Het configureren van IPSec LAN-to-LAN tunnel tussen de Cisco Pix-firewall en een NetScreenfirewall

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configuraties Verifieren Verificatieopdrachten Verificatieoutput Problemen oplossen Opdrachten voor troubleshooting Voorbeeld van output van foutopsporing Gerelateerde informatie

Inleiding

Dit document beschrijft de gewenste procedure die wordt gebruikt om een IPsec LAN-to-LAN tunnel te maken tussen een Cisco PIX-firewall en een NetScreen-firewall met de nieuwste software. Er is een privé netwerk achter elk apparaat dat aan de andere firewall door de IPsec-tunnel communiceert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De NetScreen Firewall wordt met de IP-adressen ingesteld op de trust/ontrust-interfaces.
- Connectiviteit is gevestigd op het internet.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-firewall, versie 6.3(1)
- Laatste herziening NetScreen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- PIX-firewall
- <u>NetScreen-firewall</u>

De PIX-firewall configureren

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 floodguard 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
<pre>! Configuration of IPsec Phase 1. isakmp enable</pre>
outside
<pre>! Internet Key Exchange (IKE) pre-shared key !</pre>
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

De NetScreen Firewall configureren

Voltooi deze stappen om de NetScreen Firewall te configureren.

- 1. Selecteer Lijsten > Adres, ga naar het tabblad Vertrouwd en klik op Nieuw Adres.
- Voeg het interne netwerk NetScreen toe dat versleuteld is in de tunnel en klik op OK.Opmerking: Zorg ervoor dat de optie Vertrouwen is geselecteerd.Dit voorbeeld gebruikt netwerk 10.0.3.0 met een masker van

200.200.200. NetScreen Administration Tools - M	ticrosoft Internet Explorer		×
Ele Edit Yew Favorites Tools	Belle and a second s		1 1
(3 Back + () - 🖹 2 🐔	🔎 Search 🔶 Favorites 💓 Media 🍘 🔝 - 😓 🕅	- 🖸 🕉	
Address http://10.0.3.254/keyout.html	P6,1,1.		💌 🛃 Go 🛛 Links 🍅
NETSCREEN'-5		help support	aboirt • logout
System			
Configure ADD	RESS CONFIGURATION		
Admin			
Natural	i i i i i i i i i i i i i i i i i i i		
Policy	100 L 200 C 200 C 200 C 200 C	·	
VPN	Address Name	[insideNetwork	
Virtual IP	IP Address/Domain Name	100.30	
Lists			
Address	Netmask	255.255.255.0	
Schedule	Comment	3	
Users	School and the second	Norma constant	
Monitor	Location	Trust C Untrust	
Counters	1		
Alarm	L	OK Cancel	
Log			
Copyright @ 1998-2001			
Inc.			
An ogni internet.			
(a) Go to the Untrusted Interface			Internet

- 3. Selecteer Lijsten > Adres, ga naar het tabblad Onvertrouwde en klik op Nieuw Adres.
- 4. Voeg het externe netwerk toe dat NetScreen Firewall gebruikt wanneer het pakketjes versleutelt en klik op OK.Opmerking: Gebruik geen adresgroepen wanneer u een VPN vormt naar een niet NetScreen poort. VPN-interoperabiliteit mislukt als u adresgroepen gebruikt. De niet NetScreen security gateway weet niet hoe de proxy-ID moet worden geïnterpreteerd die door NetScreen is gecreëerd wanneer de adresgroep wordt gebruikt.Hier zijn een paar redenen voor:De adresgroepen in individuele adresboekingangen scheiden. Specificeer individueel beleid op basis van een adresboekregistratie.Configureer proxy-ID om 0.0.0.0/0 op de niet NetScreen-gateway (firewallapparaat) indien mogelijk te zijn.Dit voorbeeld gebruikt netwerk 10.0.25.0 met een masker van

Text New Both Both </th <th>NetScreen Administration Tools - Microsoft</th> <th>nternet Explorer</th> <th></th>	NetScreen Administration Tools - Microsoft	nternet Explorer	
Text Image: Search Provide Sear	File Edit View Favorites Tools Help		
dees	🔾 Back + 💬 - 💌 😰 🏠 🔎 Sex	rch ☆ Pavorites 🜒 Media 🕢 🍰 🦕 🖩	8 - 🛄 🕉
NetSCREEN-S • holp • upport • about • fogut System Gandigure Admini FreenoteNetwork Polory Address Name Network Polory Value Address Name Production 100.25.0 Scheddle Scheddle Scheddle Scheddle Scheddle Comment Log OK Cancel	Address a http://10.0.3.254/kayout.html*6,1,1		▼ 🛃 Go Lini
System Configure Admini Interface Network Virtual IP Lists Address Schedule Schedule <td< th=""><th>NETSCREEN'-5</th><th></th><th>help support about fogout</th></td<>	NETSCREEN'-5		help support about fogout
Counters Alarm Log Copyright 9 1998-2001 NetScreen Technologies Inc. All rights reserved.	System Configure Admin Interface Network Policy VPN Vrtual IP Lists Address Service Schedule Users Monitor Traffic	CONFIGURATION Address Name IP Address/Domain Name Netmask Comment Location	PermoteNetwork 10.0.25.0 255.255.255.0 Trust © Untrust
	Counters Alarm Log Copyright & 1998-2001 NetScreen Technologies Ine. All rights reserved.		OK Cancel
SO TO CHE LIKENSED WARESSES LOTHAR AND	Go to the Untrusted Addresses Configuration		Internet

- 5. Selecteer **Netwerk > VPN**, ga naar het tabblad Gateway en klik op **New Remote Tunnel Gateway** om de VPN-gateway te configureren (fase 1 en fase 2 IPsec-beleid).
- Gebruik het IP-adres van de externe interface van PIX om de tunnel te sluiten en stel de opties Fase 1 IKE in om te binden. Klik op OK wanneer u klaar bent.Dit voorbeeld gebruikt deze velden en waarden.Naam gateway: To501Statisch IP-adres: 172.18.124.96Modus: Hoofdvenster (ID-bescherming)Voorgedeelde sleutel: "testme"Voorstel fase 1: pre-g2-3dessha

NetScreen Administration Tools - Microso	A Internet Explorer	1 E X
Ele Edit Yew Fgvarites Jools Help		
🔾 tack + 💭 🖉 🛋 🐔 🔎 :	learch 🎲 Pavortas 🐨 Media 🚱 🍰 🦆 🔟 🖯 🗾 🏂	
Address Ntp://10.0.3.254/kyout.html*6,1,1	2	Go Links *
NETSCREEN'-5	• help • support • abor	at • logout
System REMOTE	TUNNEL GATEWAY CONFIGURATION	÷
Configure		
Interface		
Network	Gateway Name [To501	
Policy	Remote Gateway	
VEN	Static IP Address IP Address 17218.124.96	
Lists	C Descente IB Address Base ID (optional)	
Address	C Dialun User User/Grom None *	
Constanting and the second		
Schedule	Mode (Initiator) ^{(*} Main (ID Protection) ^{(*} Aggressive	
Monitor	Phase 1 Proposal	
C Traffic	pre-g2-3des-sha 💌 none 💌	
Counters		
Alam	Preshared Key	
	Local ID (optional)	
Copyright & 1998-2001 NetScreen Technologies	Preferred Certificate (optional)	
All right: levelved,	Local Cert None •	
	Peer CA None T	
	OK	
 Go to the Gateway Configuration 	🔊 Inte	snet

Wanneer de externe tunnelgateway met succes wordt gecreëerd, verschijnt er een vergelijkbaar

scherm.



- 7. Ga naar het tabblad P1 Voorstel en klik op **Nieuw Fase 1 Voorstel** om Voorstel 1 te configureren.
- Voer de configuratieinformatie in voor het fase 1-voorstel en klik op OK.Dit voorbeeld gebruikt deze velden en waarden voor Fase 1 uitwisseling.Name: ToPIX501Verificatie: prekenDH-groep: Groep 2Encryptie: 3DES-CBCHash: SHA-1Levensduur: 3600 sec.



Wanneer fase 1 met succes is toegevoegd aan de NetScreen-configuratie, verschijnt er een scherm dat vergelijkbaar is met dit

tScreen Administration T	ools - Microsoft Internet Expl	orer					4
Edt Yew Favorites	Ioois Help						
sack • 🔘 · 🚺 💈	Search 👷 Fav	ortes 🛃 Media 🌾	3 8.31	v 🖂 🎎			
ss 📄 http://10.0.3.254/lay	out.html*6,1,1	1					60
TSCREEN'-S					• help	• support • about	• Jog
Suctom	VPN					17 Sept 200	3 15:4
System						1000000000	
Admin							Page 2
Interface						and the second second	
Network	Manual Key V AutoKey	Gateway	P1 Proposal V	2 Proposal V Certificate	L2TP	IPPool L	
THE CHION R							
PURCE -							
1 ON							
VPN							
VPN Virtual IP	Name	Method	DH Group	Encrypt/Auth.	Lifetime	Configure	
VPN Virtual IP Lists	Name dsa-g2-3des-md	Method DSA:sg	DH Group 2	Encrypt/Auth.	Lifetime 29800	Configure	
VPN Virtual IP Lists Address	Name dsa-g2-3des-md dsa-g2-3des-dsa	Method 5 DSAsg 0SAsg	DH Group 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA	Lifetime 29800 28800	Configure -	
VPN Virtual IP Lists Address Service	Name daa g2-3deo md daa g2-3deo sha TaPlid01	Method 5 DSA:sq 0 DSA:sq Preshare	DH Group 2 2 2	Encrypt/Auth, 30ES/M05 30ES/SHA 30ES/SHA	Lifetime 28800 28800 3800	Configure - - ESS Banzes	
VPN Virtual IP Lists Address Service Schedule Users	Name dia-g2-3des.md dia-g2-3des.dka ToPt:d01	Method 5 DSA-sig 0SA-pig Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3800	Configure - Ed: Bamara	
VPN Virtual IP Lists Address Service Schedule Users Manitar	Name daa g2 3dea md daa g2 3dea sha TaPid01	Method 5 DSA:sg 0SA:sg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 28800 28800 3800	Configure - - ESS Bamera	
VPN Virtual IP Lists Address Service Schedule Users Monitor	Name das g2-3des md das g2-3des sha ToPid01	Method 5 DSA-sig 0SA-sig Preshare	DH Group 2 2 2	Encrypt/Auth, 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 23800 28800 3800	Configure - Ett. Bimes	
VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic	Name da+g2-3des.md da+g2-3des.du ToPid01	Method 5 OSA-sig OSA-sig Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 25800 25800 3600	Configure - Edit Bamara	
VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters	Name daa g2 3deamd daa g2 3deasha TaPid01	Method 5 DSA-sig 5 DSA-pg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 3DES/SHA	Lifetime 25800 25800 3600	Configure - ESS Bamera	
VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm	Name das g2-3des md das g2-3des sha ToPid01	Method 5 DSA-sg DSA-sg Preshare	DH Group 2 2 2	Encrypt/Auth. 30ES/MOS 30ES/SHA 30ES/SHA	Lifetime 23800 28800 3800	Configure - Est Banesa	
VPN Virtual IP Lists Address Service Schedule Users Voers Monitor Traffic Counters Alarm Log	Name da+g2-3des.md da+g2-3des.du ToPtid01	Method 5 OSA-sig OSA-sig Preshare	DH Group 2 2 2	Encrypt/Auth. 3DES/MOS 3DES/SHA 3DES/SHA	Lifetime 25800 25800 3800	Configure - EEL Bamana	
VPN Virtual IP Lists Address Service Schedule Users Monitor Traffic Counters Alarm Log	Name dia-g2-3deamd dia-g2-3deacha TaPid01	Method 5 DSA-sig 9 DSA-pig 9 Preshare	DH Group 2 2 2	Encrypt/Auth. 3DES/MOS 3DES/SHA 3DES/SHA	Lifetime 25800 26800 3600	Configure - ESS Bamera	

- 9. Ga naar het tabblad P2 Voorstel en klik op Nieuw Fase 2 Voorstel om fase 2 te configureren.
- Voer de configuratieinformatie in voor fase 2 en klik op OK.Dit voorbeeld gebruikt deze velden en waarden voor Fase 2 uitwisseling.Name: ToPIX501Perfect voorwaartse geheimhouding: DH-2 (1024 bits)Encryptiealgoritme: 3DES-CBCVerificatiealgoritme: SHA-1Levensduur: 2640

sec			
NetScreen Administration Tools - Microsoft I	nternet Explorer		-(6) ×
Elle Edit Yew Favorites Iools Help	and the second second		
🔾 Back + 💟 - 💌 🔹 🐔 🔎 Sea	rch 🔆 Favorites 🜒 Media 🥙 🍰 🦆 🛛	5	
Address 🛃 http://10.0.3.254/keyout.htm/*6,1,1			• 🛃 Go Links **
NETSCREEN'-S		help support at	xout 👘 logout
System PHASE 2	PROPOSAL CONFIGURATION		<u> </u>
Admin Interface			
Network Policy	Name	ToPuS01	
VEN	Perfect Forward Secrecy	DH Group 2 •	
Virtual IP	Encapsulation		
	Encryption (ESP)		
Service	Encryption Algorithm	3DES-CBC -	
Schedule	Authentication Algorithm	SHA-1 •	
Uters	C Authentication Only (AH)	Arrest Con	
Traffic	Authentication Algorithm	MD5 -	
Counters			
E00 Copyright @ 1998-2001	In Time	26400 ⊙Sec ∩Mm ∩Hours ∩Days	
ling. All solds repaired	In Kbytes	0 Kbytes	

Wanneer fase 2 met succes is toegevoegd aan de NetScreen-configuratie, verschijnt er een scherm dat vergelijkbaar is met dit voorbeeld.

Edt yew Fgrontes jools joble Back <li< th=""><th>N Fgyorites [ods ight] Image: Search of Pavorites (Media (Image: Pavorites (Image:</th></li<>	N Fgyorites [ods ight] Image: Search of Pavorites (Media (Image: Pavorites (Image:
Book • () • () • () () Search () Feworites () Media () () • () () () () () () () () () () () () ()	Image: Search Search Feworites Media Image: Search
ess http://l0.0.3.254/kyvut.html%,1,1 ETSCREEN'-S * http://l0.0.3.254/kyvut.html%,1,1 ETSCREEN'-S * http://l0.0.3.254/kyvut.html%,1,1 ETSCREEN'-S * http://lo.0.3.254/kyvut.html%,1,1 ETSCREEN'-S * http://lo.0.3.254/kyvut.html%,1,1 ETSCREEN'-S * NPN * 17 Sept Configure Admin Erscriptade Network Policy VPN Vritual IP Lists Address Service Schodule USURS * 000 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 No PFS ESP 0ES / M05 900 0 - Nopth-esp-desmd5 DH Group 2 ESP 0ES / M05 900 0 - Nonitor	c/(10.0.3.254/kyrout.html*6,1,1 EN - 5 • help • support • about • log n VPN 17 Sept 2003 15:43 IP IP IP
ETSCREEN'-S Manual Key VPN 17 Sept System VPN 17 Sept 17 Sept Admin Intelefface Namual Key AutoKey IXX Gateway P1 Proposal P2 Proposal Certificates L2TP IPPoel Network Policy VPN Name PFS Encap. Encrypt/Auth. Lifetime Lifesize Configure Address Noph-sep-desmd5 No PFS ESP DES / M05 900 0 - Address noph-sep-desmd5 No PFS ESP DES / M05 9000 0 - Service noph-sep-desmd5 No PFS ESP DES / M05 3000 0 - Service noph-sep-desmd5 No PFS ESP DES / M05 3000 0 - Service noph-sep-desmd5 No PFS ESP DES / M05 3000 0 - Monitor g2-esp-desmd5 DH Group 2 ESP DES / M05 3000 0 -	EN - 5 • help • support • about • log n VPN 17 Sept 2003 15:4: Page 1 Manual Key AutoKey DQ Gateway P1 Proposal Certificates L2TP IPPool rk
System VPN 17 Sept Configure Admin Admin Receiface L3TP IPPool Network Policy Manual Key AutoKey IX2 Gateway P1 Proposal P2 Proposal Certificates L3TP IPPool Network Policy VPN Norme PFS Encap. Encrypt/Auth. Lifesize Configure Address Norph-exp-des-md5 No PFS ESP DES / M05 3000 0 - Schedule uspti-exp-des-md5 No PFS ESP JDES / M05 3000 0 - Usprix mopti-exp-des-md5 No PFS ESP JDES / M05 3000 0 - Menitorr g2-esp-des-md5 DH Group 2 ESP DES / M05 3000 0 -	n VPN 17 Sept 2003 15:4: Page 1 Manual Key AutoKey IXE Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool rk
Configure Admin Interface Network Policy VPN Virtual IP Lists Address Service Service Nopti-esp-dep-md5 No PFS ESP DES / M05 Service Nopti-esp-dep-md5 No PFS ESP DES / M05 3000 No pti-esp-dep-md5 No PFS ESP 3005 / M05 Service Nopti-esp-dep-md5 No PFS ESP 3005 / M05 3000 0 Service No PFS ESP Nopti-esp-3dep-stra No PFS ESP Schiedule No PFS ESP Usins g2-esp-dep-stra No PFS Konitorr g2-esp-dep-stra DH Group 2 ESP QES / M05 3000 0	Page 1 Manual Key AutoKey IXI Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool
Admin Interface Network Policy VPN Vrtual IP Lists Address Address Service Schedule Usins Usins Address Schedule Usins Usins Manual Key AutoKey DX Gateway PI Proposal Policy VPN Virtual IP Lists Address Nopth-exp-dep-md5 No PFS ESP DES / M05 3000 0 nopth-exp-dep-md5 No PFS ESP Schedule nopth-exp-dep-md5 No PFS Schedule g2-exp-dep-md5 PH Group 2 ESP Manitar g2-exp-dep-md5 PH Group 2 ESP Nonitar g2-exp-dep-md5 PH Group 2 ESP	Page 1 Manual Key AutoKey IXI Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool
Interface Manual Key AutoKey DKL Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool Network POESy VPN Nortural IP Nortural IP Nortural IP North-esp-dep-md5 No PFS Encop. Encrypt/Auth. Lifesize Configure Address nopto-esp-dep-md5 No PFS ESP DES / M05 3000 0 - Service nopto-esp-dep-md5 No PFS ESP DES / M05 3000 0 - Schedule nopto-esp-dep-md5 No PFS ESP 30ES / M05 3000 0 - Usins nopto-esp-3dep-md5 No PFS ESP 30ES / SHA 3000 0 - Menitorr g2-esp-dep-md5 DH Group 2 ESP QES / M05 3000 0 -	Manual Key V AutoKey DXI Gateway P1 Proposal P2 Proposal Certificates L2TP IPPool
Network Policy VPN Vrtual IP Lists Nome PFS Encop. Encrypt/Auth. Lifetime Lifesize Configure Address nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Service nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Schoolule nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Schoolule nopto-exp-dep-md5 No PFS ESP 30ES / M05 3900 0 - User/s nopto-exp-dep-md5 No PFS ESP 30ES / M05 3900 0 - Monitor g2-exp-dep-md5 DH Group 2 ESP 0ES / M05 3900 0 -	rk
Name PFS Encap. Encrypt/Auth. Lifetime Lifesize Configure Mirtual IP Nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Address nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Service nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Schiedule nopto-exp-dep-md5 No PFS ESP 30ES / M05 3900 0 - Usions nopto-exp-dep-md5 No PFS ESP 30ES / SHA 3900 0 - Usions g2-exp-dep-md5 DH Group 2 ESP QES / M05 3900 0 -	
Name PFS Encap. Encrypt/Auth. Lifetime Lifesize Configure Lists nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Address nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Service nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Schiedule nopto-exp-dep-md5 No PFS ESP 30ES / M05 3900 0 - Usins nopto-exp-3dep-sha No PFS ESP 30ES / SHA 3900 0 - Usins g2-erp-dep-md5 DH Group 2 ESP 0ES / M05 3900 0 -	
Name PFS Encap. Encrypt/Auth. Lifetime Lifesize Configure Lists Nopth-sap-dep-md5 No PFS ESP DES / M05 3900 0 - Address nopth-sap-dep-md5 No PFS ESP DES / M05 3900 0 - Services nopth-sap-dep-md5 No PFS ESP DES / M05 3900 0 - Schedule nopth-sap-dep-md5 No PFS ESP 30ES / M05 3900 0 - User/s nopth-sap-3dep-md5 No PFS ESP 30ES / SHA 3900 0 - User/s g2-esp-dep-md5 DH Group 2 ESP 0ES / M06 3900 0 -	
Name PFS Encap. Encrypt/Auth. Lifetime Lifesize Configure Lists Aopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Address nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Service nopto-exp-dep-md5 No PFS ESP DES / M05 3900 0 - Schedule nopto-exp-3dep-md5 No PFS ESP 30ES / M05 3900 0 - Usins g2-erp-dep-md5 DH Group 2 ESP 0ES / M05 3900 0 -	
Lists nopti-exp-dep-md5 No PFS ESP DES / M05 3900 0 Address nopti-exp-dep-md5 No PFS ESP DES / M05 3900 0 Service nopti-exp-dep-md5 No PFS ESP DES / M05 3900 0 Schodule nopti-exp-3dep-md5 No PFS ESP 30ES / M05 3900 0 Users sopti-exp-3dep-md5 No PFS ESP 30ES / SHA 3900 0 Monitor g2-exp-dep-md5 DH Group 2 ESP 0ES / M05 3900 0	Name PES Encap Encrypt / Auth Lifetime Lifesize Configure
Address nopti-exp-dep-tha No PFS ESP DES/SHA 3800 0 - Schedule nopti-exp-dep-tha No PFS ESP 30ES / M05 3800 0 - Usins nopti-exp-3dep-that No PFS ESP 30ES / M05 3800 0 - Usins spth-exp-3dep-that No PFS ESP 30ES / SHA 3800 0 - Monitor g2-exp-dep-that DH Group 2 ESP 0ES / M05 3900 0 -	noph-sto-deamd5 No PFS ESP DES/M06 3900 0 -
Service nopto-esp-3deo-md5 No-PFS ESP 30ES / M05 3000 0 Schedule nopto-esp-3deo-md5 No-PFS ESP 30ES / M05 3000 0 Users g2-esp-deo-md5 DH Group 2 ESP 0ES / M05 3800 0	nopti-etp-dep-tha No PFS ESP DES/SHA 3000 0
Schoolulu nepto-exp-3decodu No PFS ESP 3DES/SHA 2000 0 User/s g2-exp-decodd DH Group 2 ESP DES/M06 3800 0	nopto-exp-3des-md5 No-PFS ESP 3DES / MD5 3000 0
Monitor g2-esp-des-md5 DH Group 2 ESP DES/M06 3800 0 -	nepto-esp-3des-sha No-PFS ESP 3DES/SHA 3000 0 -
	g2.esp.des.m.d5 DH Group 2 ESP DES/MD6 3600 0
g2-esp-dep-sha DH Group 2 ESP DES/SHA 3800 0 -	g2-esp-dep-sha DH Oroup 2 ESP DES/SHA 3600 0
g2.esp-3desmd5 DH 0roup 2 ESP 30ES / MD5 3600 0 -	g2 esp-3des-m45 DH 0roup 2 ESP 30ES/MD5 3600 0 -
20 am 24 am 24 am 2 ESP 30 ESP	g2-esp-3dessha DH Group 2 ESP 3DES / SHA 3600 0 -
actory other and actory and a second and as second and a	
Topologic Topologic <thtopologic< th=""> <thtopologic< th=""> <tht< td=""><td>ToPod01 DH Group 2 ESP 30ES / SHA 20400 0 Edd</td></tht<></thtopologic<></thtopologic<>	ToPod01 DH Group 2 ESP 30ES / SHA 20400 0 Edd

- 11. Selecteer het tabblad AutoKey IKE en klik vervolgens op Nieuwe AutoKey IKE-ingang om AutoKeys IKE te maken en te configureren.
- 12. Voer de configuratieinformatie in voor AutoKey IKE in en klik vervolgens op OK.Dit voorbeeld gebruikt deze velden en waarden voor AutoKey IKE.Name: VPN-1Remote Gateway-tunnelnaam: To501(Dit werd eerder gemaakt op het tabblad Gateway.)Fase 2 Voorstel: ToPIX501(Dit is eerder gemaakt op het tabblad P2 Voorstel.)VPN-monitor: inschakelen(Dit stelt het NetScreen-apparaat in om Simple Network Management Protocol [SNMP]-traps in te stellen om de toestand van de VPN-monitor te bewaken.)

Perserven wananse adon 1946 - Paicrosol	Enternet Explorer	_161×
Ele Edit Yew Favorites Iools Help		
🔇 Back + 🕗 - 💌 🗟 🐔 🔎 Se	arch 👷 Favorites 🜒 Media 🧭 🍰 🎭 📾 🖓 🔂	
Address () http://10.0.3.254/layout.html*6,1,1		• 🔂 Go Links *
NETSCREEN'-5	• help • support	t • about • logout
System AUTOKEY	IKE CONFIGURATION	
Admin		
Naturark		
Reist	Name VPN-1	
VPN	Enable Replay Protection F Enable	
Liste	Remote Gateway Tunnel Name To501 V Ust Gateways	
Address	Phase 2 Proposal ToPb501	
Service	none	
Schedule	none	
Monitor	none	
Traffic	Lut Phase 2 Proposals	
Counters	Transport Made C South (See 1979 and 1959 and	
Log	Transport Acoust 1 Enable (For L21P+OVEr-IPSec Only)	
Cepyright @ 1999-2001	OK Cancel	
NetScreen Technologies Inc.		

Wanneer de VPN-1 regel met succes is geconfigureerd, verschijnt er een scherm dat vergelijkbaar is met dit voorbeeld.

NetScreen Administration	n Tools - Microsof	t Internet	Explorer	<u>.</u>					_6 ×
Ele Edit Yew Favorites	Look Help								
😋 Back + 🕤 · 💌	🖹 🚺 🔎 s	earch 👷	Favorites 🚷	Meda 🙆	3• 🤰 🖩 - 🚺	3			
Address 1 http://10.0.3.254	Nayout.htm ¹⁴ 6,1,1	and the second se						•	🔁 Go Links ³⁰
NETSCREEN'-5							• help •	support • about	• logout
System	VPN							17 Sept 2	003 15:46:06
Configure									Desire Laf. 1
Admin									Page 1 of 1
Interface	Manual H		toKey IXE G	deway VP1	Proposal P2 Proposal	Certificates	LITP	IPPool	
Network	1								
Policy	N	lame	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure	ſ
Virtual IP	Ň	PN-1	To501	No	ToPix501	On	Off	141	
Lists	-								*,
Address									
Service									
Schedule									
Manitor									
Traffic									
Counters									
Alam									
Log									
Copyright @ 1999-2001									
NetScreen Technologies Inc.									
20 inthe search									

- 13. Selecteer **Netwerk > Beleid**, ga naar het tabblad Uitgaande en klik op **Nieuw Beleid** om de regels te configureren die encryptie van het IPsec-verkeer toestaan.
- 14. Voer de configuratieinformatie voor het beleid in en klik op OK.Dit voorbeeld gebruikt deze velden en waarden voor het beleid. Het veld Naam is optioneel en wordt in dit voorbeeld niet gebruikt.Bronadres: Binnennetwerk(Dit is eerder gedefinieerd op het tabblad Trusted.)Bestemmingsadres: Remote-Network(Dit werd eerder gedefinieerd onder het tabblad Onvertrouwd)Service: AlleActie: TunnelVPN-tunnels: VPN-1(Dit was eerder gedefinieerd als de VPN-tunnel op het tabblad AutoKey IKE.)Een inkomend VPN-beleid wijzigen: gecontroleerd(Deze optie maakt automatisch een inkomende regel die het verkeer van het buitennetwerk van VPN aanpast.)

NetScreen Administrat	on Tools - Microsoft Internet Explorer
Ele Edt Vew Favori	es Tooje Reib
🔾 Back + 🕑 - 💌	🗟 🚯 🔎 Search 👷 Favorites 🜒 Media 🥝 🍰 🐷 - 🛄 🏂
Address http://10.0.3.2	Aflayout.html*6,1,1 💌 🛃 Go Unis 🇯
NETSCREEN-5	• http • support • about • logout
System	POLICY CONTIGUEATION
Conligure	POLICY CONFIGURATION
Admin	
Lintentace	
Network	Name (optional)
VPN	Source Address insideNetwork 💌
Virtual IP	Destination Address RemoteNetwork -
Lists	Service ANY _
Address	NAT @ Off
Service	CDIPOF
Schedule	
Manitar	C DIP On
Traffic	
Counters	Action Tunnel *
Alarm	VPN Tunnel VPN-1 -
Log	G Mathematics and Thit ster
Cepyright @ 1998-2001	Torn we address the second sec
NetScreen Technologies Inc.	L21P None
All sinkle terrared	Authentication

15. Wanneer het beleid wordt toegevoegd, zorg er dan voor dat de uitgaande VPN-regel eerst in de lijst met beleidsmaatregelen voorkomt. (De regel die automatisch voor inkomend verkeer wordt gemaakt, staat op het tabblad Inkomend.)Volg deze stappen als u de volgorde van het beleid wilt wijzigen:Klik op het tabblad Uitvoer.Klik de cirkelpijlen in de kolom Configure aan om het venster van de Micro van het Bewegingsbeleid te tonen.Wijzig de volgorde van het beleid zodat het VPN-beleid boven beleid-ID 0 staat (zodat het VPNbeleid bovenaan de lijst staat).



Ga naar het tabblad Inkomend om de regel voor inkomende verkeer te bekijken.



Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat de configuratie correct werkt.

Verificatieopdrachten

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- ping-diagnosticeert basisnetwerkconnectiviteit.
- toon crypto ipsec sa-shows the Phase 2 security associaties.
- toon crypto isakmp sa toont de fase 1 veiligheidsassociaties.

Verificatieoutput

Hier wordt een voorbeelduitvoer van ping- en show-opdrachten weergegeven.

Dit ping wordt gestart vanuit een host achter de NetScreen Firewall.

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 Uitvoer van de **show crypto ipsec als** opdracht wordt hier getoond. 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:

Uitvoer van de show crypto isakmp als opdracht wordt hier getoond.

Problemen oplossen

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

Opdrachten voor troubleshooting

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

- debug van crypto motor-displays over cryptomotoren.
- debug van crypto ipsec informatie over IPsec gebeurtenissen.
- debug van crypto isakmp-displays over IKE gebeurtenissen.

Voorbeeld van output van foutopsporing

U vindt hier voorbeelden van debug-uitvoer van de 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 second
ISAKMP: life duration (basic) of 28800
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
       length
                   : 8
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
           authenticator is HMAC-SHA
ISAKMP:
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
```

Gerelateerde informatie

- <u>IPsec-onderhandeling/IKE-protocollen</u>
- <u>Cisco PIX-firewallsoftware</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie Cisco Systems