Konfigurieren des IPSec LAN-to-LAN-Tunnels zwischen der Cisco Pix Firewall und einer NetScreen Firewall

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurationen Überprüfen Überprüfen Überprüfen Ehlerbehebung Fehlerbehebung Befehle zur Fehlerbehebung Beispielausgabe für Debugging Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zum Erstellen eines IPsec-LAN-to-LAN-Tunnels zwischen einer Cisco PIX-Firewall und einer NetScreen-Firewall mit der neuesten Software. Hinter jedem Gerät befindet sich ein privates Netzwerk, das über den IPsec-Tunnel mit der anderen Firewall kommuniziert.

Voraussetzungen

Anforderungen

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

- Die NetScreen-Firewall wird mit den IP-Adressen der vertrauenswürdigen und nicht vertrauenswürdigen Schnittstellen konfiguriert.
- Die Verbindung zum Internet wird hergestellt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- PIX Firewall Software Version 6.3(1)
- Neueste Version von NetScreen

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:

- <u>PIX-Firewall</u>
- <u>NetScreen-Firewall</u>

Konfigurieren der PIX-Firewall

PIX-Firewall

PIX Version 6.3(1) interface ethernet0 10baset interface ethernet1 100full nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pixfirewall domain-name cisco.com fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 names !--- Access control list (ACL) for interesting traffic to be encrypted and !--- to bypass the Network Address Translation (NAT) process. access-list nonat permit ip 10.0.25.0 255.255.255.0 10.0.3.0 255.255.255.0 pager lines 24 logging on logging timestamp logging buffered debugging icmp permit any inside mtu outside 1500 mtu inside 1500 !--- IP addresses on the interfaces. ip address outside 172.18.124.96 255.255.255.0 ip address inside 10.0.25.254 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm logging informational 100 pdm history enable arp timeout 14400 global (outside) 1 interface !--- Bypass of NAT for IPsec interesting inside network traffic. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Default gateway to the Internet. route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 0:05:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius aaa-server LOCAL protocol local http 10.0.0.0 255.0.0.0 inside no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodquard enable !--- This command avoids applied ACLs or conduits on encrypted packets. sysopt connection permit-ipsec

- Configuration of IPsec Phase 2. crypto ipsec transform-set mytrans esp-3des esp-sha-hmac crypto map mymap 10 ipsec-isakmp crypto map mymap 10 match address nonat crypto map mymap 10 set pfs group2 crypto map mymap 10 set peer 172.18.173.85 crypto map mymap 10 set transform-set mytrans crypto map mymap interface outside !--- Configuration of IPsec Phase 1. isakmp enable outside !--- Internet Key Exchange (IKE) pre-shared key !--that the peers use to authenticate. isakmp key testme address 172.18.173.85 netmask 255.255.255.255 isakmp identity address isakmp policy 10 authentication pre-share isakmp policy 10 encryption 3des isakmp policy 10 hash sha isakmp policy 10 group 2 isakmp policy 10 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 dhcpd lease 3600 dhcpd ping_timeout 750 terminal width 80

Konfigurieren der NetScreen-Firewall

Führen Sie diese Schritte aus, um die NetScreen-Firewall zu konfigurieren.

- 1. Wählen Sie Listen > Adresse aus, wechseln Sie zur Registerkarte Vertrauenswürdig, und klicken Sie auf Neue Adresse.
- Fügen Sie das im Tunnel verschlüsselte interne NetScreen-Netzwerk hinzu, und klicken Sie auf OK.Hinweis: Stellen Sie sicher, dass die Option "Vertrauenswürdig" ausgewählt ist.In diesem Beispiel wird das Netzwerk 10.0.3.0 mit der Maske 255.255.255.0 verwendet.

NetScreen Administration Tools - Microsoft	Internet Explorer		a ×
Ele Edit yew Favorites Iools Help			1
🔾 Back + 🔾 - 💌 🛋 🏠 🔎 See	arch 👷 Favorites 😽 Media 🚱 🔂 🖕 📓	2 - 📴 🕉	
Address http://10.0.3.254/layout.htm/*6,1,1		- 🔂 👳 🛛	nis ^{xa}
NETSCREEN - 5		help support about elogo	έι.t
System Configure Admin Interface Network Policy VPN Virtual IP Lists Address Service Schedule Upers	CONFIGURATION Address Name IP Address/Domain Name Netmask Conament	[insideNetwork [10.0.3.0 [255.255.255.0	
Monitor Traffic Counters	Location	© Trust ← Untrust	
Copyright @ 1908-2001 NetScreen Technologies Inc. All rights asserved.			
) Go to the Unitrusted Interface		anternet	

- 3. Wählen Sie Listen > Adresse aus, wechseln Sie zur Registerkarte Nicht vertrauenswürdig, und klicken Sie auf Neue Adresse.
- 4. Fügen Sie das Remote-Netzwerk hinzu, das die NetScreen Firewall bei der Verschlüsselung von Paketen verwendet, und klicken Sie auf OK. Hinweis: Verwenden Sie keine Adressgruppen, wenn Sie ein VPN für ein Nicht-NetScreen-Gateway konfigurieren. VPN-Interoperabilität schlägt fehl, wenn Sie Adressgruppen verwenden. Das Nicht-NetScreen-Sicherheits-Gateway weiß nicht, wie die von NetScreen erstellte Proxy-ID interpretiert wird, wenn Adressgruppe verwendet wird. Dafür gibt es mehrere Möglichkeiten: Trennen Sie die Adressgruppen in einzelne Adressbucheinträge. Geben Sie individuelle Richtlinien für jeden Eintrag im Adressbuch an. Konfigurieren Sie die Proxy-ID so, dass sie möglichst auf dem Nicht-NetScreen-Gateway (Firewall-Gerät) 0.0.0.0/0 lautet. In diesem Beispiel wird das Netzwerk 10.0.25.0 mit der Maske 255.255.255.0 verwendet.

NetScreen Administration	Tools - Microsoft Internet Explorer	26 ×
File Edit View Favorites	Tools Help	At 1.
🔇 Back • 🕤 · 💌 🔒	🖞 🏠 🔎 Search 👷 Favorites 🚷 Media 🍘 🍰 🎍 🗟 🖓 🛄	3
Address () http://10.0.3.254/k	yout.html#6,1,1	💌 🛃 Go Links 🏁
NETSCREEN'-5		help support about logout
System Configure Admin Interface Network Policy VPN Vertual JP Lists Address Service Schedule Users Monitor Traffic Counters Adarm Log	ADDRESS CONFIGURATION Address Name Fe IP Address/Domain Name 10 Netmask 25 Comment Location C	moteNetwork 0.25 0 5255 255 0 Trust @ Untrust OK Cancel
NetScreen Technologies Inc. All rights reserved.	Configuration	I - I for the Internet
Start D:/WINDOWS(Sys	tem32 () NetScreen Administra () DATA (E:)	≪ 5 3:35 PM

- Wählen Sie Network > VPN aus, gehen Sie zur Registerkarte Gateway, und klicken Sie auf New Remote Tunnel Gateway, um das VPN-Gateway zu konfigurieren (IPsec-Richtlinien für Phase 1 und Phase 2).
- 6. Verwenden Sie die IP-Adresse der externen Schnittstelle des PIX, um den Tunnel zu beenden, und konfigurieren Sie die IKE-Optionen für Phase 1 für die Anbindung. Klicken Sie abschließend auf OK.In diesem Beispiel werden diese Felder und Werte verwendet.Gateway-Name: Bis501Statische IP-Adresse: 172,18,124,96Modus: Haupt (ID-Schutz)Vorinstallierter Schlüssel: TestmeVorschlag für Phase 1: vor g2-3dessha

NetScreen Administration Tools - Microsomer Statement Processor (1998)	oft Enternet Explorer	18 ×
Bie Edit Yew Favorites Iools Help		
🔾 Sook • 💭 🔺 🖉 🞧 🔎	Search 🎇 Pavortas 💕 Media 🚱 <table-cell> 😨 🖕 🔟 💈 🍱</table-cell>	
Aggress Al http://10.0.3.254/layout.html*6.1.1		Go Unis *
NETSCREEN'-5	• help · • support • abo	iut • lagaut
System REMOTE	TUNNEL GATEWAY CONFIGURATION	-
Configure		
Interface		
Network	Gateway Name [To501	
Policy	Remote Gateway	
VPN	Static IP Address IP Address 172.18.124.36	
Virtual IP	Peer ID (optional)	
Address	Dynamic IF Address Peer ID	
Service		
Schedule	Mode (Initiator) ^(*) Main (ID Protection) ^(*) Aggressive	
Manitar	Phase 1 Proposal	
Traffs	pre-g2-3des-sha 🛫 none 💌	
Counters	none Inone I	
Alarm	Preshared Key	
Log	Local ID (optional)	
Copyright @ 1996-2001 NetScreen Technologies	Proferred Cartificate (onlineal)	
Inc. All rights received.	Local Cert None -	
	Peer CA None .	
	Peer Type NONE	
	OK Cancel	
Go to the Gateway Configuration	Dirth Control of the	ernet

Wenn das Remote-Tunnel-Gateway erfolgreich erstellt wurde, wird ein ähnlicher Bildschirm angezeigt.



- 7. Rufen Sie die Registerkarte "P1 Proposal" (P1-Angebot) auf "New Phase 1 Proposal" (Neues Angebot aus Phase 1 konfigurieren), um Angebot 1 zu konfigurieren.
- B. Geben Sie die Konfigurationsinformationen f
 ür Phase-1-Angebot ein, und klicken Sie auf OK.In diesem Beispiel werden diese Felder und Werte f
 ür den Austausch in Phase 1 verwendet.Name: ToPix501Authentifizierung: VorteilenDH-Gruppe: Gruppe 2Verschl
 üsselung: 3DES-CBCHash: SHA-1Lebensdauer: 3600 Sek.



Wenn Phase 1 der NetScreen-Konfiguration erfolgreich hinzugefügt wurde, wird ein Bildschirm ähnlich dem folgenden Beispiel

Eat Yew Favorites	Toole Filelb	-		21			
sack • 🕑 • 💌 🚨	Search 👷 Favorite	es 🛃 Media 🌾	9 😹 👙 🛙	ल - 🔜 🎿			
ss 📄 http://10.0.3.254/lay	out.html*6,1,1					≥ →	60
SCREEN -5					• help	• support • about	• Jog
System	VPN					17 Sept 2003	15:4
Confidure							
Admin						P	age 2
Interface					-		
Network	Manual Key V AutoKey IK	Gateway	P1 Proposal V	P2 Proposal V Certificate	L2TP	IPPool L	
NEUTOTK							
Policy							
VPTN	14						
Virtual IP	Name	Method	DH Group	Encrypt/Auth.	Lifetime	Configure	
Virtual IP Lists	Name ds#g2-3desmd5	Method DSA:sg	DH Group 2	Encrypt/Auth. 30ES/M05	Lifetime 29900	Configure -	
Virtual IP Lists Address	Name das g2 3 des meti das g2 3 des des	Method DSA-sig DSA-pg	DH Group 2 2	Encrypt/Auth. 30ES/M05 30ES/SHA	Lifetime 29800 29800	Configure -	
Virtual IP Lists Address Service	Name dsa-g2-3des-md5 dsa-g2-3des-dha ToPtid601	Method DSA:sg DSA:sg Preshaw	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 29800 29800 3800	Configure - - Edit Bamana	
Virtual IP Lists Address Service Schedule	Name daa g2 3deo md5 daa g2 3deo sha TaPbd01	Method DSA:sq DSA:sq Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 23800 28800 3800	Configure - - Edit Bemane	
Virtual IP Lists Address Service Schedule Users Menitor	Name dax ş2-3des mdö dax ş2-3des da ToPbd01	Method DSA-sig DSA-sig Preshaw	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 23800 20800 3800	Configure - - Elite Bamara	
Virtual IP Lists Address Service Schedule Users Monitor	Name dsa-g2-3des-md5 dsa-g2-3des-dha ToPtid01	Method DSA:sg DSA:sg Preshaw	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3800	Configure - - Edd-Bambas	
Virtual IP Lists Address Service Schedule Users Monitor Traffic	Name da+g2/3desmd5 da+g2/3desdka ToPid01	Method DSA:sg DSA:pg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3800	Configure - - Est-Remark	
Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters	Name darg23desmd5 darg23desdha ToP6601	Method DSA:sg DSA:sg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3600	Configure - Edit Bemare	
Vern Victual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm	Name daa g2 3deo md5 daa g2 3deo cha ToPic601	Method DSA-sig DSA-sig Preshaw	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 23800 28800 3800	Configure - - Est Remove	
Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters Aflarm Log	Name dsa-g2-3des-md5 dsa-g2-3des-dha ToPtid01	Method DSA:sg DSA:sg Prishaw	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 26800 3600	Configure - - Ed: Bamara	
Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm Log	Name dia-g2/3desmd5 dia-g2/3desdia ToPid601	Method DSA:sg DSA:sg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3600	Configure - Est Remark	
Vertual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm Loo	Name dia-g23deo.md5 dia-g23deo.dha ToP6d01	Method DSA-sig DSA-sig Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/SHA 3DES/SHA 3DES/SHA	Lifetime 25800 25800 3600	Configure - Edit Bemare	

- 9. Öffnen Sie die Registerkarte "P2 Proposal" (P2-Angebot), und klicken Sie auf **New Phase 2 Proposal (Neuer** Vorschlag für Phase 2), um Phase 2 zu konfigurieren.
- Geben Sie die Konfigurationsinformationen f
 ür Phase-2-Angebot ein, und klicken Sie auf OK.In diesem Beispiel werden diese Felder und Werte f
 ür den Austausch in Phase 2 verwendet.Name: ToPix501Perfekte Rufweiterleitung: DH-2 (1024 Bit)Verschl
 üsselungsalgorithmus: 3DES-CBCAuthentifizierungsalgorithmus: SHA-1Lebensdauer: 26400

Sec			
NetScreen Administration To	ols - Microsoft Internet Explorer		_6 X
Elle Edit yew Figvorites Is	xds ttep		
🚱 Back + 💟 - 💌 😰	🐔 🔎 Search 🔆 Favorites 🜒 Meda 🥝 🍰 🤪 🕅	· 🔁 🍪	
Address Http://10.0.3.254/layor	£.htmi*6,1,1		🔹 🛃 🐼 Links 🎽
NETSCREEN -5		• help • su	sport • about • logout
System	PHASE 2 PROPOSAL CONFIGURATION		
Configure			
Interface	1		71 ⁻¹
Network	122000		
Policy	Name	ToPtx501	
VEN	Perfect Forward Secrecy	DH Group 2 •	
Vitter P	Encapsulation		
LISIS	· Encryption (ESP)		
Service	Encryption Algorithm	3DES-CBC ·	
Schedule	Authentication Algorithm	SHA-1 ·	
Users	C Authentication Only (AH)	1 Arres 1994	
Monitor	Authentication Algorithm	MD5 +	
Counters			
Alam	Lifetime		
E00	and the second second	Inc. eng	
Copyright @ 1998-2001	In Time	CSec CMm CHours CDars	
NetScreen Technologies Inc	In Kbytes	0 Khates	8
All sights repaired.		- stopus	

Wenn Phase 2 der NetScreen-Konfiguration erfolgreich hinzugefügt wurde, wird ein Bildschirm angezeigt, der diesem Beispiel ähnelt.

Contraction of the second									
Edit Yew Favorite	es Iools Help				in the second second				
Back • 🕗 - 💌	3 🏠 🖇	Search 👷 Favorites 😽 1	Media 🧭 🔒	• 😓 🖻	· 🛃 🕉				
ss 💽 http://10.0.3.25	4/layout.html*6,1	.1						•	-) Go
TSCREEN-5						• help	• sup	port 🔹 about	· • log
System	VPN	j.						17 Sept 20	003 15:4
Configure									
Admin									Page 1
Interface	Alter	al Key AutoKey DO	Di Di		Continues	A (1)		PPool	
Network		names for wanted me for the	centry U PIPO	oposai 🖉 🖓	Proposal V Certificate	* U	. <u>.</u>	rrugi (1.21
STREET, STREET									
Palicy									
Policy VPN									
Policy VPN Virtual IP		Name	PFS	Encap.	Encrypt/Auth.	Lifetime	Lifesize	Configure	1
Policy VPN Virtual IP Lists	1	Name naptisesp-dep-md5	PFS No PFS	Encap. ESP	Encrypt/Auth.	Lifetime 9900	Lifesize	Configure	1
Policy VPN Virtual IP Lists Address		Name nopti-esp-dep-md5 nopti-esp-dep-sha	PFS No PFS No PFS	Encap. ESP ESP	Encrypt/Auth.	Lifetime 3900 3900	Lifesize 0 0	Configure	1
Policy VPN Virtual IP Lists Address Service Schedula		Name nopti-esp-dep-md5 nopti-esp-dep-sha nopti-esp-3dep-md5	PFS No PFS No PFS No PFS	Encap. ESP ESP ESP	Encrypt/Auth. DES/M05 DES/SHA 30ES/M05	Lifetime 3800 3800	Lifesize 0 0	Configure - -	1
Policy VPN Virtual IP Lists Address Service Schedule Users		Name nopti-esp-dep-md5 nopti-esp-dep-md5 nopti-esp-3dep-md5 nopti-esp-3dep-md5	PFS No PFS No PFS No PFS No PFS	Encap. ESP ESP ESP ESP	Encrypt/Auth. DES/MOS DES/SHA 30ES/MOS 3DES/SHA	Lifetime 3900 3900 3900	Lifesize 0 0 0	Configure - - -	
Policy VPN Virtual IP Lists Address Service Schedule Users Menitor		Name nopti-esp-dep-md5 nopti-esp-dep-sha nopti-esp-3dep-sha g2-esp-dep-md5	PFS No PFS No PFS No PFS No PFS DH Group 2	Encap. ESP ESP ESP ESP ESP	Encrypt/Auth. DES/M05 DES/SHA 30ES/M05 3DES/SHA DES/M05	Lifetime 3000 3000 3000 3000 3000	Lifesize 0 0 0 0 0	Configure - - - -	
Policy VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic		Name nopti-esp-dep-md5 nopti-esp-dep-md5 nopti-esp-3dep-md5 g2-esp-dep-md5 g2-esp-dep-md5	PFS No PFS No PFS No PFS No PFS DH Group 2 DH Group 2	Encap. ESP ESP ESP ESP ESP ESP	Encrypt/Auth. DES/MOS DES/SHA 3DES/MOS 3DES/SHA DES/MOS DES/SHA	Lifetime 3000 3000 3000 2000 3000 3000	Lifesize 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Configure - - - -	
Policy VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters		Name nopti-esp-dep-md5 nopti-esp-dep-md5 nopti-esp-3dep-md5 nopti-esp-3dep-md5 g2-esp-dep-md5 g2-esp-dep-md5 g2-esp-3dep-md5	PFS No PFS No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2	Encap. ESP ESP ESP ESP ESP ESP	Encrypt/Auth. DES/MOS DES/SHA 3DES/MOS 3DES/SHA DES/SHA 3DES/SHA 3DES/MOS	Lifetime 5000 3000 3000 3000 3000 3000 3000	Lifesize 0 0 0 0 0 0 0 0	Configure	
Policy VPN Virtual IP Lists Address Servce Schedule Users Monitor Traffic Counters Alarm		Name nopti-esp-dep-md5 nopti-esp-dep-md5 nopti-esp-3dep-md5 g2-esp-dep-md5 g2-esp-dep-md5 g2-esp-3dep-md5 g2-esp-3dep-md5 g2-esp-3dep-md5	PFS No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2 DH Group 2	Encap. ESP ESP ESP ESP ESP ESP ESP ESP	Encrypt/Auth. DES/M05 DES/SHA 30ES/M05 3DES/SHA 0ES/SHA 30ES/M05 3DES/SHA	Lifetime 3900 3900 3900 3900 3900 3900 3900	Lifesize 0 0 0 0 0 0 0 0 0 0	Configure 	
Policy VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm Log		Name nopti-esp-des-md5 nopti-esp-des-md5 nopti-esp-des-md6 nopti-esp-des-md6 g2-esp-des-md5 g2-esp-des-md5 g2-esp-des-md5 g2-esp-des-md5 g2-esp-des-md5 g2-esp-des-md5 g2-esp-des-md5	PFS No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2	Encap. ESP ESP ESP ESP ESP ESP ESP ESP	Encrypt/Auth. DES/MOS DES/SHA 3DES/MOS 3DES/SHA DES/MOS DES/SHA 3DES/SHA 3DES/SHA	Lifetime 3000 3000 2000 3000 3000 3000 3000 20400	Lifesize 0 0 0 0 0 0 0 0 0 0 0	Configure	

- 11. Wählen Sie die Registerkarte **AutoKey IKE** aus, und klicken Sie dann auf **Neuer AutoKey IKE-Eintrag**, um AutoKeys IKE zu erstellen und zu konfigurieren.
- 12. Geben Sie die Konfigurationsinformationen f
 ür AutoKey IKE ein, und klicken Sie dann auf OK.In diesem Beispiel werden diese Felder und Werte f
 ür AutoKey IKE verwendet.Name: VPN-1Name des Remote-Gateway-Tunnels: Bis501(Dies wurde zuvor auf der Registerkarte Gateway erstellt.)Angebot f
 ür Phase 2: ToPix501(Diese wurde zuvor auf der Registerkarte "P2 Proposal" (P2-Angebot) erstellt.)VPN-Monitor: Aktivieren(Dadurch kann das NetScreen-Ger
 ät Simple Network Management Protocol [SNMP]-Traps einrichten, um den Zustand des VPN-Monitors zu überwachen.)

NetScreen Administrati	ion Tools - Microsoft Internet Explorer	_ 6 ×
Ele Edit Yew Favorito	ter Tools Help	- 1
😮 Back + 🕑 - 💌	😰 🐔 🔎 Search 🐈 Favorites 🜒 Media 🥝 🍰 - 🤪 📾 - 📴 🖓	
Address http://10.0.3.25	54/Jayout.Honi*6,1,1 🕑	io Links **
NETSCREEN-5	. • help . • support . • about	e, fogoùt
System Configure Admin	AUTOKEY IKE CONFIGURATION	
Interface Network Policy VPN	Name VPN-1 Enable Replay Protection □ Enable	
Lists Address Service	Remote Gateway Tunnel Name To501 Ust Gateways Phase 2 Proposal ToPb501	
Schedule Users Monitor	none	
Counters Alerm	VPN Monitor P Enable Transport Mode C Enable (For L2TP-over-IPSec only)	
Copyright © 1995-2001 NetSoreen Technologies Inc.	OK Cancel	

Wenn die VPN-1-Regel erfolgreich konfiguriert wurde, wird ein Bildschirm angezeigt, der diesem Beispiel ähnelt.

NetScreen Administration	n Tools - Microsoft Inte	met Explorer	-					_ 5 X
Ele Edit Yew Favorites	Icols Help							1
🕒 Back - 🕥 · 📘	👔 🚮 🔎 Search	📌 Favorites 📢	Media 🙆	🔗 · 🍃 🖩 - 🚺	3			
Address 1 http://10.0.3.254	layout.html*6,1,1						•	🔁 Go Links XX
NETSCREEN'-5						• help •	support • abou	t Flogout
System	VPN						17 Sept 2	003 15:46:06
Configure								1.1.1
Admin								Page 1 of 1
Interface	Manual Key	AutoKey IKE	ateway P1	Proposal P2 Proposa	Certificates	LITP	IPPool	
Network								
Policy	Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure	r I
Virtual IP	VPN-	To501	No	ToPix501	On	Off	Lds.	
Lists	_							
Address								
Service								
Schedule Users								
Monitor								
Traffic								
Counters								
Alam								
Log								
Copyright @ 1008-2001								
NetScreen Technologies Inc.								
all order pressed								

- 13. Wählen Sie Network > Policy, gehen Sie zur Registerkarte Outgoing (Ausgehend), und klicken Sie auf New Policy (Neue Richtlinie), um die Regeln zu konfigurieren, die die Verschlüsselung des IPsec-Datenverkehrs ermöglichen.
- 14. Geben Sie die Konfigurationsinformationen für die Richtlinie ein, und klicken Sie auf OK.In diesem Beispiel werden diese Felder und Werte für die Richtlinie verwendet. Das Feld Name ist optional und wird in diesem Beispiel nicht verwendet.Quelladresse: InsideNetwork(Dies wurde zuvor auf der Registerkarte Vertrauenswürdig definiert.)Zieladresse: Remote-Netzwerk(Dies wurde zuvor unter der Registerkarte "Nicht vertrauenswürdig" definiert.)Service: BeliebigAktion: TunnelVPN-Tunnel: VPN-1(Dies wurde zuvor auf der Registerkarte AutoKey IKE als VPN-Tunnel definiert.)Ändern Sie die übereinstimmende eingehende VPN-Richtlinie: Aktiviert(Mit dieser Option wird automatisch eine eingehende Regel erstellt, die dem externen Netzwerk-VPN-Datenverkehr entspricht.)

NetScreen Administration Tools - 1	Microsoft Internet Explorer	_18 ×
Elle Edit Yew Favorites Iools	Beb	10 At
🔾 Back + 🕑 - 🛃 🗟 🐔	🔎 Search 🔆 Favorites 🛞 Media 🍘 🍰 🦕 📓 - 🛄 🍪	
Address http://10.0.3.254/layout.htm	r6,1,1 🕑 🔂 60	Links ³⁰
NETSCREEN -5	● help >● support ● about >● 1	logout
System Dor	INV CONTROL BATION	-
Conligure	ICY CONFIGURATION	
Admin		
Interface		
Network	Name (optional)	
Policy	Source Address InsideNetwork -	
Mittal IP	Destination Address RemoteNetwork -	
Lists	Service ANY *	
Address	NAT 6 OF	
Service	C C C C C C C C C C C C C C C C C C C	
Schedule	C DIP Off	
Users	⊂ D₽ On	
Monitor		
Traffic		
Counters	Action Tunnel *	
- Lon	VPN Tunnel VPN-1	
A CONTRACTOR OF	🖓 Modify matching incoming VPN policy	
Cepyright @ 1998-2001 NetScreen Tectinalogies	L2IP None -	1
Inc. All fighth sprayed	Authentication C 1980	

15. Wenn die Richtlinie hinzugefügt wird, stellen Sie sicher, dass die ausgehende VPN-Regel zuerst in der Liste der Richtlinien aufgeführt ist. (Die Regel, die automatisch für eingehenden Datenverkehr erstellt wird, befindet sich auf der Registerkarte "Eingehend".)Gehen Sie wie folgt vor, wenn Sie die Reihenfolge der Richtlinien ändern müssen:Klicken Sie auf die Registerkarte Ausgehend.Klicken Sie in der Spalte Konfigurieren auf die runden Pfeile, um das Fenster Verschieben von Policy Micro anzuzeigen.Ändern Sie die Reihenfolge der Richtlinien, sodass die VPN-Richtlinie über der Richtlinien-ID 0 liegt (sodass die VPN-Richtlinie ganz oben in der Liste steht).



Öffnen Sie die Registerkarte "Eingehend", um die Regel für eingehenden Datenverkehr anzuzeigen.



<u>Überprüfen</u>

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

<u>Überprüfungsbefehle</u>

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**.

- ping Dient zur Diagnose der grundlegenden Netzwerkverbindungen.
- show crypto ipsec sa Zeigt die Sicherheitszuordnungen für Phase 2 an.
- show crypto isakmp sa Zeigt die Sicherheitszuordnungen für Phase 1.

Prüfergebnisse

Hier wird eine Beispielausgabe von Ping- und Show-Befehlen angezeigt.

Dieser Ping wird von einem Host hinter der NetScreen-Firewall initiiert.

C:\>ping 10.0.25.1 -t Request timed out. Request timed out. Reply from 10.0.25.1: bytes=32 time<105ms TTL=128 Reply from 10.0.25.1: bytes=32 time<114ms TTL=128 Reply from 10.0.25.1: bytes=32 time<106ms TTL=128 Reply from 10.0.25.1: bytes=32 time<121ms TTL=128 Reply from 10.0.25.1: bytes=32 time<110ms TTL=128 Reply from 10.0.25.1: bytes=32 time<116ms TTL=128 Reply from 10.0.25.1: bytes=32 time<109ms TTL=128 Reply from 10.0.25.1: bytes=32 time<110ms TTL=128 Reply from 10.0.25.1: bytes=32 time<118ms TTL=128 Hier wird die Ausgabe des Befehls show crypto ipsec sa angezeigt. pixfirewall(config)#show crypto ipsec sa interface: outside Crypto map tag: mymap, local addr. 172.18.124.96 local ident (addr/mask/prot/port): (10.0.25.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.0.3.0/255.255.255.0/0/0)current_peer: 172.18.173.85:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11 #pkts decaps: 11, #pkts decrypt: 13, #pkts verify 13 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors 1 local crypto endpt.: 172.18.124.96, remote crypto endpt.: 172.18.173.85 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: f0f376eb inbound esp sas: spi: 0x1225ce5c(304467548) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607974/24637) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xf0f376eb(4042487531) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607999/24628) IV size: 8 bytes

```
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

Hier wird die Ausgabe des Befehls show crypto isakmp sa angezeigt.

pixfirewall(config)#show crypto isakmp sa Total : 1 Embryonic : 0 dst src state pending created 172.18.124.96 172.18.173.85 QM_IDLE 0 1

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

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 Meldungen über Krypto Engines an.
- debug crypto ipsec: Zeigt Informationen über IPsec-Ereignisse an.
- debug crypto isakmp: Zeigt Meldungen über IKE-Ereignisse an.

Beispielausgabe für Debugging

Hier finden Sie Beispiele für Debug-Ausgaben der PIX Firewall.

```
debug crypto engine
debug crypto ipsec
debug crypto isakmp
crypto_isakmp_process_block:src:172.18.173.85,
 dest:172.18.124.96 spt:500 dpt:500
OAK MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP:
          hash SHA
ISAKMP:
          default group 2
ISAKMP:
           auth pre-share
ISAKMP:
           life type in seconds
        life duration (basic) of 28800
ISAKMP:
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
ISAKMP (0): SA is doing pre-shared key authentication
  using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
```

```
dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): ID payload
       next-payload : 8
       type
               : 1
       protocol
                   : 17
       port
                   : 500
                   : 8
       length
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.173.85/500
  Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.173.85/500 Ref cnt
  incremented to:1
  Total VPN Peers:1
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
ISAKMP (0): processing DELETE payload. message ID = 534186807,
  spi size = 4IPSEC(key_engin
e): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas):
   delete all SAs shared with 172.18.173.85
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode: OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4150037097
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
         SA life type in seconds
ISAKMP:
ISAKMP:
            SA life duration (VPI) of 0x0 0x0 0x67 0x20
ISAKMP:
           encaps is 1
ISAKMP:
          authenticator is HMAC-SHA
ISAKMP:
           group is 2
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
   dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x24
```

```
ISAKMP (0): processing KE payload. message ID = 4150037097
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
  prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.0.25.0/255.255.255.0
  prot 0 port 0IPSEC(key_engine)
: got a queue event...
IPSEC(spi_response): getting spi 0x1225ce5c(304467548) for SA
        from 172.18.173.85 to 172.18.124.96 for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK OM AUTH AWAITmap alloc entry: allocating entry 3
map_alloc_entry: allocating entry 4
ISAKMP (0): Creating IPSec SAs
        inbound SA from 172.18.173.85 to 172.18.124.96
          (proxy 10.0.3.0 to 10.0.25.0)
       has spi 304467548 and conn_id 3 and flags 25
        lifetime of 26400 seconds
        outbound SA from 172.18.124.96 to 172.18.173.85
          (proxy 10.0.25.0 to 10.0.3.0)
       has spi 4042487531 and conn_id 4 and flags 25
        lifetime of 26400 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
   dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
   src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 26400s and 0kb,
    spi= 0x1225ce5c(304467548), conn_id= 3,
      keysize= 0, flags= 0x25
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.96, dest= 172.18.173.85,
    src_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
   dest_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 26400s and 0kb,
    spi= 0xf0f376eb(4042487531), conn_id= 4, keysize= 0, flags= 0x25
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
  incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation Cisco Systems