

Palo Alto Firewall로 보안 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[보안 액세스에서 VPN 구성](#)

[터널 데이터](#)

[Palo Alto에서 터널 구성](#)

[터널 인터페이스 구성](#)

[IKE 암호화 프로파일 구성](#)

[IKE 게이트웨이 구성](#)

[IPSEC 암호화 프로파일 구성](#)

[IPSec 터널 구성](#)

[정책 기반 전달 구성](#)

소개

이 문서에서는 Palo Alto Firewall로 Secure Access를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- [사용자 프로비저닝 구성](#)
- [ZTNA SSO 인증 컨피그레이션](#)
- [원격 액세스 VPN 보안 액세스 구성](#)

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Palo Alto 11.x 버전 방화벽
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- 클라이언트리스 ZTNA

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Palo Alto 11.x 버전 방화벽

- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

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

배경 정보



보안 액세스 - Palo Alto

Cisco는 온프레미스 및 클라우드 기반 프라이빗 애플리케이션을 보호하고 액세스를 제공하도록

Secure Access를 설계했습니다. 또한 네트워크에서 인터넷으로의 연결도 보호합니다. 이는 여러 보안 방법 및 레이어의 구현을 통해 달성되며, 모두 클라우드를 통해 정보에 액세스할 때 정보를 보존하는 데 목적이 있습니다.

구성

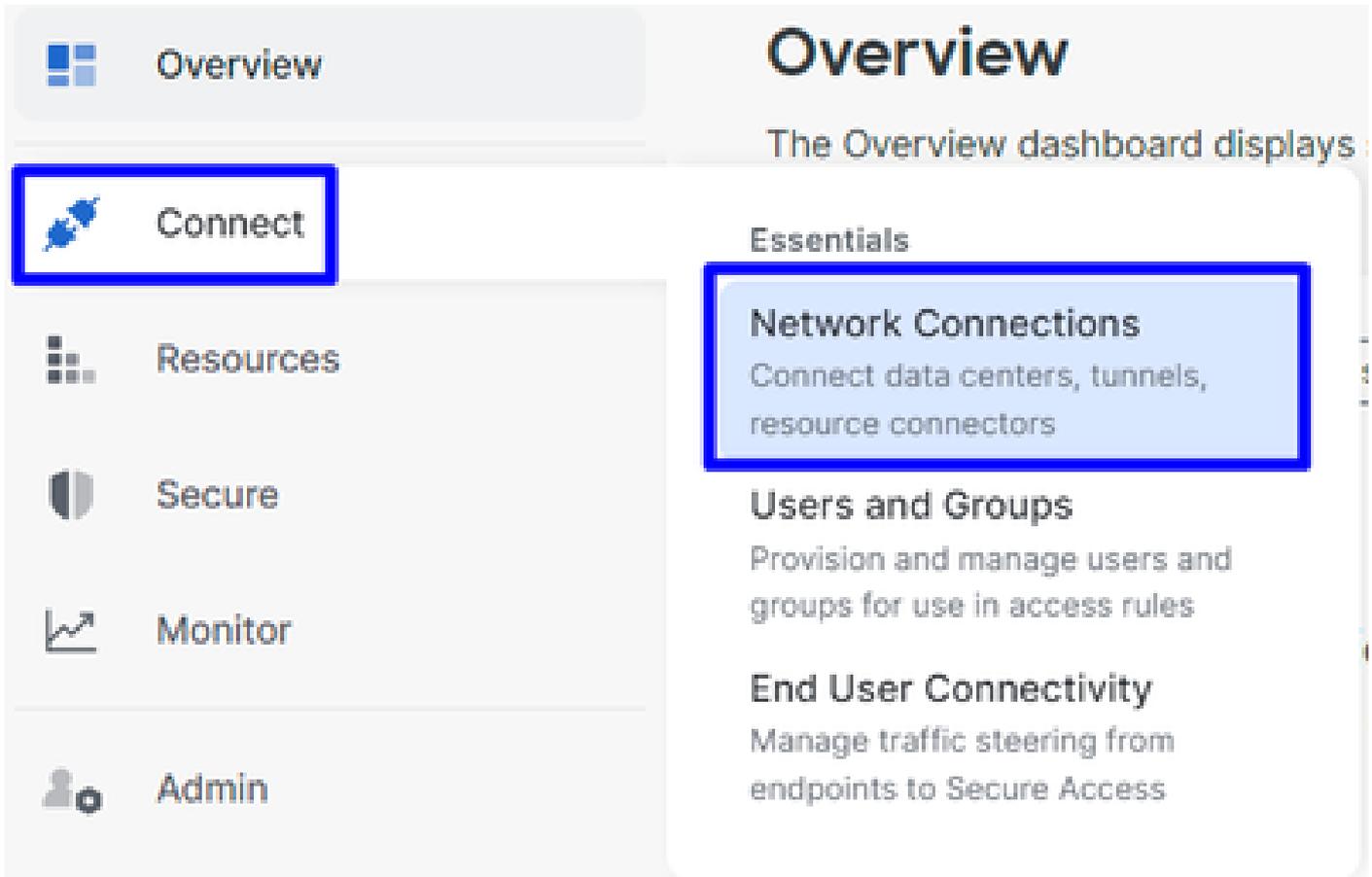
보안 액세스에서 VPN 구성

[Secure Access](#)의 관리자 패널로 [이동합니다](#).



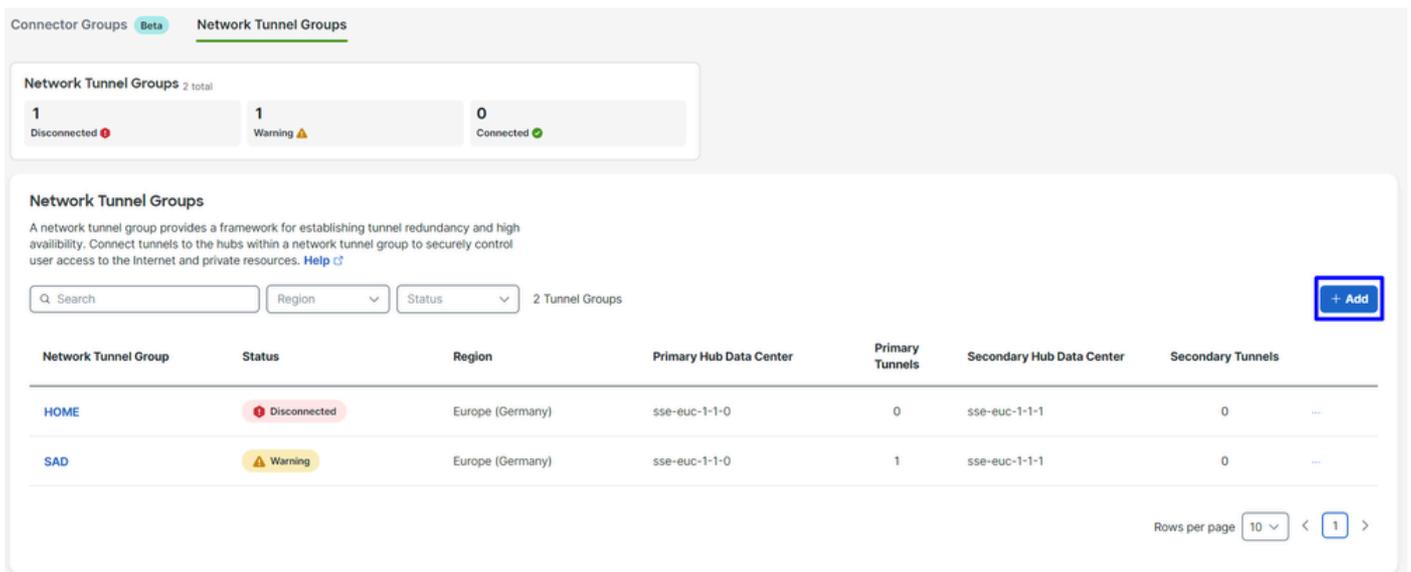
보안 액세스 - 기본 페이지

- **클릭** Connect > Network Connections



보안 액세스 - 네트워크 연결

- 에서 Network Tunnel Groups 클릭 + Add



보안 액세스 - 네트워크 터널 그룹

- 구성 Tunnel Group Name, Region 및 Device Type
- 클릭 Next

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

 ⊗

Region

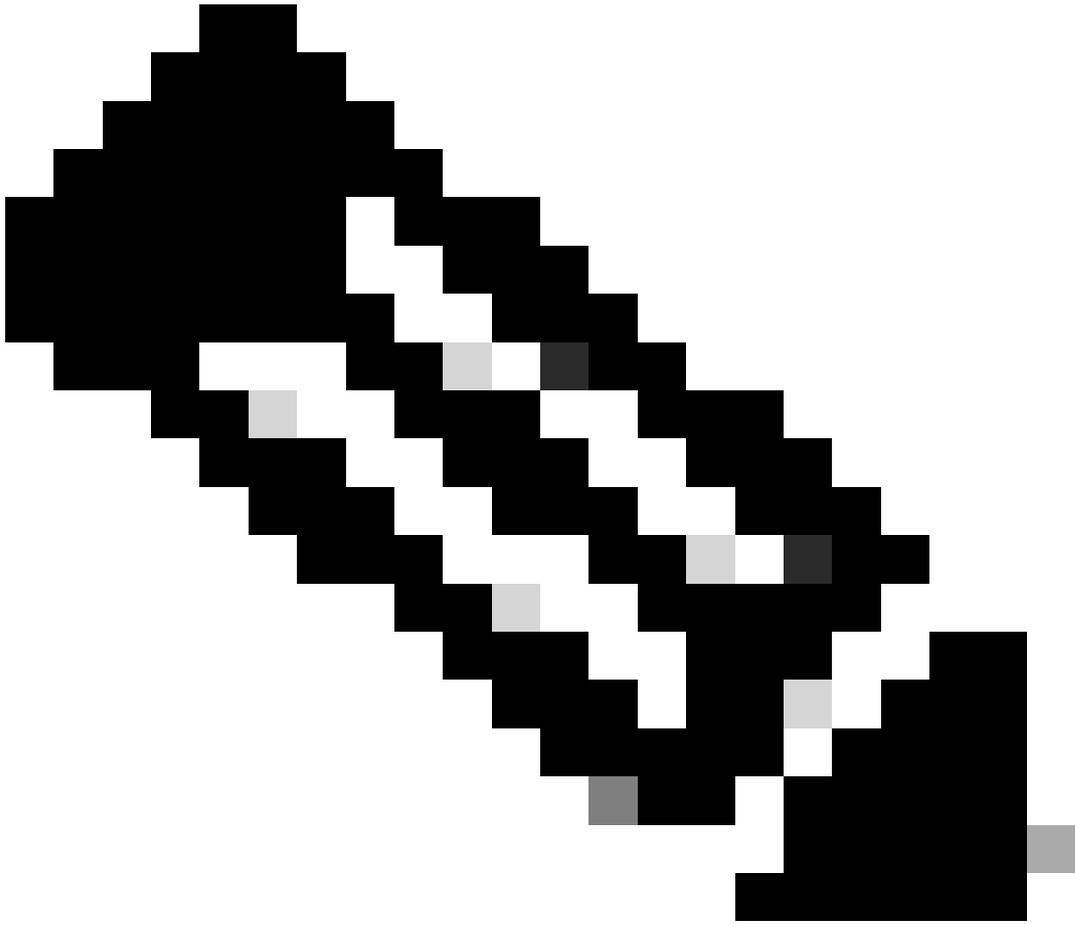
 ∨

Device Type

 ∨

[Cancel](#)

[Next](#)



참고: 방화벽 위치에서 가장 가까운 지역을 선택합니다.

-
- 및 를 Tunnel ID Format 구성합니다 Passphrase
 - 클릭 Next

Tunnel ID Format

Email IP Address

Tunnel ID

@<org>
<hub>.sse.cisco.com

Passphrase

[Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

[Show](#)

[Cancel](#)

[Back](#) [Next](#)

- 네트워크에서 구성했으며 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호스트를 구성합니다
- 클릭 **Save**

Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

[Add](#)

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

[Cancel](#)

[Back](#) [Save](#)

보안 액세스 - 터널 그룹 - 라우팅 옵션

터널에 대한 정보 **Save** 가 표시되면 다음 단계를 위해 해당 정보를 저장하십시오 **Configure the tunnel on Palo Alto.**

터널 데이터

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	PaloAlto@	-sse.cisco.com	
Primary Data Center IP Address:	18.156.145.74		
Secondary Tunnel ID:	PaloAlto@	-sse.cisco.com	
Secondary Data Center IP Address:	3.120.45.23		
Passphrase:		CP	

Palo Alto에서 터널 구성

터널 인터페이스 구성

Palo Alto Dashboard(Palo Alto 대시보드)로 이동합니다.

- Network > Interfaces > Tunnel
- Click Add

Ethernet | VLAN | Loopback | **Tunnel** | SD-V

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS
tunnel		none
tunnel.1		Interface_CSA
tunnel.2		169.253.0.1

+ Add - Delete PDF/CSV

- 메뉴Config 아래에서 Virtual Router, Security Zone를 구성하고Suffix Number

Tunnel Interface

Interface Name: tunnel . 1

Comment:

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: Router

Security Zone: CSA

OK Cancel

- 에서IPv4 라우팅 불가 IP를 구성합니다. 예를 들어, 169.254.0.1/30
- 클릭OK

Tunnel Interface ?

Interface Name .

Comment

Netflow Profile

Config | **IPv4** | IPv6 | Advanced

<input type="checkbox"/>	IP
<input type="checkbox"/>	169.254.0.1/30

IP address/netmask. Ex. 192.168.2.254/24

그런 다음 다음과 같은 구성을 수행할 수 있습니다.

Ethernet | VLAN | Loopback | **Tunnel** | SD-WAN

INTERFACE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	SECURITY ZONE	FEATURES
tunnel		none	none	CSA	
tunnel.1		169.254.0.1/30	Router	CSA	
tunnel.2		169.253.0.1	Router	CSA	

이렇게 구성한 경우 **Commit** 를 클릭하여 컨피그레이션을 저장하고 다음 단계인 **Configure IKE Crypto Profile** 를 계속 진행할 수 있습니다.

IKE 암호화 프로파일 구성

암호화 프로필을 구성하려면 다음 사이트로 이동합니다.

- Network > Network Profile > IKE Crypto
- **클릭Add**

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

Clientless App Groups QoS LLDP Network Profiles GlobalProtect IPSec Crypt IKE Gateways IPSec Crypto IKE Crypto Monitor Interface Mgmt Zone Protection QoS Profile LLDP Profile BFD Profile SD-WAN Interface Profile

4 items

<input type="checkbox"/>	NAME	ENCRYPTION	AUTHENTICATI...	DH GROUP	KEY LIFETI
<input type="checkbox"/>	default	aes-128-cbc, 3des	sha1	group2	8 hours
<input type="checkbox"/>	Suite-B-GCM-128	aes-128-cbc	sha256	group19	8 hours
<input type="checkbox"/>	Suite-B-GCM-256	aes-256-cbc	sha384	group20	8 hours
<input type="checkbox"/>	CSAIKE	aes-256-gcm	non-auth	group19	8 hours

+ Add - Delete Clone PDF/CSV

- 다음 매개변수를 구성합니다.
 - **Name:** 프로필을 식별하기 위한 이름을 구성합니다.
 - **DH GROUP:** 그룹19
 - **AUTHENTICATION:** 비 인증
 - **ENCRYPTION:** aes-256-gcm
 - Timers
 - Key Lifetime:8시간
 - **IKEv2 Authentication:**0
- 모든 항목을 구성한 후 **OK**

IKE Crypto Profile ?

Name

<input type="checkbox"/> DH GROUP	<input type="checkbox"/> ENCRYPTION
<input type="checkbox"/> group19	<input type="checkbox"/> aes-256-gcm

+ Add - Delete ↑ Move Up ↓ Move Down

<input type="checkbox"/> AUTHENTICATION	Timers Key Lifetime <input type="text" value="Hours"/> <input type="text" value="8"/> <small>Minimum lifetime = 3 mins</small> IKEv2 Authentication Multiple <input type="text" value="0"/>
<input type="checkbox"/> non-auth	

+ Add - Delete ↑ Move Up ↓ Move Down

이와 같이 구성한 경우 을 클릭하여 컨피그레이션 **Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IKE Gateways.

IKE 게이트웨이 구성

IKE 게이트웨이를 구성하려면

- Network > Network Profile > IKE Gateways
- **클릭Add**

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

2 items

	NAME	PEER ADDRESS	Local Address		ID
			INTERFACE	IP	
<input checked="" type="checkbox"/>	CSA_IKE_GW	18.156.145.74	ethernet1/1	192.168.0.204/24	18.156.145.74
<input type="checkbox"/>	CSA_IKE_GW2	3.120.45.23	ethernet1/1	192.168.0.204/24	3.120.45.23

Add Delete Enable Disable PDF/CSV

- 다음 매개변수를 구성합니다.
 - Name: Ike 게이트웨이를 식별하기 위한 이름을 구성합니다.
 - **Version** : IKEv2 전용 모드
 - Address Type : IPv4
 - **Interface** : 인터넷 WAN 인터페이스를 선택합니다.
 - Local IP Address: 인터넷 WAN 인터페이스의 IP를 선택합니다.
 - **Peer IP Address Type** :IP
 - Peer Address: [터널 데이터](#) 단계에서 Primary IP Datacenter IP Address지정한 의 IP를 [사용합니다](#).
 - Authentication: 사전 공유 키
 - Pre-shared Key : [터널 데이터 passphrase](#) 단계에서 지정된 값을 [사용합니다](#).
 - **Confirm Pre-shared Key** : [터널 데이터 passphrase](#) 단계에서 지정된 값을 [사용합니다](#).
 - **Local Identification** : Tunnel Data(데이터 User FQDN (Email address) 터널) **Primary Tunnel ID** 단계에서 지정한 항목을 [선택하고 사용합니다](#).
 - **Peer Identification** : IP Address을 선택하고 Primary IP Datacenter IP Address사용합니다.

General | Advanced Options

Name	CSA_IKE_GW		
Version	IKEv2 only mode		
Address Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
Interface	ethernet1/1		
Local IP Address	192.168.0.204/24		
Peer IP Address Type	<input checked="" type="radio"/> IP <input type="radio"/> FQDN <input type="radio"/> Dynamic		
Peer Address	18.156.145.74		
Authentication	<input checked="" type="radio"/> Pre-Shared Key <input type="radio"/> Certificate		
Pre-shared Key	●●●●●●		
Confirm Pre-shared Key	●●●●●●		
Local Identification	User FQDN (email address)	paloalto@	-sse.cisco.c
Peer Identification	IP address	18.156.145.74	
Comment			

- 클릭Advanced Options

- **Enable NAT Traversal**

- Configure **IKE Crypto Profile** IKE Crypto Profile(IKE 암호화 프로파일 [구성](#) 단계에서 생성한 를 선택합니다
- 확인란을 선택합니다. **Liveness Check**
- 클릭 **OK**

General | **Advanced Options**

Common Options

 Enable Passive Mode Enable NAT Traversal

IKEv2

IKE Crypto Profile CSAIKE

 Strict Cookie Validation Liveness Check

Interval (sec) 5

OK

Cancel

이와 같이 구성한 경우 을 클릭하여 컨피그레이션 **Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IPSEC Crypto.

IPSEC 암호화 프로파일 구성

IKE 게이트웨이를 구성하려면 Network > Network Profile > IPSEC Crypto

- 클릭Add

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

Clientless App Groups 4 items

- QoS
- LLDP
- Network Profiles
- GlobalProtect IPSec Crypt
- IKE Gateways
- IPSec Crypto
- IKE Crypto
- Monitor
- Interface Mgmt
- Zone Protection
- QoS Profile
- LLDP Profile
- BFD Profile
- SD-WAN Interface Profile

<input type="checkbox"/>	NAME	ESP/AH	ENCRYPTI...	AUTHENTI...	DH GROUP	LIFETIME	LIFE
<input type="checkbox"/>	default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
<input type="checkbox"/>	Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
<input type="checkbox"/>	Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	1 hours	
<input type="checkbox"/>	CSA-IPsec	ESP	aes-256-gcm	sha256	no-pfs	1 hours	

+ Add - Delete Clone PDF/CSV

- 다음 매개변수를 구성합니다.
 - **Name:** 이름을 사용하여 보안 액세스 IPsec 프로필을 식별합니다.
 - IPSec Protocol: ESP
 - **ENCRYPTION:** aes-256-gcm
 - DH Group: no-pfs, 1시간
- 클릭 OK

IPSec Crypto Profile



Name

IPSec Protocol

ENCRYPTION

aes-256-gcm

AUTHENTICATION

sha256

DH Group

Lifetime

Minimum lifetime = 3 mins

Enable

Lifeseize

Recommended lifeseize is 100MB or greater

OK

Cancel

이와 같이 구성한 경우 을 클릭하여 컨피그레이션 **Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IPSec Tunnels.

IPSec 터널 구성

구성하려면 **IPSec Tunnels**로 이동합니다 **Network > IPSec Tunnels**.

- 클릭 Add

The screenshot shows the PA-VM Network configuration page. The left sidebar has 'IPSec Tunnels' selected. The main area displays a table of IKE Gateway/Satellite tunnels:

	NAME	STATUS	TYPE	IKE Gateway/Satellite			
				INTERFA...	LOCAL IP	PEER ADDRESS	STATUS
<input type="checkbox"/>	CSA	● Tunnel Info	Auto Key	ethernet...	192.168...	18.156.1...	● IKE Info
<input type="checkbox"/>	CSA2	● Tunnel Info	Auto Key	ethernet...	192.168...	3.120.45...	● IKE Info

At the bottom of the interface, there is a toolbar with buttons: '+ Add', 'Delete', 'Enable', 'Disable', and 'PDF/CSV'. The '+ Add' button is highlighted with a red box.

- 다음 매개변수를 구성합니다.
 - **Name:** 이름을 사용하여 보안 액세스 터널을 식별합니다.
 - **Tunnel Interface:** 단계에서 구성된 터널 인터페이스, [터널 인터페이스 구성을 선택합니다.](#)
 - **Type:** 자동 키
 - **Address Type:** IPv4
 - **IKE Gateways:** 단계에서 구성된 IKE 게이트웨이, IKE 게이트웨이 [구성을 선택합니다.](#)
 - **IPsec Crypto Profile:** 단계에서 구성된 IKE 게이트웨이, IPSEC 암호화 [프로파일 구성을 선택합니다.](#)
 - 확인란을 선택합니다. **Advanced Options**
 - **IPsec Mode Tunnel:** 터널을 선택합니다.

- 클릭 OK

IPsec Tunnel

General | Proxy IDs

Name: CSA

Tunnel Interface: tunnel.1

Type: Auto Key Manual Key GlobalProtect Satellite

Address Type: IPv4 IPv6

IKE Gateway: CSA_IKE_GW

IPsec Crypto Profile: CSA-IPsec

Show Advanced Options

Enable Replay Protection

Anti Replay Window: 1024

Copy ToS Header

IPsec Mode: Tunnel Transport

Add GRE Encapsulation

Tunnel Monitor

Destination IP:

Profile: None

Comment:

OK Cancel

이제 VPN이 성공적으로 생성되었으므로, 단계를 진행할 수 있습니다 **Configure Policy Based Forwarding**.

정책 기반 전달 구성

구성하려면 다음 **Policy Based Forwarding**으로 이동하십시오. Policies > Policy Based Forwarding.

- 클릭 Add

PA-VM DASHBOARD ACC MONITOR **POLICIES**

NAT
QoS
Policy Based Forwarding

Policy Optimizer

- Rule Usage
 - Unused in 30 days 0
 - Unused in 90 days 0
 - Unused 0

	NAME	TAGS	ZONE/INTERFA
1	CSA	none	LAN LAN2

Object : Addresses + **+** Add - Delete Clone Enable Disable

- 다음 매개변수를 구성합니다.

- General

- **Name:** 이름을 사용하여 보안 액세스, 정책 기반 전달(발신지별 라우팅)을 식별합니다.

- Source

- **Zone:** 출발지를 기준으로 트래픽을 라우팅할 계획이 있는 Zones를 선택합니다

- **Source Address:** 소스로 사용할 호스트를 구성합니다.
- **Source Users:** 트래픽을 라우팅할 사용자를 구성합니다(해당되는 경우에만).

- Destination/Application/Service

- Destination Address: Any로 남겨두거나 Secure Access(100.64.0.0/10)의 주소 범위를 지정할 수 있습니다.

- Forwarding

- Action: 앞으로

- Egress Interface: 단계에서 구성된 터널 인터페이스, [터널 인터페이스 구성을 선택합니다.](#)

- Next Hop:None

- 클릭OK 및 Commit

Policy Based Forwarding Rule ?

General | Source | Destination/Application/Service | Forwarding

Name

Description

Tags

Group Rules By Tag

Audit Comment

[Audit Comment Archive](#)

Policy Based Forwarding Rule



General | **Source** | Destination/Application/Service | Forwarding

Type	Zone	<input type="checkbox"/> Any	any
<input type="checkbox"/> ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	
<input type="checkbox"/> LAN	<input type="checkbox"/> 192.168.30.2		
<input type="checkbox"/> LAN2	<input type="checkbox"/> 192.168.40.3		
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	

Negate

Policy Based Forwarding Rule



General | Source | **Destination/Application/Service** | Forwarding

<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any
<input type="checkbox"/> DESTINATION ADDRESS v	<input type="checkbox"/> APPLICATIONS ^	<input type="checkbox"/> SERVICE ^
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

Negate

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.