在FMC管理的FTD上設定路由型站台到站台 VPN通道

| 目錄 | | |
|-----------------|--|--|
| <u>簡介</u> | | |
| <u>必要條件</u> | | |
| <u>需求</u> | | |
| 採用元件 | | |
| <u>背景資訊</u> | | |
| 限制和限制 | | |
| <u>FMC的配置步驟</u> | | |
| 驗證 | | |
| <u>從FMC GUI</u> | | |
| <u>從FTD CLI</u> | | |

簡介

本文檔介紹如何在由Firepower管理中心管理的Firepower威脅防禦上配置基於靜態路由的站點到站 點VPN隧道。

必要條件

需求

思科建議您瞭解以下主題:

- 對VPN隧道如何工作有基本的瞭解。
- 瞭解如何在FMC中導航。

採用元件

本檔案中的資訊是根據以下軟體版本:

- Cisco Firepower管理中心(FMC)版本6.7.0
- Cisco Firepower威脅防禦(FTD)版本6.7.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

基於路由的VPN允許確定要加密或透過VPN隧道傳送的相關流量,並且使用流量路由而不是策略/訪問清單(如基於策略或基於加密對映的VPN所示)。加密域設定為允許任何進入IPSec隧道的流量。IPsec本地和遠端流量選擇器設定為0.0.0/0.0.0.0。這意味著路由到IPSec隧道的所有流量都會被加密,無論源/目標子網如何。

本檔案將重點介紹靜態虛擬通道介面(SVTI)組態。有關安全防火牆上的動態虛擬隧道介面(DVTI)配置,請參閱此<u>文檔</u>。

限制和限制

以下是FTD上基於路由的隧道的已知限制和限制:

- 僅支援IPsec。不支援GRE。
- 僅支援IPv4介面,以及IPv4、受保護的網路或VPN負載(不支援IPv6)。
- 為VPN分類流量的VTI介面支援靜態路由和僅BGP動態路由協定(不支援OSPF、RIP等其它協定)。
- 每個介面僅支援100個VTI。
- FTD叢集不支援VTI。
- 以下策略不支援VTI:
 - · Qos
 - \cdot NAT
 - ·平台設定

新VPN通道的FMC/FTD 6.7.0版不再支援這些演演算法(FMC支援所有移除的密碼以管理FTD < 6.7):

- IKE策略不支援3DES、DES和NULL加密。
- DH組1、2和24在IKE策略和IPsec提議中不受支援。
- IKE策略不支援MD5完整性。
- IKE策略不支援PRF MD5。
- DES、3DES、AES-GMAC、AES-GMAC-192和AES-GMAC-256加密演算法在IPsec提議中 不受支援。

✤ 注意:這對於基於站點到站點路由的VPN隧道以及基於策略的VPN隧道都適用。若要將舊版 FTD從FMC升級到6.7,會觸發預先驗證檢查,警告使用者有關封鎖升級之已移除密碼的變更

| 透過FMC 6.7管理的FTD 6.7 | 可用組態 | 站點到站點VPN隧道 |
|----------------------------|---|-----------------------------------|
| 全新安裝 | 弱密碼可用,但無法用於配置 FTD 6.7裝置。 | 弱密碼可用,但無法用於配置 FTD 6.7裝置。 |
| 升級:FTD僅設定弱式密碼 | 從FMC 6.7 UI升級,預先驗證檢 查會顯示錯誤。在重新配置之前 ,升級會被阻止。 | 進行FTD升級後,並假設對等體 未變更其設定,則通道會終止。 |
| 升級:FTD僅設定一些弱式密碼 和某些強式密碼 | 從FMC 6.7 UI升級,預先驗證檢 查會顯示錯誤。在重新配置之前 ,升級會被阻止。 | FTD升級後,假設對等點具有強 式密碼,然後通道重新建立。 |
| 升級:C類國家/地區(沒有強大 的加密許可證) | 允許DES | 允許DES |

💊 注意:不需要其他許可,可以在許可模式和評估模式下配置基於路由的VPN。 如果沒有加密 規範(已啟用導出控制功能),則只有DES可用作加密演算法。

FMC的配置步驟

步驟 1.導航到裝置>VPN >站點到站點。

| Overview Analysis | Policies | Devices | Objects | AMP Inte | lligence | | |
|--------------------------|----------|---------------------------|--------------|---------------|------------------|------------------|--------|
| Device Management | NAT | VPN V | oS Pla | form Settings | FlexConfig | Certificates | |
| | | Site To Site | | | | | |
| View By : Group | į | Remote Acc Troubleshoo | ess oting | Warning (0) | Offline (0) No | ormal (1) Depl | loymer |

步驟 2.按一下Add VPN,然後選擇Firepower Threat Defense Device,如圖所示。

o



步驟 3.提供拓撲名稱並選擇基於路由(VTI)的VPN型別。選擇IKE Version。

在本演示中:

拓撲名稱:VTI-ASA

IKE版本:IKEv2

| Topology Name:* | VTI-ASA | VTI-ASA | | |
|-------------------|----------------------|--------------------|-------------|--|
| | O Policy Based (Cryp | to Map) 💿 Route Ba | ased (VTI) | |
| Network Topology: | ↔ Point to Point | 🛠 Hub and Spoke | 🔶 Full Mesh | |
| IKE Version:* | 🗌 IKEv1 🗹 IKEv2 | | | |
| | | | | |

步驟 4.選擇需要在其上配置隧道的裝置,您可以選擇增加新的虛擬隧道介面(點選+圖示),或者從清 單中選擇一個已存在的介面。

| ndpoints | IKE | IPsec | Advanced | | | |
|-----------|-------------------------------|----------|----------|-------------------------------|----------|---------|
| | Node A | | | Node B | | |
| Device:* | | | D | evice:* | | |
| FTD | | Y | E | Empty | * | |
| Virtual T | unnel Interface:* | | | irtual Tunnel Interface:* | | |
| | | * | | Empty | ~ | \odot |
| U Tunne | I Source IP is Private | Edit V H | | J Tunnel Source IP is Private | Edit VII | |
| Connect | ion Type:* | | C | connection Type:* | | |
| Bidirecti | onal | * | E | Bidirectional | * | |
| Tuppel I | P. Addrosec | | | uppel TD Address | | |
| Tunnel | F Address Source Interface | 1 | | unnel Source Interface | | |
| Tunnel S | Source Interface IP | - | Ť | unnel Source Interface IP | | |

步驟 5.定義新虛擬隧道介面的引數。按一下「OK」(確定)。

- 在本演示中:
- 名稱:VTI-ASA
- 說明(可選):VTI隧道和外聯網ASA
- 安全區域:VTI-Zone
- 通道ID:1
- IP地址:192.168.100.1/30
- 隧道源:GigabitEthernet0/0(外部)

| Add Virtual Tunnel | Interface | ? |
|--------------------|------------------------------|-------------|
| General | | |
| Name *: | VTI-ASA | abled |
| 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) | |
| | | |
| | | |
| | | |
| | ſ | OK Cancel |

步驟 6.點選彈出窗口中的OK,通知已建立新的VTI。

| _ | | 1 | | Node B |
|---------|--|-----------------------|---|----------|
| Virtual | Tunnel Inter | fac | e Added | |
| the VT | VTI has been of Please go to th Interfaces pag | crea he D je to | ted successfully. evice > delete/update | erface: |
| | | | ок | is Priva |
| | | | Connection Typ | e:* |

步驟 7.選擇新建立的VTI或虛擬隧道介面下存在的VTI。提供節點B(對等裝置)的資訊。

在本演示中:

裝置:Extranet

裝置名稱:ASA-Peer

終端IP地址:10.106.67.252

| 16 | Create New VPN Topo | logy | | 1 | × |
|----|--|---|--|---|---|
| | Topology Name:* | VTI-ASA O Policy Based (Cry | pto Map) 💿 Route B | Based (VTI) | |
| | Network Topology: IKE Version:* | Point to Point IKEv1 IKEv2 | ✤ Hub and Spoke | e 💠 Full Mesh | |
| I. | Endpoints IKE | IPsec | Advance | ed | |
| | No Device:* FTD Virtual Tunnel Inte VTI-ASA Tunnel Source IP | de A rface:* | V Edit VTI | Node B Device:* Extranet Device Name*: ASA-Peer | |
| | Connection Type:* Bidirectional | | ¥ | Endpoint IP Address*: 10.106.67.252 | |
| | Tunnel IP Address Tunnel Source Inte Tunnel Source Inte Additional Configur Route traffic to the Permit VPN traffic | : 192.16 : Outside rface IP : 10.197 ration () : VTI : <u>Routing</u> : <u>AC Poli</u> | 8.100.1 224.90 <u>7 Policy</u> CY | | |
| | | | | Save Cancel | |

步驟 8.導航到IKE 頁籤。您可以選擇使用預定義的策略,也可以按一下策略頁籤旁邊的+ 按鈕並建 立一個新策略。

| IKEv2 Settings | | _ |
|-------------------------|--------------------------|----------|
| Policy:* | AES-GCM-NULL-SHA-LATEST | ▼ |
| Authentication Type: | Pre-shared Automatic Key | ~ |
| Pre-shared Key Length:* | 24 Characters (Range 1-1 | .27) |
| | | |

第9步:(如果建立新的IKEv2策略,則可選。) 為策略提供名稱並選擇要用於策略的演算法。按一 下Save。

在本演示中:

名稱:ASA-IKEv2-Policy

完整性演算法:SHA-512

加密演算法:AES-256

PRF演算法:SHA-512

Diffie-Hellman組:21

| New IKEv2 Policy | | | ? × |
|---|--|---------------------------------------|-----|
| Name:* | ASA-IKEv2-Policy | | |
| Description: Priority: Lifetime: | 1 86400 | (1-65535) seconds (120-2147483647) | |
| Integrity Algorithms | Available Algorithms | Selected Algorithms | |
| Encryption Algorithms PRF Algorithms Diffie-Hellman Group | MDS SHA SHA512 SHA556 SHA384 SHA384 | Add | |
| | | Save | cel |

步驟 10.選擇新建立的策略或現有的Policy。選擇Authentication Type。如果使用預共用手動金鑰 ,請在金鑰和確認金鑰框中提供金鑰。

在本演示中:

策略:ASA-IKEv2-Policy

驗證型別:預先共用手動金鑰

金鑰:cisco123

確認金鑰:cisco123

| KEv1 Settings | | | |
|--|---|--------|---|
| Policy:* | preshared_sha_aes256_dh14_3 | ~ | ٢ |
| Authentication Type: | Pre-shared Automatic Key | ~ | |
| Pre-shared Key Length:* | 24 Characters (Range 1- | -127) | |
| KEv2 Settings | | | |
| KEv2 Settings Policy:* | ASA-IKEv2-Policy | ~ | 0 |
| KEv2 Settings Policy:* Authentication Type: | ASA-IKEv2-Policy Pre-shared Manual Key | × × | 0 |
| KEv2 Settings Policy:* Authentication Type: Key:* | ASA-IKEv2-Policy Pre-shared Manual Key | * | 0 |

S 注意:如果兩個終端在同一FMC上註冊,還可以使用預共用自動金鑰選項。

步驟 11.導航到IPsec頁籤。 您可以選擇使用預定義的IKEv2 IPsec建議或建立新建議。點選IKEv2 IPsec Proposal頁籤旁的Edit按鈕。

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

第12步:(可選,如果您建立新的IKEv2 IPsec提議。) 為建議提供名稱,並選擇建議中所用的演 算法。按一下Save。

在本演示中:

名稱: ASA-IPSec-Policy

ESP雜湊:SHA-512

ESP加密:AES-256

| lame:* | ASA-IPSec-Policy | |
|----------|--|---------------------|
| ESP Hash | Available Algorithms | Selected Algorithms |
| | AES-GCM-256 AES-GCM-192 AES-192 AES-GCM AES AES AES DES AES-GMAC-256 | Add |
| | | |

步驟 13. 從可用提案清單中選擇存在的新建立的提案或提案。按一下「OK」(確定)。

| on:* | IKEv2 IPsec Proposal | | | ? × |
|------------|----------------------------|----------------|-------------------------|--------|
| | Available Transform Sets C | <mark>۲</mark> | Selected Transform Sets | |
| o Tr | Search Res-GCM Res-SHA | l | (ASA-IPSec-Policy) | |
| e: | ASA-IPSec-Policy | | | |
| Se | @ DES_SHA-1 | Add | | |
| Sec | | | | |
| Perl | | | | |
| s G | | | | |
| ura ze: | | | ок | Cancel |

步驟14. (選擇性)選擇「完全向前保密」設定。配置IPSec生存期持續時間和生存期大小。 在本演示中:

完全正向保密:模陣列21

存留期期間:28800 (預設)

| 存留時間大小: | 4608000 (| (預設) |) |
|---------|-----------|------|---|
|---------|-----------|------|---|

| Ļ | Enable Security Ass | ociation (SA) Str | enath Enforce | ement |
|---|---------------------|-------------------|---------------|--------------------------------|
| L | Enable Perfect Forw | ard Secrecy | | |
| L | Modulus Group: | 21 | * | |
| L | Lifetime Duration*: | 28800 | | Seconds (Range 120-2147483647) |
| L | Lifetime Size: | 4608000 | | Kbytes (Range 10-2147483647) |
| | ─▼ ESPv3 Settings | - | | |

步驟 15.檢查配置的設定。按一下Save,如下圖所示。

| Topology Name:* | VTI-ASA | | |
|---|--------------------------------|------------------------------|------|
| | O Policy Based (Cry | pto Map) 💿 Route Based (VTI) | |
| Network Topology | Point to Point | 🛠 Hub and Spoke 💠 Full Mesh | |
| IKE Version:* | 🗌 IKEv1 🗹 IKEv2 | | |
| | | | |
| Endpoints | IKE IPsec | Advanced | |
| Crypto Map Type: | Static Opynamic | | |
| IKEv2 Mode: | Tunnel | | |
| Transform Sets: | IKEv1 IPsec Proposals 🥜 | IKEv2 IPsec Proposals* 🥜 | |
| | tunnel_aes256_sha | ASA-IPSec-Policy | |
| Enable Security | Association (SA) Strength Enfo | rcement | |
| Enable Perfect For the second seco | orward Secrecy | | |
| Modulus Group: | 21 🗸 | | |
| Lifetime Duration*: | 28800 | Seconds (Range 120-214748364 | 7) |
| Lifetime Size: | 4608000 | Kbytes (Range 10-2147483647) | |
| — 💌 ESPv3 Settin | gs | | |
| | | | |
| | | | |
| | | | |
| | | | Save |

步驟 16.配置訪問控制策略。導航到策略>訪問控制>訪問控制。編輯套用至FTD的策略。

✤ 注意:sysopt connection permit-vpn不適用於基於路由的VPN隧道。需要為IN-> OUT區域和 OUT -> IN區域配置訪問控制規則。

在Zones 頁籤中提供Source Zones 和Destination Zones。

在網路頁籤中輸入源網路和目標網路。按一下Add。

在本演示中:

來源區域:區域內與區外

目標區域:區域外和區域內

源網路:內聯網和遠端網路

目的網路:遠端網路和內聯網

| lame | VTI-Traffic | | C Enabled | Insert into Mand | atory | ~ |
|--|---|--|--|--|--|---------------|
| ction | Allow | .00.8 | 215 | | | |
| Time Range | None 🗸 🔾 | | | | | |
| Zones | Networks VLAN Tags A User | Applications | Ports URLS SGT/IS | SE Attributes | Inspection Logo | aina Comments |
| vailable Zor | nes Ĉ | rippinedentitie | Source Zones (2) | | Destination Zones (2) | ang comments |
| Search by | name | | in-Zone | 6 | in-Zone | ß |
| - In-Zone | | | - Out-Zone | 6 | Out-Zone | 6 |
| Dut-Zone | | | | | | |
| VTI-Zone | | Add to | | | | |
| | | Source | | | | |
| | | Add to Destination | | | | |
| | | Descination | | | | |
| u Rule | | | | | | 3 |
| ame | VTI-Traffic | | Z Enabled | Insert into Mand | latory | ? |
| ame | VTI-Traffic | • 0 0.8 | Enabled | Insert into Mand | latory | 1 |
| ame ction ime Range | VTI-Traffic Allow None | V D 28 | Enabled | Insert into Mand | latory | 1 |
| ame ttion ime Range Zones | VTI-Traffic Allow None VLAN Tags User | S Applications | Enabled The Derts URLs SGT/I | Insert Into Mand | latory Inspection Log | ging Comments |
| ame ttion me Range Zones | VTI-Traffic Allow None VLAN Tags A User works C C | S Applications | Enabled Ports URLs SGT/I Source Networks (2) | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| ame ttion ime Range Zones | VTI-Traffic Allow None VLAN Tags A User works C C | s Applications | Enabled Ports URLs SGT/I Source Networks (2) Source | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| ame ttion me Range Zones N ailable Netwo | VTI-Traffic VTI-Traffic None VLAN Tags User works C Geolocation | s Applications | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk | Insert into Mand | Inspection Log Destination Networks (2) In-Netwrk Remote-Network | ging Comment: |
| ame ttion ime Range Zones N railable Netro Netwo a IPv4-Privat | VTI-Traffic VTI-Traffic None None VLAN Tags A User works C Geolocation te-172.16.0.0-12 | s Applications | | Insert Into Mand SE Attributes Original Client | Inspection Log Destination Networks (2) | ging Comments |
| ame ction ime Range Zones N vailable Net Netwo IPv4-Privat IPv4-Privat | VTI-Traffic Allow None VLAN Tags A User works C works Geolocation te-172.16.0.0-12 te-192.168.0.0-16 | Applications | Enabled Ports URLs SGT/I Source Networks (2) Source Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| ame ction ime Range Zones N railable Netr Netwo IPv4-Privat IPv4-Privat | VTI-Traffic Allow None VLAN Tags A User Works C Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 | Applications | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| Arrive Range Zones N Vallable Net Vetwo IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4- | VTI-Traffic VII-Traffic None None VLAN Tags User Works VLAN Tags User Works C C VLAN Tags () User Works C C C C C C C C C C C C C C | Applications | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) In-Netwrk Remote-Network | ging Comments |
| ame ction ime Range Zones N vailable Net Pv4-Privat IPv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-Link- IPv6-Privat | VTI-Traffic VII-Traffic None None VLAN Tags A User works C Works C Works C Works Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses | Add To Source Networks Add to Destination | Enabled Ports URLs SGT/I Source Networks (2) Source Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) In-Netwrk Remote-Network | ging Comments |
| ame ttion ime Range Zones N railable Net Pv4-Privat IPv4-Privat IPv4-Privat IPv6-IPv4- IPv6-IPv4- IPv6-Link-1 IPv6-to-IPv | VTI-Traffic VII-Traffic None None VLAN Tags A User works C Works C Works Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast | Add To Source Networks Add to Destination | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| Arrier Ange Arrier Ange Arrie | VTI-Traffic VII-Traffic None None VLAN Tags A User Works C C Trks Geolocation te-172.16.0.0-12 te-192.168.0.0-16 te-All-RFC1918 Mapped Local te-Unique-Local-Addresses v4-Relay-Anycast etwork | Applications Add To Source Networks Add to Destination | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk Remote-Network | Insert into Mand | Inspection Log Destination Networks (2) | ging Comments |
| Arrier ame ame ction ime Range Zones N vallable Netro Prot-Privat IPv6-IPv4- IPv6-IPv4- IPv6-Privat IPv6-to-IP Remote-Ne VTI-ASA-T | VTI-Traffic VTI-Traffic None None VLAN Tags User Works VLAN Tags User Works C C VLAN Tags User Works C C C C C C C C C C C C C C | Add To Source Networks Add to Destination | Enabled Ports URLs SGT/I Source Networks (2) Source In-Netwrk Remote-Network Enter an IP address | Insert into Mand | Inspection Log Destination Networks (2) In-Netwrk Remote-Network Enter an IP address | ging Comments |

步驟 17.透過VTI隧道增加路由。導航到裝置>裝置管理。編輯配置VTI隧道的裝置。

導航到Routing 頁籤下的Static Route。按一下Add Route。

提供介面,選擇網路,提供網關。按一下「OK」(確定)。

在本演示中:

介面:VTI-ASA

網路:遠端網路

網關:VTI-ASA隧道

| Add Static Ro | ute Configuratio | n | | | ? X |
|---|--|-----------------|--|-----------------------|---------|
| Type: Interface* | IPv4 O IPv6 VTI-ASA (Interface starting wi | ith this icon 👩 | ▼ signifies it is av | ailable for rout | e leak) |
| Available Net | twork C ③ | Add | Selected I | Network xe-Network | |
| Gateway* Metric: Tunneled: Route Tracking: | VTI-ASA-Tunnel | fault Route) | (1 - 254) (254) | | |
| | | | | ок | Cancel |

步驟 18.導航到部署>部署。選擇需要將配置部署到的FTD,然後按一下Deploy。

成功部署後,組態已推送到FTD CLI:

<#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 192.168.100.1 255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4

tunnel protection ipsec profile FMC_IPSEC_PROFILE_1

驗證

從FMC GUI

按一下Check Status選項以從GUI本身監控VPN隧道的即時狀態



其中包括從FTD CLI取得的以下命令:

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

| extranet : ASA-Peer | Ph | • 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 #MTUs 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 local crypto endpt.: 10.197.224.90/500, remote crypto endpt.:</pre> |
| show vpn-sessiondb detail l2l filter ipaddress | | <pre>> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252</pre> |
| Not applicable for extranet peer | | Session Type: LAN-to-LAN Detailed Connection : 10.106.67.252 Index : 44 IP Addr : 10.106.67.252 Protocol : IKEV2 IPsec Encryption : IKEV2: (1)AE5256 IPsec: (1)AE5256 Hashing : IKEV2: (1)SHA512 IPsec: (1)SHA512 Bytes Tx : 10000 Bytes Rx : 10000 Login Time : 03:54:57 UTC Thu Nov 12 2020 Duration : 0h:02m:12s Tunnel Zone : 0 IKEV2 Tunnels: 1 IPsec Tunnels: 1 |
| | | IKEv2: Tunnel ID : 44.1 UDP Src Port : 500 Rem Auth Mode: preSharedKeys Loc Auth Mode: preSharedKeys Encryption : AE5256 Rekey Int (T): 86400 Seconds PRF : SHA512 D/H Group : 21 |

從FTD CLI

這些命令可從FTD CLI中使用,以檢視VPN通道的組態和狀態。

show running-config crypto
show running-config nat
show running-config route

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。