Cisco PIX 방화벽과 NetScreen 방화벽 간의 IPSec LAN-to-LAN 터널 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>구성</u> <u>네트워크 다이어그램</u> <u>구성</u> <u>다음을 확인합니다.</u> <u>확인 명령</u> <u>확인 충력</u> <u>문제 해결 명령</u> <u>딘버그 출력 샘플</u> 관련 정보

<u>소개</u>

이 문서에서는 최신 소프트웨어가 포함된 Cisco PIX 방화벽과 NetScreen 방화벽 사이에 IPsec LAN-to-LAN 터널을 생성하는 데 필요한 절차에 대해 설명합니다. 각 디바이스 뒤에 IPsec 터널을 통해 다른 방화벽과 통신하는 사설 네트워크가 있습니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- NetScreen 방화벽은 신뢰/신뢰 해제 인터페이스의 IP 주소로 구성됩니다.
- 인터넷에 대한 연결이 설정되었습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

• PIX Firewall Software 버전 6.3(1)

• NetScreen 최신 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

<u>구성</u>

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: <u>명령 조회 도구(등록된</u> 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



<u>구성</u>

이 문서에서는 다음 구성을 사용합니다.

- <u>PIX 방화벽</u>
- <u>NetScreen 방화벽</u>

<u>PIX 방화벽 구성</u>

PIX 방화벽
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 !--- 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

<u>NetScreen 방화벽 구성</u>

NetScreen 방화벽을 구성하려면 다음 단계를 완료하십시오.

- 1. 목록 **> 주소**를 선택하고 신뢰할 수 있는 탭으로 이동한 다음 **새 주소**를 클릭합니다.
- E. 터널에서 암호화된 NetScreen 내부 네트워크를 추가하고 OK(확인)를 클릭합니다.참고: Trust(신뢰) 옵션이 선택되어 있는지 확인합니다.이 예에서는 마스크255.255.255.0 있는 네트 워크 10.0.3.0을 사용합니다

Ele Edit Yew Favorites Tools Help	Reinfernet Explorer		_10) A
🔾 🚱 😰 🖌 - 💭 - 🔊	Search 👷 Favorites 🜒 Media 🚱 🍰 🍹 🗟	1 - 🛄 🤹	
Address Abtp://10.0.3.254/layout.html*6,1,1			🔹 🛃 Go 🛛 Links ?
NETSCREEN - 5		 help support ab 	tiogol, •, logout
System ADDRESS Configure Admin Interface Network Policy VPN Virtual IP Lists Address Service Scherbule Users Monitor	Address Name IP Address/Domain Name Netmask Comment Location	[InsideNetwork [10.0.3.0 [255.255.255.0	
Traffic Counters Alarm Log		OK Cancel	
Copyright & 1998-2001 NetStreen Technologies Ine. All tights asserved.			
(Go to the Untrusted Interface			nterriet.

- 3. 목록 > 주소를 선택하고 신뢰할 수 없는 탭으로 이동한 다음 새 주소를 클릭합니다.
- 4. NetScreen 방화벽이 패킷을 암호화할 때 사용하는 원격 네트워크를 추가하고 OK(확인)를 클 릭합니다.**참고:** 비 NetScreen 게이트웨이에 VPN을 구성할 때 주소 그룹을 사용하지 마십시오 . 주소 그룹을 사용하면 VPN 상호운용성이 실패합니다. 비 NetScreen 보안 게이트웨이는 주

소 그룹을 사용할 때 NetScreen에서 생성한 프록시 ID를 해석하는 방법을 알지 못합니다.다음 과 같은 몇 가지 해결 방법이 있습니다.주소 그룹을 개별 주소록 항목으로 구분합니다. 주소록 항목 기준으로 개별 정책을 지정합니다.가능한 경우 비 NetScreen 게이트웨이(방화벽 디바이 스)에서 프록시 ID를 0.0.0.0/0으로 구성합니다.이 예에서는 마스크255.255.255.0 있는 네트워 크 10.0.25.0을 사용합니다

NetScreen Administration Tools - Micro	osoft Internet Explorer		
File Edit View Favorites Tools Help	1		
🔇 Back • 💬 · 💌 😰 🏠 🎾	🛛 Search 🐈 Favorites 🚷 Media 🚱 🔗 🖕 🖩	1 - 🤳 🍪 .	
Address a http://10.0.3.254/layout.html*6,1	1,1		💌 🔁 Go Links X
NETSCREEN'-5		help support	• about • logout
System	THE CONTROL TION		· · · · · · · · · · · · · · · · · · ·
Configure	255 CONFIGURATION		6
Admin			
Network	Π		
Policy	All Non-	(Countribution)	
VPN	Address Name	Inemotervetwork	
Virtual IP	IP Address/Domain Name	10.0.25.0	
Lists		terret and the second se	
Service	Netmask	[255.255.255.0	
Schedule	Comment		
Users	anno anna	M	
Monitor	Location	C Trust C Untrust	
Counters		in an in a second	
Alarm		OKCancel	
Log			
Copyright @ 1998-2001			
Inc.			
An ogna menned.			
e) Go to the Untrusted Addresses Configuration	n.		🔮 Internet
Start D:/WINDOWS(System32	NetScreen Administra 🔛 DATA (E:)		« 🝠 🔏 3:35 PM

- 5. Network(**네트워크**) > VPN을 선택하고 Gateway(게이트웨이) 탭으로 이동한 다음 New Remote Tunnel Gateway(새 원격 터널 게이트웨이)를 클릭하여 VPN 게이트웨이를 구성합니다(1단계 및 2단계 IPsec 정책).
- 6. 터널을 종료하고 1단계 IKE 옵션을 바인딩하려면 PIX의 외부 인터페이스의 IP 주소를 사용합니다. 완료되면 OK(확인)를 클릭합니다.이 예에서는 이러한 필드와 값을 사용합니다.게이트웨이이름: 501까지고정 IP 주소: 172.18.124.96모드로 들어갑니다: 주(ID 보호)사전 공유 키: "testme"1단계 제안: pre-g2-3des-sha

NetScreen Administration Tools - Micro	rosoft Internet Explorer	_1@ ×
Elle Edit Yew Favorites Iools Help		2
🔾 took + 💭 - 💌 🔊 🐔 🌽	🔎 Search 👷 Pavortas 🜒 Media 🚱 🍰 🤤 😳 🔝 🕗 🧾 🎿	
Aggress Ntp://10.0.3.254/kyout.html*6.1	1.1 ·	🔁 Go Links *
NETSCREEN'-5	• http://e.support//e.about	 logout
System REMOT	TE TUNNEL GATEWAY CONFIGURATION	
Configure		
interface		
Network	Gateway Name [1050]	
Policy	Remote Gateway	
VPN Virtual IP	Static IP Address IP Address 172.18.124.96	
Lists	Dynamic IP Address Peer ID	
Address	C Dialup User User/Group None -	
Service	Made (Initiated) C. Marcola (C. Marcola)	
Users	Ander (Decator) (* Idam (LD Protection) * Aggressive	
Monitor	Phase 1 Proposal	
Traffic	none	
Counters		
Log	Preshared Key	
CreviteM & 1995-2001	Local ID (optional)	
NetScreen Technologies Inc.	Preferred Certificate (optional)	
All rights received,	Peer CA None *	
	Peer Type NONE	
	Contract Contract	
	OK Cancel	
No. of the local distance of the local dista		-
I on co mis retrowsk counting acroy	li ncen	

원격 터널 게이트웨이가 성공적으로 생성되면 이와 유사한 화면이 나타납니다

.



- 7. P1 Proposal(P1 제안) 탭으로 이동하여 New Phase 1 Proposal(새 단계 1 제안)을 클릭하여 Proposal 1(제안 1)을 구성합니다.
- 8. 1단계 제안의 컨피그레이션 정보를 입력하고 확인을 클릭합니다.이 예에서는 1단계 교환에 대해 이러한 필드와 값을 사용합니다.이름: 대상Pix501인증: 사전 공유DH 그룹: 그룹 2암호화: 3DES-CBC해시: SHA-1수명: 3600초



1단계가 NetScreen 구성에 성공적으로 추가되면 이 예와 유사한 화면이 나타납니다

NetScreen Administrati	ion Tools - Micro	osoft Internet Explorer						_ 6]
Ele Edit Yew Favorito	es Iocis Help)						
🔵 Back + 🕑 - 🚺	3 6	Search 🛃 Favorite	is 🛃 Media 🌾	3 3.31	e - 🔁 🍪			
gåress 📄 http://10.0.3.25	54/layout.html*6,1	Ļt.	10.7				•	🔁 Go 🛛 Links 🤅
NETSCREEN -5						• help	• support • about	• Jogout
System	VPN						17 Sept 20	003 15:42:19
Configure								-
Admin								Page 2 of 2
Interface	Man	and Key AutoKey 100	Gateran	P1 Dupper	2 Descent) Contificates	LISTR	IPPool	
Network	1.000	and Construction	C. onematical	TA COPUSA U	a cropolar 🖉 Germinate	- Mic. 1		
Policy								
VPN								
Virtual 1P				an a sta	and the second second			1
Lists	1.1	Nome	Method	DH Group	Encrypt/Auth.	Lifetime	Configure	
Address		dsa-g2/3des/md5	DSArsig	2	30ES/M06	29800		
Service		dta-g2-3des-sha	0SA-pig	2	SDES / SHA	29900	+1 	
Schedule		ToPb501	Preshare	1 (R)	30ES/SHA	3600	Edit Bemann	
Users								
Monitor								
Tell								
Counters								
Alarm								
Log								
alari ya shini katisa								
Copyright @ 1998-2001 NetScreen Technologies								
inc,								
All sixthic second								

9. P2 Proposal(P2 제안) 탭으로 이동하여 New Phase 2 Proposal(새 단계 2 제안)을 클릭하여

2단계를 구성합니다.

10. 2단계 제안의 컨피그레이션 정보를 입력하고 확인을 클릭합니다.이 예에서는 단계 2 교환에 대해 이러한 필드와 값을 사용합니다.이름: 대상Pix501PFS(Perfect Forward Secrecy): DH-2(1024비트)**암호화 알고리즘:** 3DES-CBC**인증 알고리즘:** SHA-1**수명:** 2,6400초

NetScreen Administration Tools - Mi	crosoft Internet Explorer		_ # X
Elle Edit Yew Figworites Tools H	• <u> </u>	-	(i) 🍂
🚱 Back + 🕤 - 💌 😫 🐔	🔎 Search 🔆 Favorites 🜒 Media 🙆 🍰 🤤 🗹 -	93	
Address Ntp://10.0.3.254/layout.html*	6,1,1		🕑 🛃 Go Links "
NETSCREEN -5		• help	support about logout
System Du	ASE 2 PROPOSAL CONFICURATION		
Configure	ASE I TROPOSAL CONFIDERATION		
Admin			
Network	A CONTRACTOR OF		
Policy	Name	ToPx501	
VRN	Perfect Forward Secrecy	DH Group 2 💌	
Liele	Encapsulation		
	F Encryption (ESP)		
Service	Encryption Algorithm	3DES-CBC -	
Schedule	Authentication Algorithm	SHA-1 .	
Uters	Authentication Only (AH)		
PEDIACOT	Authentication Algorithm	MD5 ·	
Counters			
Alam	Lifetime		
E00	To Time	26400	artifica - 1 ar
Copyright @ 1998-2001 NetScreen Technologies	IN 11800	€ Sec € Mm € Hours	Days
ling. All sights reserved.	In Kbytes	0 Rbytes	

2단계가 NetScreen 구성에 성공적으로 추가되면 이 예와 유사한 화면이 나타납니다

	1 10 1	N	0 0	ुक स				
http://10.0.3.254/i	ayout.html*6,1,1							🗾 🔁 G
SCREEN-5						 help 	• sup	oort • about -
System	VPN	_).						17 Sept 2003 1
Configure								
Admin								Pa
Interface	Marriel	Key AutoKey DO Co	Animan P1 Da		Cotificate	127		PPool
Network	200	weld for warmed over for the	ocient 🖉 er en	posai 😈 🖓	ropolai 😈 Certificate	• U		
Policy								
1/0/1								
Advertise of 10	1.0							
1 late		Name	PFS	Encap.	Encrypt/Auth.	Lifetime	Lifesize	Configure
		nopts esp-dep-md5	No PFS	ESP	DES/MOS	3900	0	1.1.1
055			10.000			5000	34	1 A
Address		nopti-esp-dep-sha	36.125	\$25	DES/SHA	3000	0	
Address Service		nopti-esp-dep-sha nopti-esp-3dep-md5	No PFS	ESP	DES/SHA 3DES/MD5	3600	0	
Address Service Schedule		nopti-esp-dep-tha nopti-esp-3des-md5 nopti-esp-3des-sha	No PFS No PFS	ESP ESP ESP	0ES / SHA 30ES / M05 30ES / SHA	3600	0	
Address Service Schedule Users		nopti-esp-des-sha nopti-esp-3des-md5 nopti-esp-3des-sha g2-esp-des-md5	No PFS No PFS No PFS DH Group 2	ESP ESP ESP ESP	0ES/SHA 30ES/M05 30ES/SHA 0ES/M06	3600 3600 3600	0	
Address Service Schedule Users Monitor		nopti-esp-des-sha nopti-esp-3des-mdt nopti-esp-3des-mdt g2-esp-des-mdt g2-esp-des-mdt g2-esp-des-mdt	No PFS No PFS No PFS DH Group 2 DH Group 2	ESP ESP ESP ESP	DES/SHA 3DES/MD5 3DES/SHA DES/MD5 DES/SHA	3600 3600 3600 3600	0	
Address Service Schedule Users Monitor Traffic		nopti-esp-des-sha nopti-esp-3des-md5 nopti-esp-3des-sha g2-esp-des-md5 g2-esp-des-sha g2-esp-des-sha g2-esp-3des-md5	No PFS No PFS DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP	DES / SHA 30ES / MD5 3DES / SHA 0ES / MD5 0ES / SHA 30ES / MD5	3600 3600 3600 3600 3600	0 0 0 0	
Address Service Schedule Users Monitor Traffic Counters Alarm		nopti-esp-des-sha nopti-esp-3des-md5 nopti-esp-3des-sha g2-esp-des-md5 g2-esp-des-sha g2-esp-des-sha g2-esp-3des-sha	No PPS No PPS No PPS DH Group 2 DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP ESP ESP	DES / SHA 30ES / M06 30ES / SHA 0ES / M05 0ES / SHA 30ES / M05 30ES / SHA	3600 3600 3600 3600 3600 3600	0 0 0 0 0	
Address Service Schedule Users Monitor Traffic Counters Alarm		nopti-esp-des-sha nopti-esp-des-sha nopti-esp-des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-des-sha ToPodO1	No PPS No PFS No PFS DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP ESP ESP ESP	DES / SHA 30ES / M05 3DES / SHA 0ES / M05 0ES / M05 30ES / M05 30ES / SHA 30ES / SHA	3000 3000 3000 3000 3000 3000 3000 20400	0 0 0 0 0 0 0	Edd

- 11. AutoKey IKE 탭을 선택한 다음 New AutoKey IKE Entry를 클릭하여 AutoKeys IKE를 생성하 고 구성합니다.
- 12. AutoKey IKE에 대한 컨피그레이션 정보를 입력한 다음 OK(확인)를 클릭합니다.이 예에서는 AutoKey IKE에 대해 이러한 필드와 값을 사용합니다.이름: VPN-1원격 게이트웨이 터널 이름 : 501까지(이는 이전에 게이트웨이 탭에서 생성되었습니다.)2단계 제안: 대상Pix501(이는 P2 제안 탭에서 이전에 생성되었습니다.)VPN 모니터: 사용(이렇게 하면 NetScreen 디바이스에 서 SNMP(Simple Network Management Protocol) 트랩을 설정하여 VPN 모니터의 상태를 모 니터링할 수 있습니다

.)

NetScreen Administration Tools - Microsoft Internet	t Explorer		_(6) ×
Elle Edit Yew Favorites Tools Help			
🔇 Back + 🕗 - 💌 🖻 🐔 🔎 Search 💡	Fevortes 🜒 Meda 🚱 🍰 🔩 🗑	- <mark>- 3</mark>	
Address () http://10.0.3.254/layout.html*6,1,1			🔹 🛃 Go 🛛 Links 🏁
NETSCREEN - 5		. • help	support about fogout
System Autovev tve or	ONFICUENTION		
Configure	SANGERATION		
Admin			
Natural			
Police	Name	MPN-1	
VPN	Enable Replay Protection	Enable.	
Virtual IP	Ramata Catagory Taunal Nama	ToSOL .	
Lists	Temote Gateway Tutale Italie	Dist Gateways	
Address	Phase 2 Proposal	105601	
Service		none 📩	
Users		none	
Monitor		none	
Traffic		List Phase 2 Proposals	
Counters	VPN Monitor	P Enable	
Alarm	Transport Mode	F Enable (For L2TP-over-IPSe	ic only)
Log	-	Terrendinter	
Copyright @ 1996-2001		OK Cance	
Netschen Fechnisogies			

VPN-1 규칙이 성공적으로 구성되면 이 예와 유사한 화면이 나타납니다

.

NetScreen Administratio	in Tools - Micr	osoft Interne	t Explorer	-					_ 6
Ele Edit Yew Favorite	s Icols Hel	P							
3 Back + 🕤 · 💽	3 🏠 🌶	Search 5	Favorites 🚷	Meda 🙆	🔗 · 🎐 🖩 - 🚺	3			
Address 110.0.3.254	(layout.html*6,	1,1						-	🔁 Go Links
NETSCREEN'-5							• hilp •	support • abou	t Flogout
System	VPN							17 Sept 2	003 15:46:06
Configure									Daria L of 1
Admin									Page 1 of 1
Interface	Na	sual Key	utoKey IKE	atemay P1	Proposal P2 Proposa	Certificates	LITP V	IPPool	
Network									
VPN		Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure	1
Virtual IP		VPN-1	To501	No	ToPix501	On	Off	Ldt.	1
Lists		-							
Address									
Service									
Schedule									
Monitor									
Traffic									
Counters									
Alam									
Log									
Copyright @ 1999-2001									
Netscreen Technologies Inc.									
20 odde optional									

- 13. Network > Policy를 선택하고 Outgoing(발신) 탭으로 이동한 다음 New Policy(새 정책)를 클 릭하여 IPsec 트래픽의 암호화를 허용하는 규칙을 구성합니다.
- 14. 정책에 대한 컨피그레이션 정보를 입력하고 OK(확인)를 클릭합니다.이 예에서는 정책에 대 해 이러한 필드와 값을 사용합니다. Name 필드는 선택 사항이며 이 예에서는 사용되지 않습 니다.Source address: 내부 네트워크(이는 이전에 Trusted(신뢰할 수 있는) 탭에서 정의되었 습니다.)대상 주소: 원격 네트워크(이는 이전에 Untrusted(신뢰할 수 없음) 탭에서 정의되었 습니다.)서비스: 모두작업: 터널VPN 터널: VPN-1(이는 이전에 AutoKey IKE 탭에서 VPN 터 널로 정의되었습니다.)일치하는 수신 VPN 정책 수정: 선택(이 옵션은 외부 네트워크 VPN 트 래픽과 일치하는 인바운드 규칙을 자동으로 생성합니다 .)

NetScreen Administrat	on Tools - Microsoft Internet Explorer
Elle Edit View Favoria	es Tooje Redo
🔇 Back + 🕑 - 💌	🗟 🐔 🔎 Search 👷 Favorites 🜒 Media 🥝 🍰 🐷 😓 📓
Address http://10.0.3.2	Aflayout.html*6,1,1 💌 🛃 Go Links 🏁
NETSCREEN-5	belp >* support ** about: ** logout
System	POLICY CONTIGUE ATION
Configure	P OLICY COMPIGURATION
Admin	
Notwork	News (astimut)
Police	a vane (opuma)
VPN	Source Address InsideNetwork *
Virtual IP	Destination Address RemoteNetwork -
Lists	Service ANY *
Address	NAT © OE
Service	C DIP Off
Schedule	
Monitor	C DiP On
Traffic	
Counters	Action Tunnel -
Alarm	VPN Tunnel VPN-1 *
Log	Modific matching incoming VDN solver
Cepyright @ 1998-2001	I 2TP None v
NetScreen Technologies Inc.	
All rights interved	AuthenDcation

15. 정책이 추가되면 아웃바운드 VPN 규칙이 정책 목록에서 먼저 나타나는지 확인합니다. 인바 운드 트래픽에 대해 자동으로 생성되는 규칙은 Incoming(수신) 탭에 있습니다.정책의 순서를 변경해야 하는 경우 다음 단계를 완료합니다.발송 탭을 클릭합니다.Move Policy Micro 창을 표시하려면 Configure 열에서 순환 화살표를 클릭합니다.VPN 정책이 정책 ID 0보다 높도록 정책의 순서를 변경합니다(VPN 정책이 목록의 맨 위에 있도록).



인바운드 트래픽에 대한 규칙을 보려면 Incoming(수신) 탭으로 이동합니다



<u>다음을 확인합니다.</u>

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

<u>확인 명령</u>

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력의 분석을 봅니다.

- ping 기본 네트워크 연결을 진단합니다.
- show crypto ipsec sa 2단계 보안 연결을 표시합니다.
- show crypto isakmp sa 1단계 보안 연결을 표시합니다.

<u>확인 출력</u>

ping 및 show 명령의 샘플 출력이 여기에 표시됩니다.

이 ping은 NetScreen 방화벽 뒤의 호스트에서 시작됩니다.

```
C:\>ping 10.0.25.1 -t

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<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
```

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 pcp sas:

show crypto isakmp sa 명령의 출력이 여기에 표시됩니다.

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

<u>문제 해결</u>

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

참고: debug **명령**을 사용하기 전에 디버그 <u>명령에 대한 중요 정보</u>를 참조하십시오.

- debug crypto engine 암호화 엔진에 대한 메시지를 표시합니다.
- debug crypto ipsec IPsec 이벤트에 대한 정보를 표시합니다.
- debug crypto isakmp IKE 이벤트에 대한 메시지를 표시합니다.

<u>디버그 출력 샘플</u>

PIX 방화벽의 샘플 디버그 출력이 여기에 표시됩니다.

```
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
           default group 2
ISAKMP:
           auth pre-share
ISAKMP:
           life type in seconds
ISAKMP:
        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
                    : 500
        port
        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:
ISAKMP:
           SA life type in seconds
           SA life duration (VPI) of 0x0 0x0 0x67 0x20
ISAKMP:
ISAKMP:
           encaps is 1
           authenticator is HMAC-SHA
ISAKMP:
TSAKMP:
            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 NONCE payload. message ID = 4150037097
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_QM_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
```

<u>관련 정보</u>

- IPSec 협상/IKE 프로토콜
- <u>Cisco PIX 방화벽 소프트웨어</u>
- Cisco Secure PIX Firewall 명령 참조
- <u>보안 제품 필드 알림(PIX 포함)</u>
- <u>RFC(Request for Comments)</u>
- <u>기술 지원 및 문서 Cisco Systems</u>