for this interface.		
		Filter	2. Public (Detault)		Select the filter for this interface.		
		Speed	10/100 auto 💌		Select the speed for this interface.		
		Duplex	Auto 💌		Select the duplex mode for this interface.		
		MTU	1500		Enter the Mazimum Transmit Unit for this interface (68 - 1500).		
			C Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission		agment prior to interface transmission		
		Public Interface IPSec Fragmentation Palicy	C Fragment prior to IPSec e	Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)			
		C Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF kit)					
Cisco Systems	Aş	oply Cancel					

3. Wählen Sie Configuration > System > IP Routing > Default Gateways aus, konfigurieren Sie das Standard-Internet-Gateway und das Tunnel-Standardgateway (innen), damit IPsec die anderen Subnetze im privaten Netzwerk erreicht.In diesem Szenario ist im internen Netzwerk nur ein Subnetz verfügbar.

Configuration		
	Configuration System IP Routing D	efault Gateways
- ()-System		
- Bervers	Configure the default gateways for your system.	
- III <u>Tunneting Protocols</u>	n.e. a.e	
- G-P Routing	Default Gateway 20.20.20.2	Enter the IP address of the default gateway or router. Enter UUUU for an default router.
Static Routes	Metrie 1	Enter the metric, from 1 to 16
Default Galeways		Land do hour, from t to ro.
OSPE	Tunnel Default 172.16.1.2	Enter the IP address of the default geteway or router for tunnels. Enter 0.0.0.0 for no
OSPF Arees	Gateway	defeuit router.
OHCP Parameters	Override Default	Check to allow learned default suteways to override the configured default suteway.
OHCP Relay	Gateuray	construction of the second
Reduncionary	Applu Concel	
Reverse Route Injection	- Abbia	
- La Management Protocols		
- (+) Events		
- U-General		
-ter <u>chem Updata</u>		
Losd Calancing		
EPuser Management		
- Internet and a second second		
Theophoring		

4. Wählen Sie Configuration > Policy Management > Traffic Management > Network Lists > Add aus, um die Netzwerklisten zur Definition des zu verschlüsselnden Datenverkehrs zu erstellen.Die in der Liste aufgeführten Netzwerke sind für das Remote-Netzwerk erreichbar. Die Netzwerke in der folgenden Liste sind lokale Netzwerke. Sie können die Liste Lokaler Netzwerke auch automatisch über RIP erstellen, wenn Sie auf Lokale Liste generieren

klicken.		
Configuration	Configurati	on Policy Management Traffic Management Network ists Modify
- Constem		en pronog wondgement prono Honogement protocil clow proving
GPolicy Management	Modify a confi	gured Network List. Click on Generate Local List to generate a network list based on routing entries on the Private interface.
Access Hours	List Name	vpn_local_network Name of the Network List you are adding. The name must be unique.
Citetwork Lists Guiss SAS Filters Citetra Citetwork Lists Citetwork Citetwork Lists Citetwork Citetwork Lists Citetwork Citet	Network List	 172.16.0.0/0.0.255.255 Eater the Networks and Wildcard masks using the following format: n.n.n.ah.n.n.n (e.g. 10.10.0.000.255.255). Note: Enter a wildcard mask, which is the reverse of a submet mask. A wildcard mask, which is the reverse of a submet mask. A wildcard mask, which is the reverse of a submet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.0.00.255 = all 10.10.1.00.00.255 = all 10.00.1.00.00.255 = all 10.00.1.00.00.255 = all 10.00.1.00.00.255 = all 10.00.1.00.00.255 = all 10.00.00.255 = all 10.00.00.00.255 = all 10.00.00.00.255 = all 10.00.00.00.255 = all 10.00.00.255 = all 10.00.00.00.255 = all 10.00.00.00.00.255 = all 10.00.00.00.255 = all 10.00.00.00.00.00.00.00.00 = all 10.00.00.00.00.00.00.00.00 = all 10.00.00.00.00.00 = all 10.00.00.00.00.00 = all 10.00.00.00 = all 10.00.00 = all 10.00 = all 10.00.00 = all 10.00.00 = all 10.00 = all 10.00
	Apply	Concel Generate Local List

5. Die Netzwerke in dieser Liste sind Remote-Netzwerke und müssen manuell konfiguriert werden. Geben Sie dazu das Netzwerk/den Platzhalter für jedes erreichbare Subnetz

ein.	
<u>Configuration</u> <u>interfaces</u>	Configuration Policy Management Traffic Management Network Lists Modify
	Modify a configured Network List. Click on Generate Local List to generate a network list based on routing entries on the Private interface.
Access Hours	List Name wpn_remote_network Name of the Network List you are adding. The same must be unique.
- Cietwork Lists - Cietwork Lists - Cietas - Cietas	 Network List Enter the Networks and Wildowid masks using the following format: a.m.n/m.n.n. (e.g. 10.10.0.00.0.255.253). Note: Enter a wildowid mask, which is the reverse of a subnet mask. S wildowid mask, her is in bit positions to ignore. Os in bit positions to match. For example, 10.101.00.0.0.255 = all 10.101.nm addresses. Each Network and Wildowid mask, size much the submet is a single line. The Wildowid mask, may be omitted if the submet is to be used.
	Apply Cancel Generate Local List

Nach Fertigstellung werden die folgenden beiden Netzwerklisten angezeigt:

E)Configuration	Configuration Policy Managem	ent Traffic Management Netw	ork Lists	f
Access Hours A	This eaction lets you add, modify, copy, a Click Add to create a Network List, or sed	and dalate Network Lists et a Network List and click Modify. Copy Network List VPN Client Local LAN (Default) Vpn_remole_network Vpn_local_network	r, or Delete Actions Add	Save
			Modity Copy Delete	

6. Wählen Sie Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add and define the LAN-to-LAN tunnel. Dieses Fenster hat drei Bereiche. Der obere Bereich dient zur Anzeige der Netzwerkinformationen, die beiden unteren Abschnitte sind für die Listen "Lokales Netzwerk" und "Remote". Wählen Sie im Abschnitt "Netzwerkinformationen" die AES-Verschlüsselung, den Authentifizierungstyp und das IKE-Angebot aus, und geben Sie den vorinstallierten Schlüssel ein. Zeigen Sie in den unteren Abschnitten auf die bereits erstellten Netzwerklisten (sowohl lokale als auch Remote-

Listen).		
-3-Configuration Interfaces	Configuration System Tunneling Protocols IPSe	e LAN-to-LAN Add
- <u>System</u> - <u>Genvers</u> - <u>G</u> -Address Management	Add a new IPSec LAN-to-LAN connection	
-G+Tunnelino Protocols PPTP	Enable 😥	Check to enable this LAN-to-LAN connection.
	Name best	Enter the name for this LAN-to-LAN connection.
LAN-to-LAN	Interface Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAN-to-LAN connection.
	Connection Type Bi-directional	Choose the type of LAN-to-LAN connection. An <i>Orginate Only</i> connection may have multiple peers specified below.
Alerts	30.30.30.1 · ·	Inter the tenacte peer IP addresses for this LAN-to-LAN connection. Originate $\Omega(p)$ connection may specify up to ten peer IP addresses. Eater one IP address per line.
	Digini None (Use Preshared Keys) 💌	Select the digital cartificate to use.
- 38 Monitorina	Certificate C Entire certificate chain. Transmission © Identity contificate only	Choose how to send the digital certificate to the DCE peer.
	Preshared Key cisco123	Enter the preschared key for this LAN-to-LAN connection.
	Authentication ESP/MD5/HMAC-128 -	Specify the packet authentication mechanism to use.
CISCO SYSTEMS	Encryption AES-256	Specify the encryption mechanism to use.
adhoadhoa	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN econection.

- Denfiguration Interfaces 		
- E-Servers		
- E-Address Management		
- E- <u>Tunneling Protocols</u>		
	Filter -None-	Choose the filter to apply to the traffic that is transled through this LAN-to-LAN
		convection.
<u></u>		Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN
LanceLan	IPSer NAT-T	rearer time through a NAT device. You must also enable IPSec over NAT-T under
MAT Transporter		NAT Transparency.
6 keeks	Bandwidth Policy -None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Walk to		Change the resting rescharging to use Personation helper are innered if Network
- Wanage pent Protocols	Rowting None	Autodisenvery is chosen.
- Exercise - Foreign - For		
-ff-General	Local Neurank: If a L6N-to-LAN N&T rule is used. Dis is the Transla	ted Network oddress
- El-Cient Update		Coordinates and antisent address for so the ID address and address aces. So this
Load Balancing	Network List vpn_local_network	[AN.to.] AN opposition
- Tolicy Management	IP Address	Note: Enter a wildcard mark, which is the ownerse of a submet mark. A
Access Hours		wildrand mask has 1s in bit positions to imore. Us in hit positions to match. For
- E-Traffic Management	Wildcard Mask	szaruple, 10.10.1.000.0.0.255 = all 10.10.1 nrn addresses.
- E-Group Matching		
-33 <u>Administration</u>	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Rem	ote Network address.
- Monitoring		Specify the remote network address list or the IP address and wildcard mask for
	Memory Last wpn_remote_network	this LAN-to-LAN connection.
	IP ildrer	
	n onnese	Note: Enter a wildowd mask, which is the reverse of a subnet mask. A
	Wildcaml Mask	wildcard mark has 1s in bit positions to ignore, 0s in bit positions to match. For
0		ransple, 10.10.1.00.0.0.255 = all 10.10.1 ann adáresses.
CISCO SPETEMS	Add Contel	
million and a second		

7. Wenn Sie auf **Hinzufügen** klicken, wird Ihnen das Fenster IPSec LAN-to-LAN-Add-Done angezeigt, wenn Ihre Verbindung korrekt ist.Dieses Fenster zeigt eine Zusammenfassung der Tunnelkonfigurationsinformationen. Außerdem werden der Gruppenname, der SA-Name und der Filtername automatisch konfiguriert. Sie können alle Parameter in dieser Tabelle

Dearbeilen.	
Configuration	
	Configuration System Tunneling Protocols IPSec LAN to LAN Add Done
	Save Needed
- CEI Servers	
Address Management	An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:
Tunneling Protocols	
	Authentication Server Internal
	Comm. 20:20:20:1
	Security Acceleration 117 - bot
IVE Proposals	
NAT Tentisme prov	Filter Rules Lat. test Out
-diarts	Let. Bet III
- THP Routing	
- CEManagement Protocols	blocklying any of taske mena will affect the LAN-to-LAN configuration. The Group is the same as your LAN-to-LAN gent. The Security Association and Stars Board and with 20 At the indicate the data for the same as the LAN configuration.
- Cleventa	Finey Kurs an start with "Late" to indicate that they been a LAW-ID-LAW configuration.
- GKGeneral	
- Client Update	OK
Load Balancing	
- E-User Management	
EPolicy Management	
Monitoring	

An diesem Punkt wurde der IPsec LAN-to-LAN-Tunnel eingerichtet, und Sie können mit der Arbeit beginnen. Wenn der Tunnel aus irgendeinem Grund nicht funktioniert, können Sie nach Fehlkonfigurationen suchen.

8. Sie können die zuvor erstellten LAN-to-LAN-IPsec-Parameter anzeigen oder ändern, wenn Sie Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN auswählen. In dieser Grafik wird "test" angezeigt, da der Name des Tunnels und die öffentliche Schnittstelle des Remote-Endgeräts gemäß dem Szenario 30.30.30.1 lautet.

GConfiguration		
	Configuration System Tunneling Protocols IPSec LAN-to-LAN	
- G-System		Save
- @Servers		
	This section late you configure IESse LAN-to-LAN connections. LAN-to-LAN connections are as	tablished with other VPN 3000 Concentrators
	PEX firewalls, 7100/4000 series contens and other IPSec-compliant security gateways. To configure	a VPN 3002 or other remote access
PPTP	connection, go to User Management and configure a Group and User. To configure NAT over LAN	1-to-LAN, go to LAN-to-LAN NAT Rules.
12TP		
- EHEZeo	If you want to define a set of actworks on the local or remote side of the LAN-to-LAN connection.	, configure the necessary Network Lists prior
LAN-to-LAN	to creating the connection.	
IKE Proposals	•	
NAT Transparency	Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or	Delete.
- <u>Verts</u>	· · ·	
- OHP Routing	(D) indicates a disabled LAN-to-LAN connection.	
- (Hitemagement Protocols		
- the venus	LAN to LAN	
- ErGeneral	Connection	Actions
- Ciem Uponce		
Cost Basicing	test (30.30.30.1) on Ethernet 2 (Public)	
Elization Management		Add
-Access Hours		
-ETratile Management		Modify
Network Lists		
Rules		Delete
<u>——SA8</u>		
<u>Elters</u>		
- THAI		
ENV Policies		
L-⊕ <u>Group Metching</u>		
Administration		
- Monitoring		

9. Manchmal wird Ihr Tunnel möglicherweise nicht angezeigt, wenn Ihr IKE-Vorschlag in der Liste der inaktiven Vorschläge enthalten ist. Wählen Sie Configuration > System > Tunneling Protocols > IPSec > IKE Proposals aus, um das aktive IKE-Angebot zu konfigurieren.Wenn Ihr IKE-Angebot in der Liste "Inaktive Vorschläge" enthalten ist, können Sie ihn aktivieren, wenn Sie das IKE-Angebot auswählen und auf die Schaltfläche Aktivieren klicken. In dieser Grafik befindet sich der ausgewählte Vorschlag "IKE-AES256-SHA" in der Liste "Aktive Vorschläge"

Configuration Histories System General General Géneral	Configuration System Tunneling Protocol	ls IPSec. IKE Propos	als	Save
CPLInnelina Protocols PPTP L2TP LAN-to-LAN HEE Proposals	Select an Inactive Proposal and chick Artivate to make it Select an Artive Proposal and click Deactivate to make it Click Add or Copy to add a new Inactive Proposal. IKE	Artive, or click Modify, Co it Inartive, or click More Up Proposels are used by <u>Secur</u>	py or Delete as appropriate. or Mave Dawn to change its priority. my Associations to specify IKE parameters.	
NAT Transparency	Active		Inactive	
Alerts	Proposals	Actions	Proposals	
	Ciscot/PNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5-DH7 Ciscot/PNClient-3DES-MD5-DH5 Ciscot/PNClient-AES128-SH4 IKE-AES128-SH4 IKE-3DES-MD5-RSA IKE-AES256-SH4	<cade clivate="" clivate<="" th=""><th>IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA</th><th></th></cade>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA	

10. Wählen Sie Configuration > Policy Management > Traffic Management > Security Associations (Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement > Sicherheitszuordnungen aus, um zu überprüfen, ob die SA-Parameter korrekt sind.

	Configuration Policy Management Traffic Management Security Associations
- Bysten	Save
- #Servers	
- El-Address Management	This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to recordiate IKE.
- E-Tunneling Protocols	parameters.
PPTP	
	Click Add to wid an SA, or select an SA and click Mudify or Delete
	San and is defined and, to below an extended monthly in between
LAN-to-LAN	The second se
KE Proposals	IPSec SAs Artions
MAIT Transparency	ESP-3DES-MD5
Alerts	ESP-3DES-MD5-DH5
- DP Routing	ESP-3DES-MD5-DH7
- FManagement Protocols	ESP-3DES-NONE Add
- El-Events	ESP-AES128-SHA Manufak
- E-General	ESP-DES-MD5
- Elient Update	ESP4.2TP-TRANSPORT Delete
Load Balancing	ESP/KE-3DES-MD5
	L2L: test
Policy Management	
Access Hours	
Entraffic Manacement	
Network Lists	
584	
- E-MAT	
<u>B/VPolicies</u>	
Group Matching	
Administration	
Monitoring	

11. Klicken Sie auf den SA-Namen (in diesem Fall L2L: Test), und klicken Sie dann auf Ändern, um die SAs zu überprüfen.Wenn einer der Parameter nicht mit der Remote-Peer-Konfiguration übereinstimmt, kann er hier geändert

werden.		
Configuration	Configuration Policy Management Traffic Managem	ent Security Associations Modify
	Modify a configured Security Association.	
Adviness Management D Tunneling Protocols Log IP	SA Name L2L: test Inheritance From Pule	Specify the name of this Security Association (SA). Select the granularity of this SA.
	IPSec Parameters	
NAT Transperency	Algerithm ESP/MD5/HMAC-128	Select the packet authentication algorithm to use.
<u>Alerts</u> E.c.ting	Encryption Algorithm AES-256 💌	Select the ESP encryption algorithm to use.
-ED-Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
Events Events Events Events Events	Perfect Forward Servery Disabled	Select the use of Perfect Forward Secrecy.
Load Balancing	Lifetime Mocroment Time	Select the lifetime measurement of the IPSec keys
- (HUser Manasiement		
- Policy Management	Data Litetime 10000	Specify the data internae in subsystes (RIB).
-ETraffic Management	Time Lifetime 28800	Specify the time lifetime in seconds.
<u>(letwork Lists</u>		
Bules	IKE Parameters	
	Connection Type Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a lot Mark 1 MM Connection
- GRAT	IKE Peers 30 30 30.1	6 LAN-IO-LAN COSINETION.
EX/Policies	Negatiation Mode Main	Select the IKE Negotiation mode to use.
	Digital Certificate None (Use Preshered Keys) 💌	Select the Digital Centificate to use.
- E-Monitoring	Certificate C Entire certificate chain Transmission © Identity certificate only	Chooses how to send the digital certificate to the IKE power.
	IKE Proposal IKE : AES256-SHA	Select the IKE Proposal to use as IKE initiator.
CISCO SYSTEMS	Apply Concel	

<u>Überprüfen</u>

Überprüfen der Router-Konfiguration

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

 show crypto isakmp sa: Zeigt alle aktuellen IKE-SAs in einem Peer an. Der Status QM_IDLE gibt an, dass die SA mit dem zugehörigen Peer authentifiziert bleibt und für spätere Schnellwechselvorgänge verwendet werden kann. Es ist ruhig.
 ipsec_router#show crypto isakmp sa

dst src state conn-id slot 20.20.20.1 30.30.30.1 **QM_IDLE** 1 0

 show crypto ipsec sa - Zeigt die von aktuellen SAs verwendeten Einstellungen an. Pr
üfen Sie, ob die Peer-IP-Adressen, die Netzwerke, auf die sowohl die lokalen als auch die Remote-Endger
äte zugreifen k
önnen, und das verwendete Transformationssatz verwendet werden. Es gibt zwei ESP-SAs, eine in jede Richtung. Da AH-Transformationss
ätze verwendet werden, sind sie leer.

ipsec_router#show crypto ipsec sa

```
interface: Ethernet1/0
```

Crypto map tag: vpn, local addr. 30.30.30.1

protected vrf:

```
local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
```

remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

```
current_peer: 20.20.20.1:500
```

PERMIT, flags={origin_is_acl,}

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145

#pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 6, #recv errors 0

```
local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1
```

path mtu 1500, media mtu 1500

current outbound spi: 54FA9805

inbound esp sas:

spi: 0x4091292(67703442)

transform: esp-256-aes esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn

```
sa timing: remaining key lifetime (k/sec): (4471883/28110)
IV size: 16 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x54FA9805(1425709061)
transform: esp-256-aes esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4471883/28110)
IV size: 16 bytes
replay detection support: Y
outbound ah sas:
outbound ah sas:
```

• show crypto engine connections active - Zeigt die aktuell aktiven verschlüsselten session connections für all crypto engines an. Jede Verbindungs-ID ist eindeutig. Die Anzahl der verschlüsselten und entschlüsselten Pakete wird in den letzten beiden Spalten angezeigt. ipsec_router#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0

Überprüfen der Konfiguration des VPN Concentrators

Gehen Sie wie folgt vor, um die Konfiguration des VPN-Konzentrators zu überprüfen.

 Ähnlich wie bei der Anzeige von crypto ipsec sa und der Anzeige von crypto isakmp sa Befehlen auf Routern können Sie die IPsec- und IKE-Statistiken anzeigen, wenn Sie Überwachung > Statistics > IPSec auf den VPN-Konzentratoren auswählen.

-=- <u>Configuration</u>	Monitoring Statistics IPSec Thursday,	U1 Ja	inuary 2004 19:32:36
ElStaten			Reset 🥔 Refresh 🔞
FPUser Management	IKE (Phase 1) Statistics IPSec (Phase 2) Statistics		
EPfolicy Management	Active Tunnels 1 Active Tunnels	l	
Access Hours	Total Tunnels 2 Total Tunnels	2	
Network Lists	Received Bytes 3545268 Received Bytes	3632	
Rulez	Sent Bytes 5553204 Sent Bytes	5376	
<u>SAs</u>	Received Packets 60187 Received Packets	145	
Eller2	Sent Packets 60299 Sent Packets	-51	
BAY Policies	Received Parkets Dropped 0 Received Parkets Dropped	0	
Group Matching	Sent Packets Dropped O Received Packets Dropped (Anti-Replay)	U	
GAdministration	Received Notifies 60084 Sent Packets Dropped	0	
-ErSoftware Undete	Sent Notifies 120172 Inhound Authentirations	145	
Concentrator	Received Phase-2 Eachanges 2 Failed Inbound Authentications	0	
Cients Curtos Dabast	Sent Phase-2 Exchanges 49 Outbound Authentirations	St	
	Invalid Phase-2 Exchanges Received D Failed Outbound Authentications	U	
Eina	Invalid Phase 2 Eachanges Sent 0 Decryptions	145	
Monitoring Refresh	Rejected Received Phase-2 Exchanges 0 Failed Decryptions	0	
- Ele Management	Rejected Sent Phase-2 Exchanges 0 Encryptions	-51	
Swap Config File	Phase-2 SA Delete Requests Received 0 Failed Encryptions	0	
TFTP Transfor	Phase-2 SA Delete Requests Sent 30 System Capability Failures	0	
XM_ Export	Initiated Tunnels 0 No. SA Failures	0	
EPCertificate Management	Failed indifated Tunnels 0 Protocol Use Failures	0	
Enrollment	Failed Remote Tunnels 0		
	Authentication Failures 0		
	Decryption Failures 0		
Dynamic Filters	Hash Validation Failures 0		
Cisco Systems	System Capability Failures 0		
ومتألية متألية	No-SA Failures 0		

2. Ähnlich wie der Befehl **show crypto engine connections active** auf Routern können Sie das Fenster Administration-Sessions im VPN Concentrator verwenden, um die Parameter und Statistiken für alle aktiven IPsec-LAN-to-LAN-Verbindungen oder -Tunnel

anzuzeigen.										
GConfiguration								-		
hterfaces	Administration Ad	iminister Ses	stons					Thursday	, U1 Jani	ary 2004-19:00:20
- # <u>Systen</u>									R	:set 🥔 Refresh 🕲
HEHLaser Management										
- E/Policy Management	This screen shows statis	tics for sessions.	To refleck the stat	stias, cliak	Refresh 3	Select a Group b	o filter the se	estions. For n	ore informe	tion on a session, clic)
Activity Hours	on that session's pane. T	lo log out a seesio	a, click Legent in	the table be	slow. To te	et the petwork o	connection to	a session, chi	ck Ping.	
historic Manadement										
PACKAGE LINE	Group -AI-	-								
<u>SA2</u>	Legout All: PPTP User	12TP User IPS	lec User IPSec LA	N-to-LAN	L					
There are a second and a second area and area and a second area and area an	Carrian Commence									
BM Prácies	session summary									
TO Group Matching	Active LAN-to- LAN Spectrum	Active Remot Access Section	e Active Man Sacch	agement	Total A	rive Peak C	ioncurrent scienc	Conrur	vent i	fotal Cumulative Sourcess
Administration	1				30334		2	400		10
Administer Sessions		0	-		6		2	1 400	·	19
<u>Concentrator</u>	LAN-10-LAN Sessio	8					[Rep	cte Access Si	essione Mi	nagement Sessions]
System Reboot Refeat Status	Connection Name	IP Address	Protocol	Eng	yption	Legia Tino	Duration	Bytes Tx	Bytes Rx	Actions
-Ping	test	30.30.30.1	IPSeoLAN-to-LA	N AE	2-256	Jan 1 19:57:29	0:02:51	2128	2128	[Logent Ping]
Monitorine Retreats										
THE Management	Remote Access Sea	sions					[[.6	N-to-LAN S	sations Mi	ingement Sessions]
- H24 <u>Certricate Management</u> (3)Monitoring	Username	Assigned IP Ad Public IP Add	dress <u>Gra</u>	ар <mark> </mark>	Protocol acception	Login Ti Duratio	ime <u>(</u> m	lient Type Version	Bytes	Tx Rx Artions
	No Remote Access Sessions									
	Management Sessio	11.8					[LAN-	to-LAN See	ione Rema	da Accesa Sassiona]
	Administrator	IP Addre	ss Protocol	En	rryption	Legin	Time	Duratie	h	Ardeas
	a dania	173.14.1.2	111111							

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Fehlerbehebung beim Router

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

- debug crypto engine: Zeigt den verschlüsselten Datenverkehr an. Die Krypto-Engine ist der eigentliche Mechanismus, der Verschlüsselung und Entschlüsselung durchführt. Eine Krypto-Engine kann Software oder Hardware-Beschleuniger sein.
- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen (Internet Security Association and Key Management Protocol) der IKE-Phase 1 an.
- debug crypto ipsec: Zeigt die IPsec-Aushandlungen für IKE Phase 2 an.

Weitere Informationen und Beispielausgabe finden Sie unter <u>IPSec-Fehlerbehebung -</u> <u>Understanding and Using **debug** Commands</u> (<u>IPSec-Fehlerbehebung - Understanding and Using</u> <u>**debug** Commands</u>).

Fehlerbehebung beim VPN Concentrator

Ähnlich wie die **Debugbefehle** auf den Cisco Routern können Sie Ereignisklassen so konfigurieren, dass alle Alarme angezeigt werden.

1. Wählen Sie Configuration > System > Events > Classes > Add aus, um die Protokollierung der Ereignisklassen zu aktivieren.Diese Klassen sind für IPsec verfügbar:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE

Configuration	
	Configuration System Events Classes
- C System	Save Needed
- ERServers	-
 E)Address Monogement 	This section lets you configure special handhaz of specific event chases.
- EF <u>Turneling Protocols</u>	
- Ele Routine	Click the Add button to odd on event chose, or select on event chose and thick Modify or Delete.
E-Management Protocols	,,,,,
- Events	Click here to configure smeet event committee.
General	
ETP Backup	CarGaurad
	Comparison Actions
Trep Desanascris	
GMTB Servers	IKEDECODE
Empl Bacinianto	PECUDIC
EGeneral	MB2TRAP Add
-Fi-Client Update	
Load Balancing	Modily
	Take
	Detete
Administration	
#Honitoring	

2. Beim Hinzufügen können Sie auch den Schweregrad für jede Klasse auswählen, basierend auf dem Schweregrad, der gesendet wird.Die Alarme können mit einer der folgenden Methoden behandelt werden:Nach ProtokollAuf der Konsole angezeigtGesendet an UNIX Syslog-ServerAls E-Mail gesendetGesendet als Trap an einen SNMP-Server (Simple Network Management Protocol)

- Configuration		
	Configuration System Events Classes Add	
- EPSystem		
- El Servers	This screen lets you add and configure an event class for speci	al bandling.
Address Management		•
El Turneling Protocols	Chur News INCODE	Falastala anna alassa an 6-m
- EHP Routing	Class Hame REDBG	Select the event class to configure.
- Management Protocols	Enable 🔽	Check to enable special handling of this class.
General	Home of the following values has been out to the Event List	the Event List can be even by viewing Configuration System Fronts General
FTP Backup	is one of the following values has control to one even and,	the president concerned and the state of the state of the second of the
<u></u>	Changing a value set to Use Event List will override the section	as of the Event List referring to this event class.
	Dented Inc. Dente March D.	Coloritation consistentia di Alteriani
System Servers	Takura to rog Perendes 1-2	Select the events to enter in the log.
<u>SMIP Servers</u>	Events to Consols Severities 1-3 💌	Select the events to display on the consols.
The Section	Events to Syslog None	Select the events to send to a Syslog Server.
Line Salancing	Events to Email None	Select the events to send to an Ersail Recipient.
- Die laar Management	THE PARTY OF THE P	
El Color Manageria II	Events to Trap None 💌	Select the events to send to an SNMP Trap Destination.
- Monitoring	Add Cancel	

3. Wählen Sie Monitoring > Filterable Event Log (Überwachung > Filterbares Ereignisprotokoll) aus, um die aktivierten Alarme zu

überwachen.

-E-Configuration				
	Monitorina Filterable Event Lon			
Destature				
The heither an Management	Select Filter Options			
- HARVER RESERVED TO THE PROPERTY.	Event Class Al Closses Severifies ALL			
	AUTH E			
- IP Routing	AUTHORG 2			
- III Management Protocols	AUTHDECODE VI 3 VI			
- CHEVERIA				
General	Client IP Address 0.0.0.0 Events/Page 100			
ETP Backup				
<u>Closses</u>	Geoup —AI— Direction Oldest to Newest			
Trap Destinations				
Systog Servers	GetLog SaveLog GearLog			
SMTP Servers				
Enal Recipients				
	37463 01/02/2004 11-50-20 540 CUV-6 TUTBEROBE/0 885-21007 20 20 20 1			
Load Balancing	TAREN WINDER			
- EHUser Management	Internet Handword, in the end of the second se			
EPplicy Management	Responder Cookie(0): 60 DZ 66 0Z 86 CD 1Z 60			
- Administration	Next Payload : HASH (8)			
- Monitoring	Exchange Type : Dakley Informational			
Routing Table	Flags : 1 (HCOYPT)			
Ovpanio Filtera	Berrage ID : a3000ced			
Ellerable Event Log	Length : 92			
it we Event Lon	97488 04/84/9004 44.50.98 548 586 4 VUREFORD/0 885./4088 00 00 08 4			
-ElSystem State a	arbad ulgerious integra and bette integrably apreside bolog as i			
-ElSerring	DOT : IPSEC (1)			
- El Statistica	Protocol : IEANCP (1)			
- C) satisfies	Herrage : DPD R-U-THERR-ACK (S6137)			
	Spi : AD AD OC 53 09 CA 55 25 60 12 66 02 06 00 12 60			
	Length : 32			
	30005 01/02/2004 11:55:40.540 SEV-# IKENECUDE/0 NUT-61095 30.30.30.1			
	INDERVISED (VERSION 1.0)			
CISCO SYSTEMS	Technical contractor: 60 52 65 00 86 00 12 60			
de de	Bach Daving : HARK (2)			
and the second second second	Exchange Type : Oakley Informational			

Zugehörige Informationen

- Advanced Encryption Standard (AES)
- DES/3DES/AES-VPN-Verschlüsselungsmodul
- IPSec-Beispielkonfigurationen
- <u>Cisco VPN Client Support-Seite der Serie 3000</u>
- Support-Seite für IPSec-Aushandlung/IKE-Protokolle