Een IPSec-tunnelband configureren tussen een Cisco VPN 3000 Concentrator en een checkpoint NGO-firewall

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Netwerkdiagram Configuraties De VPN 3000-concentratie configureren Het selectieteken configureren Verifiëren Controleer de netwerkcommunicatie Tunnelstatus op checkpoint NG bekijken Tunnelstatus op VPN-centrator bekijken Problemen oplossen Netwerksamenvatting Debugs voor het checkpoint NG Debugs voor de VPN-concentratie Gerelateerde informatie

Inleiding

Dit document toont hoe te om een IPSec-tunnel met pre-gedeelde sleutels te vormen om tussen twee privé netwerken te communiceren. In dit voorbeeld zijn de communicerende netwerken het privé-netwerk van 192.168.10.x binnen Cisco VPN 3000 Concentrator en het privé-netwerk van 10.32.x.x binnen het Checkpoint Next Generation (NG) Firewall.

Voorwaarden

Vereisten

- Het verkeer van binnen de VPN Concentrator en binnen het checkpoint NG naar het internet — hier vertegenwoordigd door de 172.18.124.x netwerken — moet vóór het begin van deze configuratie stromen.
- De gebruikers moeten bekend zijn met de onderhandeling van IPSec. Dit proces kan in vijf

stappen worden opgesplitst, waaronder twee IKE-fasen (Internet Key Exchange).Een IPSectunnel wordt geïnitieerd door interessant verkeer. Het verkeer wordt als interessant beschouwd wanneer het tussen de IPSec-peers reist.In IKE Fase 1 onderhandelen de IPSecpeers over het vastgestelde beleid van de IKE Security Association (SA). Zodra de peers authentiek zijn, wordt een veilige tunnel gecreëerd met het Protocol van de Veiligheid van Internet en het Protocol van het Toetsbeheer (ISAKMP).In IKE fase 2 gebruiken de IPSecpeers de geauthentiseerde en beveiligde tunnel om te onderhandelen over IPSec SAtransformaties. De onderhandelingen over het gedeelde beleid bepalen hoe de IPSec-tunnel tot stand wordt gebracht.De IPSec-tunnel wordt gecreëerd, en de gegevens worden tussen de peers van IPSec overgebracht op basis van de parameters die in de IPSec transformatiesets worden gevormd.De IPSec-tunnel eindigt wanneer de IPSec SAs worden verwijderd of wanneer hun levensduur verstrijkt.

Gebruikte componenten

Deze configuratie is ontwikkeld en getest met behulp van deze software en hardwareversies:

- VPN 3000 Series Concentrator 3.5.2
- Selectietekenfirewall

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: het IP-adresseringsschema dat in deze configuratie wordt gebruikt, is niet wettelijk routeerbaar op internet. Ze zijn RFC 1918-adressen, die in een labomgeving zijn gebruikt.

Configuraties

De VPN 3000-concentratie configureren

Volg deze stappen om de VPN 3000 Concentrator te configureren:

1. Ga naar **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** om de LAN-to-LAN sessie te configureren. Stel de opties in voor verificatie- en IKE-algoritmen, voorgedeelde sleutel, peer IP-adres en lokale en externe netwerkparameters. Klik op **Apply** (Toepassen).In deze configuratie werd de verificatie ingesteld als ESP-MD5-HMAC en werd de codering ingesteld als

3DES.

Configuration System Tunneling Protocols IPSec LAN-to-LAN Modify			
Modify an IPSec LAN-to-LAN connection.			
-			
Name Checkpoint	Enter the name for this LAN-to-LAN connection.		
Interface Ethernet 2 (Public) (172.18.124.131) •	Select the interface to put this LAN-to-LAN connection on.		
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.		
Digital None (Use Preshared Keys) *	Select the Digital Certificate to use.		
Certificate Entire certificate chain Transmission Identity certificate only	Choose how to send the digital certificate to the IKE peer.		
Preshared Key ciscortprules	Enter the preshared key for this LAN-to-LAN connection.		
Authentication ESP/MD5/HMAC-128 •	Specify the packet authentication mechanism to use.		
Encryption 3DES-168	Specify the encryption mechanism to use.		
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.		
Routing None *	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.		
Local Network			
Network List Use IP Address/Wildcard-mask below •	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.		
IP Address 192.168.10.0	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A		
Wildcard Mask 0.0.0.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.		
Remote Network			
Network List Use IP Address/Wildcard-mask below •	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.		
IP Address 10.32.0.0	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A		
Wildcard Mask 0.0.127.255	wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.		
Apply Cancel			

2. Kies Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen en stel de gewenste parameters in.Selecteer het IKE-voorstel IKE-3DES-MD5 en controleer de voor het voorstel geselecteerde parameters. Klik op Toepassen om de LAN-to-LAN sessie te configureren.Dit zijn de parameters voor deze configuratie:

Configuration System Tunneling Protocols IPSec IKE Proposals Modify			
Modify a configured IKE Proposal.			
Proposal Name IKE-3DES-MD5	Specify the name of this IKE Proposal.		
Authentication Mode Preshared Keys	Select the authentication mode to use.		
Authentication Algorithm MD5/HMAC-128 *	Select the packet authentication algorithm to use.		
Encryption Algorithm 3DES-168 -	Select the encryption algorithm to use.		
Diffie-Hellman Group Group 2 (1024-bits)	Select the Diffie Hellman Group to use.		
Lifetime Measurement Time 💌	Select the lifetime measurement of the IKE keys.		
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).		
Time Lifetime 86400	Specify the time lifetime in seconds.		
Apply Cancel			

3. Ga naar Configuration > Policy Management > Traffic Management > Security Associations,

selecteer IPSec SA dat is gemaakt voor de sessie en controleer de IPSec SA-parameters die zijn geselecteerd voor de LAN-to-LAN sessie. In deze configuratie was de naam van de LAN-to-LAN sessie "Selectieteken", zodat IPSec SA automatisch werd gemaakt als "L2L: Selectieteken."



Dit zijn de parameters voor deze

SA:	
Configuration Policy Management Traffic Management	Security Associations Modify
Modify a configured Security Association.	
SA Name L2L: Checkpoint	Specify the name of this Security Association (SA).
Inheritance From Rule 💌	Select the granularity of this SA.
IPSec Parameters	
Authentication Algorithm ESP/MD5/HMAC-128 -	Select the packet authentication algorithm to use.
Encryption Algorithm 3DES-168 -	Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled	Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time 💌	Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime 86400	Specify the time lifetime in seconds.
IKE Parameters	
IKE Peer 172.18.124.157	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode Main	Select the IKE Negotiation mode to use.
Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
Certificate Transmission [©] Entire certificate chain [®] Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.
Apply Cancel	

Het selectieteken configureren

De objecten en regels van het netwerk worden bepaald op het checkpoint NG om het beleid in te stellen dat betrekking heeft op de VPN-configuratie. Dit beleid wordt vervolgens geïnstalleerd in de Checkpoint NG Policy Editor om de checkpoint NG kant van de configuratie te voltooien.

1. Maak de twee netwerkobjecten voor het Checkpoint NG-netwerk en het VPN-centrator-

netwerk dat het interessante verkeer versleutelt.Als u objecten wilt maken, selecteert u **Bewerken > Netwerkobjecten** en vervolgens selecteert u **Nieuw > Netwerk**. Voer de juiste netwerkinformatie in en klik vervolgens op OK.Deze voorbeelden tonen de set van netwerkobjecten die CP_interne (het binnennetwerk van het Selectieteken NG) en CONC_INSIDE (het binnennetwerk van de VPN Concentrator) worden

ľ	etwork Properties - CP_inside		×
	General NAT		
	<u>N</u> ame: CP_inside		
	IP <u>A</u> ddress: 10.32.0.0		
	Net <u>M</u> ask: 255.255.128.0		
	Comment: CPINSIDE		
	Cojor:		
	Broadcast address: Included O Not included		
	OK Cancel	Help	
1.L			

Network Proper	ties - CONC_INSIDE	×
General NAT	1	
<u>N</u> ame:	CONC_INSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Concentrator network	
Color:		
Broadcast <u>I</u> nclude	address: ed <u>O No</u> t included	
	OK Cancel H	elp

2. Ga naar Manager > Netwerkobjecten en selecteer Nieuw > Workstation om werkstationobjecten voor VPN-apparaten, Checkpoint NG en VPN Concentrator te maken.N.B.: U kunt het object Controleren of het werkstation is aangemaakt tijdens de eerste installatie van Selectieteken. Selecteer de opties om het werkstation in te stellen als Gateway en Interoperable VPN-apparaat en klik vervolgens op OK.Deze voorbeelden tonen de set van objecten cisco.p (Checkpoint NG) en CISCO_CONC (VPN 3000 Concentrator):

Workstation Properties - c	iscocp	×
Workstation Properties - c	iscocp General Name: Ciscocp IP Address: 172.18.124.157 Genment: Checkpoint External IP Color:	×
	Type: C Host C Gateway Check Point Products ✓ Check Epint products installed: Version NG ✓ Get Version ✓VPN-1 & FireWall-1 ✓FloodGate-1 Policy Server ✓ Primary Management Station	
	Object Management Image: Managed by this Management Server (Internal) Image: Managed by another Management Server (External) Secure Internal Communication Image: Description of the transformation Image: Description of the transformation <td< td=""><td></td></td<>	
	OK Cancel He	alp

Workstati	on Properties -	ISCO_CONC	×
Gene	ral	General	
- NAT	logy	Name: CISCO_CONC	
	nced	IP Address: 172.18.124.131	<u>G</u> et address
		Comment: VPN Concentrator	
		Cojor:	
		Type: C <u>H</u> ost CGate <u>w</u> ay	
		Check Point Products	<u></u>
		Check Point products installed: Version	G 💌 Get Version
		□VPN-1 & FireWall-1 □ FloodGate-1 □ Policy Server □ Management Station	-
		Object Management	
		C Managed by this Management Server (Inter	nel)
		C Managed by another Management Server (E	[xternal]
		Interoperable ⊻PN Device	
1		OK	Cancel Help

3. Ga naar Manager > Netwerkobjecten > Bewerken om het venster Workstation Properties te openen voor het Checkpoint NG-werkstation (ciscop in dit voorbeeld). Selecteer Topologie uit de keuzes aan de linkerkant van het venster en selecteer vervolgens het netwerk dat moet worden versleuteld. Klik op Bewerken om de interfaceeigenschappen in te stellen. In dit voorbeeld is CP_interne het netwerk van het checkpoint NG.

	ciscocp			
General	Topology			
- NAT	<u>G</u> et Interface	s		
VPN	Name	IP Address	Network Mask	IP Addresses behind
- Management	E100B0	10.32.50.50	255.255.128.0	CP_inside
- Advanced	E100B1	172.18.124.157	255.255.255.0	External
	•			
	Add	Edit	Remove	Show
	Show all IPa b			
	STIOW all IP's D	Jenina Gateway		
	VPN Domain			
	With Domain =			
	All IP Address information.	sses <u>b</u> ehind Gateway b	ased on Topology	Show
	All IP Address information.	sses <u>b</u> ehind Gateway b	ased on Topology	Show
	 All IP Address information. <u>Manually Description</u> 	sses <u>b</u> ehind Gateway b sfined	ased on Topology	Show Show
	 All IP Address information. Manually Department 	sses <u>b</u> ehind Gateway b efined	ased on Topology	Sh <u>o</u> w Sho <u>w</u>
	 All IP Address information. <u>Manually De</u> 	sses <u>b</u> ehind Gateway b	ased on Topology	Show
	 All IP Addressinformation. Manually De Exportable for 	sses <u>b</u> ehind Gateway b efined or SecuRemote	ased on Topology	Show Sho <u>w</u>
	 All IP Addresinformation. Manually De Exportable for 	sses <u>b</u> ehind Gateway b fined	ased on Topology	Sh <u>o</u> w Sho <u>w</u>
	 All IP Addresinformation. Manually De Exportable fr 	sses <u>b</u> ehind Gateway b efined	ased on Topology	Sh <u>o</u> w Sho <u>w</u>
	 All IP Address information. Manually De Exportable for a second seco	sses <u>b</u> ehind Gateway b fined	ased on Topology	Show Show

4. Selecteer in het venster Interface Properties de optie om het werkstation als intern aan te wijzen en geef vervolgens het juiste IP adres op. Klik op **OK**.De weergegeven topologie selectie wijst het werkstation aan als intern en specificeert IP adressen achter de CP_interne

Interface Properties		×
General Topology QoS		
Topology		
C External (leads out to the internet)		
[Internal (leads to the local network)]		
IP Addresses behind this interface:		
◯ <u>N</u> ot Defined		
O Network defined by the interface IP and the in	d Net Mask	
	•	
Anti-Spoofing		
Review Anti Specifing based on interface tor	ologu	
Speef Tracking: O. News O. Less O	Alex	
	Alen	
OK Cancel H	Help	

interface:

5. Selecteer in het venster Werkstationeigenschappen de externe interface in het vak Selectieteken dat naar het internet leidt en klik vervolgens op **Bewerken** om de interfaceeigenschappen in te stellen. Selecteer de optie om de topologie als extern aan te

I	Interface Properties
	General Topology QoS
	Topology
	 External (leads out to the internet)
	Internal (leads to the local network)
	IP Addresses behind this interface:
	C Not Defined
	$igcap_{ ext{o}}$ Network defined by the interface IP and Net Mask
	C Specific:
	Anti Specifina
	Perform Anti-Spoofing based on interface topology
	Spoof Tracking: 🔿 None 💽 Log 🔿 Alert
	OK Cancel Help

wijzen, dan klik op OK.

6. Selecteer in het venster Workstation Properties op Checkpoint NG de optie **VPN** van de keuzes aan de linkerkant van het venster en selecteer vervolgens de IKE parameters voor encryptie en authenticatie algoritmen. Klik op **Bewerken** om de IKE-eigenschappen te configureren.

Workstation Properties - o	iscocp	×
General Topology NAT VEN Authentication Management € Advanced	VPN Encryption schemes Image: Imag	
	Nickname DN Certificate Authority Image: Certificate Authority Add Egit OK Certificate Authority	

7. Stel de IKE-eigenschappen in om de eigenschappen in de VPN-Concentrator aan te passen.Selecteer in dit voorbeeld de coderingsoptie voor **3DES** en de hashing optie voor

IKE Properties	×		
General			
Support key exchange encryption w	/ith:		
DES			
CAST			
I I I I I I I I I I I I I I I I I I I	SHA <u>1</u>		
- Support authentication methods:			
Support authentication methods: Pro Shared Secret	E dit Secrete		
	Edit <u>Secrets</u>		
Public Key Signatures	Specify		
<u>A</u> dvanced			
UK Ca	ncel Help		

MD5.

 Selecteer de authenticatieoptie voor Vooraf gedeelde geheimen en klik vervolgens op Geheimen bewerken om de voorgedeelde sleutel in te stellen die compatibel is met de voorgedeeld toets op de VPN-centrator. Klik op Bewerken om de toets zoals weergegeven in te voeren en klik vervolgens op Instellen,

Shar	ed Secret	
Г	Shared Secrets List:	
	Peer Name Shared Secret CISCO_CONC ****	<u>E</u> dit <u>R</u> emove
	Enter secret: ciscortprules Set	J
	OK Cancel	Help

9. Klik in het venster IKE-eigenschappen op **Geavanceerd...** en wijzig deze instellingen:Deselecteer de optie voor **Support agressief modus**.Selecteer de optie voor de **Support-toets voor subnetten**.Klik na voltooiing op **OK**,

Advanced IKE properties			×
Use <u>UDP</u> encapsulation			
Support Diffie-Hellman groups	UDP VPN1_IPS	SEC_encapsi 💌]
	Group 1 (76	i8 bit)	
	Group 2 (10	(24 bit) (36 bit)	
Rekeying Parameters			J
Renegotiate IKE security assoc	iations	1440 🕂	Minutes
Renegotiate IPSEC Security as:	sociations every	3600 📑	Seconds
Renegotiate IPSEC Security	associations eve	ary 50000 🚊	KBytes
Misc			
Support IP <u>compression</u> for	SecureClient		
Support <u>aggresive</u> mode	. h t.		
Support Key exchange for s	ubnets		
ОК	Cancel	Help	

10. Ga naar Manager > Netwerkobjecten > Bewerken om het venster Workstation Properties te openen voor VPN Concentrator. Selecteer Topologie uit de keuzes aan de linkerkant van het venster om het VPN-domein handmatig te definiëren. In dit voorbeeld wordt CONC_INSIDE (het interne netwerk van de VPN Concentrator) gedefinieerd als het VPNdomein.

Workstation Properties	- CISCO_CONC			Ē.	×
- General	Topology				
NAT	<u>G</u> et Interfaces				
VPN Advanced	Name	IP Address	Network Mask		
	Add Show all IPs beh	Edt	<u>B</u> emove	how	
	VPN Domain C All IP Addresse information. C <u>M</u> anually Defin	ed + CONC INS	ased on Topology	Sh <u>o</u> w Sho <u>w</u>	_] 1
	Egortable for 9	SecuRemote			,
			ок с	ancel Help	<u> </u>

11. Selecteer **VPN** vanuit de bestandsindelingen aan de linkerkant van het venster en selecteer vervolgens **IKE** als coderingsschema. Klik op **Bewerken** om de IKE-eigenschappen te configureren.

Workstation Properties -	CISCO_CONC			×
General Topology NAT Advanced	VPN Encryption gchemes			
		OK	Cancel	Help

12. Stel de IKE-eigenschappen in om de huidige configuratie op de VPN-concentratie weer te geven.Stel in dit voorbeeld de coderingsoptie voor **3DES** en de hashing optie voor **MD5**

IKE Properties General	د
Support key exchange encryptio	n with: Support data integrity with: MD <u>5</u>
Support authentication methods:	Edit <u>S</u> ecrets
□ Public Key Signatures □ VPN-1 & FireWall-1 authent	<u>Matching Criteria</u> ication for SecuRemote (Hybrid Mode)
	Advanced

13. Selecteer de authenticatieoptie voor **Vooraf gedeelde geheimen** en klik vervolgens op **Geheimen bewerken** om de voorgedeelde sleutel in te stellen. Klik op **Bewerken** om de toets zoals weergegeven in te voeren en klik vervolgens op **Instellen**.

Shar	ed Secret				2
- ۲ ⁹	Shared Secrets Lis	st:			1
	Peer Name	Shared S	ecret		
	ciscocp	****		<u>E</u> dit	
				<u>H</u> emove	
	,				
	Enter secret: ci	scortprules	Set		
	OK	Can	cel	<u>H</u> elp	

14. Klik in het venster IKE-eigenschappen op Geavanceerd... en wijzig deze instellingen:Selecteer de groep Diffie-Hellman die geschikt is voor de IKEeigenschappen.Deselecteer de optie voor Support agressief modus.Selecteer de optie voor de Support-toets voor subnetten.Klik na voltooiing op OK,

Advanced IKE propertie	:5			×
Use UDP encapsulation	m			
Support Diffie-Hellman gro	oups	P VPN1_IPSE	C_encapsi 💌]
		Group 1 (768 Group 2 (1024	bit) 4 bit)	
		Group 5 (1538	S bit)	
Rekeying Parameters —	-			
Renegotiate IKE sec	urity associations	3	1440 📑	Minutes
Renegotiate IPSEC 9	ecurity associat	ions every	3600 📑	Seconds
🔲 Renegotiate IPS	EC Security asso	ciations every	50000 🚊	KBytes
Misc Support IP <u>c</u> omp Support <u>agg</u> resiv	ession for Secur	eClient		
🔽 Support key excł	hange for <u>s</u> ubnet	s		
ОК	Canc	el	<u>H</u> elp	

15. Selecteer Regels > Toevoegen Regels > Boven om de coderingsregels voor het beleid te configureren. Plaats in het venster Policy Editor een regel met bron als CP_interne (binnen netwerk van het checkpoint NG) en bestemming als CONC_INSIDE (binnen netwerk van de VPN-centrator) in. Stel waarden voor Service = Any, Action = Encrypt en Track = Log in. Wanneer u het gedeelte Encrypt Action van de regel hebt toegevoegd, klikt u met de rechtermuisknop op Actie en vervolgens selecteert u Eigenschappen bewerken.

CISCOCP - Check Point Policy Editor	- Standard				Second and	_IO ×
File Edit View Manage Rules Policy	Topology Search Window I	Help				
」■● X℃睛 畳趣液	A] 🗉] 🖳 💣 🛎	' ≘ ". ↔	54 🛛 🖄 🍈			
1 Pa 🖬 💷 🐉 🤌 🗛 🖉	1 Q Q 🖸 💊 👘	•				
\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	🗱 Security - Standard 🗮	Address Translation - St	andard 🙀 QoS - S	tandard 🛄 Desktop Se	ecurity - Standard	
E - L Network Objects	NO SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
Workstation	Ho. Sounce	DESTIMATION	SERVICE	PACITION	THEYLAR	INSTALL
CISCO_CONC	1 CP_inside + CONC_INSIDE	부 CONC_INSIDE 부 CP_inside	* Any	Edit propert	ies	Gateway:
-++ CONC_INSIDE	2 4 CP_inside	* Any	* Any	Add Encrypt	.on	Gateway:
CP_inside CP_inside CSE Device Enbedded Device CSE	Name CISCO_CONC ciscocp	IP 172.18.1 172.18.1	Comment 24.131 VPN Conc 24.157 Checkpoir	Accept Accept Accept Accept Accept Clert Auth Clert Auth Clert Auth Clert Auth Clert From Clert Encrypt Clert Encrypt Clert Colur Clear Query Colur	s uth ypt	2

16. Selecteer IKE en klik op

Encryption Properties		×
General		
Encryption <u>s</u> chemes defined:		
<u>E</u> dit		
OK Can	cel Help	

Bewerken.

17. Wijzig in het venster IKE Properties de eigenschappen om met de VPN Concentratortransformatie overeen te komen.Stel de optie Omzetten in op Encryption + Data Integrity (ESP).Stel het Encryption Algorithm in op 3DES.Stel de gegevensintegriteit in op MD5.Stel de toegestane gateway van peer in om de VPN-concentratie (CISCO_CONC) aan te passen.Klik na voltooiing op

IKE Properties	
General	
Transform	
Encryption + Data Integril	y (ESP)
O Data Integrity Only (AH)	
Encryption Algorithm:	3DES 🔽
<u>D</u> ata Integrity	MD5
Compression method:	None
Allowed Peer Gateway	
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit) 💌
Perform IP <u>P</u> ool NAT	
ОК Са	ancel Help

18. Nadat het selectieteken NGO is geconfigureerd, slaat u het beleid op en selecteert u **Beleidsbeleid > Installatie** om het in te



Het installatievenster toont voortgangsnoten bij het samenstellen van het



beleid.

Wanneer het installatievenster aangeeft dat de beleidsinstallatie is voltooid, klikt u op **Sluiten** om de procedure te

voltooien.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer de netwerkcommunicatie

Om communicatie tussen de twee privé netwerken te testen, kunt u een ping van één van de privé netwerken naar het andere privé netwerk initiëren. In deze configuratie is een ping van de kant Checkpoint NG (10.32.50.51) naar het VPN Concentrator-netwerk verzonden (192.168.10.2).

```
C:\WINNT\System32\cmd.exe
```

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = Oms, Maximum = 10ms, Average =
                                                5ms
C:\>
C:\>
C:\>
C:\>
```

Tunnelstatus op checkpoint NG bekijken

Om de tunnelstatus te bekijken, gaat u naar de Policy Editor en selecteert **Windows > System Status**.

CISCOCP - Check Point System Status			
Ele View Modules Products Iools Window Help			
🗩 🎯 🖳 🛝 🛄 🔦 🧱 🛼 💭 🚔	59		
Modules IP Address	VPN-1 Details		
	Status:	ок	
E-Ciscocp 172.18.124.157	Packets		
FireWal-1	Encrypted:	19	
FloodGate-1	Decrypted:	18	
Management	Errors		
SVN Foundation	Encryption errors:	0	
	Decryption errors:	0	
	IKE events errors:	3	
	Hardware		
	HW Vendor Name:	none	
	HW Status:	none	
For Help, press F1			Last updated:09:34:14 PM

Tunnelstatus op VPN-centrator bekijken

Om de tunnelstatus op de VPN Concentrator te controleren ga naar **Administratie > Sessies beheren**.

his screen shows st formation on a sess	nister Sessions atistics for sessions. ' ion, click on that sess	To refresh the statis sion's name. To log	tics, click Refr out a session, cl	sh. Sel ick Log	ect a Group gout in the tal	Vedneso to filter ble belov	the sessions w. To test th	ember 2002 20:37: Reset @ Refresh . For more he network
roupAll ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/U	JDP Us	er IPSec/TC	P User	IPSec LAN	I-to-LAN
Active LAN-to-	Active Remote	Active Management	Total Active	Peak	Concurrent	Cone	urrent	Total Cumulative
LAN Sessions	Access Sessions	Sessions	Sessions		essions	262210	ns Lanut	Sessions
LAN Sessions	Access Sessions	Sessions 3	4		4	1	500	17
LAN Sessions	Access Sessions 0 essions	Sessions 3	4		4	1 Cess Ses	500 sions Man	17 agement Sessions
LAN Sessions 1 LAN-to-LAN S Connection Nan	Access Sessions 0 essions IP Address	Sessions 3 Protoco	4	yption	4 [Remote Acc	1 cess Ses	500 sions Man	17 agement Sessions Actions

Selecteer onder LAN-to-LAN sessies de verbindingsnaam voor het checkpoint om gegevens over de gemaakte SA's en het aantal verzonden/ontvangen pakketten weer te geven.

Connection Name IP Ad		dress Protocol		Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
Checkpoint	172.18.12	4.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	25		
	Session TD	1	IK	E Session	Encryption Algorit	m 3DES-1	68	242322-23223-2722322		
a occ oconomi i			IK	E Session						
	Session ID	1			Encryption Algorit	hm 3DES-1	3DES-168			
Hashing	Algorithm	MD5			Diffie-Hellman Gro	up Group 2	Group 2 (1024-bit)			
Authentica	tion Mode	Pre-Sh	ared Keys	I	KE Negotiation Mo	de Main				
Rekey Tin	e Interval	86400	seconds							
			IPS	ec Session						
:	Session ID	2			Remote Addr	ess 10.32.0.	10.32.0.0/0.0.127.255			
Loc	al Address	192.16	8.10.0/0.0.0.255		Encryption Algorith	hm 3DES-1	3DES-168			
Hashing	Algorithm	MD5			S	EP 1	1			
	then Made	Tunnel			Rekey Time Inter	val 28800 s	28800 seconds			
Encapsula	tion Mode	a summer								

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opmerking: Het verkeer moet niet PATed via de IPSec-tunnel zijn met behulp van het VPN Concentrator openbare IP-adres (externe interface). Anders faalt de tunnel. Het IP-adres dat voor PATing wordt gebruikt, moet dus een ander adres zijn dan het adres dat op de externe interface is ingesteld.

Netwerksamenvatting

Wanneer meerdere, aangrenzende netwerken in het encryptie-domein op het Selectieteken worden geconfigureerd, kan het apparaat automatisch de netwerken met betrekking tot interessant verkeer samenvatten. Als de VPN Concentrator niet is geconfigureerd om aan elkaar te koppelen, zal de tunnel waarschijnlijk falen. Als bijvoorbeeld de interne netwerken van 10.0.0.0/24 en 10.0.1.0/24 zodanig zijn geconfigureerd dat ze in de tunnel worden opgenomen, kunnen deze netwerken worden samengevat tot 10.0.0.0/23.

Debugs voor het checkpoint NG

Selecteer Venster > Log in om de logbestanden te bekijken.

1	CISCOCP - C	heck Poi	int Log Vie	wer - [fv	[pol.v												X
6	Ele Elos Far Secon Ken Tors Kluon Beb																
	Date	Time	Product		Inter.	Orig	Туре	Action	Source	Destinati	Pr	Rule	S_P	Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireIV.	📻 dae	. ciscocp	📄 log	0- key instali	ciscocp	CISCO_CONC							
2	13Aug2002	21:32:	VPN-1	& FireVV	. 🕒 dae	. ciscocp	🔳 log	Ow key instal	ciscocp	CISCO_CONC					0x5879f30d	0xt1351129	

Ga naar **Configuration > System > Event > Classes** om **uitvindingen** op **de** VPN-centrator **in te** schakelen. Schakel AUTH, AUTHDBG, IKE, IKEDBG, IPSEC en IPSECDBG in om als 1-13 te loggen. Om **beelden** te bekijken, selecteert u **Monitoring > Filterable Event Log**.

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128 3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 processing SA payload 4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 Oakley proposal is acceptable 14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157 processing VID payload 15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157 processing IKE SA 16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated) 22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3 26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp 27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84 29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157

RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send TOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 25648 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157]

Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDEG/1 RPT=10 AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10 Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10 AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10 AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10 AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10 Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10 AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10 Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10 AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10 AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10 Reply timer started: handle = 4B0018, timestamp = 1163319, timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10 AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19 IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19 IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10 xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20 IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10 IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10 AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20 IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10 IntDB_Rcv(51a6b48)

74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10

AUTH_DeleteTimer(51a6b48, 0, 0) 75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10 Reply timer stopped: handle = 4B0018, timestamp = 1163329 76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10 AUTH_Callback(51a6b48, 0, 0) 77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157 Authentication successful: handle = 9, server = Internal, group = 172.18.124.15778 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157 Group [172.18.124.157] Found Phase 1 Group (172.18.124.157) 79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10 AUTH_GetAttrTable(9, 748420) 80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157 Group [172.18.124.157] Authentication configured for Internal 81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: IP Compression = disabled 82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157 Group [172.18.124.157] IKEGetUserAttributes: Split Tunneling Policy = Disabled 83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10 AUTH_Close(9) 84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157 Group [172.18.124.157] constructing ID 85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527 Group [172.18.124.157] construct hash payload 86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157 Group [172.18.124.157] computing hash 87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157 Group [172.18.124.157] constructing dpd vid payload 88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) ... total length : 80 90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157 Group [172.18.124.157] PHASE 1 COMPLETED 91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157 Keep-alive type for this connection: None 92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157

Keep-alives configured on but peer does not support keep-alives (type = None) 93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157 Group [172.18.124.157] Starting phase 1 rekey timer: 64800000 (ms) 94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16 User 172.18.124.157 connected 95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10 AUTH_UnbindServer(51a6b48, 0, 0) 96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10 Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0 97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10 AUTH_Int_FreeAuthCB(51a6b48) 98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10 Authentication session closed: handle = 9 99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 156 102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157 Group [172.18.124.157] processing hash 103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157 Group [172.18.124.157] processing SA payload 104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157 Group [172.18.124.157] processing nonce payload 105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157 Group [172.18.124.157] Processing ID 106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157 Group [172.18.124.157] Received remote IP Proxy Subnet data in ID Payload: Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0 109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157 Group [172.18.124.157] Processing ID 110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157 Group [172.18.124.157] Received local IP Proxy Subnet data in ID Payload: Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0 113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534 QM IsRekeyed old sa not found by addr 114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157 Group [172.18.124.157] IKE Remote Peer configured for SA: L2L: Checkpoint

115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157 Group [172.18.124.157]

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157 Group [172.18.124.157] IPSec SA Proposal # 1, Transform # 1 acceptable 117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157 Group [172.18.124.157] IKE: requesting SPI! 118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39 IPSEC key message parse - msgtype 6, len 200, vers 1, pid 0000000, seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300 122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139 Processing KEY_GETSPI msg! 123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10 Reserved SPT 305440147 124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10 IKE got SPI from key engine: SPI = 0x1234a593 125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157 Group [172.18.124.157] oakley constucting quick mode 126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157 Group [172.18.124.157] constructing blank hash 127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157 Group [172.18.124.157] constructing ISA_SA for ipsec 128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157 Group [172.18.124.157] constructing ipsec nonce payload 129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157 Group [172.18.124.157] constructing proxy ID 130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157 Group [172.18.124.157] Transmitting Proxy Id: Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0 Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0 134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157 Group [172.18.124.157] constructing qm hash 135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157 SENDING Message (msgid=54796f76) with payloads : HDR + HASH (8) + SA (1) ... total length : 152 137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157 RECEIVED Message (msgid=54796f76) with payloads : $HDR + HASH (8) + NONE (0) \dots total length : 48$

processing IPSEC SA

139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157

Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msghdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA 158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255 159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success 160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147

Processing KEY_UPDATE msg!

165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148

Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150 No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151 KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152 KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7 IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547 pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157 Group [172.18.124.157] PHASE 2 COMPLETED (msgid=54796f76)

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- <u>Cisco VPN 3000 Series clientondersteuningspagina</u>
- IPsec-ondersteuningspagina
- Technische ondersteuning Cisco-systemen