IPsec 터널 구성 - Cisco VPN 5000 Concentrator를 Checkpoint 4.1 방화벽으로 구성

목차

<u>소</u>개 사전 요구 사항 요구 사항 <u>사용되는 구</u>성 요소 표기 규칙 구성 네트워크 다이어그램 구성 Checkpoint 4.1 방화벽 다음을 확인합니다. 문제 해결 VPN 5000 Concentrator 문제 해결 명령 네트워크 요약 검사점 4.1 방화벽 디버그 디버그 출력 샘플 과련 정보

<u>소개</u>

이 문서에서는 두 개의 프라이빗 네트워크에 연결하기 위해 사전 공유 키를 사용하여 IPsec 터널을 구성하는 방법을 보여 줍니다.Cisco VPN 5000 Concentrator(192.168.1.x) 내부의 사설 네트워크를 Checkpoint 4.1 방화벽(10.32.50.x) 내부의 프라이빗 네트워크에 연결합니다. 이 컨피그레이션을 시 작하기 전에 VPN Concentrator 내부 및 Checkpoint에서 인터넷(이 문서에서 172.18.124.x 네트워 크로 표시됨)으로의 트래픽이 플로우된다고 가정합니다.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

Cisco VPN 5000 Concentrator

- Cisco VPN 5000 Concentrator 소프트웨어 버전 5.2.19.0001
- Checkpoint 4.1 방화벽

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 Cisco 기술 팁 표기 규칙을 참고하십시오.

<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 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

<u>네트워크 다이어그램</u>

이 문서에서는 다음 네트워크 설정을 사용합니다.



<u>구성</u>

이 문서에서는 이 구성을 사용합니다.

Cisco VPN 5000 Concentrator
[IP Ethernet 0:0]

Mode	=	Routed
SubnetMask	=	255.255.255.0
IPAddress	=	192.168.1.1
[General]		
EthernetAddress	=	00:00:a5:e9:c8:00
DeviceType	=	VPN 5002/8 Concentrator
ConfiguredOn	=	Timeserver not configured
ConfiguredFrom	=	Command Line, from Console
DeviceName	=	"cisco endpoint"
IPSecGateway	=	172.18.124.34
1100000000000		1,1,1,1,0,1,1,1,0,1
[IKE Policy]		
Protection	=	SHA DES G2
11000001011		5m1_515_62
[Tunnel Partner VDN 1]		
KevLifeSecs	=	28800
	_	"192 168 1 0/24"
Deer	_	
PindTo	_	10.32.30.0724
Sharodkow	_	
KowManago	_	Auto
Tranaform	_	Auto
	=	esp(sila, des)
Partner	=	1/2.18.124.15/
Mode	=	Main
Numbered	=	
Mode	=	Routed
[IP Ethernet 1:0]		
IPAddress	=	172.18.124.35
SubnetMask	=	255.255.255.240
Mode	=	Routed
[IP Static]		
10.32.50.0 255.255.255.0	VI	2N 1 1
Configuration size is 113	31	out of 65500 bytes.

<u>Checkpoint 4.1 방화벽</u>

Checkpoint 4.1 방화벽을 구성하려면 다음 단계를 완료하십시오.

1. Properties(**속성) > Encryption(암호화**)을 선택하여 Checkpoint IPsec 수명을 KeyLifeSecs = **28800** VPN Concentrator 명령에 맞게 설정합니다.**참고:** Checkpoint IKE(Internet Key Exchange) 수명을 기본값으로 둡니다

Properties Setup	×
High Availability IP Pool NAT Acces Security Policy Traffic Control Services L Authentication SYNDefender LDAP	ss Lists Desktop Security Log and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every 120 Seconds (0 for infinity)	<u>E</u> rom 100
or E⊻ery 10485760 Bytes (0 for infinity)	<u>I</u> o ffff
Renegotiate I <u>K</u> E Security Associations every	1440 minutes
Renegotiate I <u>P</u> SEC Security Associations every	28800 seconds
OK Cancel	Help

2. Manage(**관리) > Network objects(네트워크 개체) > New(또는 Edit) > Network(네트워크)**를 선 택하여 체크포인트 뒤에 있는 내부("cpinside") 네트워크에 대한 개체를 구성합니다.이는 **Peer** = **"10.32.50.0/24"** VPN Concentrator 명령과 일치해야 합니다

Network Properties
General NAT
Name: Cpinside
IP Address: 10.32.50.0 Get address
Net <u>M</u> ask: 255.255.255.0
Color:
Location: ● Internal ● External ● Broadcast: ● Allowed ● Disallowed
OK Cancel Help

3. Manage(관리) > Network objects(네트워크 개체) > Edit(편집)를 선택하여 VPN Concentrator가 Partner = <ip> 명령에서 가리키는 게이트웨이("RTPCPVPN" Checkpoint) 엔 드포인트의 개체를 편집합니다.위치(Location)에서 내부를 선택합니다.유형에 대한 게이트웨 이를 선택합니다.Modules Installed(모듈 설치됨)에서 VPN-1 및 FireWall-1 및 Management Station을 확인합니다

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Name: RTPCFVPN
IP Address: 172.18.124.157 Get address
Comment: Firewalled gateway to internet
Location:Type:
Modules Installed
▼ VPN-1 & EireWall-1 Version: 4.1 ▼ Get
□ FloodGate-1 Version: 4.1 ▼
Compression Version: 4.1
Management Station Color:
OK Cancel Help

4. Manage(관리) > Network objects(네트워크 개체) > New(또는 Edit) > Network(네트워크)를 선 택하여 VPN Concentrator 뒤에 있는 외부("inside_cisco") 네트워크에 대한 개체를 구성합니다 .이는 LocalAccess = <192.168.1.0/24> VPN Concentrator 명령과 일치해야 합니다

Network Properties
General NAT
Name: inside_cisco
IP Address: 192.168.1.0 Get address
Net <u>M</u> ask: 255.255.255.0
Color:
Location: O Internal ⊙ External ⊙ Allowed O Disallowed
OK Cancel Help

5. Manage(관리) > Network objects(네트워크 개체) > New(새로 만들기) > Workstation(워크스 데이션)을 선택하여 외부("cisco_endpoint") VPN Concentrator 게이트웨이에 대한 개체를 추 가합니다.체크포인트에 연결된 VPN Concentrator의 "외부" 인터페이스입니다(이 문서에서 172.18.124.35은 IPAddress = <ip> 명령의 IP 주소).위치(Location)에서 외부를 선택합니다.유 형에 대한 게이트웨이를 선택합니다.참고: VPN-1/FireWall-1을 선택하지 마십시오

Workstation Properties
General Interfaces SNMP NAT VPN
Name: airco, andpoint
IP Address: 172.18.124.35 Get address
<u>C</u> omment:
Location: Type:
O Internal ⊙ External O Host ⊙ Gateway
Modules Installed
□ VPN-1 & <u>F</u> ireWall-1 Version: 4.1 <u>Get</u> <u>Get</u>
FloodGate-1 Version: 4.1
Compression Version: 4.1
Management Station Color: ▼
OK Cancel Help

6. Manage(관리) > Network objects(네트워크 개체) > Edit(편집)를 선택하여 Checkpoint gateway endpoint(일명 "RTPCPVPN") VPN 탭을 편집합니다.Domain(도메인)에서 Other(기 타)를 선택한 다음 드롭다운 목록에서 Checkpoint 네트워크의 내부("cpinside")를 선택합니다 .Encryption schemes defined(정의된 암호화 체계)에서 IKE를 선택한 다음 Edit(수정)를 클릭

7. SHA_DES_G2 VPN Concentrator 명령에 동의하도록 IKE 속성을 DES encryption 및 SHA1 해 싱으로 변경합니다.참고: "G2"는 Diffie-Hellman 그룹 1 또는 2를 의미합니다. 테스트에서 체크 포인트가 "G2" 또는 "G1"을 수락한 것으로 확인되었습니다.다음 설정을 변경합니다 .Aggressive Mode를 선택 취소합니다.Supports Subnets(서브넷 지원)를 선택합니다 .Authentication Method(인증 방법) 아래에서 Pre-Shared Secret(사전 공유 암호)을 선택합니

General Interfaces SNMP NAT Certificates	VPN Authe
KE Properties	×
General	
Key <u>N</u> egotiation Encryption Method(s):	- <u>H</u> ash Method: - ☐ MD <u>5</u> ☑ SHA <u>1</u>
Authentication Method: Pre-Shared Secret Edit Secret	ecrets
Supports Aggresive <u>M</u> ode 🔽 Supports	s Su <u>b</u> nets
OK Cancel H	Help

8. Edit **Secrets**를 클릭하여 SharedKey **= <key>** VPN Concentrator 명령에 동의하도록 사전 공

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties 💦 💌
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
Cisco_endpoint Edit <u>R</u> emove
OK Cancel
OK Cancel Help
OK Cancel Help

유 키를 설정합니다.

9. Manage(관리) > Network objects(네트워크 개체) > Edit(편집)를 선택하여 "cisco_endpoint" VPN 탭을 편집합니다.Domain(도메인)에서 Other(기타)를 선택한 다음 VPN Concentrator 네 트워크("inside_cisco"라고 함)의 내부를 선택합니다. Encryption schemes defined(정의된 암 호화 체계)에서 IKE를 선택한 다음 Edit(수정)를 클릭합니다

Workstation Properties	×
General Interfaces SNMP NAT	VPN
Domain: Disabled Valid Addresses(of Interfaces) Disabled Uther: Construction Disabled Disabled Construction Disabled Disabled Construction Disabled Disabled Construction Disabled Disabled Construction Disabled Disabled Construction Disabled Dis	Encryption <u>s</u> chemes defined:
□ Fraffic Control Logging □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	ng
OK Car	ncel Help

10. SHA_DES_G2 VPN Concentrator 명령에 동의하도록 IKE 속성을 DES encryption 및 SHA1 해싱으로 변경합니다.참고: "G2"는 Diffie-Hellman 그룹 1 또는 2를 가리킵니다. 테스트에서 체크포인트에서 "G2" 또는 "G1"을 수락한 것으로 확인되었습니다.다음 설정을 변경합니다 .Aggressive Mode를 선택 취소합니다.Supports Subnets(서브넷 지원)를 선택합니다 .Authentication Method(인증 방법) 아래에서 Pre-Shared Secret(사전 공유 암호)을 선택합니

General Interfaces SNMP NAT Certificates	VPN Authe
KE Properties	×
General	
Key <u>N</u> egotiation Encryption Method(s):	Hash Method: -
	□ MD <u>5</u>
D 🖾 3DES	I™ SHA <u>1</u>
Authentication Method:	
Pre-Shared Secret Edit Secret	ecrets
Public Key Signatures <u>Confi</u>	igure
Supports Aggresive <u>M</u> ode V Supports	s Su <u>b</u> nets
OK Cancel H	telp
it.	

11. Edit **Secrets**를 클릭하여 SharedKey **= <key>** VPN Concentrator 명령에 동의하도록 사전 공 유 키를 설정합니다

IKE Properties	X
General	
Shared Secret	×
Shared Secrets List:	
Peer Name Shared Secret	
RTPCPVPN ****	
Bemove	
OK Cancel	
OK Cancel Help	

12. Policy Editor(정책 편집기) 창에서 Source(소스)와 Destination(대상)을 모두 "inside_cisco" 및 "cpinside"(양방향)로 포함하는 규칙을 삽입합니다. Set **Service=Any**, **Action=Encrypt** 및 **Track=Long**.

Ĩ	RTPO	CPVPN - Check P	oint Policy Editor				- 🗆 ×
ŀ	ile <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy Window <u>H</u>	elp			
	- 5	🗅 O 👗 🖻	Ē 월 즉 办	🖳 🌮 🗽 🗳	📙 🖀 🛲 🖷	u 🖡 🕪 🛃	🐻 🎹 🚯
	😫 Secu	urity Policy - Standard	🖥 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - St	andard	
l	No.	Source	Destination	Service	Action	Track	In≜
1	1	🚆 inside_cisco	💂 cpinside 💂 inside_cisco	Any	Encrypt	Long	
ĮI.	•						►
F	or Help,	press F1		RTPC	PVPN Read	d/Write	

13. Action(작업) 제목 아래에서 녹색 Encrypt(암호화) 아이콘을 클릭하고 Edit properties(속성 편 집)를 선택하여 암호화 정책을 구성합니다

rity Policy - Standard	🛃 Address Translation	- Standard 🛛 😿 Band	dwidth Policy - Standard	_ [
∼ FW1 Host	∼ Ldap-Servers	🕑 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	
🔁 inside_cisco	cpinside	Any	dit properties	hg
		kmp dest-unreach	Edit Encryption	
		icmp echo-request	accept	am
		icmp info-reply	drop	
Any	Any	icmp mask-reply	Fiect	hg i
•				•

14. IKE**를** 선택하고 Edit를 **클릭합니다**

General	
Encryption schemes defined:	
OK Cancel Help	

15. IKE Properties(IKE 속성) 창에서 이러한 속성을 Transform **= esp(sha,des)** VPN Concentrator 명령에 맞게 변경합니다.Transform(변형)에서 **Encryption + Data Integrity (ESP)를** 선택합니다. 암호화 알고리즘은 DES, 데이터 무결성은 **SHA1**이어야 하며, 허용된 피어 게이트웨이는 외부 VPN Concentrator 게이트웨이("cisco_endpoint"라고 함)여야 합니 다. **확인을 클릭합니다**

IKE Properties	×
General	
- Transform:	
Encryption + Data Integrity (ESP)	
C Data Integrity Only (AH)	
Encryption Algorithm: DES	j
Data Integrity SHA1	
Allowed Peer Gateway:	
Use Perfect Forward Secrecy	
OK Cancel Help	

16. Checkpoint를 구성한 후 Checkpoint 메뉴**에서 Policy > Install**을 선택하여 변경 사항을 적용 합니다.



현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

<u>문제 해결</u>

VPN 5000 Concentrator 문제 해결 명령

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

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

- vpn trace dump all 시간, VPN 번호, 피어의 실제 IP 주소, 스크립트가 실행된 경우 오류가 발 생한 소프트웨어 코드의 루틴 및 라인 번호를 포함하여 모든 일치하는 VPN 연결에 대한 정보를 표시합니다.
- show system log buffer 내부 로그 버퍼의 내용을 표시합니다.
- show vpn statistics(vpn 통계 표시) 사용자, 파트너 및 둘 모두에 대한 총 정보를 표시합니다 .(모듈형 모델의 경우 각 모듈 슬롯에 대한 섹션이 표시됩니다.샘플 디버그 <u>출력</u> 섹션을 참조하 십시오.Current Active(현재 활성) - 현재 활성 연결입니다.In Negot(Negot에서) - 현재 협상 연결 .High Water(고수) - 마지막 재부팅 이후 최대 동시 활성 연결 수입니다.Running Total—마지막 재부팅 이후 성공한 총 연결 수입니다.Tunnel OK(터널 확인) - 오류가 없는 터널 수입니다.Tunnel Starts() - 터널 시작 수입니다.Tunnel Error(터널 오류) - 오류가 있는 터널 수입니다.
- show vpn statistics verbose ISAKMP 협상 통계 및 더 많은 활성 연결 통계를 표시합니다.

<u>네트워크 요약</u>

Checkpoint의 암호화 도메인에 인접한 여러 내부 네트워크가 구성된 경우, 해당 디바이스는 흥미로 운 트래픽과 관련하여 이를 자동으로 요약할 수 있습니다.VPN Concentrator가 일치하도록 구성되 지 않으면 터널이 실패할 가능성이 높습니다.예를 들어 10.0.0.0 /24 및 10.0.1.0 /24의 내부 네트워 크가 터널에 포함되도록 구성된 경우 10.0.0.0 /23으로 요약될 수 있습니다.

<u>검사점 4.1 방화벽 디버그</u>

이것은 Microsoft Windows NT 설치입니다.추적이 정책 편집기 창 Long으로 설정되었으므로(<u>12단</u> <u>계</u>에서 표시됨) 거부된 트래픽은 로그 뷰어에 빨간색으로 표시되어야 합니다.자세한 디버그 정보를 확인하려면 다음을 수행하십시오.

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d 다른 창에서 다음을 수행합니다.

c:\winnt\Fw1\4.1\fwstart 체크포인트에서 SA(Security Associations)를 지우려면 다음 명령을 실행합니다.

fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t ISAKMP_AH_table -x 예를 프롬프트에서 중단될 수 있습니다.

<u>디버그 출력 샘플</u>

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
  new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing l2lp_init, (0 @ 0)
        38 seconds doing l2lp_do_negotiation, (0 @ 0)
  new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
  next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
  new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing iph2_pkt_2_wait, (0 @ 0)
        39 seconds doing ihp2_process_pkt_2, (0 @ 0)
        39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
        39 seconds doing l2lp_open_tunnel, (0 @ 0)
        39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
```

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0
IOP slot 3	1:						

cisco_endpoint#show vpn stat

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

cisco_endpoint#**show vpn stat verb**

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	U 1	0	0	0	0	0	0
Tatal	1	0	1	1	1	0	0
IOLAI	T	0	T	T	T	0	0
Stats		VPN0:1					
Wrapped		13					
Unwrapped		9					
BadEncap		0					
BadAuth		0					
BadEncrypt		0					
rx IP		9					
rx TPX		0					
rx Other		0					
ty TP		13					
tx IPX		0					
tx Other		0					
TKE reken		0					
TUT TOVEÀ		0					
Input VPN	pkts dro	pped due	to no SA:	0			
Input VPN	pkts dro	pped due	to no fre	e queue e	entries: ()	
ISAKMP Nec	otiation	stats					
Admin pack	cets in	4					
Fastswitch	n nackets	in 0					
No cookie	found	0					
Can't inge	rt cooki	e 0					
Theortod		1					
Inserted (CONTE(L)	1 O					
Inserted (ingente						
Cookie not	ingerte						
Cookie not	, inserce						
Cookie cor	in change						
COOKIE ali	ready ins	erted U					
Deleted co	DOKIE(L)	0					
Deleted co	pokie(R)	0					
Cookie not	t deleted	L(L) 0					
Cookie not	t de⊥eted	I(R) 0					
Forwarded	to RP	0					
Forwarded	to IOP	0					
Bad UDP ch	necksum	0					
Not fastsv	vitched	0					
Bad Initia	ator cook	ie O					
Bad Respor	nder cook	ie O					
Has Respor	nder cook	ie O					
No Respond	der cooki	e 0					
No SA		0					
Bad find o	conn	0					
Admin queu	ue full	0					
Priority o	queue ful	1 0					
Bad IKE pa	acket	0					
No memory		0					
Bad Admin	Put	0					
IKE pkt dr	copped	0					
No UDP PRI	ıf	0 0					
No Manager	~^	n					
Mar w/ no	- cookie	0					
Cookie Co-	Wende 14	d 1					
COOKIE SCO	AVELIYE AU	m O					
COOKIE SCS	аленде ке	U					

Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Ucorc	0	0	0	0	0	0	0
Dartnerg	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0
IUCAI	0	0	0	0	0	0	0
Stats Wrapped Unwrapped BadEncap BadAuth BadEncryp rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey	t						
Input VPN	pkts dro	pped due	to no SA:	0			
Input VPN	pkts dro	pped due	to no fre	e queue e	ntries: O		
ISAKMP Ne	gotiation	stats					
Admin pac	kets in	0					
Fastswitc	h packets	in 3					
No cookie	found	0					
Can't ins	ert cooki	e 0					
Inserted	cookie(L)	0					
Inserted	cookie(R)	1					
Cookie no	t inserte	d(L) 0					
Cookie no	t inserte	d(R) 0					
Cookie co	nn change	d 0					
Cookie al:	ready ins	erted 0					
Deleted c	ookie(L)	0					
Deleted c	ookie(B)	0					
Cookie no	t deleted	(T.) 0					
Cookie no	t deleted	(E) (D)					
Forwarded	to PP	(1())					
Forwarded	to TOP	3					
Bad UDP d	hecksum	0					
Not fasts	witched	0					
Rad Initia	ator cook	ie O					
Bad Regno	nder cook	ie O					
Has Respon	nder cook	ie O					
No Respon	der cooki						
No SA	acr cookr	0					
Rad find	conn	0					
Admin que	ue full	0					
Priority	queue ful	1 0					
Bad IKE n	acket	_ 0					
No memory		0					
Bad Admin	Put	0					
IKE okt d	ropped	0					
NO TIDP PR	uf	0					
No Manage:	r	0					
		-					

Mgr w/ n	o cookie	0
Cookie S	cavenge Add	1
Cookie S	cavenge Rem	0
Cookie S	cavenged	0
Cookie h	as mgr err	0
New conn	limited	0



- <u>Cisco VPN 5000 Series Concentrator 판매 중단 발표</u>
- IPsec 협상/IKE 프로토콜
- <u>기술 지원 및 문서 Cisco Systems</u>