FMC에서 관리하는 FTD에 듀얼 ISP VTI 구성

목차

소개 <u>사전 요구 사항</u> <u>기본 요구 사항</u> <u>사용되는 구성 요소</u> <u>FMC의 컨피그레이션</u> <u>토플로지 컨피그레이션</u> <u>엔드포인트 컨피그레이션</u> <u>IKE 컨피그레이션</u> <u>IPsec 컨피그레이션</u> <u>라우팅 컨피그레이션</u>

소개

이 문서에서는 FMC에서 관리하는 FTD 디바이스에서 가상 터널 인터페이스를 사용하여 듀얼 ISP 설정을 구축하는 방법에 대해 설명합니다.

사전 요구 사항

기본 요구 사항

- Site-to-Site VPN을 기본적으로 이해하는 것이 좋습니다. 이 배경은 관련된 주요 개념 및 구성 을 포함하여 VTI 설정 프로세스를 파악하는 데 도움이 됩니다.
- Cisco Firepower 플랫폼에서 VTI를 구성 및 관리하는 기본 사항을 이해하는 것은 필수적입니다.
 다. 여기에는 VTI가 FTD 내에서 작동하는 방식과 FMC 인터페이스를 통해 제어되는 방식에 대한 지식이 포함됩니다.

사용되는 구성 요소

- Cisco FTD(Firepower Threat Defense) for VMware: 버전 7.0.0
- FMC(firepower Management Center): 버전 7.2.4(빌드 169)

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.

FMC의 컨피그레이션

토폴로지 컨피그레이션

1. Devices(디바이스) >VPN > Site To Site(사이트 대 사이트)로 이동합니다.

	Devices	Objects	Int	tegration			
	Device Ma	anagement	1	VPN		Troubleshoot	_
	Device Upgrade NAT QoS Platform Settings			Site To Site Remote Access Dynamic Access Policy Troubleshooting		File Download	
_						Threat Defense CLI	
						Packet Tracer	Distr
						Packet Capture	_
	FlexConfig	g		Site to Site Monitoring			
	Certificate	es					

2. VPN 토폴로지를 추가하려면 Add를 클릭합니다.

Deploy	Q	₩	?	aamin 🔻	cisc	SECU	RE
Last L	lpdate	ed: 10:02 F	M	Refresh		Add	
							×

3. 토폴로지의 이름을 지정하고 VTI 및 Point-to-Point를 선택한 다음 IKE 버전(이 경우 IKEv2)을 선 택합니다.

	Create New VPN Topology	0
	Topology Name:* Dual-ISP-VTI	
1	 Policy Based (Crypto Map) Route Based (VTI) Network Topology: 	
ł	Point to Point Hub and Spoke Full Mesh	
	IKE Version:* 🗌 IKEv1 🗹 IKEv2	

엔드포인트 컨피그레이션

1. 터널을 구성해야 하는 디바이스를 선택합니다.

원격 피어 세부 정보를 추가합니다.

"+" 아이콘을 클릭하여 새 가상 템플릿 인터페이스를 추가하거나 기존 목록에서 하나를 선택할 수 있습니다.

Node A	Node B
Device:*	Device:*
New_FTD •	Extranet
Virtual Tunnel Interface:*	Device Name*:
• +	VTI-Peer
Tunnel Source IP is Private Edit VTI	Endpoint IP Address*:
Send Local Identity to Peers	10.10.10.2
+ Add Backup VTI (optional)	
Connection Type:*	

	Cancel Sa	ave
새 VTI 인터페이스를 생성하는 경우 올바른 매개변수를 추가하고 활성화한	한 다음 "OK(확인)"를	클릭
합니다.		

참고: 이는 기본 VTI가 됩니다.

Add Virtual Tunnel Interface

General	
General	
Name:*	- 1
VTI-1	
Enabled	
Description:	
This is the primary VTI tunnel. This VTI goes through ISP 1.	
Security Zone:	
OUT 🔻]
Priority:	
0	(0 - 65535)
Virtual Tunnel Interface Details An interface named Tunnel <id> is configured</id>	1. Tunnel Source is a physical interface where VPN tunnel terminates for the

Tunnel ID:*

1	(0 - 10413)	
Tunnel Source:*		
GigabitEthernet0/0 (outside1) 🔻	10.106.52.104	•

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPeee	Tunnel Mede:*	
IP	Pv4 O IPv6	
192	2.168.10.1/30	0

3. "+ "를 클릭합니다. Add Backup VIT(백업 VIT 추가)"를 클릭하여 보조 VIT를 추가합니다.

0

Device:*

 10.106.50.55
 ▼

 Virtual Tunnel Interface:*

 VTI-1 (IP: 192.168.10.1)
 ▼

 *Tunnel Source: outside1 (IP: 10.106.52.104)*Edit VTI

 Tunnel Source IP is Private

 Send Local Identity to Peers

 + Add Backup VTI (optional,

 Connection Type:*

 Bidirectional
 ▼

 Additional Configuration ⁽ⁱ⁾

 Route traffic to the VTI
 : <u>Routing Policy</u>

4. 보조 VTI에 대한 매개변수를 추가하려면 "+"를 클릭합니다(아직 구성되지 않은 경우).

· AC Policy

Permit VPN traffic

Endpoints	IKE	IPsec	Advanced					
10.1								
Virtua	Virtual Tunnel Interface:*							
VTI-	-1 (IP:	192.168	.10.1)	•	+			
Tunnel Source: outside1 (IP: 10.106.52.104)Edit VTI Tunnel Source IP is Private								
S	end Lo	cal Ident	ity to Peers					
Backu	ıp VTI:				Remove			
Virtua	l Tunne	el Interfa	ce:*					
				_	+			
Τι	unnel S	Source IP	is Private		Edit VTI			
S	end Lo	cal Ident	ity to Peers					

Connection Type:*

5. 새 VTI 인터페이스를 생성하는 경우 올바른 매개변수를 추가하고 활성화한 다음 "확인"을 클릭합 니다.

참고: 보조 VTI가 됩니다.

Add Virtual Tunnel Interface

General	
Name.	
VTI-2	
Enabled	
Description:	
This is the secondary VTI tunnel VTI goes through ISP 2.	
Security Zone:	
OUT 🔻	
Priority:	
0	(0 - 65535)
Virtual Tunnel Interface Details An interface named Tunnel <id> is configured. VTI. Tunnel ID:*</id>	Tunnel Source is a physical interface where VPN tunnel terminates for the
2	(0 - 10413)
Iunnel Source:*	
GigabitEthernet0/1 (outside2) ▼	10.106.53.10 ▼
IPsec Tunnel Details IPsec Tunnel mode is decided by VPN traffic I	P type. Configure IPv4 and IPv6 addresses accordingly.
IDeee Tunnel Mede:*	
● IPv4 ○ IPv6	
192.168.20.1/30	0
	Cancel OK

IKE 컨피그레이션

1. IKE 탭으로 이동합니다. 미리 정의된 정책을 사용하도록 선택하거나 Policy(정책) 탭 옆에 있는 연필 버튼을 클릭하여 새 정책을 생성하거나 요구 사항에 따라 사용 가능한 다른 정책을 선택할 수 있습니다.

0

Endpoints IKE IPsec Advanced			
Authentication Type: Pre-shared	Automatic Key 🔻		
Pre-shared Key Length:* 24	Characters (Range 1-127)		
IKEv2 Settings			I
Policies:* AES-GCM-NU	LL-SHA-LATEST		l
Authentication Type: Pre-shared	Automatic Key 🔻		l
Pre-shared Key Length:* 24	Characters (Range 1-127)		l
		Cancel Save	
IKEv2 Policy		0	
Available IKEv2 Policy C	+		
Q Search		Selected IKEv2 Policy	
AES-GCM-NULL-SHA	Add	AES-GCM-NULL-SHA-LATEST	
AES-GCM-NULL-SHA-LAT			
AES-SHA-SHA			
AES-SHA-SHA-LATEST	•		
Arko_Test_IKEv2			
DES-SHA-SHA	•		

2. 인증 유형을 선택합니다. 사전 공유 수동 키를 사용하는 경우 Key(키) 및 Confirm Key(키 확인) 상 자에 키를 입력합니다.

OK

Cancel

Endpoints IKE	IPsec Ad	vanced		
IKEv	2 Settings Policies:*	AES-GCM-NULL-SHA-LATEST	-	•
Authen	tication Type: Key:*	Pre-shared Manual Key 🔹]	
	Confirm Key:*	Enforce hex-based pre-shared key	y only	
				Cancel Save

IPsec 컨피그레이션

IPsec 탭으로 이동합니다. 제안 탭 옆의 연필 버튼을 클릭하여 새로운 제안을 생성하거나 필요에 따 라 사용 가능한 다른 제안을 선택하여 사전 정의된 제안을 사용하도록 선택할 수 있습니다.

Endpoints	IKE IPsec	Advanced	
	INCLVZ WOUE.	Tunner	
	Transform Sets:	IKEv1 IPsec Proposals 💉	IKEv2 IPsec Proposals* 🖍
		tunnel_aes256_sha	AES-GCM
		Enable Security Association	n (SA) Strength Enforcement
		Enable Reverse Route Injec	tion
		Enable Perfect Forward Sec	crecy

라우팅 컨피그레이션

1. Device(디바이스) > Device Management(디바이스 관리)로 이동하고 연필 아이콘을 클릭하여 디 바이스를 편집합니다(FTD).

Firewall Management Center Overview Analysis	Policies	Devices Objects Inte	egration		Deploy Q 🎸	Contraction of the second secure
View By: Group • All (4) • Error (2) • Warning (0) • Offline (2) • Normal (0)	Deployme	Device Management Device Upgrade	VPN Site To Site Remote Access	Troubleshoot File Download		Deployment History Q, Search Device Add •
Collapse All Name	Model	QoS Platform Settings FlexConfig	Dynamic Access Policy Troubleshooting Site to Site Monitoring	Packet Tracer Packet Capture	Access Control Policy	Auto RollBack
Vingrouped (4)	FTDv for VMwar	e 7.0.0	N/A	Base, AnyConnect Plus	s (1 more) new_pol	N/A

2. Routing(라우팅) > Static Route(고정 경로)로 이동하고 "+" 버튼을 클릭하여 기본 및 보조 VTI에 경로를 추가합니다.

참고: 트래픽이 터널 인터페이스를 통과하도록 적절한 라우팅 방법을 구성할 수 있습니다. 이 경우 고정 경로가 사용되었습니다.

Device Routing I	Interfaces	Inline S	ets DHO	CP				
Manage Virtual Routers	S							+ Add Foute
Global	¥	Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
Virtual Router Properties		► IPv4 R	outes					
OSPF		► IPv6 R	outes					
OSPFv3								
EIGRP								
RIP								
BGP								
Static Route								
^r Multicast Routing								

3. 보호된 네트워크에 대해 두 개의 경로를 추가하고 보조 경로에 대해 더 높은 AD 값(이 경우 2)을 설정합니다.

첫 번째 경로는 VTI-1 인터페이스를 사용하고 두 번째 경로는 VTI-2 인터페이스를 사용합니다.

Network 🔺		Interface		Leaked from Virtual Router	Gateway	Tunneled		Metric		
▼ IPv4 Routes										
	protected-network		VTI-1		Global	VTI-1-Gateway		false	1	
	protected-network		VTI-2		Global	VTI-2-Gateway		false	2	

다음을 확인합니다.

1. Devices(디바이스) > VPN > Site to Site Monitoring(사이트 간 모니터링)으로 이동합니다.

	Devices	Objects	Integ	gration		
	Device	Management		VPN	Troubleshoot	
	Device	Upgrade		Site To Site	File Download	
	NAT			Remote Access	Threat Defense CLI	: 1
	QoS			Dynamic Access Policy	Packet Tracer	opo
	Platform	n Settings	_	Troubleshooting	Packet Capture	G
	FlexCor	nfig		Site to Site Monitoring		
-	Certifica	ates				0.1
						sł

2. 눈을 클릭하여 터널 상태에 대한 자세한 내용을 확인합니다.

	Dual-ISP-VTI	Active	2024-06-11 06:55:26
View ft. It information	Dual-ISP-VTI	Active	2024-06-12 14:27:22

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.