Cisco VPN 3000 Concentrator와 AES 컨피그레 이션을 사용하는 라우터 간 LAN-to-LAN IPsec 터 널 예

목차

소개 사전 요구 사항 요구 사항 <u>사용되</u>는 구성 요소 표기규칙 구성 네트워크 다이어그램 구성 VPN Concentrator 구성 다음을 확인합니다. 라우터 컨피그레이션 확인 VPN Concentrator 컨피그레이션 확인 문제 해결 라우터 문제 해결 VPN Concentrator 문제 해결 관련 정보

<u>소개</u>

이 문서에서는 Cisco VPN 3000 Concentrator와 AES(Advance Encryption Standard)가 포함된 Cisco 라우터 간에 IPsec 터널을 암호화 알고리즘으로 구성하는 방법을 보여줍니다.

AES는 NIST(National Institute of Standards and Technology)가 암호화 방법으로 사용하기 위해 만 든 새로운 FIPS(Federal Information Processing Standard) 발행물입니다.이 표준은 IPsec 및 IKE(Internet Key Exchange) 모두의 프라이버시 변환으로 DES(Data Encryption Standard)를 대체 하는 AES 대칭 암호화 알고리즘을 지정합니다.AES에는 세 가지 키 길이, 128비트 키(기본값), 192비트 키 및 256비트 키가 있습니다.Cisco IOS®의 AES 기능은 CBC(Cipher Block Chaining) 모 드를 사용하여 IPsec에 새로운 암호화 표준 AES를 지원합니다.

AES에 대한 자세한 내용은 <u>NIST 컴퓨터 보안 리소스 센터 사이트</u> 를 참조하십시오.

VPN 3000 Concentrator<u>와 PIX</u> Firewall 간<u>의 LAN-to-LAN 터널 컨피그레이션에</u> 대한 자세한 내용은 <u>Cisco VPN 3000 Concentrator</u>와 PIX 방화벽 간 LAN-to-LAN 터널을 참조하십시오.

PIX에 소프트웨어 버전 7.1<u>이</u> 있는 경우<u>자세한 내용은 PIX 7.x와 VPN 3000 Concentrator 구성 예</u> 를 참조하십시오.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에서는 IPsec 프로토콜에 대한 기본적인 이해가 필요합니다.IPsec<u>에</u> 대한 자세한 내용은 <u>IPSec 암호화 소개</u>를 참조하십시오.

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 라우터 요구 사항 AES 기능은 Cisco IOS Software 릴리스 12.2(13)T에서 도입되었습니다 .AES를 활성화하려면 라우터가 IPsec을 지원하고 "k9" 긴 키("k9" 하위 시스템)로 IOS 이미지 를 실행해야 합니다.참고: AES에 대한 하드웨어 지원은 Cisco 2600XM, 2691, 3725 및 3745 AES 가속화 VPN 모듈에서도 제공됩니다.이 기능은 컨피그레이션에 영향을 미치지 않으며, 두 기능을 모두 사용할 수 있는 경우 하드웨어 모듈이 자동으로 선택됩니다.
- VPN Concentrator 요구 사항 AES 기능에 대한 소프트웨어 지원은 릴리스 3.6에서 도입되었 습니다. 하드웨어 지원은 새로운 SEP-E(enhanced, scalable encryption processor)에서 제공됩 니다. 이 기능은 컨피그레이션에 영향을 미치지 않습니다.참고: Cisco VPN 3000 Concentrator 릴리스 3.6.3에서는 Cisco 버그 ID CSCdy88797(등록된 고객만 해당) 때문에 터널이 AES로 협 상하지 않습니다. 이 문제는 릴리스 3.6.4에서 해결되었습니다.참고: Cisco VPN 3000 Concentrator는 SEP 또는 SEP-E 모듈을 사용하지만 둘 다 사용하지는 않습니다.동일한 디바 이스에 둘 다 설치하지 마십시오.SEP 모듈이 이미 포함된 VPN Concentrator에 SEP-E 모듈을 설치할 경우 VPN Concentrator는 SEP 모듈을 비활성화하고 SEP-E 모듈만 사용합니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 3600 Series Router with Cisco IOS Software 릴리스 12.3(5)
- Cisco VPN 3060 Concentrator with Software 릴리스 4.0.3

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>IPsec 라우터</u>
- <u>VPN 집선 장치</u>

ipsec_router 컨피그레이션

version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption !
hostname ipsec_router
1
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
! Configuration for IKE policies. crypto isakmp
policy 1
<pre>! Enables the IKE policy configuration (config-</pre>
isakmp) command mode, ! where you can specify the
parameters to be used during ! an IKE negotiation.
encryption aes 256
<pre>! Specifies the encryption algorithm as AES with a</pre>
256 ! bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
<pre>! Specifies the preshared key "cisco123" which !</pre>

should be identical at both peers. ! !--- Configuration for IPsec policies. crypto ipsec security-association lifetime seconds 28800 !--- Specifies the lifetime of the IPsec security association (SA). ! crypto ipsec transform-set vpn espaes 256 esp-md5-hmac !--- Enables the crypto transform configuration mode, where you can !--- specify the transform sets to be used during an IPsec negotiation. ! crypto map vpn 10 ipsecisakmp !--- Indicates that IKE is used to establish the IPsec SA for protecting !--- the traffic specified by this crypto map entry. set peer 20.20.20.1 !--- Sets the IP address of the remote end (VPN Concentrator). set transform-set vpn !--- Configures IPsec to use the transform-set "vpn" defined earlier. ! !--- Specifies the traffic to be encrypted. match address 110 ! interface Ethernet1/0 ip address 30.30.30.1 255.255.255.0 ip nat outside half-duplex crypto map vpn !--- Configures the interface to use the crypto map "vpn" for IPsec. ! interface FastEthernet2/0 ip address 192.168.20.1 255.255.255.0 ip nat inside duplex auto speed auto н ip nat pool mypool 30.30.30.3 30.30.30.3 netmask 255.255.255.0 ip nat inside source route-map nonat pool mypool overload ip http server no ip http secure-server ip classless ip route 0.0.0.0 0.0.0.0 30.30.30.2 ! access-list 110 permit ip 192.168.20.0 0.0.0.255 172.16.0.0 0.0.255.255 !--- This crypto ACL-permit identifies the matching traffic !--- flows to be protected via encryption. !---Specifies the traffic not to be encrypted. access-list 120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0 0.0.255.255 !--- This crypto ACL-deny identifies the matching traffic flows not to be encrypted. ! access-list 120 permit ip 192.168.20.0 0.0.0.255 any !--- The access control list (ACL) used in the NAT configuration exempts !--- the LAN-to-LAN traffic from the NAT process, !--- but allows all traffic going to the Internet to be translated. ! route-map nonat permit 10 !--- The traffic flows not encrypted from the !--- peer network are allowed. match ip address 120 1 line con 0 line aux 0 line vty 0 4 login

end

참고: ACL 구문은 변경되지 않지만 암호화 ACL의 의미는 약간 다릅니다.암호화 ACL에서 permit은 일치하는 패킷이 암호화되어야 함을 지정하는 반면, deny는 일치하는 패킷을 암호화할 필요가 없음 을 지정합니다.

VPN Concentrator 구성

VPN Concentrator는 공장 설정에서 IP 주소로 사전 프로그래밍되지 않습니다.메뉴 기반 CLI(Command Line Interface)인 초기 컨피그레이션을 구성하려면 콘솔 포트를 사용해야 합니다. 콘솔<u>을</u> 통해 구성하는 방법에 대한 자세한 내용은 <u>콘솔을 통해 VPN Concentrator 구성</u>을 참조하십 시오.

이더넷 1(프라이빗) 인터페이스의 IP 주소를 구성한 후 나머지는 CLI를 사용하거나 브라우저 인터 페이스를 통해 구성할 수 있습니다.브라우저 인터페이스는 SSL(Secure Socket Layer)을 통한 HTTP 및 HTTP를 모두 지원합니다.

이러한 매개변수는 콘솔을 통해 구성됩니다.

• Time/Date(시간/날짜) - 올바른 시간과 날짜가 매우 중요합니다.이를 통해 로깅 및 어카운팅 엔 트리가 정확하며 시스템이 유효한 보안 인증서를 생성할 수 있는지 확인할 수 있습니다.

• Ethernet 1(private) 인터페이스 - IP 주소 및 마스크(네트워크 토폴로지 172.16.1.1/24)입니다. 이때 VPN Concentrator는 내부 네트워크에서 HTML 브라우저를 통해 액세스할 수 있습니다.CLI 모 드에서 VPN Concentrator를 구성하는 방법에 대한 자세한 내용은 CLI를 <u>사용한 빠른 구성을</u> 참조 하십시오.

 GUI 인터페이스를 활성화하려면 웹 브라우저에서 프라이빗 인터페이스의 IP 주소를 입력합니다. 다.변경 사항을 메모리에 저장하려면 필요한 저장 아이콘을 클릭합니다.공장 기본 사용자 이 름 및 비밀번호는 대/소문자를 구분하는 "admin"입니다



2. GUI를 실행한 후 Configuration(컨피그레이션) > Interfaces(인터페이스) > Ethernet 2(Public)를 선택하여 Ethernet 2 인터페이스를 구성합니다

Configuration	Confi	guration Interfaces	s Ethernet 2				
EPUser Management	Config	uring Ethernet Interfa	ce 2 (Public).				
	General RIP USPF Bandwidth General Parameters						
	Sel	Attribute	Value	able Description			
	0	Disabled			Select to disable this interface.		
	0	DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.		
	C	Static IP Addressing					
		IP Address	20.20.20.1		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this		
		Subnet Mask	255.255.255.0		interface.		
		Public Interface	ч Ч		Check to make this interface a "public" interface.		
		MAC Address	00.90 A4.00.4L F9		The MAC address for this interface.		
	Filter Speed Duplex		2. Public (Default) 10/100 suto Auto		Select the filter for this interface.		
					Select the speed for this interface.		
					Select the duplex mode for this interface.		
	MTU		1500		Enter the Maximum Transmit Unit for this interface (63 - 1500).		
			C Do not fragment prior to IP.	Sec encapsulation; fo	agneent prior to interface transmission		
		Public Interface IPSec Fragmentation Policy	C Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)				
			C Fragment prior to IPSec enc	opsulation without P	ath MTU Discovery (Clear DF kit)		
Cisco Systems	Aş	Cancel					

3. Configuration(구성) > System(시스템) > IP Routing(IP 라우팅) > Default Gateway(기본 게이 트웨이)를 선택하여 기본(인터넷) 게이트웨이와 IPsec의 터널 기본(내부) 게이트웨이를 구성 하여 사설 네트워크의 다른 서브넷에 연결합니다.이 시나리오에서는 내부 네트워크에 사용 가 능한 서브넷이 하나만 있습니다

<u>Configuration</u>		
	Configuration System IP Routing I	Detault Gateways
- D System		
- II Servers	Configure the default gateways for your system.	
-El-Address Management		
- G-Tunneling Protocols	B 4 5 8 .	
-G-IP.Routing	Default Gateway 20.20.20.2	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Static Routes	Metric 1	Eater the metric, from 1 to 16.
CONTRACT CONTRACTOR	Transal Defention	Take the IR address of the default and second seconds. Earlier 0.0.0.0 General
Source and the second s	172.16.1.2	Enter the 1P and less of the default gateway of fother for fulliels. Enter 0.0.0.0 for no
OSPF Areas	Gateway -	CEDENT LOADEL
OHCP Parameters	Override Default	Wheels to allow beyond default extensions to consuld, the confirmed default extension
OHCP Relay	Gateway	Check to allow learned detour gareways to overnae the configured detour gareway.
Reduncionary	And Court	
Reverse Route Injection	Apply Concei	
- G-Management Protocols		
- Events		
General		
- El-Client Update		
Load Balancing		
User Management		
Policy Management		
Administration		
• E Monitoring		

4. Configuration(컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Network Lists(네트워크 목록) > Add(추가)를 선택하여 암호화할 트래픽을 정의하는 네트워크 목록을 생성합니다.목록에 언급된 네트워크는 원격 네트워크에 연결할 수 있습니다 .아래 목록에 표시된 네트워크는 로컬 네트워크입니다.Generate Local List(로컬 목록 생성)를 클릭하면 RIP를 통해 로컬 네트워크 목록을 자동으로 생성할 수도 있습니다

- Configuration			
	Configurati	on Policy Management Trai	affic Management Network Lists Modify
- I System			
- E-User Management	Modify a confi	gued Network List, Click on Generat	ate Local List to generate a network list based on routing entries on the Private interface.
		, ,	· · · · · · · · · · · · · · · · · · ·
Access Hours ————————————————————————————————————	Läst Name	vpn_local_network	Name of the Network List you are adding. The name must be unique.
Crout Management Network Lists SAs SA	Network List	172.16.0.0/0.0.255.255	 Eater the Networks and Wildcard masks using the following format: n.n.n.n/n.n.n.n (e.g. 10.100.000.255.255). Note: Enter a wildcard mask, which is the reverse of a submet mask. A wildcard mask, which is the reverse of a submet mask. A wildcard mask wild is in bit positions to ignore, 0s in bit positions to match. For example, 10.10.100.00.255 = all 10.10.1 rea addresses. Each Network and Wildcard mask pair must be entered on a single line. The Wildcard mask may be omitted if the natural Wildcard mask is to be used.
	Apply	Concel Generate L	Local List

5. 이 목록의 네트워크는 원격 네트워크이므로 수동으로 구성해야 합니다.이렇게 하려면 연결 가 능한 각 서브넷에 대해 네트워크/와일드카드를 입력합니다

Configuration Interfaces Bystem GRUser Management OPtology Management	Configuration Policy Management Traffic Management Network Lists Modify Modify a configured Network List Click on Generate Local List to generate a network list based on routing entries on the Private interface.
Access itsurs Tratic Management Gitwork Lists Git	List Name vpn_remote_network Name of the Network List you are adding. The users must be unique. 192.168.20.0/0.0.0.255 • Network List • Refer the Network List you are adding. The users must be unique. Network List • Refer the Network List you are adding. The users must be unique. Network List • Network List •

완료되면 다음 두 네트워크 목록이 표시됩니다

H <u>Conflouration</u> httributs Honoces Honocenent Honocenent Honocenent Honocenent Honocenent Honocenent Honocenent Honocenent	Configuration Policy Management Traffic Management This section lets you add, modify, copy, and delete Network Lists Clark Add to create a Network List, or select a Network List and click Modify	Network Lists Save 🕞 fy, Cepy, or Delete.	
Cities =2As =78xss =790AI <u>BVPnicies</u> D Scent Michins ⊕Administration ⊕Mentoring	Network List VPN Client Local LAN (Defai Vgn_remole_network vgn_local_network	Actions ault) Add Modity Copy Delete	

6. Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec LANto-LAN > Add and define the LAN-to-LAN tunnel(LAN-to-LAN 터널 추가 및 정의)을 선택합니 다.이 창에는 세 개의 섹션이 있습니다.맨 위 섹션은 네트워크 정보에 대한 것이며 아래 두 섹 션은 로컬 및 원격 네트워크 목록에 대한 것입니다.Network Information(네트워크 정보) 섹션 에서 AES 암호화, 인증 유형, IKE 제안서를 선택하고 사전 공유 키를 입력합니다.아래 섹션에 서 이미 생성한 네트워크 목록(로컬 및 원격 목록 모두)을 각각 가리킵니다

T Continue time		
	Configuration System Tunneling Protocols IPSec	ILAN-to JAN LAdd
	congrader system remening reacters in sec	
- (I) Servers	Add a new IPSec LAN-to-LAN connection	
-G- <u>Tunnelino Protocols</u>	Enable 🖂	Check to enable this LAN-to-LAN connection.
	News Acet	Behaville event double () M to 1 / M even other
	Ivane [081	Enter the harse for this LAIN-10-LIAIN connection.
LANto-LAN	Interface Ethernet 2 (Public) (20.20.20.1)	Select the interface for this LAN-to-LAN connection.
HKE Proposale	Connection Type Birdinomic and	Choose the type of LAN-to-LAN connection. An Originate Only connection may
Alexter Alexter	condetabilit type Dearacional	have multiple peers specified below.
-GHP Routing	30.30.30.1	
		Enter the remote peer IP addresses for this LAN-to-LAN connection. Originate-
Lost Balancing	Peers	Ov() connection may specify up to ten peer IP addresses. Enter one IP address per line
- EUser Management	8	100
Access Hours		
	Distal	
- Administration	Certificate None (Use Preshared Keys)	Select the digital cortificate to use.
-38-Monitoring	Contractor O Entire anti-Entre shelp	
	Transmission @ Identificant out	Choose how to send the digital certificate to the IXE peer.
	C manage cancers only	
	Preshared Key cisco123	Enter the poschared key for this LAN-to-LAN connection.
Cases Courses	Authentication ESP/MD5/HMAC-128	Specify the packet suthentication mechanism to use.
CISCO ATSTENS	Enryption AES-256	specify the entryption methods in to use.
	IKE Proposal KE-AES256-SHA	Select the IKE Proposal to use for this LAN-to-LAN connection.
- H-Servers		
- El-Tunneling Protocols		
	Filter -None-	Choose the filter to apply to the traffic that is transled through this LAN-to-LAN
EIPSec	_	connection. That is 'n MAT T commental's 195ce maar ootsblich die 1.433 to 1.437
LAN-to-LAN	IPSee NAT-T	connection of the ugh a NAT device. You rough also enable IPSec over NAT-T under
HE Proposala		NAT Transparency.
Alarta	Baadwidth Policy -None-	Choose the bandwidth policy to apply to this LAN-to-LAN connection
E-P Mouting	Routing None	Choose the routing mechanism to use Parameters below are ignored if Network Autodisensative is choose
	·	adduction of the second s
- E General	Local Network: If a LAN-to-LAN NAT rule is used, this is the Transle	ated Network address.
Load Balancing	Network List Vpn_local_network	Specify the local network address list or the IP address and wildcard music for this [A M is 1 A M converting.
	IP Address	East-Resolution Collection.
Access Hours		Note: Enter a wildcard mask, which is the overage of a submet mask. A millionit work has to be bit waritime to mean. It is hit waritime to work. For
	Wildcard Mask	scample, 10.10.1.00.0.0.255 = all 10.10.1 mm addresses.
E-Broup Matching		
	Remote Network: If a LAN-to-LAN NAT rule is used, this is the Rem	acte Network address.
CO PERSONALING	Network List vpn_remote_notwork	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
	IP Address	
	a cannos	Note: Enter a witdowd mask, which is the reverse of a subnet mask. A
	Wildcard Mask	wildcard mask has is in bit positions to ignore, 0s in bit positions to match. For rearaple, 10.10.1.00.0.0.235 = all 10.10.1 ann addresses.
Cisco Sestems	Add Concel	•
tlbtlb		

7. Add(**추가**)를 클릭하면 연결이 올바르면 IPSec LAN-to-LAN-Add-Done 창이 표시됩니다.이 창에는 터널 컨피그레이션 정보의 개요가 표시됩니다.또한 그룹 이름, SA 이름 및 필터 이름을 자동으로 구성합니다.이 테이블에서 모든 매개변수를 편집할 수 있습니다



이 시점에서 IPsec LAN-to-LAN 터널이 설정되었으며 작업을 시작할 수 있습니다.어떤 이유로 터널이 작동하지 않을 경우 컨피그레이션 오류를 확인할 수 있습니다.

8. Configuration(컨피그레이션) > System(시스템) > **Tunneling Protocols(터널링 프로토콜)** > IPSec LAN-to-LAN(IPSec LAN-to-LAN)을 선택하면 이전에 생성한 LAN-to-LAN IPsec 매개변 수를 보거나 수정할 수 있습니다.이 그래픽은 "test"를 터널 이름으로 표시하며, 원격 끝의 공용 인터페이스는 시나리오에 따라 30.30.30.1입니다

- Configuration						
	Configuration System Tunneling Protocols IPSec LAN-to-LAN					
- G System		Save				
- @Servers						
	This section late you configure IPSec LAN-to-LAN connections LAN-to-LAN connections are se	tablished with other VPN 3000 Concentrators				
	PIX firewalls, 7100/4000 series contexs and other IPSer-compliant security gateways. To configure	a VPN 3002 or other remote access				
EPTP	connection, go to User Management and configure a Group and User. To configure NAT over LAN	I-to-LAN, go to LAN-to-LAN NAT Rules.				
L2TP						
- EHESeo	If you want to define a set of astworks on the local or remote side of the LAN-to-LAN connection	, configure the necessary Network Lists prior				
LAN-to-LAN	to creating the connection.					
IKE Proposals						
NAT Transparency	Click the Add button to add a LAN-to-LAN connection, or select a connection and click Modify or	Delete.				
<u>Nerts</u>	· · · ·					
- CHP Routing	(D) indicates a disabled LAN-to-LAN connection.					
- Management Protocols						
- @ Events	LAN to LAN					
- @ General	Connection	Actions				
	test (30.30.30.1) on Ethernet 2 (Public)					
C.P. Ser Management		Add				
- Charlie Management		Modify				
Network Lists						
Rules		Delete				
SAS						
-EMAL						
EVV Policies						
- @ Group Metching						
<u>Administration</u>						
- Monitoring						

9. IKE 제안이 Inactive Proposals(비활성 제안) 목록에 있으면 터널이 나타나지 않을 수 있습니다 .Configuration(**컨피그레이션**) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > IKE Proposals(IKE 제안)를 선택하여 활성 IKE 제안을 구성합니다.IKE 제안이 "Inactive Proposals(비활성 제안)" 목록에 있는 경우 IKE 제안서를 선택하고 Activate(활성화) 버튼을 클릭할 때 활성화할 수 있습니다.이 그림에서 선택한 제안 "IKE-AES256-SHA"가 활성 제안 목록에 있습니다



10. Configuration(**컨피그레이션**) > Policy Management(정책 관리) > Traffic Management(트래 피관리) > Security Associations(보안 연결)를 선택하여 SA 매개변수가 올바른지 확인합니 다

	Configuration Policy Management Traffic Management Security Associations	
- QSystem	Sa	VB 📊
- En Servers		
- El-Address Management	This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IEE Proposels to recordiate IF	KE.
- ETunneling Protocols	parameters.	
PPTP	2	
LZTP	("lick did to wid an 50, or solart an 58, and click Mindife or Dalate	
	Shahan Sonahan, Sonahan and an ana many si belek.	
LAN-ID-LAN		
KE Proposals	IPSec SAs Artions	
NAT Transparency	ESP-3DES-MD5	
Nerts	ESP-3DES-MD5-DH5	
- EIP Routing	ESP-3DES-MD5-DH7	
- FHManagement Protocols	ESP-3DES-NONE Add	
- EPEvents	ESP-AES128-SHA	
	ESP-DES-MD5 Modify	
Client Update	ESPI.2TP-TRANSPORT Delate	
Load Balancing	ESP/KE-3DES-MD5	
	L2L test	
Policy Management		
Access Hours	· · · · · · · · · · · · · · · · · · ·	
-EFTraffic Management		
Bulez		
Ellers		
- EI-NAT		
BA/Policies		
Higroup Matching		
Administration		
Monitoring		

11. SA 이름(이 경우 L2L:테스트)를 클릭한 다음 Modify(수정)를 클릭하여 SA를 확인합니다.매개 변수 중 하나라도 원격 피어 컨피그레이션과 일치하지 않으면 여기에서 변경할 수 있습니다

Configuration	Configuration Policy Management Traffic Managem	ent Security Associations Modify
	Modify a configured Security Association.	
District State District	SA Name L2L:test	Specify the name of this Security Association (SA). Select the granularity of this SA.
CAN-ID-LAN	IPSec Parameters	
NAT Transporancy	Algorithm ESP/MD5/HMAC-128	Select the pecket authentication algorithm to use.
<u>Aleris</u>	Encryption Algorithm AES-256	Select the ESP encryption algorithm to use.
El Management Protocols	Encapsulation Mode Tunnel 💌	Select the Encapsulation Mode for this SA.
	Perfect Forward Servery Disabled	Select the use of Perfect Forward Secrecy.
End Balancing End Balancing	Lifetime Measurement	Select the lifetime measurement of the IPSe: keys
- Policy Management	Data Lifetime 10000	Specify the data lifetime in kilobytes (ICB).
Access Hours — [Traffic Management]	Time Lifetime 28800	Specify the time lifetime in seconds.
Rules	IKE Parameters	
Elbers	Connection Type Hidrectional IKE Press 30 30 30.3	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
EXCEpticies	Negotiation Mode Main	Select the IKE Negotiation mode to use
-E-Group Metching -E-Administration	Digital Certificate None (Use Preshared Keys) 💌	Select the Digital Certificate to use.
-EMonitoring	Cardificate C Entire certificate clain Transmission © Identity certificate only	Choose how to used the digital cartificate to the $1\mathrm{K\Sigma}$ poer.
	IKE Proposal IKE AES256 SHA	 Select the IKE Proposal to use as IKE initiator.
Cisco Systems	Apply Concel	_

<u>다음을 확인합니다.</u>

<u>라우터 컨피그레이션 확인</u>

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

일부 show 명령은 <u>출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면</u> show 명 령 출력의 분석 결과를 볼 수 있습니다.

• show crypto isakmp sa - 피어의 현재 모든 IKE SA를 표시합니다.QM_IDLE 상태는 SA가 피어 로 인증되고 후속 빠른 모드 교환에 사용할 수 있음을 나타냅니다.그것은 조용한 상태에 있다. ipsec_router#show crypto isakmp sa

dst src state conn-id slot

20.20.20.1 30.30.30.1 **QM_IDLE** 1 0

• show crypto ipsec sa - 현재 SA에서 사용하는 설정을 표시합니다.피어 IP 주소, 로컬 및 원격 모두에서 액세스할 수 있는 네트워크, 사용되는 변형 집합을 확인합니다.ESP SA는 각 방향에 하나씩 2개 있습니다.AH 변형 집합을 사용하므로 비어 있습니다. ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

Crypto map tag: vpn, local addr. 30.30.30.1

protected vrf:

local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

current_peer: 20.20.20.1:500

```
PERMIT, flags={origin_is_acl,}
```

#pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145 #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1 path mtu 1500, media mtu 1500 current outbound spi: 54FA9805 inbound esp sas: spi: 0x4091292(67703442) transform: esp-256-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4471883/28110) IV size: 16 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x54FA9805(1425709061) transform: esp-256-aes esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4471883/28110) IV size: 16 bytes replay detection support: Y outbound ah sas:

outbound pcp sas:

 show crypto engine connections active(암호화 엔진 연결 활성 표시) - 모든 암호화 엔진에 대한 현재 활성 암호화 세션 연결을 표시합니다.각 연결 ID는 고유합니다.암호화 및 암호 해독된 패 킷 수는 마지막 두 열에 표시됩니다.

ipsec_	ipsec_router# show crypto engine connections active						
ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt	
1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0	
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19	
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0	

VPN Concentrator 컨피그레이션 확인

.

VPN Concentrator 컨피그레이션을 확인하려면 다음 단계를 완료하십시오.

1. show crypto ipsec sa 및 **show crypto isakmp sa** 명령과 유사하게 VPN Concentrator에서 Monitoring(모니터링) > Statistics(통계) > **IPSec**을 선택하면 IPsec 및 IKE 통계를 볼 수 **있습 니다**

-=	Monitoring Statistics IPSec		Thursday	, U1 Janu	uary 2004-19:32:36
Filenaces				R	eset 🥔 Refresh 🔞
FiUser Management	IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics		
DPolicy Management	Active Tunnels	L	Active Tunnels	L	
Access Hours	Total Tunnels	2	Total Tunnels	2	
Network Lists	Received Bytes	3545268	Received Bytes	3602	
Fules	Sent Bytes	5553204	Sent Bytes	5376	
5.6.8	Received Packets	60187	Received Packets	145	
Eller2	Sent Packets	60299	Sent Packets	51	
BAY Policies	Received Parkets Dropped	0	Received Parkets Dropped	0	
Group Matching	Sent Packets Dropped	D	Received Parkets Dropped (Anti-Replay)	0	
	Received Notifies	60084	Sent Packets Dropped.	0	
ElSoftware Uniste	Sent Notifies	120172	Inbound Authentirations	145	
Consentrator	Received Phase-2 Eachanges	2	Failed Inbound Authentications	0	
Clients Sustan Bahast	Sent Phase-2 Exchanges	49	Outhound Authentirations	51	
Rebot Status	Invalid Phase-2 Exchanges Received	D	Failed Outbound Authentications	0	
Elba	Invalid Phase 2 Eachanges Sent	0	Decryptions	145	
Monitoring Refresh	Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0	
Erwecess regits	Rejected Sent Phase-2 Exchanges	0	Encryptions	51	
Swap Confid File	Phase-2 SA Delete Requests Received	0	Failed Encryptions	0	
TETP Transfer	Phase-2 SA Delete Requests Sent	50	System Capability Failures	U	
XML Export	Initiated Tunnels	0	No-SA Failures	0	
ERCentricate Management	Failed initiated Tunnels	0	Protocol Use Failures	0	
Encoliment	Failed Remote Tunnels	0			
-T-Monitoring	Authentication Failures	0			
Routing Table	Decryption Failures	D			
Dynanic Filtere	Hash Validation Failures	0			
CISCO SYSTEMS	System Capability Failures	0			
เป็นเป็น	No-SA Failures	0			

2. 라우터에서 show crypto engine connections active 명령과 마찬가지로 VPN Concentrator의 Administration-Sessions 창을 사용하여 모든 활성 IPsec LAN-to-LAN 연결 또는 터널에 대한 매개변수 및 통계를 볼 수 있습니다

Configuration	Administration I Ad	iminister Sea	sions						Thursday	. 01.Jan	uary 2004-19:30:20	
- Er Systen										R	eset 🥔 Refresh 🕲	
Elliser Management												
Access Hours	This screen shows statistics for sessions. To reflech the statistics, click Refresh . Select a Group to filter the sessions. For more information on a session, click on that sessions name. To log out a session, click Legent in the table below. To best the network connection to a session, click Fing .											
Hetwork Lists	Group -AI- Legout All: PPTP Uper	I2TP User IP	Sec User []	PSec LAN-b	o-LAN							
- <u>filars</u> -EttAI	Session Summary											
Group Matching	Active LAN-to- LAN Sessions	ive LAN-to- N Sessions Access Sessions		Active Managemen s Sessions		lative ious	ive Peak Conre Is Session		Concur Sessions	vent i Limit	Total Cumulative Sessions	
Administration Administer Sessions	1	0		L			3		4000		19	
Concentrator Cientz	LAN-ta-LAN Sessions [Reacte Access Sessions Management Sessions]											
Reboot Status	Connection Name	IP Address	Pro	iocol	Encryption	Lagi	a Tinus	Duration	Byns Tx	Bytes Rx	Actions	
Ping	test	30.30.30.1 IPSecLAN-to-LAN AES-256 J				Jaal	a 1 19:57:29 0:02:51 21		2128	2128	[Logent Ping]	
Evaluation instructure Evaluation Evaluat								integratent Sessions]				
	STRANGE	Public IP Ad	dress	Second.	Encryption		Duratio	n	Version	Bytes	Rx	
	No Remote Access Sessions											
Management Sessions [LAN-to-LAN Sessions Benote Access Sees										ris Access Sessions]		
	Administrator	IP Addr	ess I	Protocol	Encryption		Legin	Time	Duratie	h	Artions	
	admin.	172.161.2	нт	TP	None	Jac	01 19:17	42	0:12:38	[100	out Ping]	

<u>문제 해결</u>

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

<u>라우터 문제 해결</u>

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.

- debug crypto engine 암호화된 트래픽을 표시합니다.암호화 엔진은 암호화 및 암호 해독을 수 행하는 실제 메커니즘입니다.암호화 엔진은 소프트웨어 또는 하드웨어 가속기가 될 수 있습니 다.
- debug crypto isakmp IKE 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.

• debug crypto ipsec - IKE 2단계의 IPsec 협상을 표시합니다.

자세한 정보 및 샘플 출력은 <u>IPSec 문제 해결 - 디버그 명령 이해 및 **사용**을</u> 참조하십시오.

VPN Concentrator 문제 해결

Cisco 라우터의 debug 명령과 유사하게 Event 클래스를 구성하여 모든 경보를 볼 수 있습니다.

1. Configuration(컨피그레이션) > System(시스템) > Events(이벤트) > Classes(클래스) > Add(추 가)를 선택하여 이벤트 클래스의 로깅을 설정합니다.다음 클래스는 IPsec에 사용할 수 있습니 다

.IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. 추가하는 동안 경보가 전송되는 심각도 레벨을 기준으로 각 클래스에 대해 심각도 레벨을 선 택할 수도 있습니다.경보는 다음 방법 중 하나로 처리할 수 있습니다.로그 기준콘솔에 표시됨 UNIX Syslog 서버로 전송이메일로 전송SNMP(Simple Network Management Protocol) 서버 에 트랜으로 전송

Configuration	Configuration System Events Clas	ses Add					
- Er System - Er Servers	This screen lets you add and configure an event class for special handling.						
	Class Name KEDBG	 Select the event class to configure. 					
Ottanogenent Protocols Operants	Enable 🖂	Check to enable special bandling of this class.					
General FTP Backup	If one of the following values has been set to Use Event List, the Event List can be seen by viewing Configuration System Events General.						
Trao Destinations	Changing a value set to Use Scent List will over	ide the sections of the Event List referring to this event class.					
Systog Servers	Events to Log Seventies 1–5	 Select the events to enter in the log. 					
Dnal Recipients	Events to Consols Severities 1-3	 Select the events to display on the consols. 					
	Events to Syslog None	 Select the events to send to a Syslog Server. 					
Loed Balancing	Events to Email None	 Select the events to send to an Enail Recipient. 					
User Management Decicy Management	Events to Trap None	 Select the events to send to an SNMP Trap Destination. 					
-D <u>Administration</u> -D <u>Monitoring</u>	Add Cancel						

3. Monitoring(**모니터링**) > Filterable Event Log(필터링 이벤트 로그)를 선택하여 활성화된 경보 를 모니터링합니다



<u>관련 정보</u>

- <u>고급 암호화 표준(AES)</u>
- DES/3DES/AES VPN Encryption Module
- IPSec 샘플 컨피그레이션
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 협상/IKE 프로토콜 지원 페이지