Configurar o túnel VPN site a site baseado em rota no FTD gerenciado pelo FMC

Contents
Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Limitações e restrições
Etapas de configuração no FMC
Verificar
na GUI do FMC
Da CLI do FTD

Introdução

Este documento descreve como configurar um túnel VPN site a site baseado em rota estática em um Firepower Threat Defense gerenciado por um Firepower Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica de como um túnel VPN funciona.
- Entender como navegar pelo FMC.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center (FMC) versão 6.7.0
- Cisco Firepower Threat Defense (FTD) versão 6.7.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A VPN baseada em rota permite que a determinação do tráfego interessante seja criptografada ou enviada pelo túnel VPN e use o roteamento de tráfego em vez da política/lista de acesso como na VPN baseada em política ou em mapa de criptografia. O domínio de criptografia é definido para permitir qualquer tráfego que entre no túnel IPsec. Os seletores de tráfego local e remoto IPsec são definidos como 0.0.0/0.0.0.0. Isso significa que todo o tráfego roteado para o túnel IPsec é criptografado, independentemente da sub-rede de origem/destino.

Este documento se concentra na configuração da Interface de túnel virtual estático (SVTI). Para obter a configuração da Dynamic Virtual Tunnel Interface (DVTI) no Secure Firewall, consulte este <u>documento</u>.

Limitações e restrições

Estas são limitações e restrições conhecidas para túneis baseados em rota no FTD:

- Suporta somente IPsec. Não há suporte para GRE.
- Suporta somente interfaces IPv4, bem como IPv4, redes protegidas ou payload de VPN (Sem suporte para IPv6).
- O roteamento estático e somente o protocolo de roteamento dinâmico BGP são suportados para interfaces VTI que classificam o tráfego para VPN (Sem suporte para outros protocolos como OSPF, RIP e assim por diante).
- Somente 100 VTIs são suportados por interface.
- Não há suporte para VTI em um Cluster FTD.
- O VTI não é suportado nestas políticas:
 - •qos •NAT · Configurações de plataforma

Esses algoritmos não são mais suportados no FMC/FTD versão 6.7.0 para novos túneis VPN (o FMC suporta todas as cifras removidas para gerenciar o FTD < 6.7):

- Não há suporte para 3DES, DES e Criptografia NULL na Política IKE.
- Os grupos DH 1, 2 e 24 não têm suporte na Política IKE e na Proposta IPsec.

- Não há suporte para a Integridade MD5 na Política IKE.
- PRF MD5 não é suportado na política IKE.
- Os algoritmos de criptografia DES, 3DES, AES-GMAC, AES-GMAC-192 e AES-GMAC-256 não são suportados na Proposta IPsec.

Observação: isso é válido tanto para a rota de site para site quanto para túneis VPN baseados em políticas. A fim de atualizar um FTD antigo para 6.7 do FMC, desencadeia uma verificação de pré-validação que alerta o utilizador sobre as alterações que dizem respeito às cifras removidas que bloqueiam a atualização.

FTD 6.7 gerenciado via FMC 6.7	Configuração disponível	Túnel VPN de Site a Site
Instalação nova	Cifras fracas disponíveis, mas não podem ser usadas para configurar o dispositivo FTD 6.7.	Cifras fracas disponíveis, mas não podem ser usadas para configurar o dispositivo FTD 6.7.
Atualização: FTD configurado apenas com cifras fracas	Atualização do FMC 6.7 UI, uma verificação de pré- validação exibe um erro. A atualização está bloqueada até a reconfiguração.	Após a atualização do FTD, e suponha que o peer não tenha alterado suas configurações, o túnel será encerrado.
Atualização: FTD configurado apenas com algumas cifras fracas e algumas cifras fortes	Atualização do FMC 6.7 UI, uma verificação de pré- validação exibe um erro. A atualização está bloqueada até a reconfiguração.	Após a atualização do FTD, e suponha que o peer tenha cifras fortes, o túnel será restabelecido.
Atualização: país de classe C (não possui uma licença de criptografia forte)	Permitir DES é permitido	Permitir DES é permitido

Observação: não é necessário licenciamento adicional, a VPN baseada em rota pode ser configurada nos Modos licenciado e de avaliação. Sem a conformidade de criptografia (Export Controlled Features Enabled), somente o DES pode ser usado como algoritmo de criptografia.

Etapas de configuração no FMC

Etapa 1. Navegue até Devices >VPN >Site To Site.

Overview Analysis	Policies	Devic	es Obj	jects	AMP Inte	lligence		
Device Management	NAT	VPN v	QoS	Pla	form Settings	FlexConfig	Certificates	
		Site To S	Site					
View By : Group	į	Remote Troubles	Access	D)	Warning (0)	Offline (0) No	ormal (1) Dep	loymer

Etapa 2. Clique em Add VPN e escolha Firepower Threat Defense Device, como mostrado na imagem.

S	Deploy	System	Help 🔻	admin 🔻
			A (2)	dd VPN 👻
	Fire	epower Dev	ice	
6	Fire	epower Thre	eat Defense	e Device

Etapa 3. Forneça um Nome da Topologia e selecione o Tipo de VPN como Baseado em Rota (VTI). Escolha a Versão IKE.

Para efeitos desta demonstração:

Nome da topologia: VTI-ASA

Versão do IKE: IKEv2

Topology Name:*	VTI-ASA		
	O Policy Based (Crypto Map) O Route Based (VTI)		
Network Topology:	Point to Point 😽 Hub and Spoke 💠 Full Mesh		
IKE Version:*	□ IKEv1		
KE Version:*	🗌 IKEv1 🗹 IKEv2		

Etapa 4. Escolha o dispositivo no qual o túnel precisa ser configurado. Você pode optar por adicionar uma nova interface de túnel virtual (clique no ícone +), ou selecionar uma na lista que existe.

Endpoints	IKE	IPsec	Advanced			
	Node A			Node B		
Device:*	:		1	Device:*		
FTD		¥		Empty	*	
Virtual T	unnel Interface:*			Virtual Tunnel Interface:*		0
Tunne	Source IP is Private	Edit VII	-	Tunnel Source IP is Private	Edit VTI	U
Connect	ion Type:*			Connection Type:*		
Bidirectio	onal	*		Bidirectional	*	
Tunnel I Tunnel S Tunnel S	P Address Jource Interface Jource Interface IP	:		Tunnel IP Address Tunnel Source Interface Tunnel Source Interface IP	:	

Etapa 5. Defina os parâmetros da New Virtual Tunnel Interface. Click OK.

Para efeitos desta demonstração:

Nome: VTI-ASA

Descrição (Opcional): Túnel VTI com Extranet ASA

Zona de segurança: VTI-Zone

ID do túnel: 1

Endereço IP: 192.168.100.1/30

Origem do Túnel: GigabitEthernet0/0 (Externo)

Add Virtual Tunne	el Interface	? ×
General		
Name *:	VTI-ASA	bled
Description:	VTI Tunnel with Extranet ASA	
Security Zone:	VTI-Zone 👻	
Tunnel ID *:	1 Range:	0 - 10413
IP Address *:	192.168.100.1/30	
Tunnel Source *:	GigabitEthernet0/0 (Outside)	
		OK Cancel

Etapa 6. Clique em OK no pop-up que menciona que o novo VTI foi criado.



Passo 7. Escolha o VTI recém-criado ou um VTI que exista em Virtual Tunnel Interface. Forneça as informações para o Nó B (que é o dispositivo peer).

Para efeitos desta demonstração:

Dispositivo: Extranet

Nome do dispositivo: ASA-Peer

Endereço IP do endpoint: 10.106.67.252

11	Create New VPN Topo	logy					? ×
1	Topology Name:*	VTI-ASA					
l		\bigcirc Policy Based (C	rypto Map) 💿 R	toute Base	ed (VTI)		
l	Network Topology:	↔ Point to Poi	nt 🛠 Hub and	Spoke	🕈 Full Mesh		
l	IKE Version:*	🗆 ikevi 🗹 ike	v2				
l							
l	Endpoints IKE	IPsec	Ad	vanced			
	Nor Device:* FTD Virtual Tunnel Inter VTI-ASA Tunnel Source IP i Bidirectional Tunnel IP Address Tunnel Source Inter Tunnel Source Inter Additional Configur Route traffic to the Permit VPN traffic	de A rface:* is Private rface IP : 192. : Outs : Outs : Tface IP : 10.1 : AC P	 ▼ ► Edit VII ● 168.100.1 ide 97.224.90 ing Policy olicy]	Node B Device:* Extranet Device Name*: ASA-Peer Endpoint IP Address*: 10.106.67.252		
ľ						Save Can	cel

Etapa 8. Navegue até a guia IKE. Você pode optar por usar uma política predefinida ou clicar no botão + ao lado da guia Política e criar uma nova.

IKEv2 Settings		
Policy:*	AES-GCM-NULL-SHA-LATEST	0
Authentication Type:	Pre-shared Automatic Key	·
Pre-shared Key Length:*	24 Characters (Range 1-127)

Etapa 9. (Opcional, se você criar uma nova Política IKEv2.) Forneça um Nome para a Política e selecione os Algoritmos a serem usados na política. Click Save.

Para efeitos desta demonstração:

Nome: ASA-IKEv2-Política

- Algoritmos de integridade: SHA-512
- Algoritmos de criptografia: AES-256

Algoritmos PRF: SHA-512

Grupo Diffie-Hellman: 21

ew IKEv2 Policy			?
Name:*	ASA-IKEv2-Policy		
Description:			
Priority:	1	(1-65535)	
Lifetime:	86400	seconds (120-2147483647)	
Integrity Algorithms	Available Algorithms	Selected Algorithm	s
PRF Algorithms Diffie-Hellman Group	Image: MD5 Image: SHA Image: SHA256 Image: SHA384 Image: SHA384 Image: NULL	Add	
		Save	Cancel

Etapa 10. Escolha a política recém-criada ou a política existente. Selecione o Tipo de autenticação. Se uma chave manual pré-compartilhada for usada, forneça a chave nas caixas Key e Confirm Key .

Para efeitos desta demonstração:

Política: ASA-IKEv2-Política

Tipo de autenticação: chave manual pré-compartilhada

Tecla: cisco123

Confirmar chave: cisco123

Endpoints IKE	IPsec	Advanced	
IKEv1 Settings			
Policy:*	preshared_sha_aes256_dh1	4_3 💙	0
Authentication Type:	Pre-shared Automatic Key	~	
Pre-shared Key Length:*	24 Characters	(Range 1-127)	
IKEv2 Settings	ASA-IKEv2-Policy	~	a
Authentication Type:	Pre-shared Manual Key	×	
Key:*	•••••		
Confirm Key:*	•••••		
	Enforce hey-based pre-sh	ared key only	

Nota: Se ambos os terminais estiverem registrados no mesmo CVP, a opção de chave automática pré-compartilhada também pode ser utilizada.

Etapa 11. Navegue até a guia IPsec. Você pode optar por usar uma proposta de IPsec IKEv2 predefinida ou criar uma nova. Clique no botão Editar ao lado da guia IKEv2 IPsec Proposal.

Crypto Map Type:	Static Opynamic	
IKEv2 Mode:	Tunnel 💙	
Transform Sets:	IKEv1 IPsec Proposals 🥜	IKEv2 IPsec Proposals* 🥜
	tunnel_aes256_sha	AES-GCM
Enable Security A	ssociation (SA) Strength Enforcer	nent

Etapa 12. (Opcional, se você criar uma nova Proposta IKEv2 IPsec.) Forneça um Nome para a Proposta e selecione os Algoritmos a serem usados na Proposta. Click Save.

Para efeitos desta demonstração:

Nome: ASA-IPSec-Policy

Hash ESP: SHA-512

Criptografia ESP: AES-256

Name:*	ASA-IPSec-Policy			
ESP Hash	Available Algorithms	Se	lected Algorithm	15
	AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES-GCM AES AES DES AES-GMAC-256	Add	₿ AES-256	
			Saux 1	Gaard

Etapa 13. Escolha a Proposta recém-criada ou a Proposta que existe na lista de propostas disponíveis. Click OK.

on:*	IKEv2 IPsec Proposal			? ×
	Available Transform Sets C		Selected Transform Sets	
o Tr	 AES-GCM AES-SHA] [
Se	ASA-IPSec-Policy OBS_SHA-1	Add		
Sec				
Perl				
s G				
ura'			ок	Cancel
ce:				

Etapa 14. (Opcional) Escolha as configurações de Perfect Forward Secrecy. Configure a Duração e o Tamanho da Vida Útil do IPsec.

Para efeitos desta demonstração:

Segredo de encaminhamento perfeito: Grupo de módulos 21

Duração da Vida Útil: 28800 (Padrão)

Tamanho do Tempo de Vida: 4608000 (Padrão)

Ļ	Enable Security As	sociation (SA) Stree	ath Enforce	ement
L	Enable Perfect Forv	vard Secrecy		
L	Modulus Group:	21	~	
L	Lifetime Duration*:	28800		Seconds (Range 120-2147483647)
L	Lifetime Size:	4608000		Kbytes (Range 10-2147483647)
ľ	- ESPv3 Settings	\$		

Etapa 15. Verifique as configurações definidas. Clique em Salvar, conforme mostrado nesta imagem.

Topology Name:*	VTI-ASA					
		Based (Crypto M	ap) 💿 Route Based (VTI)			
Network Topology	r: 🗠 Poin	t to Point 😽	Hub and Spoke 💠 Full Mes			
IKE Version:*	IKEv1	IKEv2				
Endpoints	IKE	IPsec	Advanced			
Crypto Map Type:	Static O Dy	namic				
IKEv2 Mode:	Tunnel	~				
Transform Sets:	IKEv1 IPsec Prop	oosals 🥜	IKEv2 IPsec Proposals* 🥜			
	tunnel_aes256_	sha	ASA-IPSec-Policy			
Enable Security	Association (SA) Str	ength Enforceme	nt			
Enable Perfect Ferret	orward Secrecy					
Modulus Group:	21	*				
Lifetime Duration*:	28800	S	econds (Range 120-2147483	547)		
Lifetime Size:	4608000	K	bytes (Range 10-214748364)	7)		
	igs					
					Save	Cancel

Etapa 16. Configure a Política de Controle de Acesso. Navegue até Policies > Access Control > Access Control. Edite a Política aplicada ao FTD.

Observação: sysopt connection permit-vpn não funciona com túneis VPN Baseados em Rota. As regras de controle de acesso precisam ser configuradas para zonas IN-> OUT e OUT -> IN.

Forneça as Zonas de origem e as Zonas de destino na guia Zonas .

Forneça as redes de origem, redes de destino na guia Redes . Clique em Add.

Para efeitos desta demonstração:

Zonas de origem: na zona e fora da zona

Zonas de destino: Out-Zone e In-Zone

Redes de origem: rede interna e remota

Redes de destino: rede remota e na rede

Add Rule								? ×
Name	VTI-Traffic	1			Enabled	Insert into Ma	ndatory	~
Action	Allow				21 E			
Time Range	None	~	0					
-								
Zones	Networks	VLAN Tags	A Users	Applications	Ports URLS SGI/	SE Attributes	Inspection Loggin	g Comments
Available Zon	nes C				Source Zones (Z)		Destination Zones (2)	
Search by	name				In-Zone		in-Zone	
In-Zone					out-zone		Ult-Zone	0
Out-Zone				L				
VTI-Zone				Add to Source				
				Add to				
				Destination	J			
Action Time Range	Allow None	~	0	 O D .81 	1			
70000	latworks	VI AN Tags	A Licore	Applications	Porte LIPLE SGT	ISE Attributos	Inspection Logain	Comments
Available Net	works #	VD4IV Tags	La Users	Applications	Source Networks (2)	ISE Attributes	Destination Networks (2)	ig comments
available neu	MOTKS C				Source Networks (2)	Original Client	Describtion Networks (2)	
			_		In-Netwrk	Original clienc	B Remote-Network	6
Netwo	rks	Geolocat 0-12	ion		Remote-Network			
					and an			
IPv4-Privat	te-192.168.0	.0-16		Add To				
IPv4-Privat	te-192.168.0 te-All-RFC19	.0-16 18		Add To Source Networks				
IPv4-Privat	te-192.168.0 te-All-RFC19 Mapped	.0-16 18		Add To Source Networks				
IPv4-Privat	te-192.168.0 te-All-RFC19 Mapped Local	.0-16 18		Add To Source Networks Add to Destination				
IPv4-Privat IPv4-Privat IPv6-IPv4-I IPv6-Link-L IPv6-Link-L	te-192.168.0 te-All-RFC19 Mapped Local te-Unique-Lo	.0-16 18 cal-Addresses		Add To Source Networks Add to Destination				
IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link-L IPv6-Privat IPv6-to-IPv	te-192.168.0 te-All-RFC19 Mapped Local te-Unique-Lo v4-Relay-Any	.0-16 18 cal-Addresses rcast		Add To Source Networks Add to Destination				
IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link-L IPv6-Privat IPv6-to-IPv Remote-Ne	te-192.168.0 te-All-RFC19 Mapped Local te-Unique-Lo v4-Relay-Any stwork	.0-16 18 cal-Addresses rcast		Add To Source Networks Add to Destination				
IPv4-Privat IPv6-Privat IPv6-IPv4- IPv6-LInk-I IPv6-Privat IPv6-to-IPv Remote-Ne VTI-ASA-Tu	te-192.168.0 te-All-RFC19 Mapped Local te-Unique-Lo v4-Relay-Any atwork unnel	.0-16 18 cal-Addresses /cast		Add To Source Networks Add to Destination	Enter an IP address	Add	Enter an IP address	Add
IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link-I IPv6-Privat IPv6-to-IPv Remote-Ne VTI-ASA-Tu	te-192.168.0 te-All-RFC19 Mapped Local te-Unique-Lo v4-Relay-Any etwork unnel	.0-16 18 cal-Addresses /cast		Add To Source Networks Add to Destination	Enter an IP address	Add	Enter an IP address	bbA

Etapa 17. Adicione o roteamento sobre o túnel VTI. Navegue até Devices > Device Management. Edite o dispositivo no qual o túnel VTI está configurado.

Navegue até Static Route na guia Routing. Clique em Add Route.

Forneça a interface, escolha a rede, forneça o gateway. Click OK.

Para efeitos desta demonstração:

Interface: VTI-ASA

Rede: Rede Remota

Gateway: túnel VTI-ASA

Add Static Ro	ute Configuration	? X
Type: Interface*	IPv4 ○ IPv6 VTI-ASA VTI-ASA (Interface starting with this icon 중 signifies it is available for n	oute leak)
Available Ne	Selected Network Selected Network Selected Network Remote-Network Add Add Add Add Add Add Add	
Gateway* Metric: Tunneled: Route Tracking:	VTI-ASA-Tunnel	Consel

Etapa 18. Navegue até Implantar > Implantação. Escolha o FTD no qual a configuração precisa ser implantada e clique em Implantar.

Configuração enviada por push para a CLI do FTD após implantação bem-sucedida:

<#root>
crypto ikev2 policy 1
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400

```
crypto ikev2 enable Outside
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2
tunnel-group 10.106.67.252 type ipsec-121
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
 ip address 192.168.100.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 10.106.67.252
 tunnel mode ipsec ipv4
```

tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

Verificar

na GUI do FMC

Clique na opção Check Status para monitorar o status ao vivo do túnel VPN a partir da própria GUI



Isso inclui estes comandos extraídos da CLI do FTD:

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail I2I filter ipaddress <Peer IP Address>

extranet : ASA-Peer	P	• FTD/VTI-ASA
> show crypto ipsec sa peer		> show crypto ipsec sa peer 10.106.67.252
Not applicable for extranet peer		<pre>peer address: 10 106 67 252 Crypto map tag:vti-crypto-map-4-0-1, seq num: 65280, local addr: 10.197.224.90 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 10.106.67.252 #pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100 #pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 100, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0</pre>
Show vpn-sessiondb detail l2l filter ipaddress Not applicable for extranet peer		<pre>> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252 Session Type: LAN-to-LAN Detailed Connection : 10.106.67.252 Index : 44</pre>
		Dytes IX : 10000 Login Time : 03:54:57 UTC Thu Nov 12 2020 Duration : 00:02m:12s Tunnel Zone : 0 IKEv2 Tunnels: 1 IFsec Tunnels: 1 IKEv2: Tunnel ID : 44.1 UDP Src Port : 500 Rem Auth Mode: preSharedKeys Loc Auth Mode: preSharedKeys Encryption : AES256 Hashing : SHA512 Rekey Int (T): 86400 Seconds Rekey Left(T): 86268 Seconds PRF : SHA512 D/H Group : 21

Da CLI do FTD

Esses comandos podem ser usados na CLI do FTD para visualizar a configuração e o status dos túneis VPN.

show running-config route show crypto ikev1 sa detailed show crypto ikev2 sa detailed show crypto ipsec sa detailed show vpn-sessiondb detail 121

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.