Palo Alto Firewall로 보안 액세스 구성

목차

소개

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

사전 요구 사항

- <u>사용자 프로비저닝 구성</u>
- <u>ZTNA SSO 인증 컨피그레이션</u>
- <u>원격 액세스 VPN 보안 액세스 구성</u>

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 디바 이스는 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 보 존하는 데 목적이 있습니다.

구성

보안 액세스에서 VPN 구성

<u>Secure Access</u>의 관리자 패널로<u>이동합니다</u>.

cisco	Secure Access										A Jairo
	Overview	Overview The Overview dashboard displays status, u	sage, and healt!	h metrics for your o	ganization. Use this	information to add	fress security threat	s and monitor system	m usage. Help C?		
	Connect				-						
h.	Resources	Data Transfer Last 7 Days	~								
0	Secure	TOTAL USAGE Usage data - delayed up to 30 min.									
Ľ	Monitor	69.52 MB Total traffic	45.0 MB								🕑 Branch
2o	Admin	725.98 MB 🐄 Decrease (last 7 days)	40.0 MB								Cisco Secure Client
A	Workflows	16.45 MB Received 35.39 MB Son Decrease (last 7 days)	30.0 MB 25.0 MB 20.0 MB								 RAVPN Browser-based ZTNA
		53.07 MB Sent 690.58 MB [∨] x Decrease (last 7 days)	15.0 MB 10.0 MB 5.0 MB 0.0 MB	Thur 15	Fri 16	Sat 17	Sun 18	Mon 19	Tues 20	Wed 21	Select All

보안 액세스 - 기본 페이지

• 클릭 Connect > Network Connections

8	Overview	Overview
		The Overview dashboard displays
*	Connect	Essentials
١.	Resources	Network Connections Connect data centers, tunnels, resource connectors
U	Secure	Users and Groups Provision and manage users and
	Monitor	groups for use in access rules End User Connectivity
20	Admin	Manage traffic steering from endpoints to Secure Access
보안 액세스	- 네트워크 연결	

• 에서 Network Tunnel Groups 클릭 + Add

twork Tunnel Groups 2 tor	tal							
sconnected ()	1 Warning 🛦	O Connected 🥏						
twork Tunnel Groups								
etwork tunnel group provides alibility. Connect tunnels to tr	s a framework for establishing tunne he hubs within a network tunnel grou	l redundancy and high up to securely control						
availability. Connect tumnes to the nuos writin a network tunnel group to securely control user access to the Internet and private resources. Help C								
λ Search	Region V	Status V 2 Tunnel Group	5				+	
C. Search Network Tunnel Group	Region v	Status V 2 Tunnel Group	5 Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels	-	
2 Search Network Tunnel Group	Region V Status	Status 2 Tunnel Group Region Europe (Germany)	5 Primary Hub Data Center sse-euc-1-1-0	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels		
Search letwork Tunnel Group IOME	Region V Status O Disconnected	Status 2 Tunnel Group Region Europe (Germany) Europe (Germany)	Primary Hub Data Center sse-euc-1-1-0 sse-euc-1-1-0	Primary Tunnels 0 1	Secondary Hub Data Center sse-euc-1-1-1 sse-euc-1-1-1	Secondary Tunnels 0 0		

- 구성Tunnel 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

Palo Alto

Region

Europe (Germany)

Device Type

Other	~
-------	---

 \otimes

V

Cancel

Next



참고: 방화벽 위치에서 가장 가까운 지역을 선택합니다.

- 및 를Tunnel ID Format 구성합니다 Passphrase
- 클릭 Next

Tunnel ID Format

🔘 Email 🛛 🗍 IP Address

Tunnel ID

PaloAlto

0	1	
(X)	1	
\smile		

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

Passphrase

Show	\otimes
------	-----------

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 \otimes
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.

	128.66.0.0/16, 192.0.2.0/24	Add
	6	
	192.168.0.0/24 × 192.168.10.0/24 ×	
0	Dynamic routing Use this option when you have a BGP peer for your on-premise router.	
Can	cel	Back

보안 액세스 - 터널 그룹 - 라우팅 옵션

터널에 대한 정보Save 가 표시되면 다음 단계를 위해 해당 정보를 저장하십시오Configure 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	٦
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	D	
Palo Alto에서 터널 구성				
터널 인터페이스 구성				
Palo Alto Dashboard(Palo Alto 대시보드)로 이동합니다				
• Network > Interfaces > Tunnel				

Click Add

📼 Interfaces	• Î	Ethernet VL	AN Loopback	Tunnel SD-\
🚧 Zones	• -			
📮 VLANs	1	0		
🧧 Virtual Wires		40		
🛞 Virtual Routers			MANAGEMENT	
🤨 IPSec Tunnels	•			IT ADDRESS
🐠 GRE Tunnels	1	tunnel		none
g DHCP	U	tunnel.1		Interface_CSA
🕎 DNS Proxy	4	tunnel.2		169.253.0.1
🚍 Proxy				
🗸 👰 GlobalProtect				
🍓 Portals				
径 Gateways				
🔄 МДМ				
4 Clientless Apps	-		ete 💿 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	tunnel . 1	
Comment		
Netflow Profile	None	~
Config IPv4 I	IPv6 Advanced	
IP IP		
169.254.0.1/30		
🕂 Add 🔵 Delete	↑ Move Up 🤳 Move Down	
IP address/netmask. Ex. 192.	.168.2.254/24	
	Он	Cancel

그런 다음 다음과 같은 구성을 수행할 수 있습니다.

Ethernet VLAN Loopback Tunnel SD-WAN

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

이렇게 구성한 경우 를 클릭하여 컨피그레이션Commit 을 저장하고 다음 단계인 를 계속 진행할 수 있습니다Configure IKE Crypto Profile.

IKE 암호화 프로파일 구성

암호화 프로필을 구성하려면 다음 사이트로 이동합니다.

- Network > Network Profile > IKE Crypto
- 클릭Add

PA-VM	DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK
						5
🍖 Clientless App Groups	^Q(4 items
🚴 QoS	NAME	E	NCRYPTION	AUTHENTICATI	DH GROUP	KEY LIFETI
	default	а	es-128-cbc, 3des	sha1	group2	8 hours
GlobalProtect IPSec Cryp	Suite-B-G	СМ-128 а	es-128-cbc	sha256	group19	8 hours
→ IKE Gateways	Suite-B-G	СМ-256 а	es-256-cbc	sha384	group20	8 hours
🔒 IPSec Crypto 🏾 🔹	CSAIKE	a	es-256-gcm	non-auth	group19	8 hours
🔁 IKE Crypto 🔹						
🔥 Monitor 🛛 🔹	1					
🚳 Interface Mgmt 🛛 🔹						
🦻 Zone Protection						
💑 QoS Profile 🛛 🔹						
State Contract State Sta						
Here BFD Profile						
SD-WAN Interface Profile	• 🕂 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	0
Name CSAIKE	
DH GROUP	ENCRYPTION
group19	aes-256-gcm
Add	↔ Add
AUTHENTICATION	- Timers
non-auth	Key Lifetime Hours
	8
	Minimum lifetime = 3 mins
↔ Add	IKEv2 Authentication 0 Multiple
	OK Cancel

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

P	PA-VM	DAS	HBOARD /	ACC	MONITOR	POLICIES	OBJECTS	NETWORK
								G
뽯	DNS Proxy	1Q(2 items).
Ę	Proxy					Le col A	dduces	
P	GlobalProtect					Local A	laaress	
	🍓 Portals		NAME	PI	EER ADDRESS	INTERFACE	IP	ID
	径 Gateways		CSA_IKE_GW	18	8.156.145.74	ethernet1/1	192.168.0.204/24	18.156.145.74
	🔄 мдм							
	👆 Clientless Apps		CSA IKE GW2	3.	.120.45.23	ethernet1/1	192.168.0.204/24	3.120.45.23
	퉣 Clientless App Groups							
å	QoS	4						
	LLDP	Ľ.,						
G.	Network Profiles							
	🖯 GlobalProtect IPSec Cryp	- -						
	Herein IKE Gateways							
	🔁 IPSec Crypto 🔹 🔹	-						
	🔒 IKE Crypto 🔹	- (+)	Add 😑 Delete	\checkmark	Enable 🚫 Dis	sable 💿 PDF/CS	V	

• 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: <u>터널 데이터</u> 단계에서 Primary IP Datacenter IP Address지정한 의 IP를<u>사용합니다</u>.
- Authentication: 사전 공유 키
- Pre-shared Key : <u>터널 데이터</u> passphrase 단계에서 지정된 <u>값</u>을 <u>사용합니다</u>.
- Confirm Pre-shared Key : <u>터널 데이터</u> passphrase 단계에서 지정된<u>값을 사용합니다</u>.

• Local Identification : Tunnel Data(데이터 User FQDN (Email address) 터널) Primary Tunnel ID 단계에서 지정한 항목을 <u>선택하고 사용합니다</u>.

• Peer Identification : IP Address을 선택하고 Primary IP Datacenter IP Address사용합니다.

IKE Gateway

General Advance	d Options			
Name	CSA_IKE_GW			
Version	IKEv2 only mode			~
Address Type	 IPv4 O IPv6 			
Interface	ethernet1/1			~
Local IP Address	192.168.0.204/24			\sim
Peer IP Address Type	● IP ○ FQDN ○ Dynamic			
Peer Address	18.156.145.74			~
Authentication	 Pre-Shared Key O Certificate 			
Pre-shared Key	•••••			
Confirm Pre-shared Key	•••••			
Local Identification	User FQDN (email address)	\sim	paloalto@ -ss	e.cisco.c
Peer Identification	IP address	\sim	18.156.145.74	
Comment				



- 클릭Advanced Options
 - Enable NAT Traversal
 - Configure IKE Crypto Profile IKE Crypto Profile(IKE 암호화 프로파일 <u>구성) 단계에서 생성한 를 선택합니다</u>
 - 확인란을 선택합니다. Liveness Check
 - 클릭 OK

?

IKE Gateway	?
General Advanced Options	
Common Options	
Enable Passive Mode Fnable NAT Traversal	
IKEv2	
IKE Crypto Profile CSAIKE	~
Strict Cookie Validation	
iveness Check	
Interval (sec) 5	

ОК	Cancel	

이와 같이 구성한 경우 을 클릭하여 컨피그레이션Commit 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	DAS	HBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETW	ORK
								K (
Clientless App Groups	Q(4 items
os 😞		NAME	ESP/AH	ENCRYPTI	AUTHENTI	DH GROUP	LIFETIME	LIFE
ELLDP		default	ESP	aes-128-cbc, 3des	sha1	group2	1 hours	
🔂 GlobalProtect IPSec Cryp 🏋 IKE Gateways 🛛 🔹		Suite-B- GCM-128	ESP	aes-128-gcm	none	group19	1 hours	
IPSec Crypto		Suite-B- GCM-256	ESP	aes-256-gcm	none	group20	1 hours	
Monitor		CSA-IPsec	ESP	aes-256-gcm	sha256	no-pfs	1 hours	
Interface Mgmt • Interface Mgmt • Image: Some Protection • Image: QoS Profile • Image: LLDP Profile • Image: BFD Profile •								
🚱 SD-WAN Interface Profile	÷ (+)	Add 🕞 De	lete 🛛 💿 Cl	one 🙆 PDF/CS	V			

- 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 CSA-IPsec		
IPSec Protocol ESP	DH Group no-pfs	\sim
ENCRYPTION	Lifetime Hours V 1	
aes-256-gcm	Minimum lifetime = 3 mins Enable Lifesize MB [1 - 65535] Recommended lifesize is 100MB or greater	
↔ Add		
AUTHENTICATION		
sha256		
⊖ Add		
	ОК Са	ncel

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

IPSec 터널 구성

구성하려면 IPSec Tunnels로 이동합니다Network > IPSec Tunnels.

• 클릭 Add

🚺 PA-VM	DASHBO/	ARD A	сс мо	NITOR	POLICIES	OBJE	стѕ	NETWORK	
🚥 Interfaces 🔹 🍵	Q(
🎮 Zones 🔹					IKE Gatew	ay/Satellite			
🚰 VLANs						PEER			1
e Virtual Wires	NAME	STATUS	TYPE	INTERFA	LOCAL IP	ADDRESS	STATUS	INTERFA	F
🛞 Virtual Routers 🔹	CSA	•	Auto Key	ethernet	192.168	18.156.1	IKE	tunnel.1	1
IPSec Tunnels		Tunnel					Info		(
- GRE Tunnels		inio	A		400.470	0.400.45		1	١.
支 DHCP	CSA2	Tunnel	Auto Key	ethernet	192.168	3.120.45	IKE Info	tunnel.2	(
😴 DNS Proxy		Info							1
Proxy									
GlobalProtect									
Gateways									
Clientless Apps									
Clientless App Groups									
A QoS									
V 🕞 Network Profiles									
GlobalProtect IPSec Cry	+ Add	Delete 🧭	Enable 🚫	Disable	PDF/CSV				

- 다음 매개변수를 구성합니다.
 - Name: 이름을 사용하여 보안 액세스 터널을 식별합니다.
 - Tunnel Interface: 단계에서 구성된 터널 인터페이스, <u>터널 인터페이스 구성을 선택합니다</u>.
 - Type: 자동 키
 - Address Type: IPv4
 - IKE Gateways: 단계에서 구성된 IKE 게이트웨이, IKE 게이트웨이 <u>구성을 선택합니다</u>.
 - IPsec Crypto Profile: 단계에서 구성된 IKE 게이트웨이, IPSEC 암호화 <u>프로파일 구성을 선택합니다</u>
 - 확인란을 선택합니다. Advanced Options
 - ◎ IPSec Mode Tunnel: 터널을 선택합니다.

클릭 OK

•

IPSec Tunnel		?
General Prox	cy IDs	
Name	CSA	
Tunnel Interface	tunnel.1	~
Туре	O Auto Key ○ Manual Key ○ GlobalProtect Satellite	
Address Type	S 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	O Tunnel ○ Transport	
	Add GRE Encapsulation	
Tunnel Monitor		
Destination IP		
Profile	None	\sim
Comment		
	ок	Cancel

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

정책 기반 전달 구성

구성하려면 다음 Policy Based Forwarding으로 이동하십시오. Policies > Policy Based Forwarding.

• 클릭 Add

🔮 PA-VM		DASI	HBOARD	ACC	MONITOR	POLICIES
→ NAT	•	Q(
🚓 QoS						
Policy Based Forwarding						
Policy Optimizer	-		NAME		TAGS	ZONE/INTERFA
✓ ⋚		1	CSA		none	M LAN
ਨ Unused in 30 days	0					AN2
ស Unused in 90 days	0	1				
ស Unused	0	4				
Object : Addresses	+	(+) <i>F</i>	dd 😑 Dele	te 🔞 C	lone 🕜 Enabl	e 🚫 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, <u>터널 인터페이스 구성을 선택합니다</u>.
 - Next Hop:None

• 클릭OK 및 Commit

Policy Based Forwarding Rule		
General Sour	rce Destination/Application/Service Forwarding	
Name	CSA	
Description		
Tags		~
Group Rules By Tag	None	\sim
Audit Comment		
	Audit Comment Archive	
	ОК Са	ancel

Policy Based Forwarding Rule					
General Source Destination/Application/Service Forwarding					
Type Zone	Any SOURCE ADDRESS ^ G 192.168.30.2 G 192.168.40.3	any SOURCE USER			
Policy Based Forwarding Rule	□ Negate	OK Cancel			
General Source Destination/Application/Service Forwarding					
Any Destination Address >	Any APPLICATIONS	SERVICE ^			
Add Oelete	↔ Add ⊖ Delete	Add Delete			
		OK Cancel			

Policy Based Fo	orwarding Rule	?
General Sour	ce Destination/Application/Service Forwarding	
Action	Forward	\sim
Egress Interface	tunnel.1	\sim
Next Hop	None	\sim
Monitor —		
Profile		\sim
IP Address	Disable this rule if nexthop/monitor ip is unreachable	
II Address		
Enforce Symme	tric Return	
NEXT HOP ADDRE	ESS LIST	
O O		
🕂 Add 🕞 Del		
Schedule	None	~
÷		
	ок	Cancel

이제 모든 것이 Palo Alto에 구성되어 있습니다. 경로를 구성한 후 터널을 설정할 수 있으며, Secure Access Dashboard에서 RA-VPN, 브 라우저 기반 ZTA 또는 클라이언트 기반 ZTA를 계속 구성해야 합니다. 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 번 역 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.