

# Configurazione delle interfacce VXLAN su Secure FTD con Secure FMC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurare il gruppo peer VTEP](#)

[Configurare l'interfaccia di origine VTEP](#)

[Configurazione dell'interfaccia VTEP VNI](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come configurare le interfacce VXLAN su Secure Firewall Threat Defense (FTD) con il centro di gestione del firewall sicuro (FMC)

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nozioni base sulle VLAN/VXLAN.
- Conoscenze base di rete.
- Esperienza base di Cisco Secure Management Center.
- Esperienza base di Cisco Secure Firewall Threat Defense.

### Componenti usati

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware con versione 7.2.4.
- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware con versione 7.2.4.

Le informazioni discusse in questo documento fanno riferimento a 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 operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

La VLAN estendibile virtuale (VXLAN) fornisce servizi di rete Ethernet di layer 2 come la VLAN tradizionale. A causa dell'elevata domanda di segmenti VLAN negli ambienti virtuali, VXLAN offre maggiore estensibilità, flessibilità e definisce anche uno schema di incapsulamento MAC-in-UDP in cui il frame di layer 2 originale ha un'intestazione VXLAN aggiunta e viene quindi posizionato in un pacchetto UDP-IP. Con questo incapsulamento MAC-in-UDP, la VXLAN esegue il tunnel della rete di layer 2 sulla rete di layer 3. VXLAN offre i seguenti vantaggi:

- Flessibilità VLAN in segmenti multi-tenant:
- Maggiore scalabilità per gestire più segmenti di layer 2 (L2).
- Migliore utilizzo della rete.

Cisco Secure Firewall Threat Defense (FTD) supporta due tipi di incapsulamento VXLAN.

- VXLAN (utilizzata per tutti i modelli Secure Firewall Threat Defense)
- Geneve (utilizzata per appliance virtuale Secure Firewall Threat Defense)

L'incapsulamento Geneve è richiesto per il routing trasparente dei pacchetti tra il bilanciamento del carico del gateway di Amazon Web Services (AWS) e le appliance e per l'invio di informazioni aggiuntive.

VXLAN utilizza il VTEP (VXLAN Tunnel Endpoint) per mappare i dispositivi terminali dei tenant ai segmenti VXLAN e per eseguire l'incapsulamento e la decapsulamento VXLAN. Ogni VTEP ha due tipi di interfaccia: una o più interfacce virtuali chiamate VXLAN Network Identifier (VNI) dove possono essere applicati i criteri di sicurezza e un'interfaccia regolare chiamata VTEP source interface dove le interfacce VNI sono tunneling tra i VTEP. L'interfaccia di origine VTEP è collegata alla rete IP di trasporto per la comunicazione VTEP-VTEP, le interfacce VNI sono simili alle interfacce VLAN: sono interfacce virtuali che mantengono il traffico di rete separato su una determinata interfaccia fisica utilizzando la codifica. I criteri di sicurezza vengono applicati a ciascuna interfaccia VNI. È possibile aggiungere un'interfaccia VTEP e tutte le interfacce VNI sono associate alla stessa interfaccia VTEP. Esiste un'eccezione per il clustering virtuale di difesa dalle minacce in AWS.

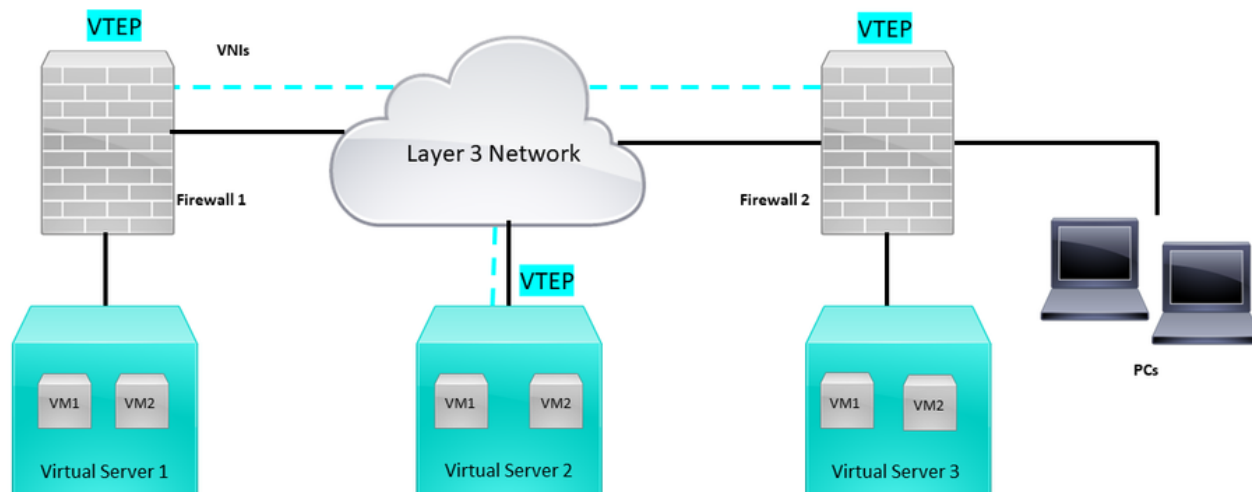
Ci sono tre modi in cui la difesa dalla minaccia incapsula e decapsula:

- È possibile configurare staticamente un singolo indirizzo IP VTEP peer sulla difesa dalle minacce.
- Un gruppo di indirizzi IP VTEP peer può essere configurato staticamente sulla difesa dalle minacce.
- È possibile configurare un gruppo multicast su ciascuna interfaccia VNI.

Questo documento si focalizza sulle interfacce VXLAN per l'incapsulamento VXLAN con un

gruppo di 2 indirizzi IP VTEP peer configurati staticamente. Se è necessario configurare le interfacce Geve, controllare la documentazione ufficiale per [le interfacce Geve](#) in AWS o configurare il VTEP con un singolo peer o gruppo multicast, controllare l'interfaccia VTEP con una guida alla configurazione di un [singolo peer o gruppo multicast](#).

## Esempio di rete



Topologia della rete

Nella sezione Configura si presume che la rete sottostante sia già configurata per la difesa dalle minacce tramite il centro di gestione del firewall protetto. Questo documento ha per oggetto la configurazione della rete di sovrapposizione.

## Configurazione

### Configurare il gruppo peer VTEP

Passo 1: passare a Oggetti > Gestione oggetti.

Objects

Integration

Object Management

Intrusion Rules

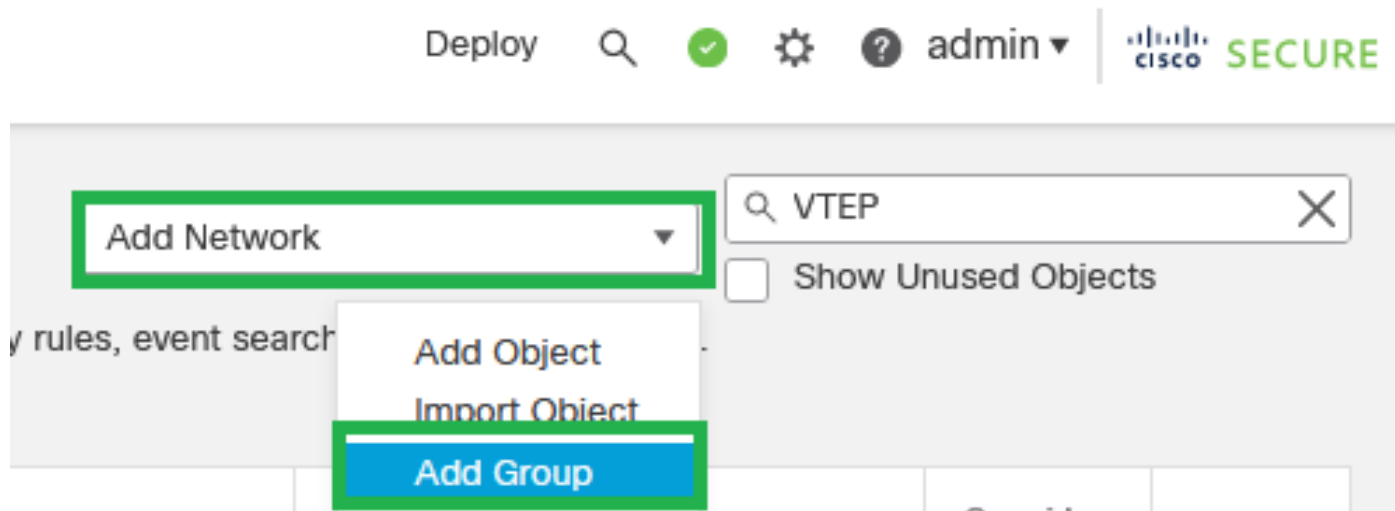
Oggetti - Gestione oggetti

2. Fare clic su Network (Rete) nel menu a sinistra.

- > AAA Server
- > Access List
- > Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- > Community List
- > Distinguished Name
- DNS Server Group
- > External Attributes
- File List
- > FlexConfig

: configurare più oggetti di rete host per ogni indirizzo IP peer VTEP disponibile. Nella presente guida alla configurazione sono presenti due oggetti.

Passo 5: creazione del gruppo di oggetti, fare clic su Aggiungi rete > Aggiungi gruppo.



Aggiungi rete - Aggiungi gruppo

Passaggio 6: Creare il gruppo di oggetti di rete con tutti gli indirizzi IP peer VTEP. Impostare il nome di un gruppo di rete e selezionare i gruppi di oggetti di rete richiesti, quindi fare clic su Salva.

# New Network Group



Name

FPR1-VTEP-Group-Object

Description

This is a network group with VTEP group peer IP addresses

Allow Overrides

Available Networks



Search

3-VTEP-172.16.207.1  
FPR1-GW-172.16.203.3  
FPR1-VTEP-Group-Object  
FPR2-GW-172.16.205.3  
**FPR2-VTEP-172.16.205.1**  
FTD1-GW1-172.16.203.2

Add

Selected Networks

Search by name

3-VTEP-172.16.207.1  
FPR2-VTEP-172.16.205.1

Add

Cancel

Save

Crea gruppo di oggetti di rete

Passaggio 7: Convalidare l'oggetto di rete e il gruppo di oggetti di rete dal filtro Oggetto di rete.

Network Add Network

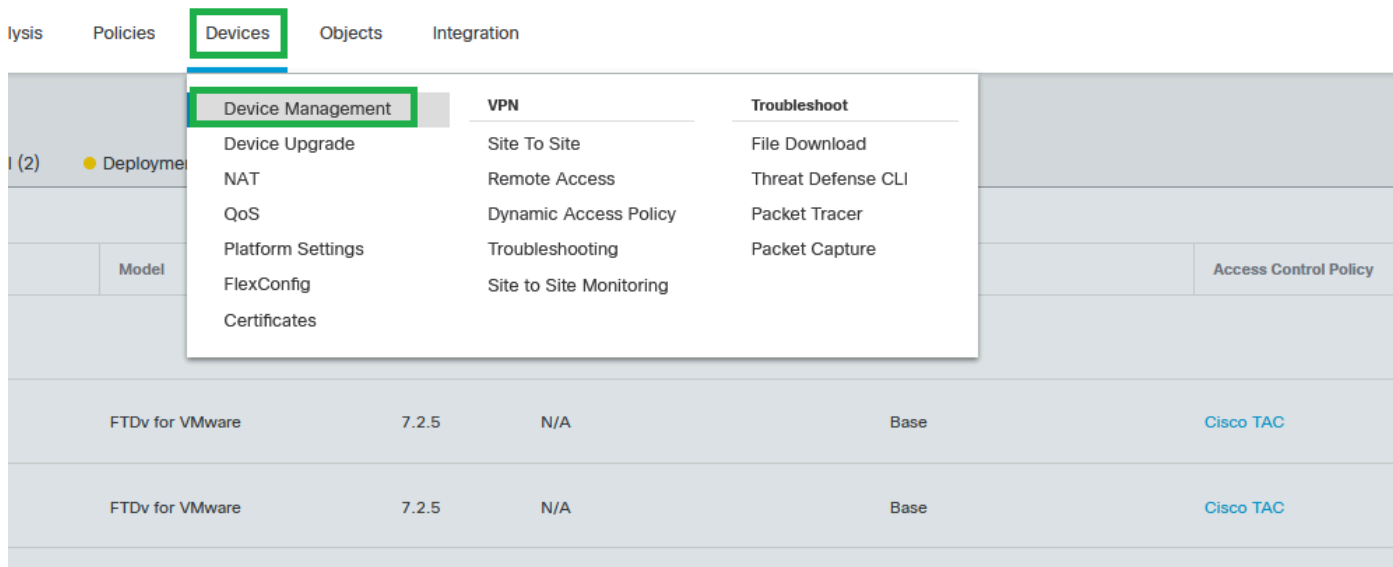
A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override	
3-VTEP-172.16.207.1	172.16.207.1	Host		
FPR1-VTEP-Group-Object	3-VTEP-172.16.207.1 FPR2-VTEP-172.16.205.1	Group		
FPR2-VTEP-172.16.205.1	172.16.205.1	Host		

Convalida il gruppo di oggetti VTEP

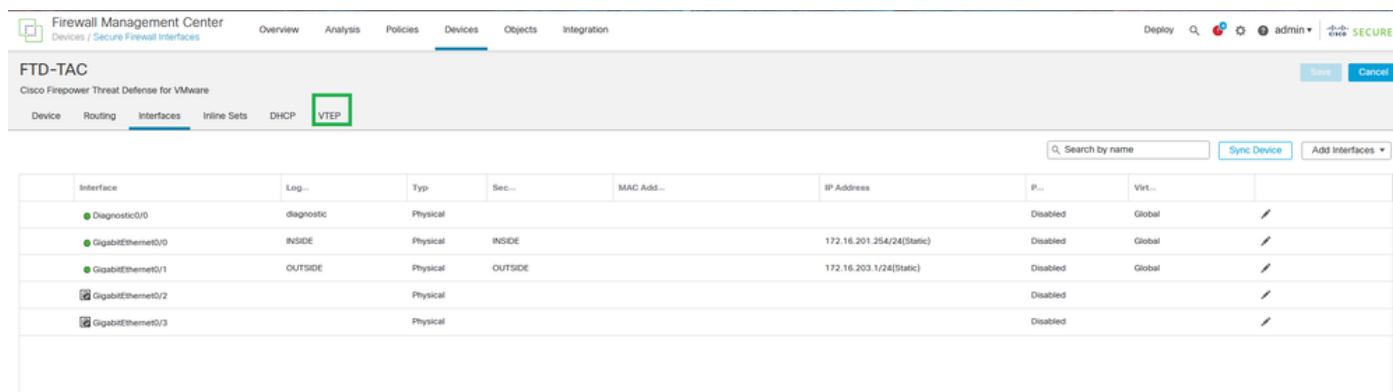
# Configurare l'interfaccia di origine VTEP

Passaggio 1: Passare a Dispositivi > Gestione dispositivi e modificare la difesa dalle minacce.



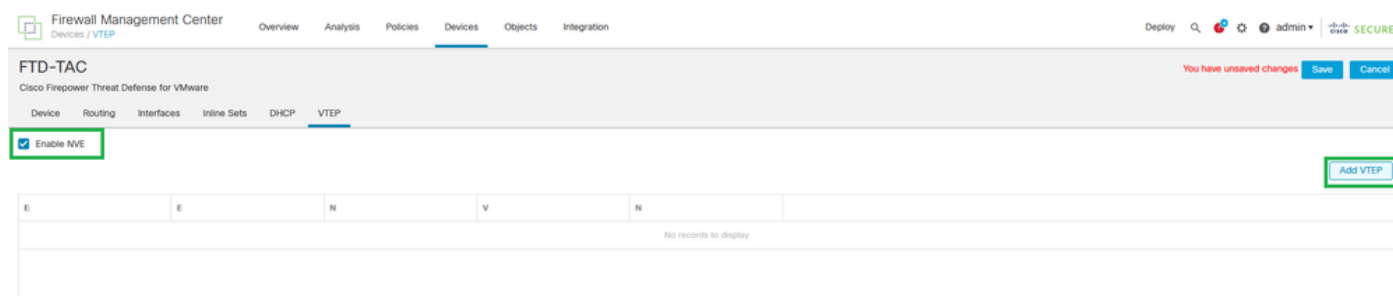
Dispositivi - Gestione dispositivi

Passaggio 2: passare alla sezione VTEP.



Sezione VTEP

Passaggio 3: Selezionare la casella di controllo Abilita VNE e fare clic su Add VTEP.



Abilitare NVE e aggiungere VTEP

Passaggio 4: Scegliere VxLAN come tipo di incapsulamento, immettere il valore di Porta di incapsulamento e scegliere l'interfaccia utilizzata per l'origine VTEP su questa difesa contro le



minacce (interfaccia esterna per questa guida alla configurazione)

## Add VTEP



Encapsulation type  
VxLAN

Encapsulation port\*  
4789 (1024 - 65535)

NVE number  
1


VTEP Source Interface  
OUTSIDE

Neighbor Address  
 None  Peer VTEP  Peer Group  Default Multicast

Cancel

OK

Aggiungi VTEP

 Nota: l'incapsulamento VxLAN è quello predefinito. Per AWS, è possibile scegliere tra VxLAN e Geneve. Il valore predefinito è 4789, quindi è possibile scegliere una porta di incapsulamento tra 1024 e 65535 in base alla progettazione.

Passaggio 5: selezionare Peer Group (Gruppo peer), scegliere il Network Object Group (Gruppo oggetti di rete) creato nella sezione di configurazione precedente, quindi fare clic su OK.

## Add VTEP



### Encapsulation type

VxLAN

### Encapsulation port\*

4789

(1024 - 65535)

### NVE number

1

### VTEP Source Interface

OUTSIDE

### Neighbor Address

None  Peer VTEP  Peer Group  Default Multicast

### Network Group\*

FPR1-VTEP-Group-Object

Cancel

OK

Gruppo peer - Gruppo oggetti di rete

Passaggio 6: salvare le modifiche.



Avviso: dopo il salvataggio delle modifiche, viene visualizzato il messaggio di modifica del frame jumbo. L'MTU viene modificata sull'interfaccia assegnata come VTEP su 1554, quindi accertarsi di usare la stessa MTU sulla rete sottostante.

Passaggio 7: fare clic su Interfacce e modificare l'interfaccia utilizzata per l'interfaccia di origine VTEP. (Interfaccia esterna su questa guida alla configurazione)

FTD-TAC  
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

Interface	Log...	Typ	Sec...	MAC Add...	IP Address	P...	Virt...	
Diagnostic0/0	diagnostic	Physical				Disabled	Global	/
GigabitEthernet0/0	INSIDE	Physical	INSIDE		172.16.201.254/24(Static)	Disabled	Global	/
GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE		172.16.203.1/24(Static)	Disabled	Global	/
GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		/

Esterno come interfaccia di origine VTEP

Passaggio 8 (Facoltativo): nella pagina Generale, selezionare la casella di controllo Solo NVE, quindi fare clic su OK.

## Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Name:

OUTSIDE

Enabled

Management Only

Description:

Mode:

None

Security Zone:

OUTSIDE

Interface ID:

GigabitEthernet0/1

MTU:

1554

(64 - 9000)

Priority:

0

(0 - 65535)

Propagate Security Group Tag:

NVE Only:



Cancel

OK

Configurazione solo NVE



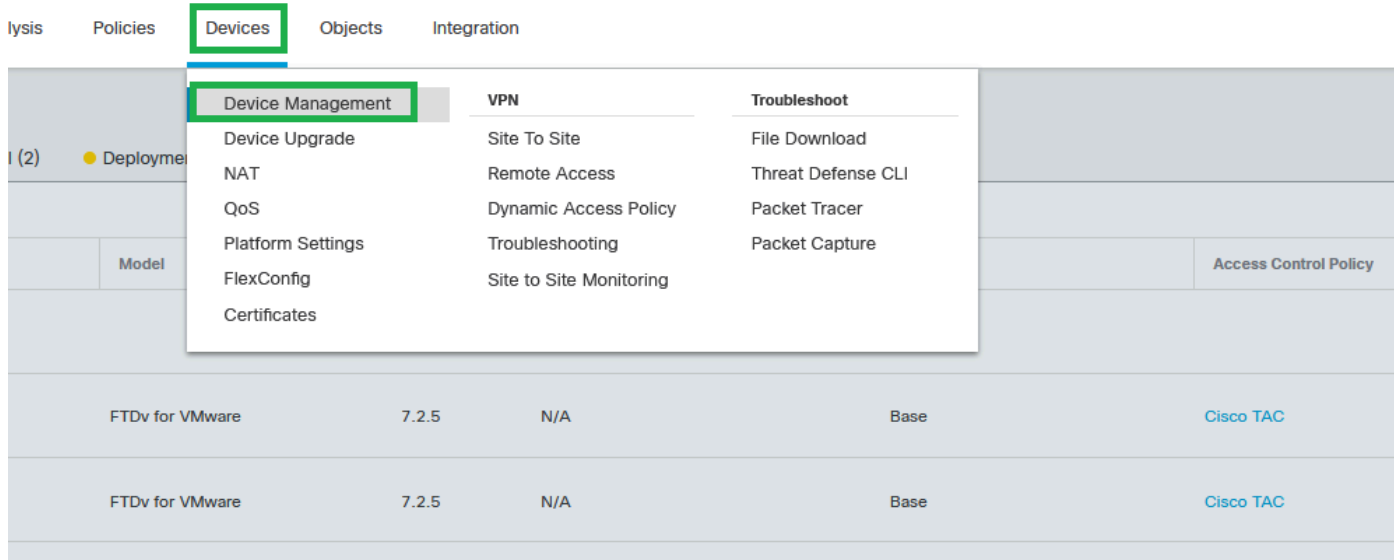
Avviso: questa impostazione è facoltativa per la modalità di routing, in cui limita il traffico alla VXLAN e il traffico di gestione comune solo su questa interfaccia. Questa impostazione viene attivata automaticamente per la modalità firewall trasparente.

---

Passaggio 9: Salvare le modifiche.

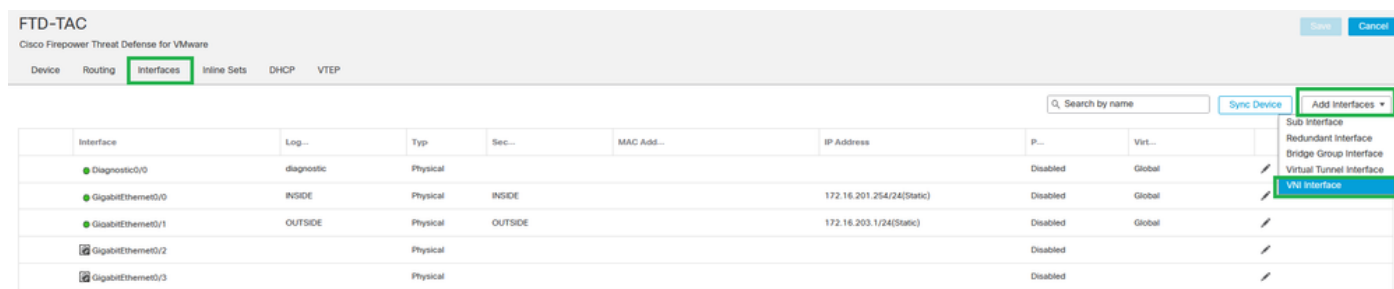
## Configurazione dell'interfaccia VTEP VNI

Passo 1: Navigare Dispositivi > Gestione dispositivi, e modificare la difesa della minaccia.



Dispositivi - Gestione dispositivi

Passaggio 2: Sotto la sezione Interfacce, fare clic su Add Interfaces > VNI Interfaces.



Interfacce - Aggiungi interfacce - Interfacce VNI

Passaggio 3: nella sezione Generale, impostare l'interfaccia VNI con nome, descrizione, area di sicurezza, ID VNI e ID segmento VNI.

## Add VNI Interface



General

IPv4

IPv6

Advanced

Name:

VNI-1

Enabled

Description:

Security Zone:

VNI-1

Priority:

0

(0 - 65535)

VNI ID\*:

100

(1 - 10000)

VNI Segment ID:

10001

(1 - 10777215)

Multicast Group IP

Address:

NVE Mapped to

VTEP Interface:

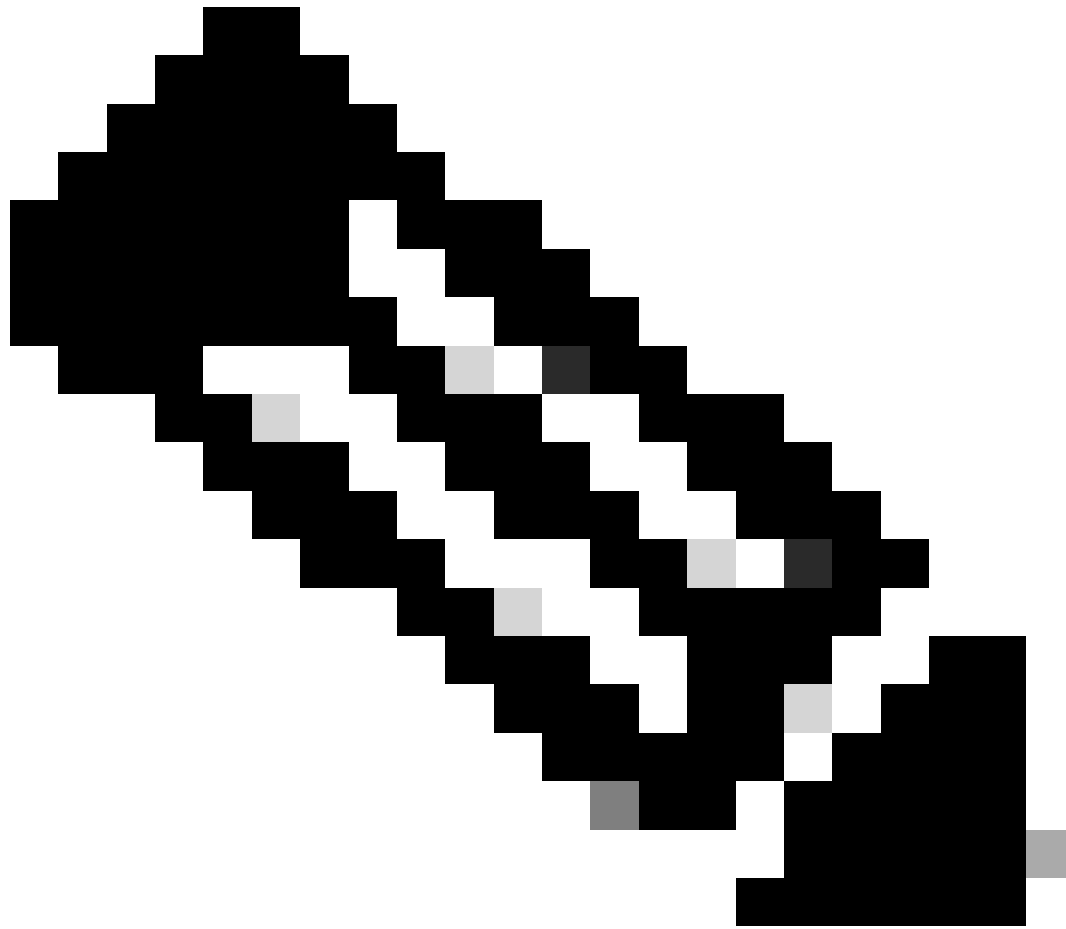
NVE Number:

1

Cancel

OK

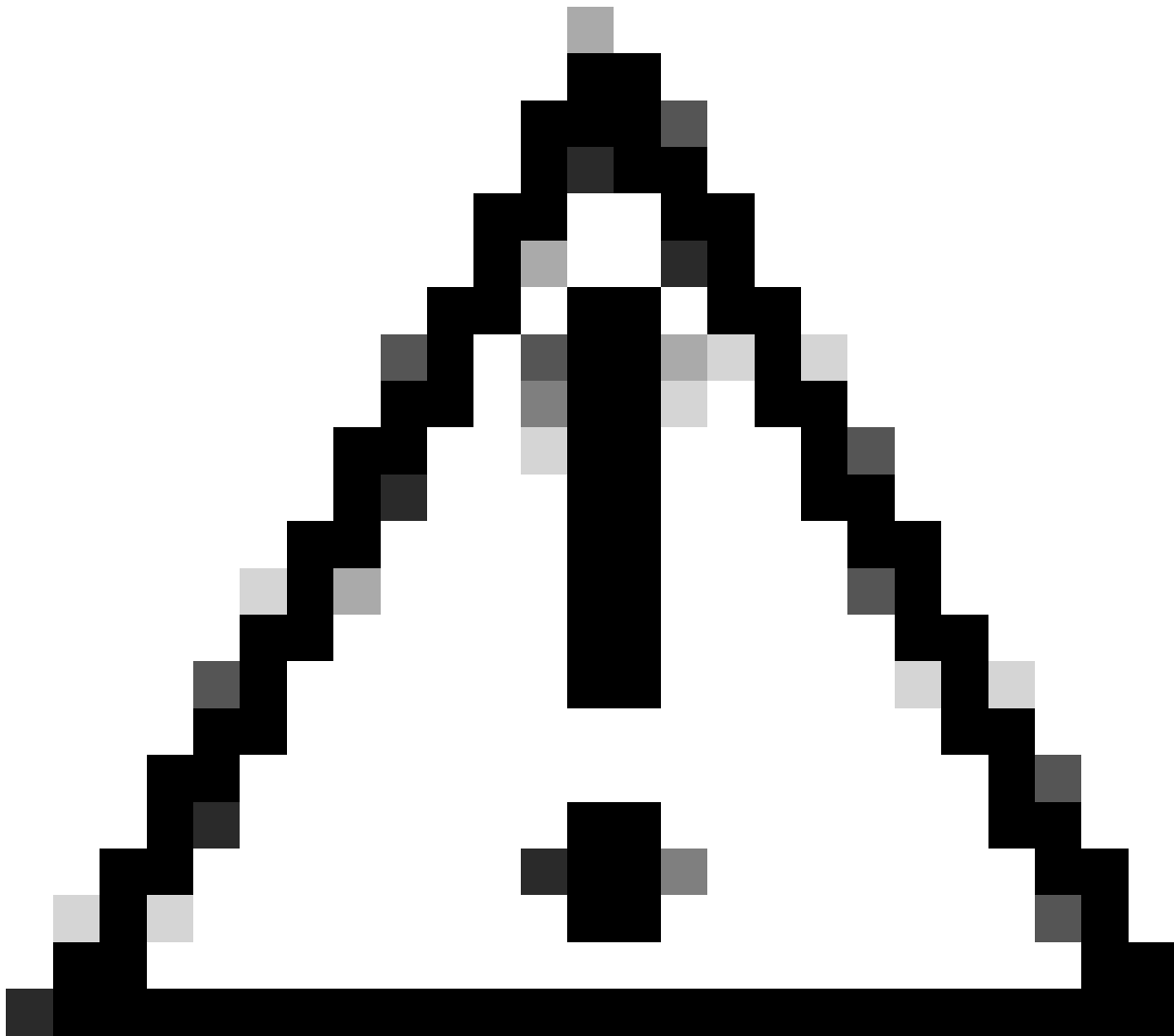
Add VNI Interface (Aggiungi interfaccia VNI)



Nota: l'ID VNI è configurato tra 1 e 10000 e l'ID segmento VNI è configurato tra 1 e 16777215 (l'ID segmento viene utilizzato per il tagging VXLAN).

---





Attenzione: se il gruppo multicast non è configurato sull'interfaccia VNI, viene utilizzato il gruppo predefinito della configurazione dell'interfaccia di origine VTEP, se disponibile. Se si imposta manualmente un IP peer VTEP per l'interfaccia di origine VTEP, non è possibile specificare un gruppo multicast per l'interfaccia VNI.

---

Passaggio 3: selezionare la casella di controllo NVE mappato sull'interfaccia VTEP e fare clic su OK.

## Add VNI Interface



General

IPv4

IPv6

Advanced

Name:

VNI-1

Enabled

Description:

Security Zone:

VNI-1

Priority:

0

(0 - 65535)

VNI ID\*:

100

(1 - 10000)

VNI Segment ID:

10001

(1 - 16777215)

Multicast Group IP

Address:

NVE Mapped to  
VTEP Interface:



NVE Number:

Cancel

OK

NVE mappato sull'interfaccia VTEP

Passaggio 4: Configurare una route statica per annunciare le reti di destinazione per la VXLAN all'interfaccia peer VNI. Selezionare Ciclo > Ciclo statico.

Firewall Management Center  
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

**FTD-TAC** Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

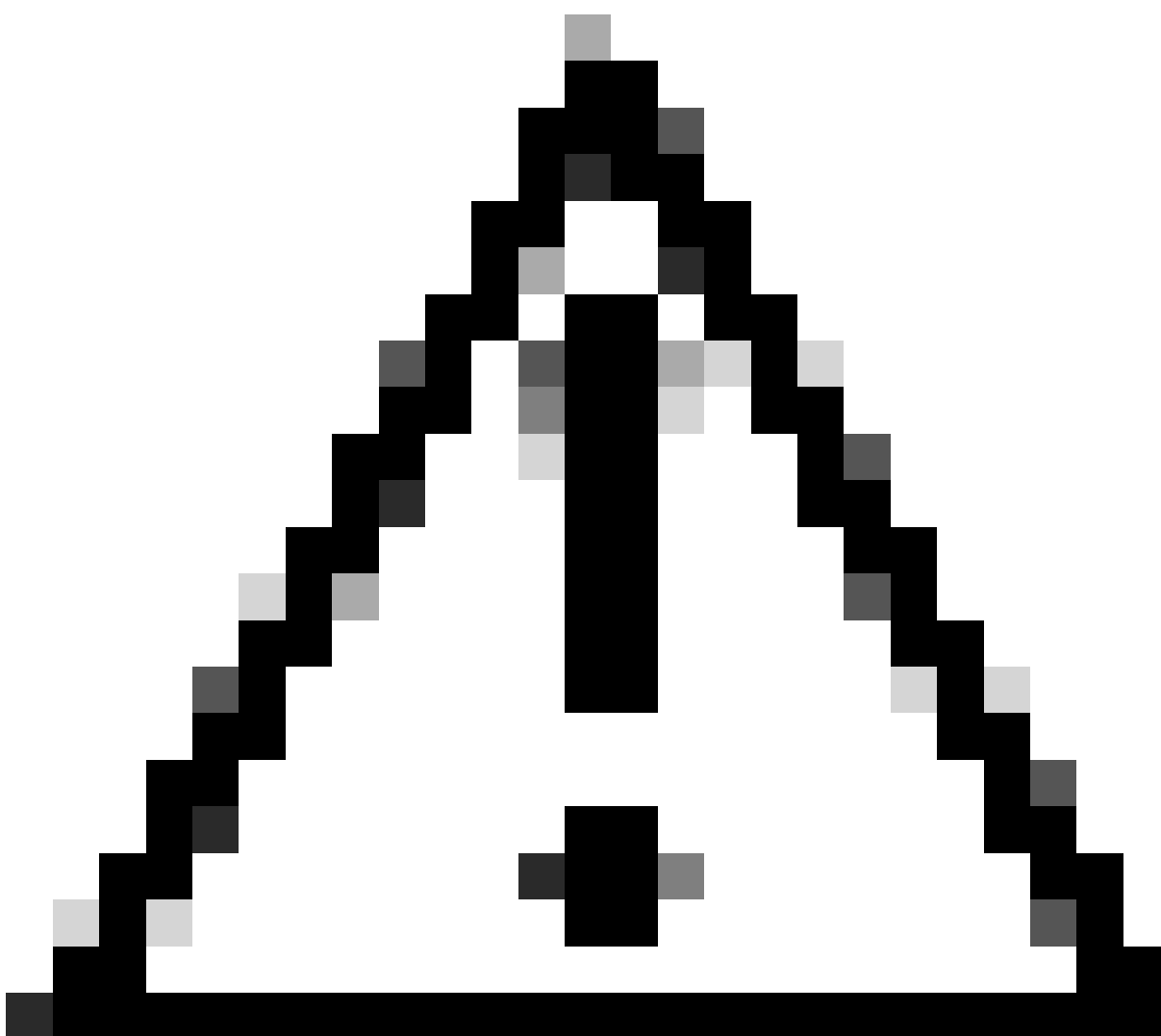
Global

Virtual Router Properties

- ECMP
- OSPF
- OSPFV3
- EIGRP
- RIP
- Policy Based Routing
- BGP
  - IPv4
  - IPv6
- Static Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
FPR2-INSIDE-172.16.212.0-24	VNI-1	Global	FPR2-VNI-IP-172.16.209.2	false	1	
any-ipv4	OUTSIDE	Global	FPR1-GW-172.16.203.3	false	10	
IPv6 Routes						

Configurazione route statica



Attenzione: le reti di destinazione per la VXLAN devono essere inviate tramite l'interfaccia VNI del peer. Tutte le interfacce VNI devono trovarsi sullo stesso dominio di trasmissione (segmento logico).

Passaggio 5: Salvare e distribuire le modifiche.



Avviso: gli avvisi di convalida possono essere visualizzati prima della distribuzione.  
Verificare che gli indirizzi IP peer VTEP siano raggiungibili dall'interfaccia di origine VTEP fisica.

---

## Verifica

Verificare la configurazione NVE.

```
firepower# show running-config nve
nve 1
encapsulation vxlan
source-interface OUTSIDE
peer-group FPR1-VTEP-Group-Object
```

```
firepower# show nve 1
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
IP address 172.16.203.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
1309 packets input, 128170 bytes
2009 packets output, 230006 bytes
142 packets dropped
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Configured static peer group VTEPs:
IP address 172.16.205.1 MAC address 0050.56b3.c30a (learned)
IP address 172.16.207.1 MAC address 0050.56b3.c30a (learned)
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 172.16.205.1
IP address 172.16.207.1
Number of VNIs attached to nve 1: 1
VNIs attached:
vni 100: proxy off, segment-id 10001, mcast-group none
NVE proxy single-arm channel is off.
```

```
firepower# show nve 1 summary
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Number of discovered peer VTEPs: 2
Number of VNIs attached to nve 1: 1
NVE proxy single-arm channel is off.
```

Verificare la configurazione dell'interfaccia VNI.

```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

Verificare la configurazione MTU sull'interfaccia VTEP.

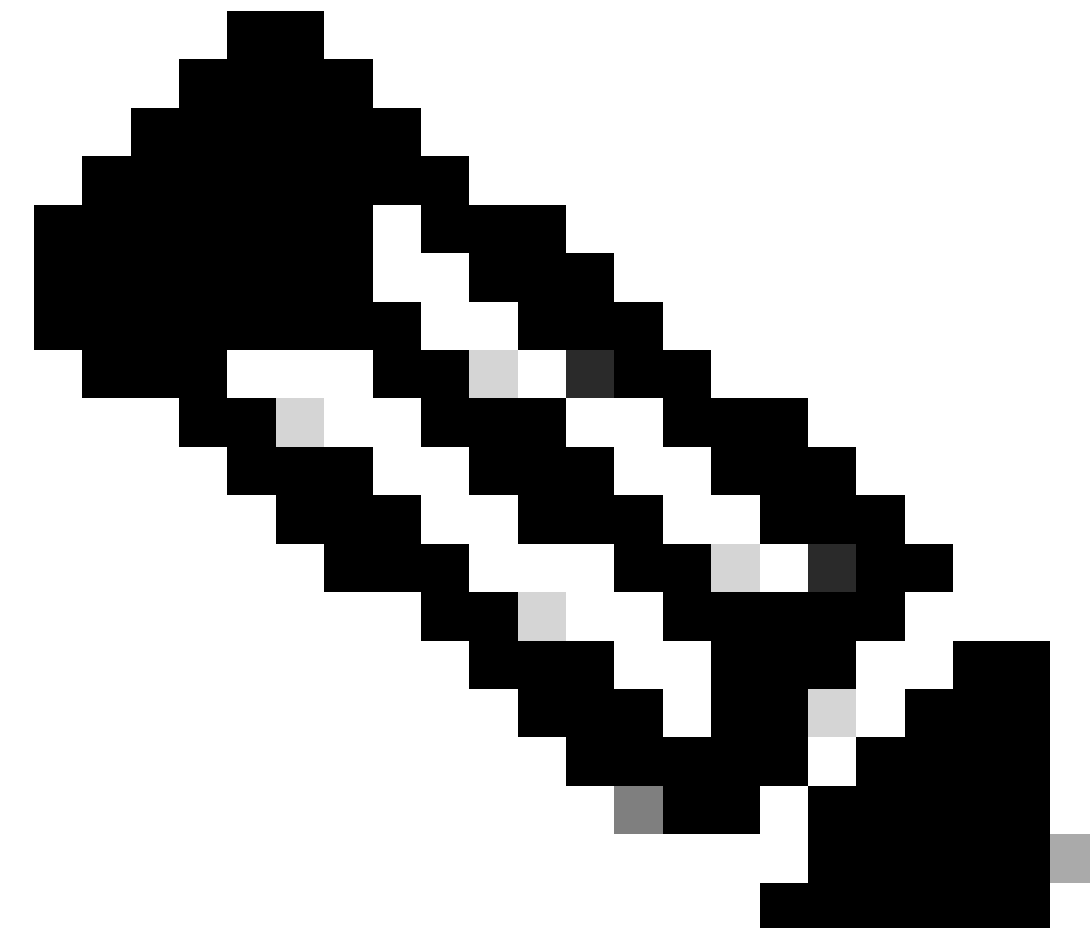
```
firepower# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0050.56b3.26b8, MTU 1554
IP address 172.16.203.1, subnet mask 255.255.255.0
```

---  
[Output omitted]  
---

Verificare la configurazione della route statica per le reti di destinazione.

```
firepower# show run route  
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.203.3 10  
route VNI-1 172.16.212.0 255.255.255.0 172.16.209.2 1  
route VNI-1 172.16.215.0 255.255.255.0 172.16.209.3 1
```

---



Nota: verificare che le interfacce VNI su tutti i peer siano configurate sullo stesso dominio di broadcast.

---

# Risoluzione dei problemi

Verificare la connettività con i peer VTEP.

Peer 1:

```
firepower# ping 172.16.205.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.205.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Peer 2:

```
firepower# ping 172.16.207.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.207.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



Nota: un problema di connettività peer VTEP può generare errori di distribuzione in Secure FMC. Assicurarsi di mantenere la connettività a tutte le configurazioni peer VTEP.

---

Verificare la connettività con i peer VNI.

.

Peer 1:

```
firepower# ping 172.16.209.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Peer 2:



```
firepower# ping 172.16.209.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

A volte, una route statica errata può generare output incompleti ARP. Configurare un'acquisizione sull'interfaccia VTEP per i pacchetti VXLAN e scaricarla in un formato pcap, uno strumento di analisi dei pacchetti aiuta a verificare se ci sono problemi con le route. Assicurarsi di utilizzare l'indirizzo IP peer VNI come gateway.

Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1

### Problema di routing

Configurare le acquisizioni drop ASP su FTD protetto in caso di perdita del firewall, controllare il contatore drop ASP con il comando show asp drop. Contattare Cisco TAC per l'analisi.

Verificare di aver configurato le regole dei criteri di controllo dell'accesso per consentire il traffico UDP VXLAN sull'interfaccia VNI/VTEP.

A volte i pacchetti VXLAN possono essere frammentati, accertarsi di modificare l'MTU in frame jumbo sulla rete sottostante per evitare la frammentazione.

Configurate l'acquisizione sull'interfaccia Ingress/VTEP e scaricate le acquisizioni in formato .pcap per l'analisi. I pacchetti devono includere l'intestazione VXLAN sull'interfaccia VTEP,

1	2023-10-01 17:10:31.039823	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3285/54540, ttl=64 (reply in 2)
2	2023-10-01 17:10:31.041593	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3285/54540, ttl=128 (request in 1)
3	2023-10-01 17:10:32.042127	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3286/54796, ttl=64 (reply in 4)
4	2023-10-01 17:10:32.043698	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3286/54796, ttl=128 (request in 3)
5	2023-10-01 17:10:33.044171	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3287/55052, ttl=64 (reply in 6)
6	2023-10-01 17:10:33.046140	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3287/55052, ttl=128 (request in 5)
7	2023-10-01 17:10:34.044797	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3288/55308, ttl=64 (reply in 8)
8	2023-10-01 17:10:34.046430	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3288/55308, ttl=128 (request in 7)
9	2023-10-01 17:10:35.046903	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3289/55564, ttl=64 (reply in 10)
10	2023-10-01 17:10:35.049527	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3289/55564, ttl=128 (request in 9)
11	2023-10-01 17:10:36.048352	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3290/55820, ttl=64 (reply in 12)
12	2023-10-01 17:10:36.049832	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3290/55820, ttl=128 (request in 11)
13	2023-10-01 17:10:37.049786	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request	id=0x0032, seq=3291/56076, ttl=64 (reply in 14)
14	2023-10-01 17:10:37.051465	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply	id=0x0032, seq=3291/56076, ttl=128 (request in 13)

### Ping eseguito con intestazione VXLAN

```
> Frame 0: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Ethernet II, Src: Whare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Whare_b3:6e:68 (00:50:56:b3:6e:68)
> Internet Protocol Version 4, Src: 172.16.209.1, Dst: 172.16.209.1
> User Datagram Protocol, Src Port: 61587, Dst Port: 4789
Virtual extensible Local Area Network
  Flags: 0x0000, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 10001
    Reserved: 0
  Ethernet II, Src: Whare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Whare_b3:26:b8 (00:50:56:b3:26:b8)
    Destination: Whare_b3:26:b8 (00:50:56:b3:26:b8)
    Source: Whare_b3:ba:6a (00:50:56:b3:ba:6a)
  Type: IPv4 (0x0000)
  Internet Protocol Version 4, Src: 172.16.212.2, Dst: 172.16.201.1
  Internet Control Message Protocol
```

### Intestazione VXLAN

## Informazioni correlate

- [Configurazione delle interfacce VXLAN](#)
- [Casi di utilizzo di VXLAN](#)
- [Elaborazione pacchetti VXLAN](#)
- [Configurazione dell'interfaccia di origine VTEP](#)
- [Configurazione dell'interfaccia VNI](#)
- [Supporto tecnico Cisco e download](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).