Konfigurieren eines IPSec-Tunnels zwischen einem Cisco VPN 3000-Konzentrator und einer Checkpoint NG-Firewall

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Netzwerkdiagramm Konfigurationen Konfigurieren des VPN 3000-Konzentrators Konfigurieren des Prüfpunkts NG Überprüfen Überprüfen der Netzwerkkommunikation Tunnel-Status auf Checkpoint NG anzeigen Anzeigen des Tunnelstatus im VPN-Concentrator Fehlerbehebung Netzwerkzusammenfassung Debugger für Checkpoint NG Debugger für den VPN Concentrator Zugehörige Informationen

Einführung

Dieses Dokument veranschaulicht, wie ein IPSec-Tunnel mit vorinstallierten Schlüsseln konfiguriert wird, um zwischen zwei privaten Netzwerken zu kommunizieren. In diesem Beispiel sind die Kommunikationsnetzwerke das private 192.168.10.x-Netzwerk im Cisco VPN 3000 Concentrator und das private 10.32.x.x-Netzwerk innerhalb der Checkpoint Next Generation Firewall (NG).

Voraussetzungen

Anforderungen

 Benutzer müssen mit IPSec-Aushandlung vertraut sein. Dieser Prozess kann in fünf Schritte unterteilt werden, darunter zwei IKE-Phasen (Internet Key Exchange). Ein IPSec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr wird als interessant angesehen, wenn er zwischen den IPSec-Peers übertragen wird. In IKE Phase 1 handeln die IPSec-Peers die festgelegte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mit der Internet Security Association und dem Key Management Protocol (ISAKMP) erstellt. In IKE Phase 2 verwenden die IPSec-Peers den authentifizierten und sicheren Tunnel, um IPSec SA-Transformationen auszuhandeln. Die Aushandlung der gemeinsam genutzten Richtlinie legt fest, wie der IPSec-Tunnel eingerichtet wird.Der IPSec-Tunnel wird erstellt, und die Daten werden zwischen den IPSec-Peers übertragen, basierend auf den in den IPSec-Transformationssätzen konfigurierten IPSec-Parametern.Der IPSec-Tunnel endet, wenn die IPSec-SAs gelöscht werden oder ihre Lebensdauer abläuft.

Verwendete Komponenten

Diese Konfiguration wurde mit den folgenden Software- und Hardwareversionen entwickelt und getestet:

- VPN Concentrator der Serie 3000 3.5.2
- Checkpoint NG-Firewall

Konventionen

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Das in dieser Konfiguration verwendete IP-Adressierungsschema ist im Internet nicht legal routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurationen

Konfigurieren des VPN 3000-Konzentrators

Führen Sie die folgenden Schritte aus, um den VPN 3000-Konzentrator zu konfigurieren:

 Gehen Sie zu Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN, um die LAN-to-LAN-Sitzung zu konfigurieren. Legen Sie die Optionen f
ür Authentifizierungs- und IKE-Algorithmen, einen vorinstallierten Schl
üssel, eine Peer-IP-Adresse sowie lokale und Remote-Netzwerkparameter fest. Klicken Sie auf Übernehmen. In dieser Konfiguration wurde die Authentifizierung als ESP-MD5-HMAC und die Verschl
üsselung als 3DES festgelegt.

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 ciscontprules	Enter the preshared key for this LAN-to-LAN connection.
Authentication ESP/MD6/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 willoand mark which is the reverse of a subnet mark 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 Wildcard Mask 0.0.127.255	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A 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. Gehen Sie zu Configuration > System > Tunneling Protocols > IPSec > IKE Proposals, und legen Sie die erforderlichen Parameter fest.Wählen Sie das IKE-Angebot IKE-3DES-MD5 aus, und überprüfen Sie die für das Angebot ausgewählten Parameter. Klicken Sie auf Apply, um die LAN-zu-LAN-Sitzung zu konfigurieren.Dies sind die Parameter für diese Konfiguration:

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. Gehen Sie zu **Configuration > Policy Management > Traffic Management > Security Associations**, wählen Sie die für die Sitzung erstellte IPSec SA aus, und überprüfen Sie die für die LAN-zu-LAN-Sitzung ausgewählten IPSec SA-Parameter.Bei dieser Konfiguration lautete der Name der LAN-zu-LAN-Sitzung "Checkpoint", sodass die IPSec SA automatisch als "L2L:

Checkpoint."

Configuration Policy Management Traffic Manag	gement Security Associatio	ns Save Needed 🖶
This section lets you add, configure, modify, and negotiate IKE parameters.	delete IPSec Security Assoc	iations (SAs). Security Associations use IKE Proposals to
Click Add to add an SA, or select an SA and clic	k Modify or Delete.	
	IPSec SAs ESP-DES-MD5 ESP-3DES-MD5 ESP/IKE-3DES-MD5 ESP-3DES-NONE ESP-12TP-TRANSPORT ESP-3DES-MD5-DH7 I2L: Checkpoint	Actions Add Modify Delete

Dies sind die Parameter für diese 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		

Konfigurieren des Prüfpunkts NG

Netzwerkobjekte und -regeln werden auf dem Prüfpunkt NG definiert, um die Richtlinie zu bilden, die sich auf die einzurichtende VPN-Konfiguration bezieht. Diese Richtlinie wird dann mit dem Checkpoint NG Policy Editor installiert, um die Checkpoint NG-Seite der Konfiguration abzuschließen.

 Erstellen Sie die beiden Netzwerkobjekte f
ür das Checkpoint NG-Netzwerk und das VPN Concentrator-Netzwerk, um den interessanten Datenverkehr zu verschl
üsseln.Um Objekte zu erstellen, w
ählen Sie Verwalten > Netzwerkobjekte und dann Neu > Netzwerk aus. Geben Sie die entsprechenden Netzwerkinformationen ein, und klicken Sie auf OK.Diese Beispiele zeigen die Einrichtung der Netzwerkobjekte CP_inside (das interne Netzwerk des Pr
üfpunkts NG) und CONC_INSIDE (das interne Netzwerk des VPN

	Network Proper	ties - CP_inside		×
	General NAT	1		
	<u>N</u> ame:	CP_inside		
	IP <u>A</u> ddress:	10.32.0.0		
	Net <u>M</u> ask:	255.255.128.0		
	<u>C</u> omment:	CPINSIDE		
	Color:			
	Broadcast	address: ed <u>O No</u> t included		
centrator).		OK Cancel	Help	

Network Prope	ties - CONC_INSIDE		×
General NAT			
<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>Includ</u>	address: ed <u>C No</u> t included		
	OK Cancel	Help	

2. Gehen Sie zu Verwalten > Netzwerkobjekte, und wählen Sie Neu > Workstation aus, um Workstation-Objekte für die VPN-Geräte, Checkpoint NG und VPN Concentrator zu erstellen.Hinweis: Sie können das Checkpoint NG-Workstation-Objekt verwenden, das während der ersten Checkpoint NG-Einrichtung erstellt wurde. Wählen Sie die Optionen aus, um die Workstation als Gateway und interoperables VPN-Gerät festzulegen, und klicken Sie dann auf OK.Diese Beispiele zeigen die Anordnung der Objekte ciscocp (Checkpoint NG) und 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

Workstation Properties -	CISCO_CONC	×
General	General	
- NAT	Name: CISCO_CONC	
	IP Address: 172.18.124.131 Get address	
	Comment: VPN Concentrator	
	Color:	
	Type: C <u>H</u> ost CGate <u>w</u> ay	
	Check Point Products	
	Check Point products installed: Version NG Cet Version	
	VPN-1 & FireWall-1 FloodGate-1 Policy Server Management Station	
	Object Management	
	C Managed by this Management Server (Internal)	
	C Managed by another Management Server (External)	
	Interoperable ⊻PN Device	
	OK Cancel Help	

3. Gehen Sie zu Verwalten > Netzwerkobjekte > Bearbeiten, um das Fenster Workstation-Eigenschaften für die Checkpoint NG-Workstation zu öffnen (in diesem Beispiel ciscocp). Wählen Sie Topology aus den Optionen links im Fenster aus, und wählen Sie dann das Netzwerk aus, das verschlüsselt werden soll. Klicken Sie auf Bearbeiten, um die Schnittstelleneigenschaften festzulegen. In diesem Beispiel ist CP_inside das interne Netzwerk des Prüfpunkts NG.

kstation Properties -	ciscocp			
General	Topology			
- Topology NAT	<u>G</u> et Interface	\$		
- VPN	Name	IP Address	Network Mask	IP Addresses behind
- Authentication	E100B0	10.32.50.50	255.255.128.0	CP_inside
- Management	E100B1	172.18.124.157	255.255.255.0	External
- Advanced				
	•			
	Add	Edit	Remove	Show
				2,1011
	Show all IPs b	ehind Gateway		
	VPN Domain			
	 All IP Address information 	sses <u>b</u> ehind Gateway b	based on Topology	Show
	information.			
	C <u>M</u> anually De	fined	*	Sho <u>w</u>
		1		
	Exportable f	or SecuRemote		
			04	Causal Halp

4. Wählen Sie im Fenster Schnittstelleneigenschaften die Option aus, die Workstation als intern festzulegen, und geben Sie dann die entsprechende IP-Adresse an. Klicken Sie auf **OK**.Die gezeigten Topologieauswahl bezeichnen die Workstation als intern und geben die IP-Adressen hinter der CP_inside-Schnittstelle

I	nterface Properties	X
	General Topology QoS	_
	Topology	
	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 Net Mask	
	Specific: + CP_inside	
	Anti-Spoofing ■ Perform Anti-Spoofing based on interface topology Spoof Tracking: ○ None Log ○ Alert	
	OK Cancel Help	

- an:
- 5. Wählen Sie im Fenster Eigenschaften von Workstations die externe Schnittstelle des Prüfpunkts NG aus, der zum Internet führt, und klicken Sie dann auf **Bearbeiten**, um die Schnittstelleneigenschaften festzulegen. Wählen Sie die Option aus, um die Topologie als extern festzulegen, und klicken Sie dann auf

Interface Properties
General Topology QoS
Topology
 External (leads out to the internet)
Internal (leads to the local network)
IP Addresses behind this interface:
O Not Defined
O Network defined by the interface IP and Net Mask.
O <u>S</u> pecific:
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Spoof Tracking: O N <u>o</u> ne 💿 Log O <u>A</u> lert
OK Cancel Help

- OK.
- 6. Wählen Sie im Fenster Workstation Properties (Workstation-Eigenschaften) des Pr
 üfpunkts NG VPN aus den Optionen links im Fenster aus, und wählen Sie dann die IKE-Parameter f
 ür Verschl
 üsselungs- und Authentifizierungsalgorithmen aus. Klicken Sie auf Bearbeiten, um die IKE-Eigenschaften zu konfigurieren.

Workstation Properties - o	iscocp X
General Topology NAT VPN Authentication Management T-Advanced	VPN Encryption schemes Image: Imag
	Nickname DN Certificate Authority Image: Conservation of the second se

 Legen Sie die IKE-Eigenschaften so fest, dass sie mit den Eigenschaften des VPN-Konzentrators übereinstimmen.Wählen Sie in diesem Beispiel die Verschlüsselungsoption für 3DES und die Hashing-Option für MD5

-	KE Properties	
	General	
	Support key exchange encryption v	with:
	Support authentication methods:	
	Pre-Snared Secret Public Key Signatures VPN 1 & First (all 1 authorities	Specify
		ition for pecanemote (Hybrid Mode)
		<u>A</u> dvanced

8. Wählen Sie die Authentifizierungsoption für vorinstallierte Geheimnisse aus, und klicken Sie dann auf Geheimnisse bearbeiten, um den vorinstallierten Schlüssel für die Kompatibilität mit dem vorinstallierten Schlüssel auf dem VPN Concentrator festzulegen. Klicken Sie auf Bearbeiten, um Ihren Schlüssel wie gezeigt einzugeben, und klicken Sie dann auf Festlegen,

Shar	ed Secret		
Г ⁹	Shared Secrets List: -		
	Peer Name CISCO_CONC	Shared Secret ****	<u>E</u> dit <u>R</u> emove
	Enter secret: cisco	rtprules Set	
	ОК	Cancel	<u>H</u> elp

 Klicken Sie im IKE-Eigenschaftenfenster auf Erweitert... und ändern Sie diese Einstellungen:Deaktivieren Sie die Option f
ür den aggressiven Support-Modus.W
ählen Sie die Option zum Austausch von Support-Schl
üsseln f
ür Subnetze aus.Wenn Sie fertig sind, klicken Sie auf OK,

Advanced IKE properties			×
Use <u>UDP</u> encapsulation			
Support Diffie-Hellman groups		EC_encapsi 🚬	
	Group 1 (768 ☐Group 2 (102	3 bit) 24 bit)	
	Group 5 (153	36 bit)	
Rekeying Parameters			
Renegotiate IKE security associal	ions	1440 📑	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 📑	Seconds
Renegotiate IPSEC Security a	associations ever	y 50000 🚊	KBytes
Mise			
Support IP <u>compression</u> for Se Support aggresive mode	ecurectient		
Support key exchange for <u>s</u> ub	onets		
OK C	ancel	<u>H</u> elp	

10. Gehen Sie zu Verwalten > Netzwerkobjekte > Bearbeiten, um das Fenster Workstation-Eigenschaften für den VPN-Konzentrator zu öffnen. Wählen Sie Topology aus den Optionen auf der linken Seite des Fensters aus, um die VPN-Domäne manuell zu definieren.In diesem Beispiel wird CONC_INSIDE (das interne Netzwerk des VPN Concentrator) als VPN-Domäne definiert.

w	orkstation Properties - C	ISCO_CONC			×
	General	Topology			
	- Topology - NAT	<u>G</u> et Interfaces			
		Name	IP Address	Network Mask	
			······	· · · · · · · · · · · · · · · · · · ·	
		Add	<u>E</u> dt	<u>B</u> emove <u>S</u> how	y
		S <u>h</u> ow all IPs behi	nd Gateway		
		VPN Domain			
		C All IP Addresses information.	s <u>b</u> ehind Gateway b	ased on Topology	Shgw
		Manually Define		SIDE 💌	Show
		Egoortable for S	ecuRemote		
				OK Cano	el Help

11. Wählen Sie VPN aus den Optionen auf der linken Seite des Fensters aus, und wählen Sie dann IKE als Verschlüsselungsschema aus. Klicken Sie auf Bearbeiten, um die IKE-Eigenschaften zu konfigurieren.

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

 Legen Sie die IKE-Eigenschaften so fest, dass sie die aktuelle Konfiguration im VPN Concentrator wiedergeben.Legen Sie in diesem Beispiel die Verschlüsselungsoption für 3DES und die Hashing-Option für MD5

IKE Prop	erties			2
Genera	L]			
Suppo	rt key exchange encryptic	n with: Supp	port data integrity wi	ith: —
	DES		MD <u>5</u>	
	≊i CAST ⊠ 3DES		SHA1	
Suppo	ort authentication methods:			
	re-Shared Secret	Edit <u>S</u> ecre	ets	
🗆 🗆 F	Public <u>K</u> ey Signatures	<u>M</u> atching Cr	iteria	
	PN-1 & FireWall-1 authen	ication for Secul	Remote (Hybrid Mo	de)
				
			<u>A</u> dvanced	
	ОК	Cancel	Help	

13. Wählen Sie die Authentifizierungsoption für **vorinstallierte Geheimnisse aus**, und klicken Sie dann auf **Geheimnisse bearbeiten**, um den vorinstallierten Schlüssel festzulegen. Klicken Sie auf **Bearbeiten**, um Ihren Schlüssel wie gezeigt einzugeben, und klicken Sie dann auf

Shared Secret				×
Shared Secrets Lis	t ———			1
Peer Name	Shared Se	cret		
ciscocp	****		<u>E</u> dit	
			<u>R</u> emove	
Enter secret: ci	scortprules	Set		
ОК	Cano	el	<u>H</u> elp	

Festlegen, OK

14. Klicken Sie im IKE-Eigenschaftenfenster auf Erweitert... und ändern Sie diese Einstellungen:Wählen Sie die für die IKE-Eigenschaften geeignete Diffie-Hellman-Gruppe aus.Deaktivieren Sie die Option für den aggressiven Support-Modus.Wählen Sie die Option zum Austausch von Support-Schlüsseln für Subnetze aus.Wenn Sie fertig sind, klicken Sie

Advanced IKE properties			×
Use UDP encapsulation			
Support Diffie-Hellman groups		SEC_encapsi 💌	
	Group 1 (76	8 bit) 24 bit)	
	Group 5 (15)	36 bit)	
Rekeying Parameters			
Renegotiate IKE security assoc	ciations	1440 🗧	Minutes
Renegotiate IPSEC Security a:	ssociations every	3600 🕂	Seconds
🔲 Renegotiate IPSEC Securi	ty associations eve	ry 50000 🚊	KBytes
Misc			
Support IP compression for	SecureClient		
Support <u>agg</u> resive mode			
Support key exchange for	<u>s</u> ubnets		
ОК	Cancel	Help	
	Cancer		

15. Wählen Sie Regeln > Regeln hinzufügen > Oben, um die Verschlüsselungsregeln für die Richtlinie zu konfigurieren. Fügen Sie im Fenster des Policy Editor eine Regel mit der Quelle CP_inside (innerhalb des Netzwerks des Prüfpunkts NG) und dem Ziel CONC_INSIDE (innerhalb des Netzwerks des VPN Concentrator) ein. Legen Sie Werte für Service = Any, Action = Encrypt und Track = Log fest. Wenn Sie den Abschnitt Encrypt Action (Aktion verschlüsseln) der Regel hinzugefügt haben, klicken Sie mit der rechten Maustaste auf Aktion, und wählen Sie Eigenschaften bearbeiten aus.

CISCOCP - Check Point Policy Editor -	Aandard	
File Edit View Manage Rules Policy	opology Search Window Help	
┃●●┃┃◎■■●◎次	\$ E E = = 1 + \$ & \$	
1 Pa 🖬 💷 🖓 🖄 🗛 🛛	Q Q 🖸 💊 🛱 🖪	
\$ € 4 @ 5 8 0 %	🇱 Security - Standard 🗮 Address Translation - Standard 🔛 QoS - Standard 🗮 Desktop S	iecurity - Standard
P. L. Network Objects	NO SOURCE DESTINATION SERVICE ACTION	TRACK INSTALL
B Workstation		
CISCO_CONC	1 CP_inside + CONC_NSDE * Any	Gateway
Retwork	+ CONC_INSIDE + CP_Inside Edit proper	ties
-++ CONC_INSIDE	2 4 CP_inside * Any * Any to at Edit Encry	Gateway
-++ O_inside	(and	
CSE Davisa		
Embedded Device		
- III Group		
Logical Server		
Address Range		*
Dupanic Object		
IN OFFICIAL COLOR	Name IP Comment	
	CISCO_CONC 172.18.124.131 VPN Concentrator Clarine End	nAbe
	Query Col	JTTT:
	Clear Quer	Y

16. Wählen Sie IKE aus, und klicken Sie auf

Encryption Properties			×
General			
Encryption <u>s</u> chemes defined:			
<u>E</u> dit			
OK Car	ncel I	Help	

Bearbeiten.

17. Ändern Sie im Fenster IKE-Eigenschaften die Eigenschaften so, dass sie mit der VPN Concentrator-Transformation übereinstimmen.Legen Sie die Option Transform auf Encryption + Data Integrity (ESP) fest.Legen Sie den Verschlüsselungsalgorithmus auf 3DES fest.Legen Sie die Datenintegrität auf MD5 fest.Stellen Sie das zulässige Peer-Gateway so ein, dass es mit dem VPN-Concentrator (CISCO_CONC) übereinstimmt.Wenn Sie fertig sind, klicken Sie auf

IKE Properties	
General	
Transform	
Encryption + Data Integrit	y (ESP)
🔿 Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
<u>D</u> ata Integrity	MD5
<u>C</u> ompression method:	None
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit)
Perform IP Pool NAT	
OK Ca	incel Help

aklivieren.							
CISCOCP - Check Point Policy	Editor - Standard				2.	_ 🗆 🗵	
File Edit View Manage Rules	Policy Topology Search Window	Help					
□	Verify Instal	° ॡ "L ↔ 🤻	1 🕹 🐉 🛛 147				
) 🎦 🔚 🖓 🏦 🖓	Uninstall						
₽ <u></u>	Access Lists	ddress Translation - Standard 🛛 🏭 QoS - Standard 🗮 Desktop Security - Standard					
Network Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL OF	
B- Workstation	Management High Availability						
CISCO_CONC	Global Properties	부 CONC_NSDE	* Any	C Encrypt	🔳 Log	Gateways	
🚊 🕂 Network			Januara Vielana estado	ud a 📥 oda i ur thuti uru			
CONC_INSIDE	2 ++ CP_inside	🛪 Arry	* Any	G accept	Log	Gateways	
CP_inside							
Domain	10						
OSE Device							
Embedded Device	10						
III Group	111						
Logical Server	10						
Address Kange						•	
Gateway Cluster	1						
Dynamic Object	Name	IP	Comment				
	CISCO_CONC	172.18.1	24.131 VPN Conc	entrator			
	ciscocp	172.18.1	24.157 Checkpoir	nt External IP			
	11						

Im Installationsfenster werden beim Kompilieren der Richtlinie Fortschrittshinweise angezeigt.



das Installationsfenster anzeigt, dass die Richtlinieninstallation abgeschlossen ist, klicken Sie auf **Schließen**, um das Verfahren

a	bzuschließen.	_
1	Install Policy	1
	Standard.W: Security Policy Script generated into Standard.pf Standard: Compiled OK.	
	Installing VPN-1/FireWall-1 policy On: ciscoop	
	VPN-1/FireWall-1 policy installed successfully on ciscocp	
	VPN-1/FireWall-1 policy Installation for all modules was successful	
	▼	

<u>Überprüfen</u>

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen der Netzwerkkommunikation

Um die Kommunikation zwischen den beiden privaten Netzwerken zu testen, können Sie einen Ping von einem der privaten Netzwerke zum anderen privaten Netzwerk initiieren. In dieser Konfiguration wurde ein Ping von der Checkpoint NG-Seite (10.32.50.51) an das VPN Concentrator-Netzwerk (192.168.10.2) gesendet.

```
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:\>
```

Tunnel-Status auf Checkpoint NG anzeigen

Um den Tunnelstatus anzuzeigen, gehen Sie zum Richtlinien-Editor, und wählen Sie **Fenster > Systemstatus aus**.

😨 CISCOCP - Check Point System Status											
Ele Yew Modules Products Iools Window Help											
🕽 🗩 🖻 🛤 🛄 🔦 🎫 🇞 🚛 🚔 🎯 🌪	52										
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									
ALIN-1	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									

Anzeigen des Tunnelstatus im VPN-Concentrator

Um den Tunnelstatus auf dem VPN Concentrator zu überprüfen, gehen Sie zu Administration > Administration Sessions.

dministration Adm	inister Sessions				1	Vednes	day, 11 Sepi	tember 2002 20:37:0 Reset @ Refresh
his screen shows st nformation on a sess onnection to a session	atistics for sessions.' ion, click on that sess on, click Ping .	To refresh the statis sion's name. To log	tics, click Refre out a session, cl	esh. Sel ick Log	ect a Group sout in the tal	to filter ble belo	the sessions w. To test th	s. For more he network
roupAll .ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/(JDP Us	er IPSec/TC	<u>P User</u>	IPSec LAN	<u>i-to-LAN</u>
Active LAN-to- LAN Sessions Access Sessions								
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak S	Concurrent essions	Con Sessio	current ons Limit	Total Cumulative Sessions
Active LAN-to- LAN Sessions	Active Remote Access Sessions	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4	Con Session	current ons Limit	Total Cumulative Sessions 17
Active LAN-to- LAN Sessions 1 LAN-to-LAN S	Active Remote Access Sessions 0 essions	Active Management Sessions 3	Total Active Sessions 4	Peak S	Concurrent essions 4 [Remote Ac	Con Session 1 cess Ser	current ons Limit 500 ssions Mar	Total Cumulative Sessions 17 agement Sessions]
Active LAN-to- LAN Sessions 1 LAN-to-LAN S Connection Nan	Active Remote Access Sessions 0 essions 1P Address	Active Management Sessions 3 Protoco	Total Active Sessions 4 bl Encr	Peak S	Concurrent essions 4 [<u>Remote Acc</u> Login T	Con Session 1 cess Ser	current ons Limit 500 ssions Man Duration	Total Cumulative Sessions 17 agement Sessions]

Wählen Sie unter LAN-to-LAN-Sitzungen den Verbindungsnamen für den Prüfpunkt aus, um Details zu den erstellten SAs und der Anzahl der übertragenen/empfangenen Pakete anzuzeigen.

Connection Name	IP Add	fress	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			
	Sandan ID	1	IK	E Session	Engrantian Algorith	2DES 1	69				
	Socion ID	1	IK	E SCSMOII	Encryption Algorith	m 3DFS-1	68				
Hashing Algorithm MD5				Diffie-Hellman Group Group 2 (1024-bit)							
Authentics	tion Mode	Pre-Sha	ared Keys	I	KE Negotiation Mo	de Main	Main				
Rekey Tin	e Interval	86400	seconds		-						
			IPS	ec Session							
	Session ID	2			Remote Addre	ss 10.32.0.	0/0.0.127.2	55			
Local Address 193			8.10.0/0.0.0.255		Encryption Algorith	un 3DES-1	3DES-168				
Hashing	Algorithm	MD5			SI	EP 1	1				
manna		and the second second second		and the second s	D.I. The Lite	1 20000 -	e e e e e e e e e e e e e e e e e e e				
Encapsula	tion Mode	Tunnel			Rekey Time Interv	a 20000 s	econds				

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hinweis: Der Datenverkehr darf nicht mithilfe der öffentlichen IP-Adresse des VPN Concentrators (externe Schnittstelle) über den IPSec-Tunnel mit PATs geleitet werden. Andernfalls schlägt der Tunnel fehl. Daher muss die für PATing verwendete IP-Adresse eine andere Adresse sein als die auf der externen Schnittstelle konfigurierte Adresse.

Netzwerkzusammenfassung

Wenn mehrere benachbarte Netzwerke in der Verschlüsselungsdomäne am Checkpoint konfiguriert sind, kann das Gerät die Netzwerke automatisch in Bezug auf den interessanten Datenverkehr zusammenfassen. Wenn der VPN-Concentrator nicht für eine Übereinstimmung konfiguriert ist, schlägt der Tunnel wahrscheinlich fehl. Wenn beispielsweise die internen Netzwerke 10.0.0.0 /24 und 10.0.1.0 /24 für die Einbindung in den Tunnel konfiguriert sind, können diese Netzwerke auf 10.0.0.0 /23 zusammengefasst werden.

Debugger für Checkpoint NG

Um die Protokolle anzuzeigen, wählen Sie Fenster > Protokollanzeige.

Ek																
6	해 🕼 🔽 Log 💿 💿 🚓 🔻 🛓 💕 🖩 및 등 🗐 🖼 🗟 🗞 🔛 약, 🏝 😌 👔															
	Date	Time	Product	1.1.1	Inter.	Orig	Туре	Action	Source	Destinati	Pr.,	Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	WPN-1	& FireN.	📻 dae	. ciscocp	📕 log	0- key instali	ciscoop	CISCO_CONC						
2	13Aug2002	21:32:	VPN-1	& FireW.	. 🕒 dae	. ciscocp	📄 log	Ow key instal	ciscocp	CISCO_CONC				0x5879f30d	0xt1351129	

Um Debugging auf dem VPN Concentrator zu aktivieren, gehen Sie zu **Configuration > System > Events > Classes**. Aktivieren Sie AUTH, AUTHDBG, IKE, IKEDBG, IPSEC und IPSECDBG, damit der Schweregrad 1-13 lautet. Um Debuggen anzuzeigen, wählen Sie **Monitoring > Filterable Event Log (Überwachung > Filterbares Ereignisprotokoll)**.

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 : 256 48 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 AUTHDBG/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 = 3000065 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] processing IPSEC SA

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 00000000, 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 SPI 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) ... total length : 48

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 0000000, 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 00000000, 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)

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- <u>Cisco VPN Client Support-Seite der Serie 3000</u>
- IPSec-Support-Seite
- Technischer Support Cisco Systems