

Configurazione tunnel IPv2 IPv6 da sito a sito tra ASA e FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione ASA](#)

[Configurazione FTD](#)

[Ignora controllo di accesso](#)

[Configura esenzione NAT](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

In questo documento viene illustrato un esempio di configurazione per configurare un tunnel da sito IPv6 a sito tra un'appliance ASA (Adaptive Security Appliance) e un protocollo FTD (Firepower Threat Defense) tramite il protocollo IKEv2 (Internet Key Exchange versione 2). L'installazione include la connettività di rete IPv6 end-to-end con ASA e FTD come dispositivi di terminazione VPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze fondamentali della configurazione ASA CLI
- Conoscenze base dei protocolli IKEv2 e IPSEC
- Informazioni sull'indirizzamento e il routing IPv6
- Conoscenze di base della configurazione FTD tramite FMC

Componenti usati

Le informazioni discusse in questo documento si basano su un ambiente virtuale creato con dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è in produzione,

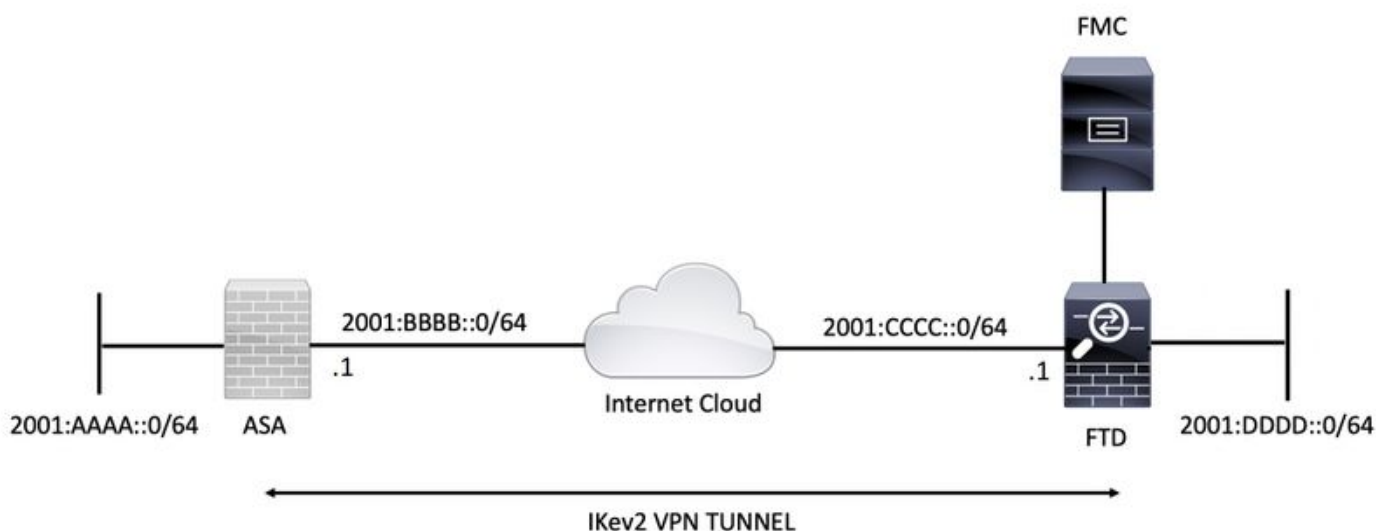
valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA con versione 9.6(4)12
- Cisco FTD con versione 6.5.0
- Cisco FMC con versione 6.6.0

Configurazione

Esempio di rete



Configurazione ASA

In questa sezione viene descritta la configurazione richiesta sull'appliance ASA.

Passaggio 1. Configurare le interfacce ASA.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Passaggio 2. Impostare una route predefinita IPv6.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Passaggio 3. Configurare il criterio IKEv2 e abilitare IKEv2 sull'interfaccia esterna.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

Passaggio 4. Configurare il gruppo di tunnel.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

Passaggio 5. Creare gli oggetti e l'Access Control List (ACL) in modo che corrispondano al traffico interessato.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

Passaggio 6. Configurare le regole NAT (Network Address Translation) dell'identità per il traffico interessato.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

Passaggio 7. Configurare la proposta IPsec IKEv2.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

Passaggio 8. Impostare la mappa crittografica e applicarla all'interfaccia esterna.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

Configurazione FTD

In questa sezione vengono fornite le istruzioni per configurare un FTD utilizzando FMC.

Definire la topologia VPN

Passaggio 1. Passare a **Dispositivi > VPN > Da sito a sito**.

Seleziona Aggiungere VPN e scegliere Firepower Threat Defense Device, come mostrato nell'immagine.

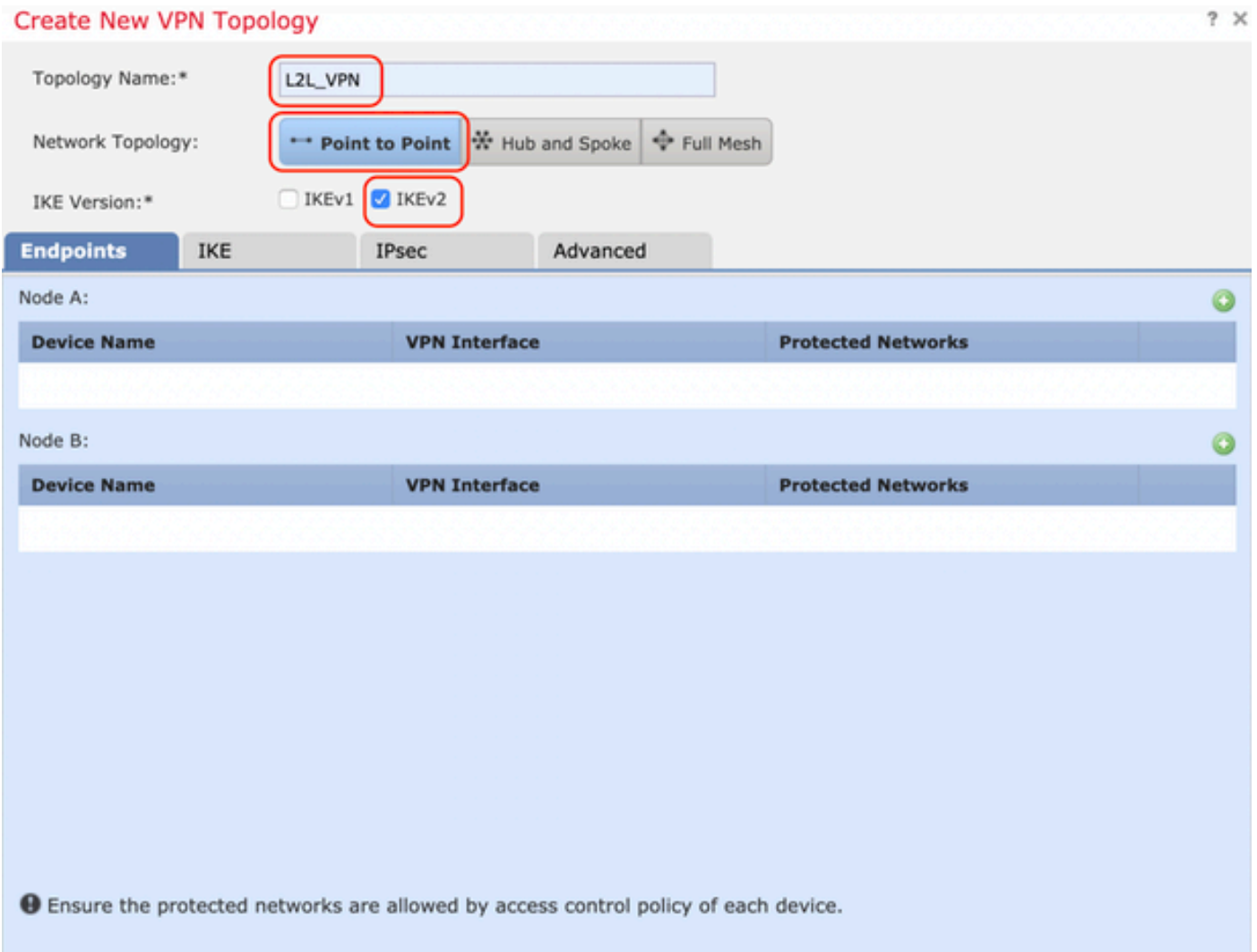


Passaggio 2. Viene visualizzata la casella 'Create New VPN Topology'. Dai alla VPN un nome facilmente identificabile.

Topologia della rete: Punto-punto

Versione IKE: IKEv2

In questo esempio, quando si selezionano gli endpoint, il nodo A è l'FTD. Il nodo B è l'ASA. Fare clic sul pulsante verde più per aggiungere dispositivi alla topologia.



Passaggio 3. Aggiungere l'FTD come primo endpoint.

Scegliere l'interfaccia a cui applicare la mappa crittografica. L'indirizzo IP deve essere popolato automaticamente dalla configurazione del dispositivo.

Fare clic sul pulsante più verde in Reti protette per selezionare le subnet crittografate tramite questo tunnel VPN. In questo esempio, l'oggetto di rete 'Proxy locale' in FMC è costituito dalla subnet IPv6 '2001:DDDD::/64'.

Edit Endpoint



Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

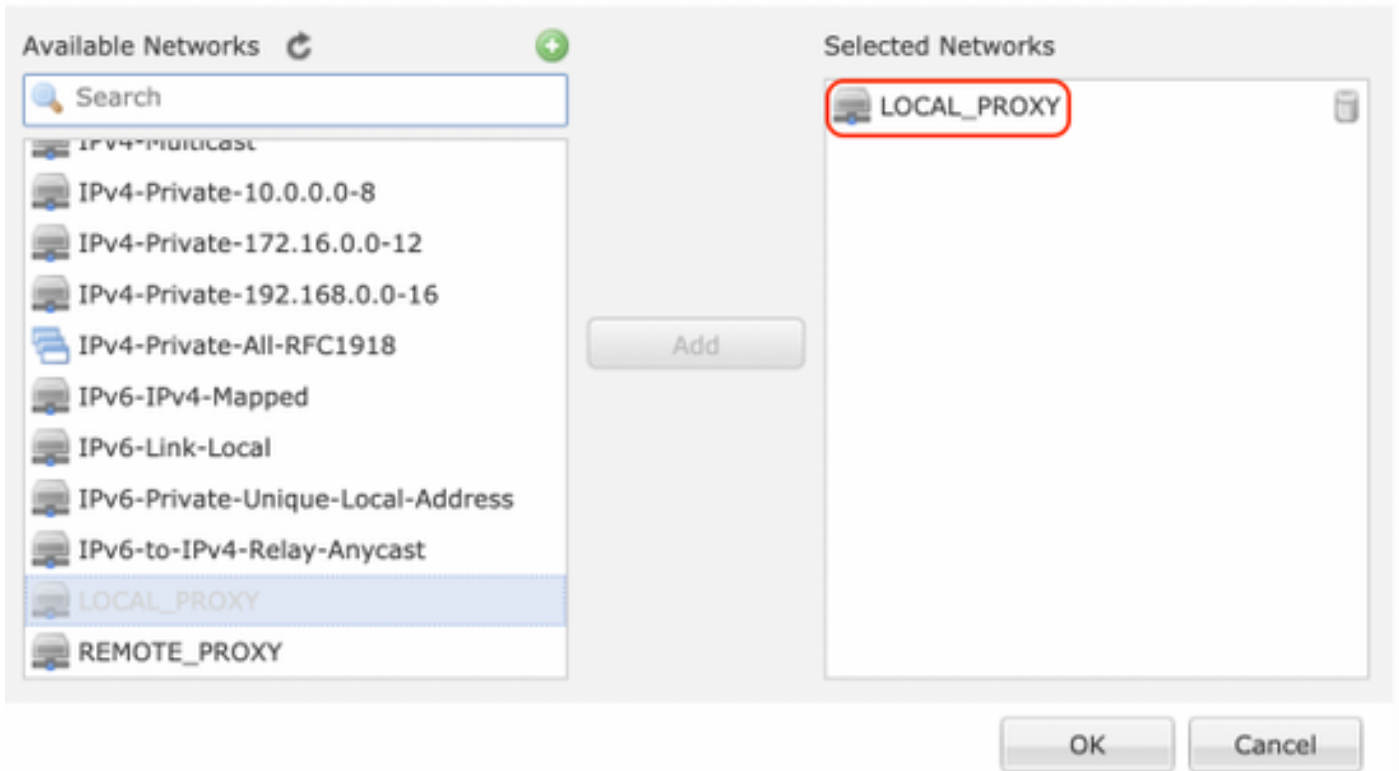


LOCAL_PROXY

OK

Cancel

Network Objects



Con il passo precedente, la configurazione dell'endpoint FTD è completa.

Passaggio 4. Nell'esempio di configurazione, fare clic sul pulsante più verde per il nodo B che è un'ASA. I dispositivi non gestiti dal FMC sono considerati Extranet. Aggiungere un nome di dispositivo e un indirizzo IP.

Passaggio 5. Selezionare il segno più verde per aggiungere le reti protette.

Edit Endpoint ? X


Device:* Extranet

Device Name:* ASA

IP Address:* Static Dynamic
2001:BBBB::1

Certificate Map: +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)

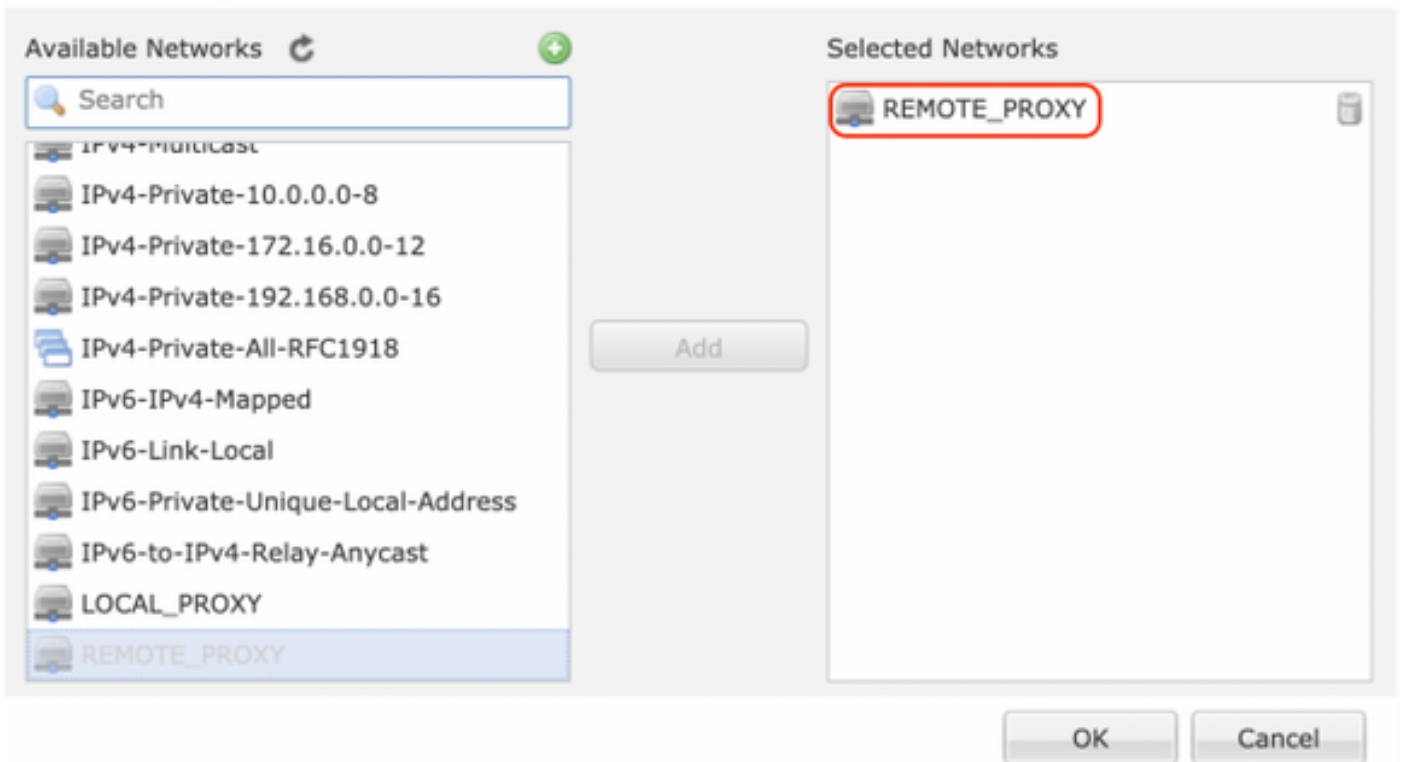
 REMOTE_PROXY +

OK Cancel

Passaggio 6. Selezionare le subnet ASA da cifrare e aggiungerle alle reti selezionate.

In questo esempio, 'Remote Proxy' è la subnet ASA '2001:AAAA::/64'.

Network Objects



Configura parametri IKE

Passaggio 1. Nella scheda IKE specificare i parametri da utilizzare per lo scambio iniziale di IKEv2. Fare clic sul pulsante più verde per creare un nuovo criterio IKE.

Edit VPN Topology



Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policy:* Ikev2_Policy

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

Passaggio 2. Nel nuovo criterio IKE specificare un numero di priorità e la durata della fase 1 della connessione. Questa guida utilizza i seguenti parametri per lo scambio iniziale:

Integrità (SHA256),

Crittografia (AES-256),

PRF (SHA256) e

Gruppo Diffie-Hellman (Gruppo 14).

Tutti i criteri IKE nel dispositivo verranno inviati al peer remoto indipendentemente dal contenuto della sezione criteri selezionata. Il primo corrispondente peer remoto verrà selezionato per la connessione VPN.

[Facoltativo] Scegliere il criterio da inviare per primo utilizzando il campo Priorità. La priorità 1 viene inviata per prima.

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Selected Algorithms

SHA256

Add

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save

Cancel

Edit IKEv2 Policy



Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

Available Algorithms

- MDS
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority:

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

Passaggio 3. Dopo aver aggiunto i parametri, selezionare il criterio configurato in precedenza e scegliere il tipo di autenticazione.

Selezionare l'opzione Chiave manuale già condivisa. Per questa guida viene utilizzata la chiave già condivisa 'cisco123'.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Configura parametri IPSEC

Passaggio 1. Passare alla scheda IPsec e creare una nuova proposta IPsec facendo clic sull'icona a forma di matita per modificare il set di trasformazioni.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Passaggio 2. Creare una nuova proposta IPSec IKEv2 selezionando l'icona più verde e immettendo i parametri della fase 2 come mostrato di seguito:

Hash ESP: SHA-1

Crittografia ESP: AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-256

Add

Selected Algorithms

- AES-256**

Save **Cancel**

Passaggio 3. Dopo aver creato la nuova proposta IPsec, aggiungerla ai set di trasformazioni selezionati.

IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

Passaggio 4. La nuova proposta IPsec selezionata viene ora elencata nelle proposte IPsec IKEv2.

Se necessario, è possibile modificare la durata della fase 2 e l'opzione PFS. In questo esempio, la durata è impostata come predefinita e PFS è disattivato.

Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals tunnel_aes256_sha IKEv2 IPsec Proposals* Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

È necessario configurare i passaggi seguenti per ignorare il controllo di accesso o creare regole dei criteri di controllo di accesso per consentire le subnet VPN tramite FTD.

Ignora controllo di accesso

Se `sysopt allow-vpn` non è abilitato, è necessario creare una policy di controllo dell'accesso per consentire il traffico VPN attraverso il dispositivo FTD. Se `sysopt allow-vpn` è abilitato, ignorare la creazione di criteri di controllo di accesso. In questo esempio di configurazione viene utilizzata l'opzione "Bypass Access Control".

Il parametro `sysopt allow-vpn` può essere abilitato in Advanced > Tunnel.

Attenzione: Questa opzione elimina la possibilità di utilizzare i criteri di controllo di accesso per ispezionare il traffico proveniente dagli utenti. È comunque possibile usare filtri VPN o ACL scaricabili per filtrare il traffico degli utenti. Questo è un comando globale e si applica a tutte le VPN se questa casella di controllo è abilitata.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | **Advanced**

IKE
IPsec
Tunnel

NAT Settings

- Keepalive Messages Traversal
- Interval: Seconds (Range 10 - 3600)

Access Control for VPN Traffic

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

- Use the certificate map configured in the Endpoints to determine the tunnel
- Use the certificate OU field to determine the tunnel
- Use the IKE identity to determine the tunnel
- Use the peer IP address to determine the tunnel

Save **Cancel**

Configura esenzione NAT

Configurare un'istruzione di esenzione NAT per il traffico VPN. L'esenzione NAT deve essere in atto per evitare che il traffico VPN corrisponda a un'altra istruzione NAT e traduca in modo errato il traffico VPN.

Passaggio 1. Passare a **Dispositivi > NAT** e creare un nuovo criterio facendo clic su **Nuovo criterio > Threat Defense NAT**.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Passaggio 2. Fare clic su **Aggiungi regola**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPK QoS Platform Settings FlexConfig Certificates

NAT_Exempt

Enter Description

Show Warnings Show Add Cancel

Policy Assignments (1)

Filter by Device

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

Passaggio 3. Creare una nuova regola NAT manuale statica.

Fare riferimento alle interfacce interne ed esterne per la regola NAT. La specifica delle interfacce nella scheda Oggetti interfaccia impedisce che queste regole influiscano sul traffico proveniente da altre interfacce.

Passare alla scheda Traduzione e selezionare le subnet di origine e di destinazione. Trattandosi di una regola di esenzione NAT, verificare che l'origine/destinazione originale e l'origine/destinazione tradotta siano uguali.

Add NAT Rule



NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Fare clic sulla scheda Avanzate e selezionare **no-proxy-arp** e **route-lookup**.

Add NAT Rule



NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

Salva questa regola e conferma l'istruzione NAT finale nell'elenco NAT.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

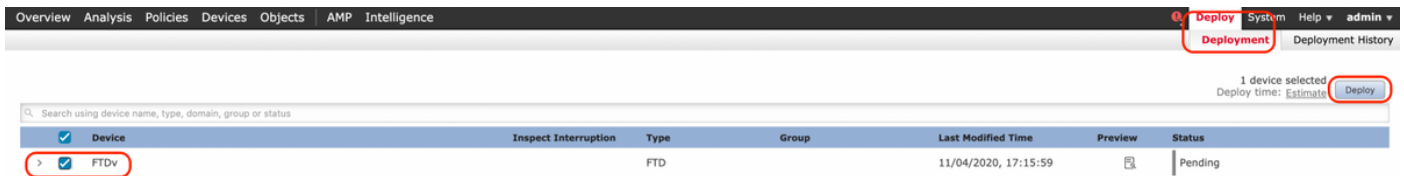
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Passaggio 4. Dopo aver completato la configurazione, salvarla e distribuirla nell'FTD.



Verifica

Inviare il traffico interessante dal computer LAN o è possibile eseguire il comando packet-tracer seguente sull'appliance ASA.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

Nota: Qui Tipo = 128 e Codice=0 rappresenta ICMPv6 "Richiesta echo".

Nella sezione seguente vengono descritti i comandi che è possibile eseguire sulla CLI di ASA v o FTD LINA per controllare lo stato del tunnel IKEv2.

Questo è un esempio di output dell'appliance ASA:

```
ciscoasa# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local                               Remote
          Status                               Role
6638313 2001:bbbb::1/500                       2001:cccc::1/500
          READY    INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
          remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
  Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

Local Addr	: 2001:aaaa::/64/0/0		
Remote Addr	: 2001:dddd::/64/0/0		
Encryption	: AES256	Hashing	: SHA1
Encapsulation	: Tunnel		
Rekey Int (T)	: 28800 Seconds	Rekey Left(T)	: 28400 Seconds
Rekey Int (D)	: 4608000 K-Bytes	Rekey Left(D)	: 4608000 K-Bytes
Idle Time Out	: 30 Minutes	Idle TO Left	: 23 Minutes
Bytes Tx	: 352	Bytes Rx	: 352
Pkts Tx	: 11	Pkts Rx	: 11

Risoluzione dei problemi

Per risolvere i problemi di impostazione del tunnel IKEv2 su ASA e FTD, eseguire i seguenti comandi di debug:

```
debug crypto condition peer <IP peer>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
```

Di seguito è riportato un esempio di utilizzo dei debug IKEv2 come riferimento:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

Riferimenti

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>