

Cisco 라우터에 Cisco VPN 3000 Concentrator 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[VPN Concentrator 컨피그레이션](#)

[다음을 확인합니다.](#)

[라우터에서](#)

[VPN Concentrator에서](#)

[문제 해결](#)

[라우터에서](#)

[문제 - 터널을 시작할 수 없습니다.](#)

[PFS](#)

[관련 정보](#)

소개

이 샘플 컨피그레이션은 Cisco IOS[®] 소프트웨어를 실행하는 라우터 뒤에 있는 사설 네트워크를 Cisco VPN 3000 Concentrator 뒤에 있는 사설 네트워크에 연결하는 방법을 보여줍니다. 네트워크의 디바이스는 개인 주소를 통해 서로를 인식합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2611 라우터(Cisco IOS Software 릴리스 12.3.(1)**참고:** Cisco 2600 Series 라우터가 VPN 기능을 지원하는 암호화 IPsec VPN IOS 이미지와 함께 설치되어 있는지 확인하십시오.

- Cisco VPN 3000 Concentrator 4.0.1 B

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

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팀 표기 규칙을 참고하십시오.](#)

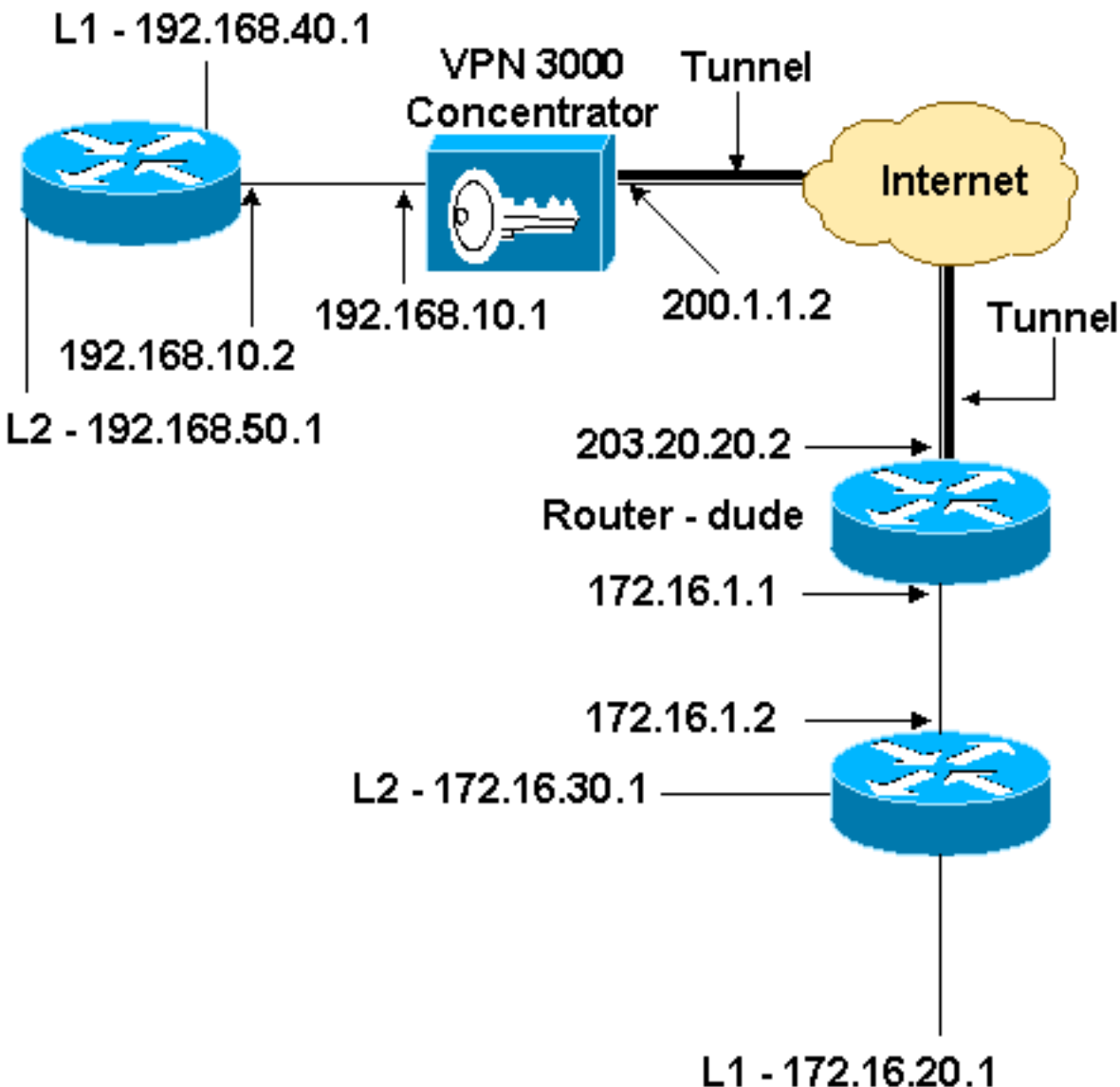
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: [명령 조회 도구](#) (등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이 구성을 사용합니다.

라우터 컨피그레이션

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
  set peer 200.1.1.2
  set transform-set to_vpn
!!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
  ip address 203.20.20.2 255.255.255.0
  ip nat outside
  half-duplex
  crypto map to_vpn
!
interface Ethernet0/1
  ip address 172.16.1.1 255.255.255.0
  ip nat inside
  half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 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 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
```

```

192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end

```

VPN Concentrator 컨피그레이션

이 Lab 설정에서 VPN Concentrator는 먼저 콘솔 포트를 통해 액세스되고 최소 컨피그레이션이 추가되어 그래픽 사용자 인터페이스(GUI)를 통해 추가 컨피그레이션을 수행할 수 있습니다.

Administration(관리) > System Reboot(시스템 재부팅)> Schedule reboot(재부팅 예약) > Reboot with Factory/Default Configuration(공장/기본 컨피그레이션으로 재부팅)을 선택하여 VPN Concentrator에 기존 컨피그레이션이 없는지 확인합니다.

VPN Concentrator가 빠른 구성에 나타나며 이러한 항목은 재부팅 후 구성됩니다.

- 시간/날짜
- Interfaces/Masks in Configuration(컨피그레이션의 인터페이스/마스크) > Interfaces(공용 =200.1.1.2/24, private=192.168.10.1/24)
- Configuration(컨피그레이션)의 Default Gateway(기본 게이트웨이) > System(시스템) > IP 라우팅 > Default_Gateway(200.1.1.1)

이때 VPN Concentrator는 내부 네트워크에서 HTML을 통해 액세스할 수 있습니다.

참고: VPN Concentrator는 외부에서 관리되므로 다음을 선택해야 합니다.

- Configuration > Interfaces > 2-public > Select IP Filter > 1. Private(기본값).
- Administration(관리) > Access Rights(액세스 권한) > Access Control List(액세스 제어 목록) > Add Manager Workstation(관리자 워크스테이션 추가)을 클릭하여 외부 관리자의 IP 주소를 추가합니다.

외부에서 VPN Concentrator를 관리하지 않는 한 이 작업은 필요하지 않습니다.

1. GUI를 표시한 후 인터페이스를 다시 확인하려면 Configuration > Interfaces를 선택합니다

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)

2. Configuration > System > IP Routing > Default Gateways를 선택하여 Default(Internet) Gateway 및 IPsec용 Tunnel Default(내부) Gateway for IPsec을 프라이빗 네트워크의 다른 서브넷에 연결하도록 구성합니다

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

3. Configuration(컨피그레이션) > Policy Management(정책 관리) > Network Lists(네트워크 목록)를 선택하여 암호화할 트래픽을 정의하는 네트워크 목록을 생성합니다.다음은 로컬 네트워크입니다

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.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
192.168.10.0/0.0.0.255
192.168.40.0/0.0.0.255
192.168.50.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* 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.
- 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 Cancel Generate Local List

다음은 원격 네트워크입니다

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.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* 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.
- 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 Cancel Generate Local List

4. 완료되면 다음 두 네트워크 목록이 표시됩니다. **참고:** IPsec 터널이 나타나지 않으면 흥미로운 트래픽이 양쪽에서 일치하는지 확인합니다. 흥미로운 트래픽은 라우터와 PIX 상자의 액세스 목록에 의해 정의됩니다. VPN Concentrator의 네트워크 목록에 의해 정의됩니다

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

5. Configuration(컨피그레이션) > System(시스템) Tunneling Protocols(터널링 프로토콜) > IPsec LAN-to-LAN을 선택하고 LAN-to-LAN 터널을 정의합니다

Add a new IPsec LAN-to-LAN connection.

<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> 203.20.20.2 </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
--	--

Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.
Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.	
Network List <input type="text" value="vpn_local_subnet"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> 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.
Wildcard Mask <input type="text"/>	
Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.	
Network List <input type="text" value="router_subnet"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> 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.
Wildcard Mask <input type="text"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

6. Apply(적용)를 클릭하면 LAN-to-LAN 터널 컨피그레이션의 결과로 자동으로 생성되는 다른 컨피그레이션과 함께 이 창이 표시됩니다

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

```

Authentication Server Internal
  Group 203.20.20.2
Security Association L2L: to_router
  Filter Rules L2L: to_router Out
               L2L: to_router In

```

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

이전에 생성한 LAN-to-LAN IPsec 매개 변수는 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec LAN-to-LAN에서 보거나 수정할 수 있습니다

Configuration | System | Tunneling Protocols | IPsec | LAN-to-LAN Save Needed

This section lets you configure IPsec LAN-to-LAN connections. LAN-to-LAN connections are established with other VPN 3000 Concentrators, PIX firewalls, 7100/4000 series routers and other IPsec-compliant security gateways. To configure a VPN 3002 or other remote access connection, go to [User Management](#) and configure a Group and User. To configure NAT over LAN-to-LAN, go to [LAN-to-LAN NAT Rules](#).

If you want to define a set of networks on the local or remote side of the LAN-to-LAN connection, configure the necessary [Network Lists](#) prior to creating the connection.

Click the **Add** button to add a LAN-to-LAN connection, or select a connection and click **Modify** or **Delete**.

(D) indicates a disabled LAN-to-LAN connection.

LAN-to-LAN Connection	Actions
to_router (203.20.20.2) on Ethernet 2 (Public)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

7. Configuration(컨피그레이션) > System(시스템) Tunneling Protocols(터널링 프로토콜) > IPsec > IKE Proposals(IKE 제안)를 선택하여 활성 IKE 제안을 확인합니다

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="<< Activate"/> <input type="button" value="Deactivate >>"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient3DES-MD5-RSA CiscoVPNClient3DES-SHA-DSA CiscoVPNClient3DES-MD5-RSA-DH5 CiscoVPNClient3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

8. Configuration(컨피그레이션) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결)를 선택하여 보안 연결 목록을 확인합니다

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-3DES-MD5	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	
L2L: to_router	

9. 보안 연결 이름을 클릭한 다음 수정을 클릭하여 보안 연결을 확인합니다

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	<input type="text" value="Bidirectional"/>	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	<input type="text" value="203.20.20.2"/>	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

다음을 확인합니다.

이 섹션에서는 이 컨피그레이션에 사용된 **show** 명령을 나열합니다.

라우터에서

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

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

- **show crypto ipsec sa** - 현재 보안 연결에서 사용하는 설정을 표시합니다.
- **show crypto isakmp sa** - 피어의 현재 모든 인터넷 키 교환 보안 연결을 표시합니다.
- **show crypto engine connection active(암호화 엔진 연결 활성 표시)** - 모든 암호화 엔진에 대한 현재 활성 암호화 세션 연결을 표시합니다.

[IOS Command Lookup Tool\(등록된 고객만\)](#)을 사용하여 특정 명령에 대한 자세한 내용을 볼 수 있습니다.

[VPN Concentrator에서](#)

로깅을 켜려면 **Configuration > System > Events > Classes > Modify**를 선택합니다. 다음 옵션을 사용할 수 있습니다.

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

기록할 심각도 = 1-13

콘솔에 대한 심각도 = 1-3

Monitoring(모니터링) > **Event Log(이벤트 로그)**를 선택하여 이벤트 로그를 검색합니다.

[문제 해결](#)

[라우터에서](#)

debug 명령을 [시도하기](#) 전에 [디버그 명령](#)에 대한 중요 정보를 참조하십시오.

- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.

[문제 - 터널을 시작할 수 없습니다.](#)

오류 메시지

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

솔루션

원하는 동시 로그인 수를 구성하거나 이 SA에 대해 동시 로그인을 5로 설정하려면 이 작업을 완료합니다.

Configuration(구성) > User Management(사용자 관리) > Groups(그룹) > Modify 10.19.187.229 > General(일반) > Simultaneous Logins(동시 로그인)로 이동하여 로그인 수를 5로 변경합니다.

PFS

IPsec 협상에서 PFS(Perfect Forward Secrecy)는 각 새 암호화 키가 이전 키와 관련이 없도록 합니다. 두 터널 피어에서 PFS를 활성화 또는 비활성화합니다. 그렇지 않으면 라우터에 LAN-to-LAN(L2L) IPsec 터널이 설정되지 않습니다.

이 암호화 맵 항목에 대해 새 보안 연결이 요청될 때 IPsec이 PFS를 요청하도록 지정하거나, 새 보안 연결에 대한 요청을 받을 때 IPsec에서 PFS를 요구하도록 지정하려면 암호화 맵 컨피그레이션 모드에서 **set pfs** 명령을 사용합니다. IPsec에서 PFS를 요청하지 않도록 지정하려면 이 명령의 **no** 형식을 사용합니다.

```
set pfs [group1 | group2]
no set pfs
```

set pfs 명령의 경우:

- *group1* - 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 768비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.
- *group2* - 새 Diffie-Hellman 교환을 수행할 때 IPsec에서 1024비트 Diffie-Hellman 프라임 모듈러스 그룹을 사용하도록 지정합니다.

기본적으로 PFS는 요청되지 않습니다. 이 명령으로 지정된 그룹이 없으면 *group10* 기본값으로 사용됩니다.

예:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

set pfs 명령에 대한 자세한 내용은 [Cisco IOS Security Command Reference](#)를 참조하십시오.

관련 정보

- [가장 일반적인 L2L 및 원격 액세스 IPsec VPN 문제 해결 솔루션](#)
- [Cisco VPN 3000 Series Concentrator](#)
- [Cisco VPN 3002 하드웨어 클라이언트](#)
- [IPsec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)