

VPN 서비스 모듈을 사용하는 Catalyst 6500과 Cisco IOS 라우터 컨피그레이션 사이의 IPsec LAN-to-LAN 터널 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[레이어 2 액세스 또는 트렁크 포트를 사용하는 IPsec 구성](#)

[라우티드 포트를 사용하는 IPsec 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[문제 해결 명령](#)

[관련 정보](#)

소개

이 문서에서는 VPN 가속화 서비스 모듈과 Cisco IOS® 라우터를 사용하여 Cisco Catalyst 6500 시리즈 스위치 간에 IPsec LAN-to-LAN 터널을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 6000 Supervisor Engine용 Cisco IOS Software 릴리스 12.2(14)SY2, IPsec VPN 서비스 모듈 포함
- Cisco IOS Software 릴리스 12.3(4)T를 실행하는 Cisco 3640 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참조하십시오](#).

배경 정보

Catalyst 6500 VPN 서비스 모듈에는 외부에 보이는 커넥터가 없는 2개의 기가비트 이더넷(GE) 포트가 있습니다. 이러한 포트는 컨피그레이션용으로만 주소를 지정할 수 있습니다. 포트 1은 항상 내부 포트입니다. 이 포트는 내부 네트워크에서 및 내부 네트워크로 가는 모든 트래픽을 처리합니다. 두 번째 포트(포트 2)는 WAN 또는 외부 네트워크에서 들어오고 나가는 모든 트래픽을 처리합니다. 이 두 포트는 항상 802.1Q 트렁킹 모드에서 구성됩니다. VPN 서비스 모듈은 패킷 플로우에 BITW(Bump In The Wire)라는 기술을 사용합니다.

패킷은 VLAN 쌍, VLAN 내부의 레이어 3 및 VLAN 외부의 레이어 2 쌍에 의해 처리됩니다. 패킷은 내부에서 외부로 라우팅되며, EARL(Encoded Address Recognition Logic)이라는 메서드를 통해 내부 VLAN으로 라우팅됩니다. 패킷을 암호화한 후 VPN 서비스 모듈은 해당 외부 VLAN을 사용합니다. 암호 해독 프로세스에서 외부에서 내부로 전달되는 패킷은 외부 VLAN을 사용하여 VPN 서비스 모듈에 브리지됩니다. VPN 서비스 모듈이 패킷을 해독하고 VLAN을 해당 내부 VLAN에 매핑한 후 EARL은 패킷을 적절한 LAN 포트에 라우팅합니다. 레이어 3 내부 VLAN 및 레이어 2 외부 VLAN은 `crypto connect vlan` 명령을 실행하여 함께 결합됩니다. Catalyst 6500 Series 스위치에는 세 가지 유형의 포트가 있습니다.

- **라우팅된 포트**—기본적으로 모든 이더넷 포트는 라우팅된 포트입니다. 이러한 포트에는 숨겨진 VLAN이 연결되어 있습니다.
- **액세스 포트** - 이 포트에는 연결된 외부 또는 VTP(VLAN Trunk Protocol) VLAN이 있습니다. 둘 이상의 포트를 정의된 VLAN에 연결할 수 있습니다.
- **트렁크 포트** - 이 포트는 많은 외부 또는 VTP VLAN을 전달하며, 모든 패킷은 802.1Q 헤더로 캡슐화됩니다.

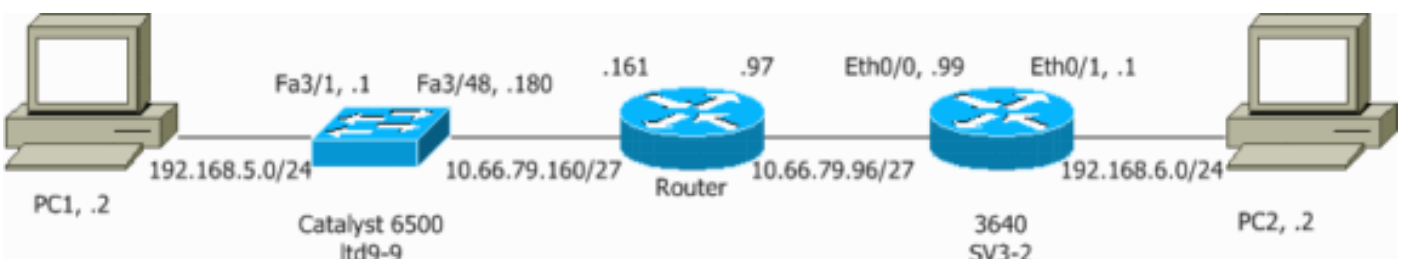
구성

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 다음 다이어그램에 표시된 네트워크 설정을 사용합니다.



레이어 2 액세스 또는 트렁크 포트를 사용하는 IPsec 구성

외부 물리적 인터페이스에 대한 레이어 2 액세스 또는 트렁크 포트의 도움을 받아 IPsec을 구성하려면 다음 단계를 수행합니다.

1. VPN 서비스 모듈의 내부 포트에 내부 VLAN을 추가합니다.VPN 서비스 모듈이 슬롯 4에 있다고 가정합니다. VLAN 100을 내부 VLAN으로, VLAN 209를 외부 VLAN으로 사용합니다.다음과 같이 VPN 서비스 모듈 GE 포트를 구성합니다.

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. VLAN 100 인터페이스와 터널이 종료되는 인터페이스를 추가합니다(이 경우 `vlan 209`가 여기에 표시된 대로).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
no ip address
crypto connect vlan 100
```

3. 외부 물리적 포트를 액세스 포트 또는 트렁크 포트 구성합니다(이 경우 `FastEthernet 3/48`과 같이).

```
!--- This is the configuration that uses an access port. interface FastEthernet3/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet3/48
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Bypass NAT를 생성합니다.이러한 네트워크 간의 연결을 제외하려면 `no nat` 문에 다음 항목을 추가합니다.

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
```

```
nat (inside) 1 192.168.5.0 255.255.255.0
```

5. 암호화할 트래픽을 정의하는 암호화 컨피그레이션 및 ACL(Access Control List)을 생성합니다. 내부 네트워크 192.168.5.0/24에서 원격 네트워크 192.168.6.0/24로의 트래픽을 정의하는 ACL(이 경우 ACL 100)을 다음과 같이 생성합니다.

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

다음과 같이 ISAKMP(Internet Security Association and Key Management Protocol) 정책을 정의합니다.

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

이 예에서 이 명령을 실행하여 사전 공유 키를 사용하고 정의합니다.

```
crypto isakmp key cisco address 10.66.79.99
```

다음과 같이 IPsec 제안서를 정의합니다.

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

다음과 같이 암호화 맵 문을 생성합니다.

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
```

6. 다음과 같이 VLAN 100 인터페이스에 암호화 맵을 적용합니다.

```
interface vlan100
crypto map cisco
```

이러한 컨피그레이션이 사용됩니다.

- [Catalyst 6500](#)
- [Cisco IOS 라우터](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
```

```

the IPsec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
crypto map cisco 10 ipsec-isakmp
  set peer 10.66.79.99
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
  ip address 192.168.5.1 255.255.255.0
!
!--- This is the outside Layer 2 port that allows VLAN
!--- 209 traffic to enter. interface FastEthernet3/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN).  switchport trunk allowed vlan
1,100,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet4/2
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- The Port VLAN (PVLAN) configuration is handled
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
a corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
  switchport mode trunk
  cdp enable
  spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224  crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address  crypto connect vlan 100
!
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route

```

```
0.0.0.0 0.0.0.0 10.66.79.161
global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (100). !--- Two separate access lists should
always be used in this configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Cisco IOS 라우터

```
SV3-2#show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!--- Define the Phase 1 policy. crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.180
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. This indicates that IKE !--- is
used to establish the IPsec !--- SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
  set peer 10.66.79.180
```

```

set transform-set cisco
match address 100
!
!
!--- Apply the crypto map to the interface. interface
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
 ip address 192.168.6.1 255.255.255.0
 half-duplex
 no keepalive
!
!
ip http server
no ip http secure-server
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
!--- This is the crypto ACL. access-list 100 permit ip
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

라우티드 포트를 사용하는 IPsec 구성

외부 물리적 인터페이스에 대해 레이어 3 라우티드 포트의 도움을 받아 IPsec을 구성하려면 다음 단계를 수행합니다.

1. VPN 서비스 모듈의 내부 포트에 내부 VLAN을 추가합니다.VPN 서비스 모듈이 슬롯 4에 있다고 가정합니다. VLAN 100을 내부 VLAN으로, VLAN 209를 외부 VLAN으로 사용합니다.다음과 같이 VPN 서비스 모듈 GE 포트를 구성합니다.

```

interface GigabitEthernet4/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 cdp enable

```

```

interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,209,1002-1005

```

```
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. VLAN 100 인터페이스와 터널이 종료되는 인터페이스를 추가합니다(이 경우 FastEthernet3/48이 여기에 표시됨).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224

interface FastEthernet3/48
no ip address
crypto connect vlan 100
```

3. Bypass NAT를 생성합니다.이러한 네트워크 간의 연결을 제외하려면 no nat 문에 다음 항목을 추가합니다.

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

4. 암호화 컨피그레이션 및 암호화할 트래픽을 정의하는 ACL을 생성합니다.내부 네트워크 192.168.5.0/24에서 원격 네트워크 192.168.6.0/24로의 트래픽을 정의하는 ACL(이 경우 ACL 100)을 다음과 같이 생성합니다.

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

다음과 같이 ISAKMP 정책 제안을 정의합니다.

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

사전 공유 키를 사용하고 정의하려면 이 명령(이 예에서는)을 실행합니다.

```
crypto isakmp key cisco address 10.66.79.99
```

다음과 같이 IPsec 제안서를 정의합니다.

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

다음과 같이 암호화 맵 문을 생성합니다.

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
```

5. 다음과 같이 VLAN 100 인터페이스에 암호화 맵을 적용합니다.

```
interface vlan100
crypto map cisco
```

이러한 컨피그레이션이 사용됩니다.

- [Catalyst 6500](#)

- [Cisco IOS 라우터](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. This indicates that IKE !--- is
used to establish the IPsec !--- SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
ip address 192.168.5.1 255.255.255.0
!--- This is the secure port that is configured in
routed port mode. !--- This routed port mode does not
have a Layer 3 IP address !--- configured. This is
normal for the BITW process. !--- The IP address is
moved from this interface to the VLAN 100 to !---
accomplish BITW. This brings the VPN service module into
!--- the packet path. This is the Layer 2 port VLAN on
which the !--- outside port of the VPN service module
also belongs. interface FastEthernet3/48 no ip address
crypto connect vlan 100
!
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
!--- VLAN 100 is defined as the IVLAN. switchport trunk
allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
!--- The PVLAN configuration is handled transparently by
the !--- VPN service module without user configuration
!--- or involvement. It also is not shown in the
```

configuration. !--- Note: For every IVLAN, a corresponding PVLAN exists.

```
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco
!
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.161
!
global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (100). !--- Two separate access lists should
always be used in this configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Cisco IOS 라우터

```
SV3-2# show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
```

```

!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!--- Define the Phase 1 policy. crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco address 10.66.79.180
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. This indicates that IKE !--- is
used to establish the IPsec !--- SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
  set peer 10.66.79.180
  set transform-set cisco
  match address 100
!
!
!--- Apply the crypto map to the interface. interface
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
  ip address 192.168.6.1 255.255.255.0
  half-duplex
  no keepalive
!
!
ip http server
no ip http secure-server
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
!--- This is the crypto ACL. access-list 100 permit ip
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 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 IPsec SA에서 사용하는 설정을 표시합니다.
- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.
- **show crypto vlan**—암호화 컨피그레이션과 연결된 VLAN을 표시합니다.
- **show crypto eli** - VPN 서비스 모듈 통계를 표시합니다.

IPsec 확인 및 문제 해결에 대한 자세한 내용은 [IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오](#).

[문제 해결](#)

이 섹션에서는 컨피그레이션 트러블슈팅을 위한 정보를 제공합니다.

[문제 해결 명령](#)

참고: debug 명령을 실행하기 전에 [디버그 명령에 대한 중요 정보를 참조하십시오](#).

- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **clear crypto isakmp** - 1단계와 관련된 SA를 지웁니다.
- **clear crypto sa** - 2단계와 관련된 SA를 지웁니다.

IPsec 확인 및 문제 해결에 대한 자세한 내용은 [IP 보안 문제 해결 - 디버그 명령 이해 및 사용을 참조하십시오](#).

[관련 정보](#)

- [IPSec 지원 페이지](#)
- [IPSec 네트워크 보안 구성](#)
- [인터넷 키 교환 보안 프로토콜 구성](#)
- [Technical Support - Cisco Systems](#)