Cisco VPN 3000 Concentrator와 Checkpoint NG 방화벽 간의 IPSec 터널 구성

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기규칙 네트워크 다이어그램 구성 VPN 3000 Concentrator 구성 체크포인트 NG 구성 다음을 확인합니다. 네트워크 통신 확인 체크포인트 NG에서 터널 상태 보기 VPN Concentrator에서 터널 상태 보기 문제 해결 네트워크 요약 검사점 NG용 디버그 VPN Concentrator용 디버그 과련 정보

<u>소개</u>

이 문서에서는 두 프라이빗 네트워크 간에 통신하기 위해 사전 공유 키를 사용하여 IPSec 터널을 구 성하는 방법을 보여 줍니다. 이 예에서 통신 네트워크는 Cisco VPN 3000 Concentrator 내의 192.168.10.x 프라이빗 네트워크와 NG(Checkpoint Next Generation) 방화벽 내의 10.32.x.x 프라이 빗 네트워크입니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

- VPN Concentrator 내부 및 Checkpoint NG에서 인터넷(172.18.124.x 네트워크로 표시)으로의 트래픽은 이 컨피그레이션을 시작하기 전에 흐름되어야 합니다.
- 사용자는 IPSec 협상에 익숙해야 합니다. 이 프로세스는 2개의 IKE(Internet Key Exchange) 단 계를 포함하여 5단계로 나눌 수 있습니다.IPSec 터널은 흥미로운 트래픽에 의해 시작됩니다. 트래픽은 IPSec 피어 간에 이동할 때 흥미로운 것으로 간주됩니다.IKE 1단계에서 IPSec 피어 는 설정된 IKE SA(Security Association) 정책을 협상합니다. 피어가 인증되면 ISAKMP(Internet

Security Association and Key Management Protocol)를 사용하여 보안 터널이 생성됩니다.IKE 2단계에서 IPSec 피어는 IPSec SA 변환을 협상하기 위해 인증되고 안전한 터널을 사용합니다. 공유 정책의 협상은 IPSec 터널의 설정 방법을 결정합니다.IPSec 터널이 생성되고 IPSec 변형 집합에 구성된 IPSec 매개변수를 기반으로 IPSec 피어 간에 데이터가 전송됩니다.IPSec 터널 은 IPSec SA가 삭제되거나 수명이 만료될 때 종료됩니다.

<u>사용되는 구성 요소</u>

이 컨피그레이션은 다음 소프트웨어 및 하드웨어 버전에서 개발 및 테스트되었습니다.

- VPN 3000 Series Concentrator 3.5.2
- 체크포인트 NG 방화벽

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙을 참고하십시오.</u>

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환 경에서 사용된 RFC 1918 주소입니다.

<u>구성</u>

VPN 3000 Concentrator 구성

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

1. LAN-to-LAN 세션을 구성하려면 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec LAN-to-LAN으로 이동합니다. 인증 및 IKE 알고리즘, 사 전 공유 키, 피어 IP 주소, 로컬 및 원격 네트워크 매개변수에 대한 옵션을 설정합니다. Apply를 클릭합니다.이 컨피그레이션에서는 인증이 ESP-MD5-HMAC로 설정되었고 암호화가 3DES로 설정되었습니다

Configuration System Tunneling Protocols IPSec LAN-to-LAN Modify					
Modify an IPSec LAN-to-LAN connection.					
Name Checkpoint	Enter the name for this LAN-to-LAN connection.				
Interface Ethernet 2 (Public) (172.18.124.131)	Select the interface to put this LAN-to-LAN connection on.				
Peer 172.18.124.157	Enter the IP address of the remote peer for this LAN-to-LAN connection.				
Digital None (Use Preshared Keys) *	Select the Digital Certificate to use.				
Certificate C Entire certificate chain Transmission @ Identity certificate only	Choose how to send the digital certificate to the IKE peer.				
Preshared Key ciscontprules	Enter the preshared key for this LAN-to-LAN connection.				
Authentication ESP/MD5/HMAC-128 •	Specify the packet authentication mechanism to use.				
Encryption 3DES-168 ·	Specify the encryption mechanism to use.				
IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use for this LAN-to-LAN connection.				
Routing None *	Choose the routing mechanism to use.Parameters below are ignored if Network Autodiscovery is chosen.				
Local Network					
Network List Use IP Address/Wildcard-mask below	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.				
IP Address 192.168.10.0	Note: Entry a sulfdament model which is the extension of a submater model. A				
Wildcard Mask 0.0.0.255	Note: Enter a windcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.				
Remote Network					
Network List Use IP Address/Wildcard-mask below	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.				
IP Address 10.32.0.0	Note: Enter a wildcard mask, which is the reverse of a subnet mask. A				
Wildcard Mask 0.0.127.265	For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.				
Apply Cancel					

2. Configuration(컨피그레이션) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > IKE Proposals(IKE 제안)로 이동하여 필요한 매개변수를 설정합니다.IKE 제안서 IKE-3DES-MD5를 선택하고 제안서에 대해 선택한 매개변수를 확인합니다. LAN-to-LAN 세션을 구 성하려면 Apply를 클릭합니다.이 컨피그레이션의 매개변수는 다음과 같습니다

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

3. Configuration(**컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결)로 이동하여 세션에 대해 생성된 IPSec SA를 선택하 고 LAN-to-LAN 세션에 대해 선택한 IPSec SA 매개변수를 확인합니다.이 컨피그레이션에서는 LAN-to-LAN 세션 이름이 "Checkpoint"이므로 IPSec SA가 "L2L: 체크포인트**

Configuration | Policy Management | Traffic Management | Security Associations

Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click Add to add an SA, or select an SA and click Modify or Delete.

IPSec SAs	Actions
ESP-DES-MD5	
ESP/SUES-MUS ESP/KE-3DES-MD5	
ESP-3DES-NONE	Add
ESP-L2TP-TRANSPORT	Modify
ESP-3DES-MD5-DH7	
LZL: Checkpoint	Delete

다음은 이 SA의 매개변수입니다

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

<u>체크포인트 NG 구성</u>

설정할 VPN 컨피그레이션과 관련된 정책을 구성하기 위해 네트워크 객체 및 규칙이 체크포인트 NG에 정의됩니다. 그런 다음 이 정책을 Checkpoint NG 정책 편집기와 함께 설치하여 컨피그레이 션의 Checkpoint NG 측면을 완료합니다.

1. Checkpoint NG 네트워크와 관심 있는 트래픽을 암호화하는 VPN Concentrator 네트워크를 위 한 두 개의 네트워크 개체를 만듭니다.객체를 생성하려면 Manage(관리) > Network Objects(네트워크 객체)를 선택한 다음 New(새로 만들기) > Network(네트워크)를 선택합니다. 적절한 네트워크 정보를 입력한 다음 OK를 클릭합니다.다음 예에서는 CP_inside(Checkpoint NG의 내부 네트워크) 및 CONC_INSIDE(VPN Concentrator의 내부 네트워크)라는 네트워크 개체의 집합을 보여 줍니다

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

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

2. Manage(관리) > Network Objects(네트워크 개체)로 이동하고 New(새로 만들기) > Workstation(워크스테이션)을 선택하여 VPN 디바이스, Checkpoint NG 및 VPN Concentrator에 대한 워크스테이션 개체를 생성합니다.참고: 초기 체크포인트 NG 설정 중에 생성된 체크포인트 NG 워크스테이션 객체를 사용할 수 있습니다. 워크스테이션을 Gateway(게이트웨이) 및 Interoperable VPN Device(상호 운용 가능한 VPN 디바이스)로 설정 하는 옵션을 선택하고 OK(확인)를 클릭합니다.다음 예에서는 ciscocp(Checkpoint NG) 및 CISCO_CONC(VPN 3000 Concentrator)라는 개체 집합을 보여 줍니다

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

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

3. Manage(관리) > Network Objects(네트워크 개체) > Edit(편집)로 이동하여 Checkpoint NG 워 크스테이션의 Workstation Properties(워크스테이션 속성) 창을 엽니다(이 예에서는 ciscocp). 창 왼쪽에 있는 선택 사항에서 Topology(토폴로지)를 선택한 다음 암호화할 네트워크를 선택 합니다. 인터페이스 속성을 설정하려면 Edit를 클릭합니다.이 예에서 CP_inside는 체크포인트 NG의 내부 네트워크입니다

.

/PN	Germenaces		[[
uthentication	Name	IP Address	Network Mask	IP Addresses behin
lanagement	E10080	172 18 124 157	255.255.128.0	External
dvanced	L'IGOT	112.10.124.101	200.200.200.0	Emolina
	•			<u> </u>
	Add	Edit	Bemove	Show
	5 <u>n</u> ow all IPs be	nind Gateway		
	VPN Domain			
	VPN Domain	es <u>b</u> ehind Gateway b	ased on Topology	Show
	VPN Domain	es <u>b</u> ehind Gateway b	ased on Topology	Show
	VPN Domain — All IP Address information. Manually Defi	:es <u>b</u> ehind Gateway b ined	ased on Topology	Show Show
	VPN Domain — All IP Address information. Manually Defi	ses <u>b</u> ehind Gateway b ined	ased on Topology	Sh <u>o</u> w Sho <u>w</u>
	VPN Domain — All IP Address information. Manually Defi	es <u>b</u> ehind Gateway b	ased on Topology	Show Sho <u>w</u>
	VPN Domain — All IP Address information. Manually Defined Exportable for	ses <u>b</u> ehind Gateway b ined	ased on Topology	Sh <u>o</u> w Sho <u>w</u>
	VPN Domain — All IP Address information. Manually Defined Exportable for	ses <u>b</u> ehind Gateway b ined	ased on Topology	Show Show

4. Interface Properties(인터페이스 속성) 창에서 워크스테이션을 internal(내부)로 지정하는 옵션 을 선택한 다음 적절한 IP 주소를 지정합니다. **확인을 클릭합니다**.표시된 토폴로지 선택 항목 은 워크스테이션을 internal로 지정하고 CP_inside 인터페이스 뒤에 IP 주소를 지정합니다

Interface Properties	×			
General Topology QoS	_			
Topology				
C External (leads out to the internet)				
Internal (leads to the local network)				
IP Addresses behind this interface:				
○ <u>N</u> ot Defined				
Network defined by the interface IP and Net Mask				
Specific: ↓↓ CP_inside				
Anti-Spoofing				
Perform Anti-Spoofing based on interface topology				
Spoof Tracking: O None 💿 Log O Alert				
OK Cancel Help				

5. Workstation Properties(워크스테이션 속성) 창의 Checkpoint NG에서 인터넷으로 연결되는 외 부 인터페이스를 선택한 다음 Edit(편집)를 클릭하여 인터페이스 속성을 설정합니다. 토폴로지 를 외부로 지정하려면 옵션을 선택한 다음 확인을 클릭합니다

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

.

6. Checkpoint NG의 Workstation Properties(워크스테이션 속성) 창에서 창 왼쪽에 있는 선택 사 항 중에서 VPN을 선택한 다음 암호화 및 인증 알고리즘에 대한 IKE 매개변수를 선택합니다. IKE 속성을 구성하려면 Edit를 클릭합니다

Workstation Properties -	iscocp		×
General Topology NAT VPN Authentication Management ⊕ Advanced	VPN Encryption schemes V V KE V V KE V V KE Certificate List	set default IKE properties	
	Nickname DN	Edit	
1		OK Cancel He	lp

7. VPN Concentrator의 속성과 일치하도록 IKE 속성을 설정합니다.이 예에서 **3DES**의 암호화 옵션 및 **MD5**의 해싱 옵션을 선택합니다

IKE Properties	×				
General					
Support key exchange encryption w	ith: – – Support data integrity with: –––				
Support authentication methods: —					
✓ Pre-Shared Secret	Edit <u>S</u> ecrets				
Public Key Signatures	Public Key Signatures Specify				
□ VPN-1 & FireWall-1 authenticat	ion for SecuRemote (Hybrid Mode)				
	<u>A</u> dvanced				

8. Pre-Shared Secrets(사전 공유 암호)에 대한 인증 옵션을 선택한 다음 Edit Secrets(보안 수정)를 클릭하여 VPN Concentrator의 사전 공유 키와 호환되도록 사전 공유 키를 설정합니다. Edit(편집)를 클릭하여 표시된 대로 키를 입력한 다음 Set, OK(설정, 확인)를 클릭합니다

Shar	ed Secret			×
_5	Shared Secrets List: -			
	Peer Name CISCO_CONC	Shared Secret	<u>E</u> dit	
			<u>R</u> emove	
	Enter secret: cisco	rtprules Se	et	
	ОК	Cancel	<u>H</u> elp	

9. IKE 속성 창에서 Advanced...를 클릭하고 다음 설정을 변경합니다.Support aggressive 모드에 대한 옵션을 선택 취소합니다.서브넷에 대한 Support key exchange(키 교환 지원) 옵션을 선 택합니다.완료되면 OK, OK를 클릭합니다

Advanced IKE properties			×
Use <u>U</u> DP encapsulation Support Diffie-Hellman groups	UDP VPN1_IPSE	SC_encapsu 💌]
	Group 1 (768 ✓ Group 2 (102- Group 5 (153)	bit) 4 bit) 6 bit)	
Rekeying Parameters			
Renegotiate IKE security associat	ions	1440 📑	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 📑	Seconds
Renegotiate IPSEC Security a	ssociations every	50000 🚊	KBytes
Misc Support IP <u>c</u> ompression for Se Support <u>agg</u> resive mode Support key exchange for <u>s</u> ub	ecureClient onets		
ОК С	ancel	<u>H</u> elp	

10. Manage(관리) > Network Objects(네트워크 개체) > Edit(편집)로 이동하여 VPN Concentrator의 Workstation Properties(워크스테이션 속성) 창을 엽니다. VPN 도메인을 수 동으로 정의하려면 창 왼쪽의 선택 항목에서 Topology를 선택합니다.이 예에서는 CONC_INSIDE(VPN Concentrator의 내부 네트워크)가 VPN 도메인으로 정의됩니다

Workstation Properties - C	ISCO_CONC				×
General	Topology				
- Topology NAT	<u>G</u> et Interfaces]			
VPN Advanced	Name	IP Address	Network Mask		
	t				
	<u>A</u> dd	<u>E</u> dt	Bemove §	how	
	S <u>h</u> ow all IPs beh	ind Gateway			
	VPN Domain C All IP Addresse information.	es <u>b</u> ehind Gateway b	ased on Topology	Show	_
	Manually Defined		IDE 💌	Show	
	Exportable for :	SecuRemote			
		F			
			OK C	ancel Help	

11. 창 왼쪽에 있는 선택 사항에서 VPN을 선택한 다음 IKE를 암호화 체계로 선택합니다. IKE 속 성을 구성하려면 Edit를 클릭합니다

.

Workstation Properties -	CISCO_CONC	C
General Topology NAT Advanced	Procuption genemes Image: I	
	UK Cancel Help	

12. VPN Concentrator의 현재 컨피그레이션을 반영하도록 IKE 속성을 설정합니다.이 예에서는 3DES의 암호화 옵션 및 MD5의 해싱 옵션을 설정합니다

E Properties			×
General			
Support key exchange encrypti	on with: — — Support	data integrity w	ith: —
	— мр	5	
CAST		۸1	
		A <u>1</u>	
-Support authentication methods	s:		
Pre-Shared Secret	Edit <u>S</u> ecrets		
Public <u>K</u> ey Signatures	Matching Criteri	a	
□ ⊻PN-1 & FireWall-1 auther	ntication for SecuRen	note (Hybrid Mo	de)
		Advanced	
ОК	Cancel H	Help	

13. **사전 공유 암호**에 대한 인증 옵션**을** 선택한 다음 Edit Secrets를 클릭하여 사전 공유 키를 설 정합니다. Edit(편집)를 클릭하여 표시된 대로 키를 입력한 다음 Set, OK(설정, 확인)를 클릭

Peer Nar	me Shared	Secret	
ciscocp	****		<u>E</u> dit
			<u>R</u> emove
Enter see	oret: ciscortprules	Set	

14. IKE 속성 창에서 Advanced...를 클릭하고 다음 설정을 변경합니다.IKE 속성에 적합한 Diffie-Hellman 그룹을 선택합니다.Support aggressive 모드에 대한 옵션을 선택 취소합니다.서브 넷에 대한 Support key exchange(키 교환 지원) 옵션을 선택합니다.완료되면 OK, OK를 클릭

Advanced IKE properties			2
✓ Use UDP encapsulation ———			
	UDP VPN1_IPS	EC_encapsi 🔽	
Support Diffie-Hellman groups			1
	Group 2 (102	(bit) 24 bit)	
	Group 5 (153	36 bit)	
Rekeying Parameters	,		
Renegotiate IKE security associa	ations	1440 🔅	Minute
Renegotiate IPSEC Security ass	ociations every	3600 ÷	Secon
Renegotiate IPSEC Security	associations ever	y 50000 🚊	KBytes
Misc			
Support IP compression for S	ecureClient		
Support <u>agg</u> resive mode			
Support key exchange for <u>s</u> u	bnets		
	Cancel	Help	
	Sancer	Teb	

15. 정책에 대한 암호화 규칙을 구성하려면 Rules > Add Rules > Top을 선택합니다. Policy Editor(정책 편집기) 창에서 소스가 CP_inside(Checkpoint NG의 내부 네트워크)이고 대상이 CONC_INSIDE(VPN Concentrator의 내부 네트워크)인 규칙을 삽입합니다. Service = Any, Action = Encrypt, Track = Log에 대한 값을 설정합니다. 규칙의 Encrypt Action(암호화 작업) 섹션을 추가한 경우 Action(작업)을 마우스 오른쪽 버튼으로 클릭하고 Edit Properties(속성 편집)를 선택합니다

CISCOCP - Check Point Policy Editor -	- Standard					_IO ×
File Edit View Manage Rules Policy	Topology Search Window H	ielp				
日 0 X 凸 略 巻 起 夜	A 🗉 🖳 🖀 🚝	≝≝≪∣♥	54 🗄 🖄 📥			
1 📬 📰 📰 🖓 🖓 BJ 🛛 🛛 🖉 🕻	1 Q Q 🖸 💊 🛍	•				
º € 4 @ 8 8 0 %	🗱 Security - Standard 🗮	Address Translation - St	andard 🙀 QoS - Si	tandard 🛄 Desktop Se	scurity - Standard	
E- State Network Objects	NO SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL
Workstation	NO. SOUNCE	DESTINATION	SERVICE	ALTION	THACK	INSTALL
CISCO_CONC	+ CP_inside	+ CONC_NSDE	+ Anu			Coteman
C C C C C C C C C C C C C C C C C C C	'	+ CP_inside	• ~~	Edit propert	ies	Concernal.
CONC INSIDE	2 4 CP inside	* Any	* Any	Add Encrypt	ion	Gateway
+ CP inside		and a second sec		End EuroAlty	AVIT	a sinteration
- 😥 Domain				💮 accept	2000	
OSE Device				🖲 drop	100 A	
Embedded Device				C reject	1993	
Group				🕒 User Auth	1999	
Logical Server				Client Auth		
Gateway Clutter	4				uth	•
Dynamic Object	1 North			C frevet		
	CISCO CONC	172.10.1	24.131 VDN Coord	Achert For	unt	
	ciscocp	172.18.1	24.157 Checkpoin	t Externa	794	
				Query Colur	m	
				Clear Query		

16. IKE**를** 선택하고 Edit**를 클릭합니다**

Encryption Properties		×
General		
Encryption <u>s</u> chemes defined:		
	ancel Help	

17. IKE Properties(IKE 속성) 창에서 VPN Concentrator 변환에 동의하도록 속성을 변경합니다 .Transform(변형) 옵션을 **Encryption + Data Integrity(ESP)로 설정합니다**.Encryption Algorithm(암호화 알고리즘)을 **3DES**로 **설정합니다**.데이터 무결성을 **MD5**로 **설정합니다** .VPN Concentrator(CISCO_CONC)와 일치하도록 Allowed Peer Gateway(허용된 피어 게이 트웨이)를 설정합니다.완료되면 **확인**을 클릭합니다

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

______ 18. Checkpoint NG가 구성된 후 정책을 저장하고 Policy(**정책) > Install(설치**)을 선택하여 활성화 합니다

CISCOCP - Check Point Policy	Editor - Standard					
File Edit View Manage Rules	Policy Topology Search Window	Help				
₩ 0 % 0 %	Verify Instal	° = "L ≪ ¶	₩ 🛔 🏦 🗍 🖗	?		
) Ta 🛄 8 12+ 8+]	View	G				
P= (<) (<) (<) (<) (<) (<) (<) (<) (<) (<)	Access Lists	ddress Translation - St	andard 🔊 QoS -	Standard 🛄 Desktop S	ecurity - Standard	
Network Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TRACK	INSTALL OF
	Management High Availability	and the second second				1
ciscop	Global Properties	CONC_INSIDE	🖈 Αειγ	Encrypt	🔳 Log	Gateways
CONC INSIDE	2 4 CP inside	* Acry	* Any	n accept	Log	Gateways
CP_inside						
- 😭 Domain						
OSE Device	10					
Embedded Device						
- III Group						
Logical Server						
Address Range						1
Dunamic Object						
Contraine Collect	Name	IP	Comme	nt		
	CISCO_CONC	172.18.1	124.131 VPN Co	ncentrator		
	Ciscocp	172.18.1	124.157 Checkp	oint External IP		

정책이 컴파일될 때 설치 창에 진행 정보가 표시됩니다



<u>다음을 확인합니다.</u>

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

<u>네트워크 통신 확인</u>

두 프라이빗 네트워크 간의 통신을 테스트하려면 사설 네트워크 중 하나에서 다른 프라이빗 네트워 크로 ping을 시작할 수 있습니다. 이 컨피그레이션에서는 Checkpoint NG 측(10.32.50.51)에서 VPN Concentrator 네트워크(192.168.10.2)으로 ping이 전송되었습니다.

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

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

<u>체크포인트 NG에서 터널 상태 보기</u>

터널 상태를 보려면 Policy Editor(정책 편집기)로 이동하여 **Window(창) > System Status(시스템 상 태)를** 선택합니다.

CISCOCP - Check Point System Status	il 🦷		-ox
Ele Yew Modules Products Iools Window Help			
🕽 🗩 🖻 🛤 🛄 🔦 🎫 🇞 🚛 🚔 🎯 🌪	R3		
Modules IP Address	VPN-1 Details		
	Status:	ок	
E-Ciscocp 172.18.124.157	Packets		
FireWal-1	Encrypted:	19	
FloodGate-1	Decrypted:	18	
Management	Errors		
SVN Foundation	Encryption errors:	0	
ALIN-1	Decryption errors:	0	
	IKE events errors:	3	
	Hardware		
	HW Vendor Name:	none	
	HW Status:	none	
For Help, press F1			Last updated:09:34:14 PM

VPN Concentrator에서 터널 상태 보기

VPN Concentrator에서 터널 상태를 확인하려면 Administration(관리) > Administer Sessions(세션 관리)로 이동합니다.

his screen shows st	inister Sessions	To refresh the statis	tics, click Refre	sh. Sel	ect a Group	Wednes to filter	day, 11 Sept	ember 2002 20:37 : Reset @ Refresh	
formation on a sess nnection to a sessi	sion, click on that sess on, click Ping .	sion's name. To log	out a session, cl	ick Log	out in the tal	ble belo	w. To test th	ae network	
roup [All ogout All: <u>PPTP U</u> Session Summa	ser L2TP User IPS	ec User L2TP/IPSe	ec User IPSec/U	JDP Us	er IPSec/TC	<u>P User</u>	IPSec LAN	I-to-LAN	
	Active Remote	Active	Total Active	Peak Concurrent Sessions		Concurrent Sessions Limit		Total Cumulative Sessions	
LAN Sessions	Access Sessions	Sessions	Sessions	S	essions	Sessio	ons Limit	Sessions	
Active LAN-to- LAN Sessions	Access Sessions	Sessions 3	Sessions 4	S	4	Sessio	500	Sessions	
LAN Sessions	Access Sessions	Sessions 3	Sessions 4	S	4 [<u>Remote Ac</u>	Session 1	500 sions Man	Sessions 17 agement Sessions	
LAN Sessions 1 LAN-to-LAN S Connection Nam	Access Sessions 0 essions ne IP Address	Sessions 3 Protoco	4 A Encr	yption	4 [<u>Remote Ac</u> Login T	Sessio	500 sions Man Duration	Sessions 17 agement Sessions Actions	

LAN-to-LAN Sessions(LAN-to-LAN 세션) 아래에서 생성된 SA에 대한 세부 정보와 전송/수신된 패 킷 수를 볼 체크포인트의 연결 이름을 선택합니다.

Connection Name	IP Add	tress	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
Checkpoint	172.18.12	4.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	250		
	Session ID	1	IK	E Session	Encryption Algorith	um 3DES-1	68			
			IK	E Session		anna 1	<i>c</i> 0			
Hashing	MDS		Diffie Hollman Group 2 (1024-bit)							
Hashing Algorithm Subb			4.87		Diffe Heiman Oroup			Main Main		
Authentication Mode Pr			red Keys	I	KE Negotiation Mo	de Main				
Rekey Tin	ie Interval	86400 s	econds							
			IPS	ec Session						
1	Session ID	2			ss 10.32.0.	10.32.0.0/0.0.127.255				
Loc	al Address	192.168	3.10.0/0.0.0.255		m 3DES-1	3DES-168				
	Algorithm	MD5			SH	2P 1	1			
Hashing							28800 seconds			
Hashing Encapsula	tion Mode	Tunnel			Rekey Time Interv	al 28800 s	econds			

<u>문제 해결</u>

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

참고: 트래픽은 VPN Concentrator 공용 IP 주소(외부 인터페이스)를 사용하여 IPSec 터널을 통해 PAT되지 않아야 합니다. 그렇지 않으면 터널이 실패합니다. 따라서 PATing에 사용되는 IP 주소는 외부 인터페이스에 구성된 주소 이외의 주소여야 합니다.

<u>네트워크 요약</u>

Checkpoint의 암호화 도메인에 여러 개의 인접 네트워크가 구성된 경우, 해당 디바이스는 관심 있 는 트래픽과 관련된 네트워크를 자동으로 요약할 수 있습니다. VPN Concentrator가 일치하도록 구 성되지 않으면 터널이 실패할 가능성이 높습니다. 예를 들어 10.0.0.0/24 및 10.0.1.0/24의 내부 네 트워크가 터널에 포함되도록 구성된 경우 이러한 네트워크는 10.0.0.0 /23으로 요약할 수 있습니다.

<u>검사점 NG용 디버그</u>

로그를 보려면 **창 > 로그 뷰어**를 선택합니다.

Ek												×			
部 🕼 🗓 Log 💿 🔹 🗛 董 🛓 🚔 🗒 😓 🗧 🚟 🗒 🗞 🏭 😘 🕙 🕴															
	Date	Time	Product	5 (S.)}	Inter.	Orig	Туре	Action	Source	Destinati	Pr., Rule	S_Port	SrcKeyID	DstKeyID	×
1	13Aug2002	21:32:	VPN-1	& FireN.	🖶 dae	. ciscocp	📕 log	0- key instali	ciscoop	CISCO_CONC					
2	13Aug2002	21:32:	VPN-1	& FireVV.	. 🕒 dae	. ciscocp	🔲 log	Ow key instal	ciscocp	CISCO_CONC			0x5879f30d	0xtf351129	

<u>VPN Concentrator용 디버그</u>

VPN Concentrator에서 디버그를 활성화하려면 Configuration(컨피그레이션) > System(시스템) >

Events(이벤트) > Classes(클래스)로 이동합니다. 심각도에 대해 AUTH, AUTHDBG, IKE, IKEDBG, IPSEC 및 IPSECDBG를 활성화하여 1 - 13으로 기록합니다. 디버그를 보려면 **모니터링 > 필터링 가능한 이벤트 로그를** 선택합니다.

1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157 processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508 Proposal # 1, Transform # 1, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Auth Method: Rcv'd: Preshared Key Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157 Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157 processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157 processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157 IKE SA Proposal # 1, Transform # 1 acceptable Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157 constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184 33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157 processing ke payload 34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157 processing ISA_KE 35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157 processing nonce payload 36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157 constructing ke payload 37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157 constructing nonce payload 38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157 constructing Cisco Unity VID payload 39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157 constructing xauth V6 VID payload 40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157 Send IOS VID 41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) 43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157 constructing VID payload 44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157 Send Altiga GW VID 45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157 Generating keys for Responder... 46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) ... total length : 256 48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60 50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157 Group [172.18.124.157] Processing ID 51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157 Group [172.18.124.157] processing hash 52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157 Group [172.18.124.157] computing hash 53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157 Group [172.18.124.157]

Starting group lookup for peer 172.18.124.157

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Keep-alives configured on but peer does not

support keep-alives (type = None)

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

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

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

processing IPSEC SA

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

Group [172.18.124.157] processing hash 140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157 Group [172.18.124.157] loading all IPSEC SAs 141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157 Group [172.18.124.157] Generating Quick Mode Key! 143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157 Group [172.18.124.157] Loading subnet: Dst: 192.168.10.0 mask: 255.255.255.0 Src: 10.32.0.0 mask: 255.255.128.0 146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157 Group [172.18.124.157] Security negotiation complete for LAN-to-LAN Group (172.18.124.157) Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959 149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40 IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000, seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0, spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140 Processing KEY_ADD msg! 154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141 key_msqhdr2secassoc(): Enter 155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142 No USER filter configured 156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143 KeyProcessAdd: Enter 157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144 KeyProcessAdd: Adding outbound SA 158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145 KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255, dst 10.32.0.0 mask 0.0.127.255 159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146 KeyProcessAdd: FilterIpsecAddIkeSa success 160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41 IPSEC key message parse - msgtype 3, len 327, vers 1, pid 0000000, seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0, spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0 164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147

Processing KEY_UPDATE msg!

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

Update inbound SA addresses

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

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

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

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

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

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

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

<u>관련 정보</u>

- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- Technical Support Cisco Systems