

Configurare PBR con Monitoraggio percorso HTTP in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurare PBR per il monitoraggio del percorso HTTP](#)

[Configurazione di Equal-cost-multi-path \(ECMP\)](#)

[Configura DNS trusted per FTD protetto](#)

[Abilita monitoraggio percorso](#)

[Aggiungi dashboard di controllo](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Policy-Based Routing (PBR) con monitoraggio dei percorsi HTTP su Cisco Secure Firewall Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base PBR
- Esperienza base di Cisco Secure Management Center
- Cisco Secure Firewall Threat Defense (FTD) di base

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 7.4

- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware con versione 7.4

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

Nel routing tradizionale, i pacchetti vengono instradati in base all'indirizzo IP di destinazione. Tuttavia, è difficile modificare il routing di un traffico che specifica un sistema di routing basato sulla destinazione. PBR offre un maggiore controllo sul routing estendendo e integrando i meccanismi esistenti forniti dai protocolli di routing.

PBR consente di impostare la precedenza IP. Consente inoltre di specificare un percorso per determinati traffici, ad esempio traffico prioritario su un collegamento ad alto costo. Con PBR, il routing si basa su criteri diversi dalla rete di destinazione, ad esempio la porta di origine, l'indirizzo di destinazione, la porta di destinazione, le applicazioni di protocollo o una combinazione di questi oggetti. PBR può essere utilizzato per classificare il traffico di rete in base all'applicazione, al nome utente, all'appartenenza ai gruppi e all'associazione dei gruppi di sicurezza. Questo metodo di routing è applicabile in situazioni in cui numerosi dispositivi accedono ad applicazioni e dati in un'installazione di rete di grandi dimensioni. In genere, le implementazioni di grandi dimensioni dispongono di topologie che eseguono il backhaul di tutto il traffico di rete verso un hub come traffico crittografato in una VPN basata su routing. Queste topologie spesso causano problemi come la latenza dei pacchetti, la larghezza di banda ridotta e la perdita dei pacchetti.

Il PBR è supportato solo nella modalità firewall instradato e non viene applicato alle connessioni embryo-sincrone. L'applicazione basata su HTTP è supportata sulle interfacce fisiche, del canale della porta, sulle sottointerfacce e sulle interfacce del tunnel di stato. Non è supportato nei dispositivi cluster.

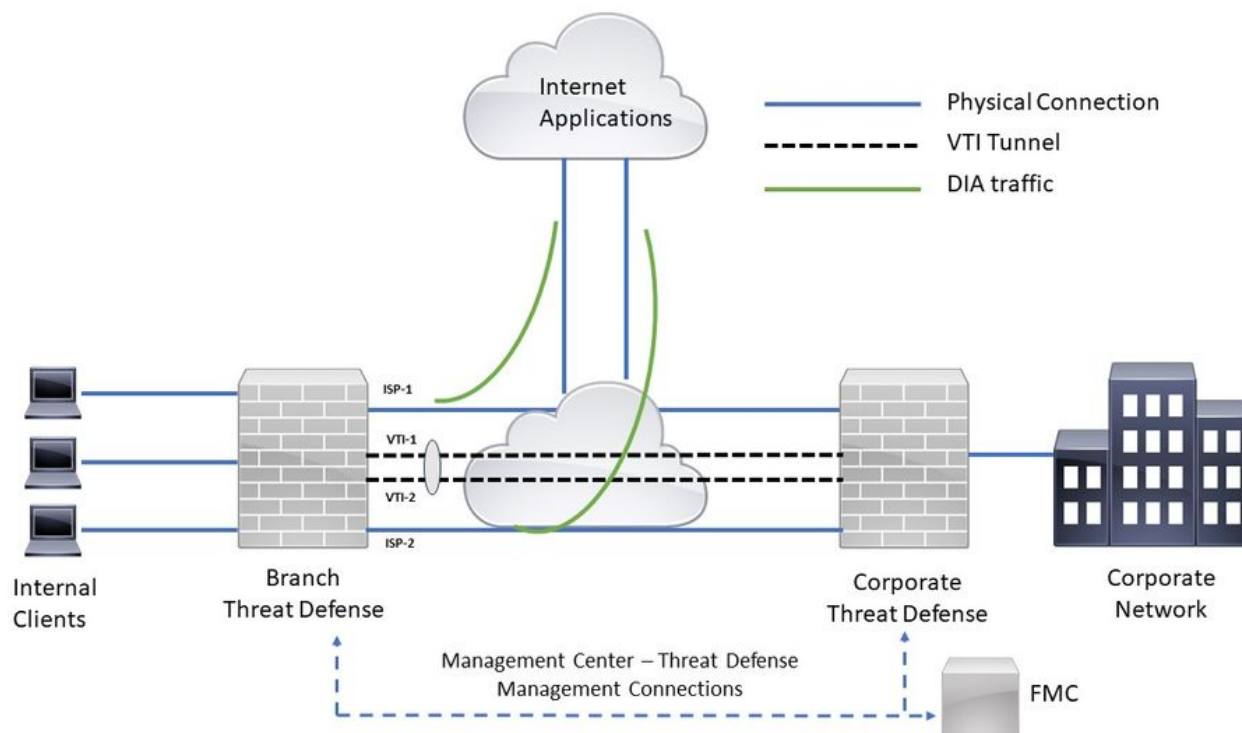
Quando le interfacce configurate derivano metriche come il tempo di andata e ritorno (RTT), lo jitter, il punteggio medio (MOS) e la perdita di pacchetti per interfaccia, vengono usate per determinare il percorso migliore per il routing del traffico PBR. Il monitoraggio dei percorsi calcola metriche flessibili per più peer remoti per interfaccia. Per monitorare e determinare il miglior percorso per più applicazioni attraverso una policy su un firewall di diramazione, il protocollo HTTP è preferito al protocollo ICMP per i seguenti motivi:

- Il ping HTTP può derivare le metriche delle prestazioni del percorso fino al livello dell'applicazione del server, in cui è ospitata l'applicazione.
- La necessità di modificare la configurazione del firewall ogni volta che l'indirizzo IP del server applicazioni viene modificato viene rimossa quando si tiene traccia del dominio applicazione anziché dell'indirizzo IP.

Configurazione

Esempio di rete

Si consideri uno scenario tipico di rete aziendale in cui tutto il traffico di rete della filiale viene inviato tramite una VPN basata su route della rete aziendale e diverge verso la rete Extranet quando è necessario. Nella topologia successiva viene illustrata una rete di filiali connessa alla rete aziendale tramite una VPN basata su route. In genere, la protezione contro le minacce aziendali è configurata per gestire sia il traffico interno che il traffico esterno della succursale. Con il criterio PBR, la difesa dalle minacce di diramazione è configurata con un criterio che instrada il traffico specifico verso la rete WAN anziché verso i tunnel virtuali. Il resto del traffico passa attraverso la VPN basata su route, come al solito.



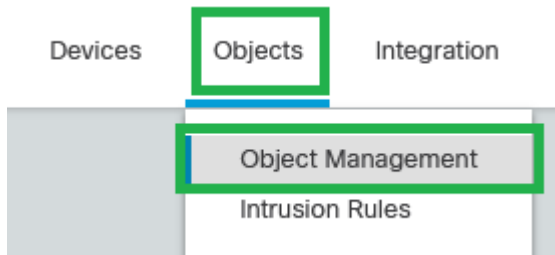
Topologia della rete

Nella sezione Configura si presume che le interfacce ISP e VTI siano già configurate per la difesa dalle minacce di branch nella console centrale protetta.

Configurare PBR per il monitoraggio del percorso HTTP

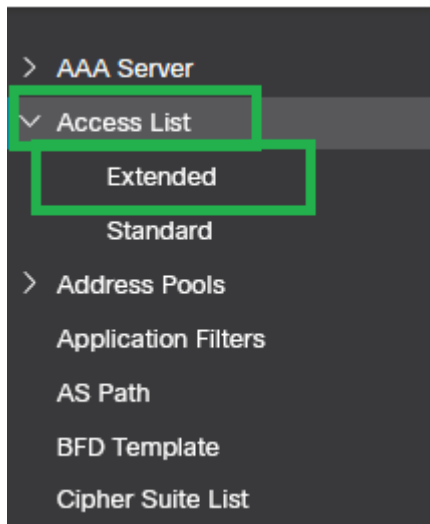
In questa sezione di configurazione viene illustrata la configurazione di Path Monitoring sulle interfacce ISP-1 e ISP-2.

Passaggio 1. Creare un elenco degli accessi estesi per le applicazioni controllate. Passare a [Objects](#) > Object Management.



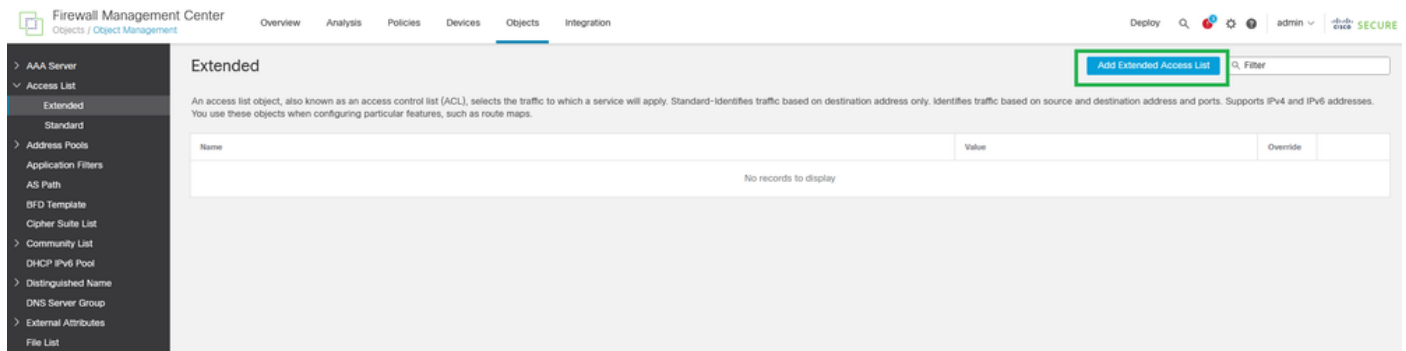
Oggetti - Gestione oggetti

Passaggio 2. Passare Access-list > Extended al menu a sinistra.



Access-list - Estesa

Passaggio 3. Fare clic su Add Extended Access List.



Aggiungi elenco accessi esteso

Passaggio 4. Impostare un nome nell'elenco degli accessi estesi e fare clic su Add.

New Extended Access List Object

Name

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

☐ Allow Overrides

Cancel Save

Nuovo oggetto elenco accessi estesi

Passaggio 5. Fare clic **Application** su e scegliere le applicazioni desiderate (per questo esempio sono state scelte alcune applicazioni Cisco). Quindi fate clic su **Add**.

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval:
 Sec.

Network Port **Application** Users Security Group Tag

Application Filters Clear All Filters

Risks (Any Selected)

- ☐ Very Low 730
- ☐ Low 622
- ☐ Medium 734
- ☐ High 1556
- ☐ Very High 577

Business Relevance (Any Selected)

- ☐ Very Low 885

Available Applications (4)

- Cisco
- Cisco Jabber
- Cisco Secure Endpoint
- Cisco Webex Assistant

Add to Rule

Selected Applications and Filters (6)

- Applications
- Cisco Jabber
- Cisco Secure Endpoint
- Cisco Webex Assistant
- WebEx
- WebEx Connect
- Webex Teams

Cancel Add

Aggiungi voce dell'elenco accessi estesi



Nota: L'elenco degli accessi esteso può essere configurato con gli IP e le porte di origine/destinazione in modo da associare il traffico specifico alle applicazioni desiderate. È possibile creare più elenchi di controllo di accesso estesi da applicare alla configurazione PBR.

Passaggio 6. Convalidare la configurazione dell'elenco degli accessi estesi e fare clic su **Save**.

New Extended Access List Object

Name
Applications

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	Any	Any	Any	Any	Cisco Jabber Cisco Secure Endpoint Cisco Webex Assistant WebEx (2 more...)	Any		 

☐ Allow Overrides

Cancel **Save**

Salva oggetto elenco accessi estesi

Passaggio 7. Passare alla difesa contro le minacce **Devices > Device Management** e modificarla.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

View By: Group

Device Management

Name	Model	Version	Platform	Access Control Policy	Auto Rollback	
FTD TAC Snort 3 172.16.1.101 - Routed	FTDv for VMware	7.4.0	N/A	Essentials, Secure Client VPN Only Cisco TAC		
FTD TAC 2 Snort 3 172.16.1.28 - Routed	FTDv for VMware	7.4.0	N/A	Essentials, Secure Client VPN Only Cisco TAC 2		

Dispositivo - Gestione dispositivi

Passaggio 8. Passare a **Routing > Policy-Based Routing**.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

FTD TAC

Cisco Firepower Threat Defense for VMware

Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

IGRP

RP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name: Global

Description: This is a Global Virtual Router

Select Interface: Q Search

Available Interfaces

management

ISP-1

ISP-2

management

VTI-1

VTI-2

Selected Interfaces

management

ISP-1

VTI-2

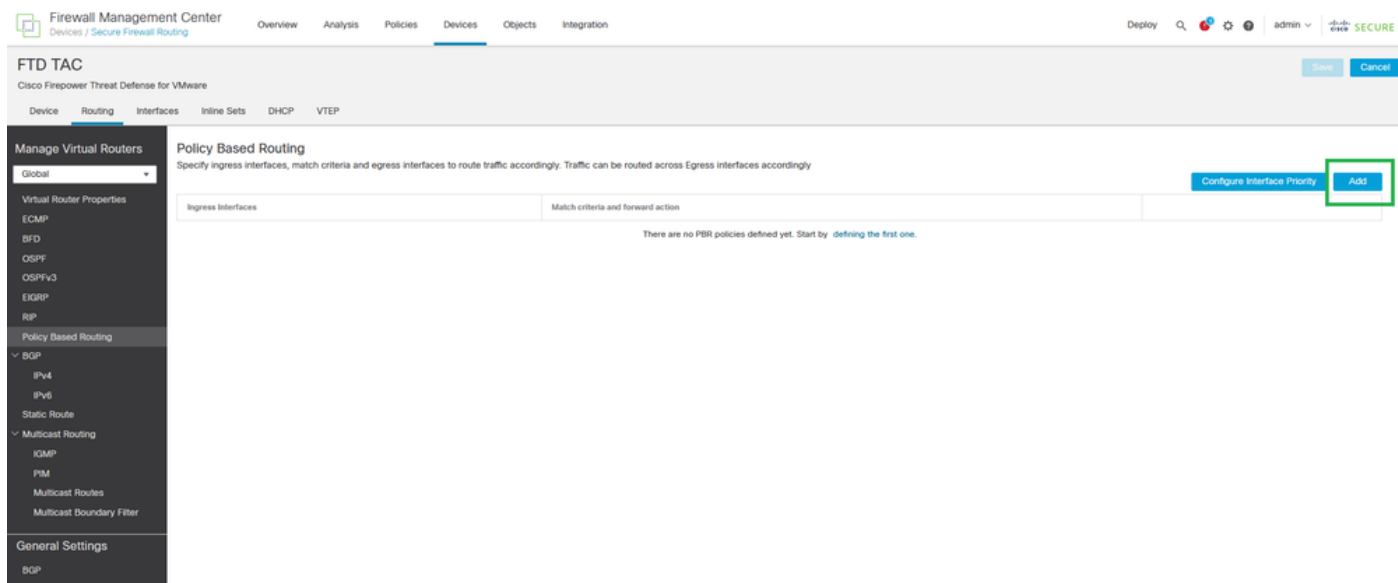
INSIDE

ISP-1

ISP-2

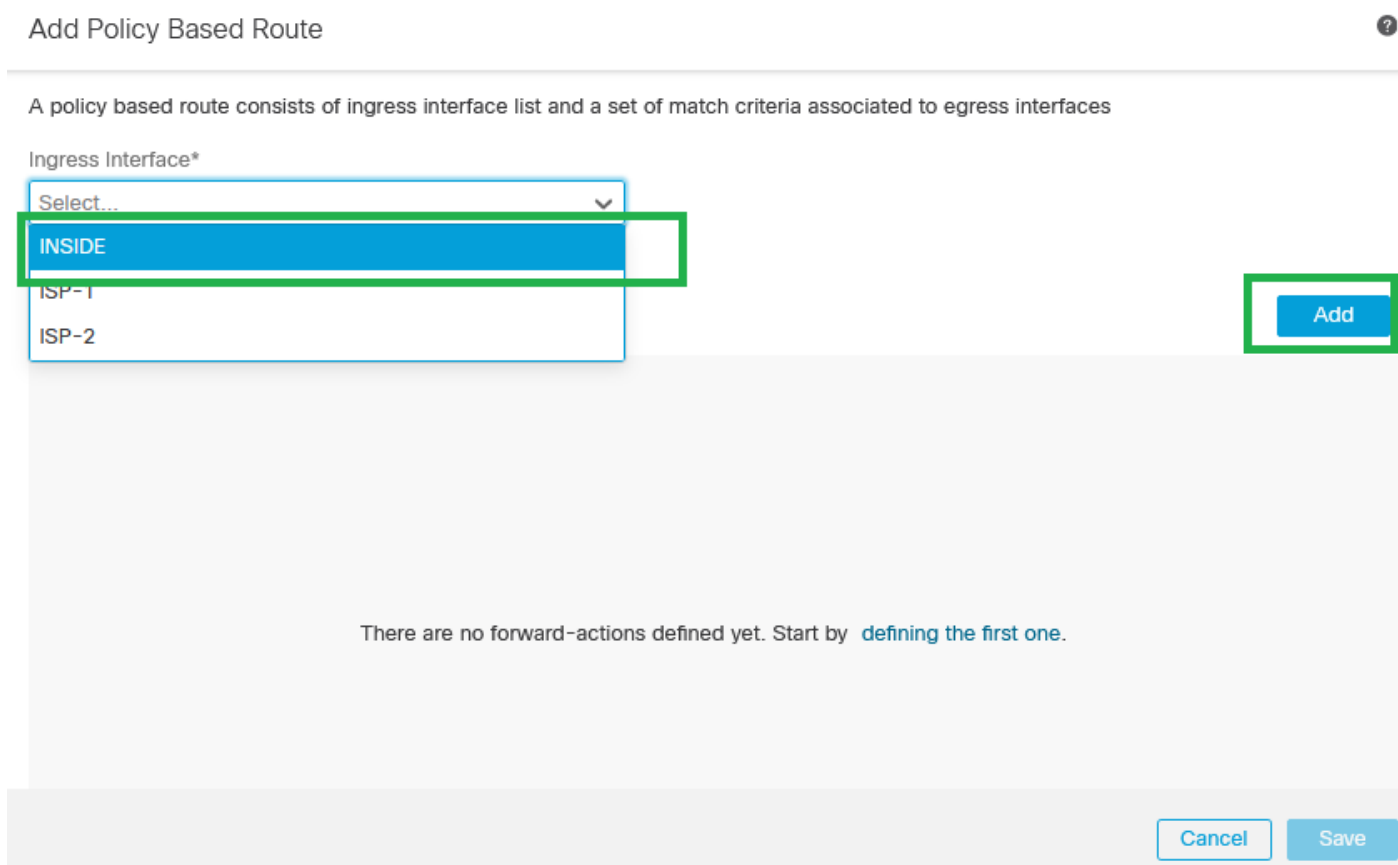
Routing - Routing basato su policy

Passaggio 9. Fare clic su **Add**.



Aggiungi routing basato su criteri

Passaggio 10. Aggiungere l'interfaccia in entrata per la configurazione PBR (INSIDE in questo esempio), quindi fare clic su **Add**.



Aggiungi route basata su criteri

Passaggio 11. Definire i criteri di corrispondenza (con l'elenco degli accessi estesi creato nei passi precedenti), le interfacce in uscita e l'ordinamento delle interfacce.

Add Forwarding Actions



Match ACL:*	Applications	+
Send To:*	Egress Interfaces	
Interface Ordering:*	Minimal Jitter	i

Available Interfaces



Interface	
INSIDE	+
ISP-1	+
ISP-2	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

No interfaces selected

Cancel

Save

Aggiungi azioni di inoltro



Nota: per questa guida alla configurazione sono stati scelti Egress Interfaces Minimal Jitter e. Per ulteriori informazioni sulle altre opzioni, consultare la [documentazione ufficiale](#) del PBR.

Passaggio 12. Scegliere le interfacce in uscita (per questo esempio ISP-1 e ISP-2), quindi fare clic su Save.

Add Forwarding Actions



Match ACL:* Applications +

Send To:* Egress Interfaces v

Interface Ordering:* Minimal Jitter v i

Available Interfaces

Search by interface name



Interface	
INSIDE	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

Interface	
ISP-1	
ISP-2	

Cancel

Save

Interfacce in uscita selezionate

Passaggio 13. Convalidare la configurazione PBR e fare clic su Save.

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

INSIDE x v

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Match ACL	Forwarding Action	
Applications	Send through minimum jitter interface	
	ISP-1	
	ISP-2	

Cancel

Save

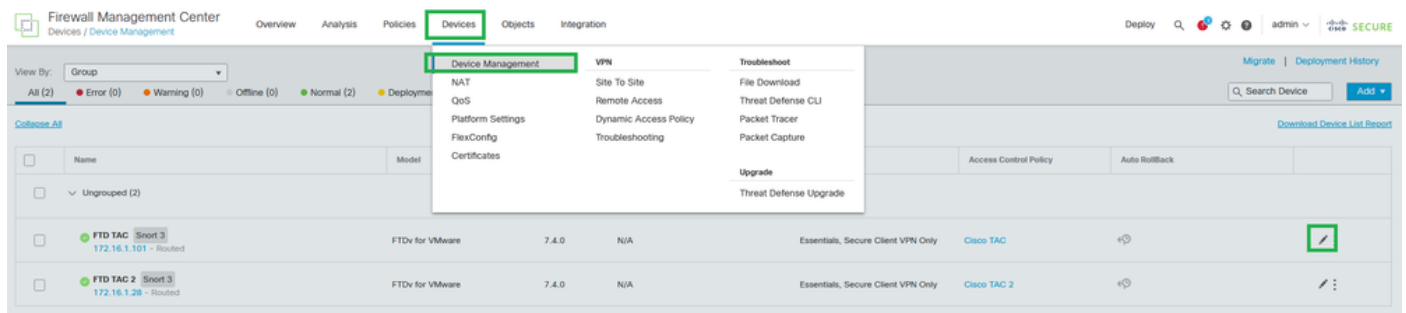
Convalida del routing basata su criteri

Passaggio 14. (Facoltativo) Ripetere i passaggi 9, 10, 11, 12 e 13 se sono stati creati più elenchi di controllo di accesso estesi o se sono disponibili più interfacce di origine a cui applicare la configurazione PBR.

Passaggio 15. Salvare e distribuire le modifiche da FMC.

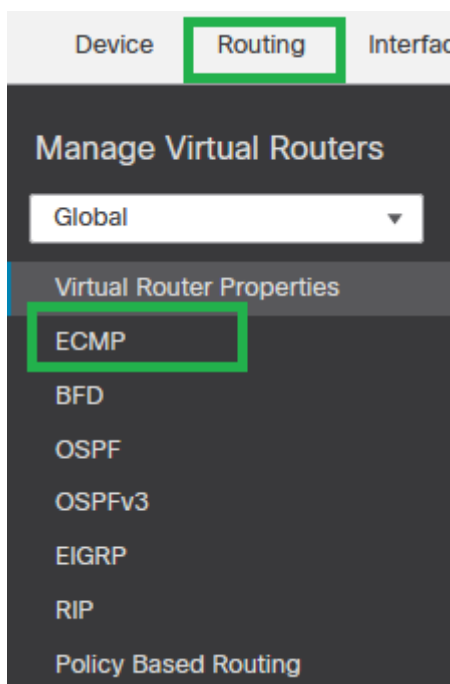
Configurazione di Equal-cost-multi-path (ECMP)

Passaggio 1. Passare alla difesa della minaccia e modificarla **Devices > Device Management**.



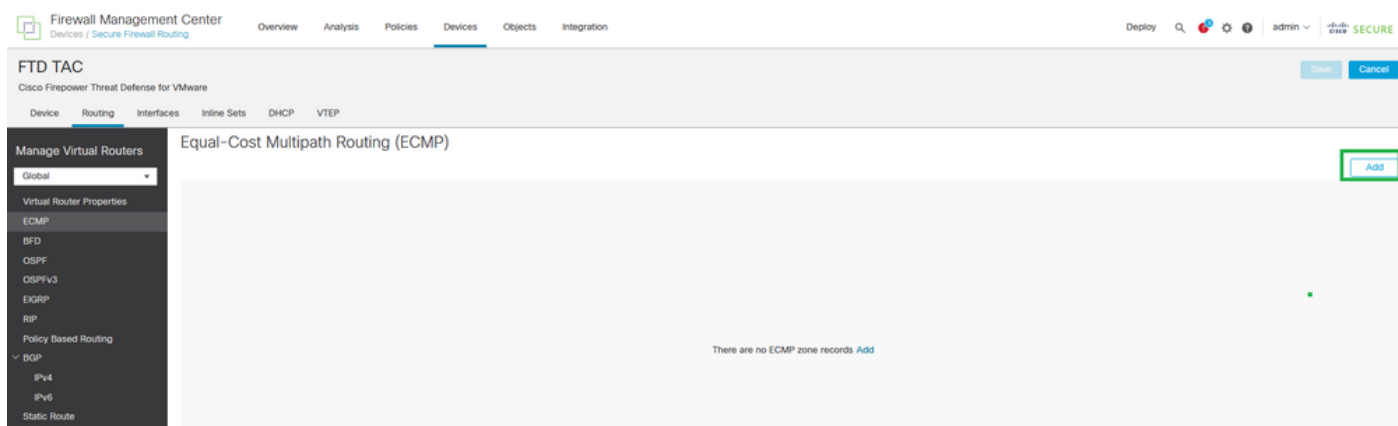
Dispositivo - Gestione dispositivi

Passaggio 2. Passare a **Routing > ECMP**.



Routing - ECMP

Passaggio 3. Fare clic su **Add** per creare un protocollo ECMP tra le VTI e le interfacce WAN (ISP-1 e ISP-2 per questa guida alla configurazione).



Equal-Cost Multipath Routing (ECMP)

Passaggio 4. Impostare il nome ECMP e scegliere tutte le interfacce VTI, quindi fare clic su Add.

Add ECMP ? ×

Name
VTI-ECMP

Available Interfaces

- INSIDE
- ISP-1
- ISP-2

Selected Interfaces

- VTI-1
- VTI-2

Add

Cancel **OK**

ECMP per VTI

Passaggio 5. Ripetere i passaggi 3 e 4 per creare un ECMP tra le interfacce WAN (ISP-1 e ISP-2 per questa guida alla configurazione).

Add ECMP

Name

ISP-ECMP

Available Interfaces

INSIDE

VTI-1

VTI-2

Add

Selected Interfaces

ISP-2

ISP-1

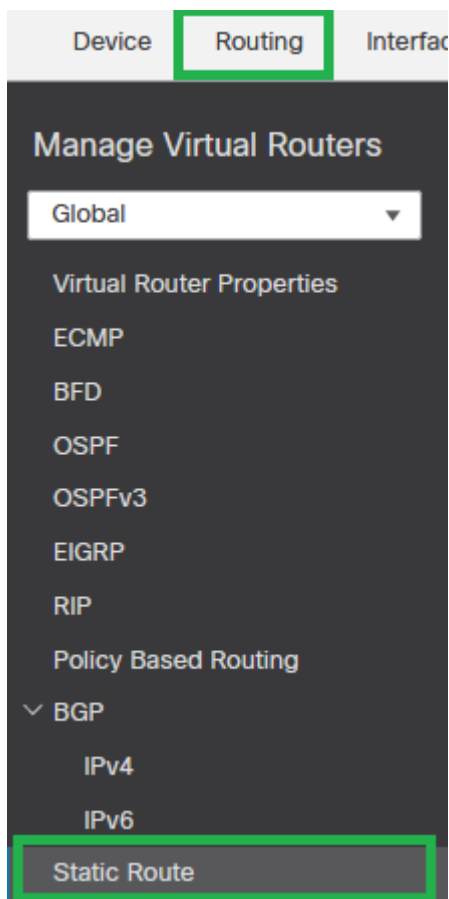
Cancel

OK

ECMP per interfacce ISP

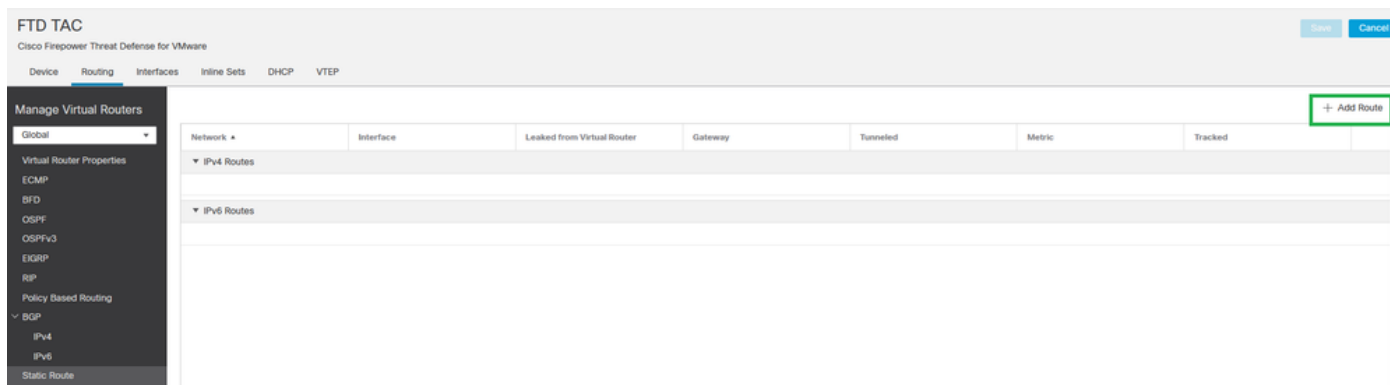
Passo 6: salvare la configurazione ECMP.

Passaggio 7. Configurare le route statiche per le interfacce della zona per il bilanciamento del carico. Passa a [Routing > Static Route](#).



Routing - Route statica

Passaggio 8. Fare clic su + Add Route.



+ Aggiungi route

Passaggio 9. Creare una route statica predefinita per le interfacce VTI (VTI-1 per questa guida alla configurazione) con 1 come valore della metrica, quindi fare clic su OK.

Add Static Route Configuration



Type:

☒ IPv4 ☐ IPv6

Interface*

VTI-1

(Interface starting with this icon  signifies it is available for route leak)

Available Network 



any



Add

Selected Network

any-ipv4



any-ipv4

IPv6-to-IPv4-Relay-Anycast

Gateway*

VTI-Tunnel1-FPR2



Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Route statica predefinita per VTI-1

Passaggio 10. Ripetere il passaggio 8. se sono state configurate più interfacce VTI.



Nota: Creare un percorso predefinito per ciascuna interfaccia VTI configurata.

Passaggio 11. Creare una route statica predefinita per le interfacce WAN/ISP (ISP-1 per questa guida alla configurazione) con un valore di metrica superiore a VTI, quindi fare clic su OK.

Add Static Route Configuration



Type: ☒ IPv4 ☐ IPv6

Interface*

ISP-1

(Interface starting with this icon  signifies it is available for route leak)

Available Network 



any-

Add

any-ipv4

Selected Network

any-ipv4



Gateway*

172.16.1.254GW-24



Metric:

10

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Route statica predefinita per ISP-1

Passaggio 12. Ripetere il passaggio 10. se sono state configurate più interfacce WAN/ISP.



Nota: Creare un percorso predefinito per ciascuna interfaccia WAN/ISP configurata.

Passaggio 13. Convalidare la configurazione dei cicli di lavorazione predefiniti e fare clic su OK.

FTD TAC
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

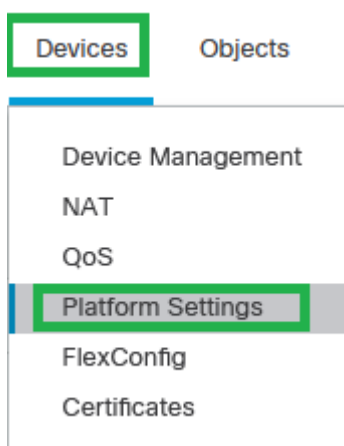
Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
any-ipv4	ISP-2	Global	172.16.11.254-GW-24	false	10	
any-ipv4	ISP-1	Global	172.16.1.254GW-24	false	10	
any-ipv4	VTI-2	Global	VTI-Tunnel2-FPR2	false	1	
any-ipv4	VTI-1	Global	VTI-Tunnel1-FPR2	false	1	
IPv6 Routes						

+ Add Route

Configurazione route statica

Configura DNS trusted per FTD protetto

Passaggio 1. Passare a **Devices > Platform Settings**.



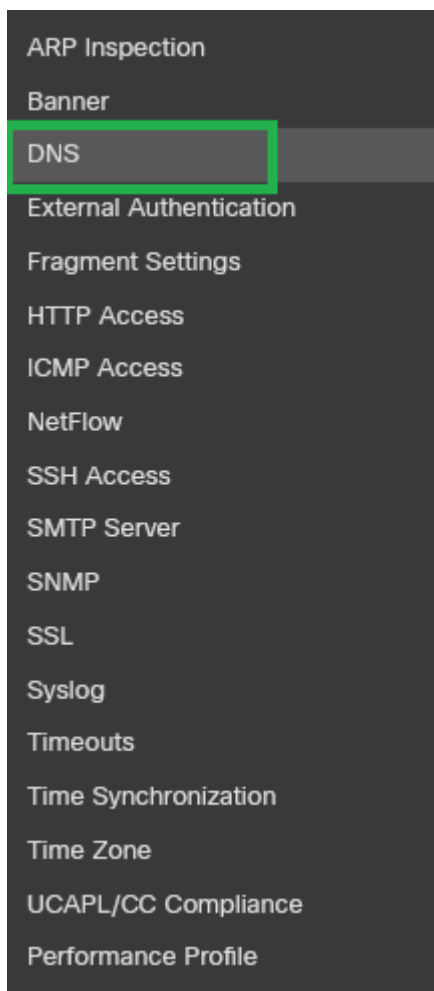
Dispositivi - Impostazioni piattaforma

Passaggio 2. Creare o modificare un criterio di impostazioni della piattaforma esistente.



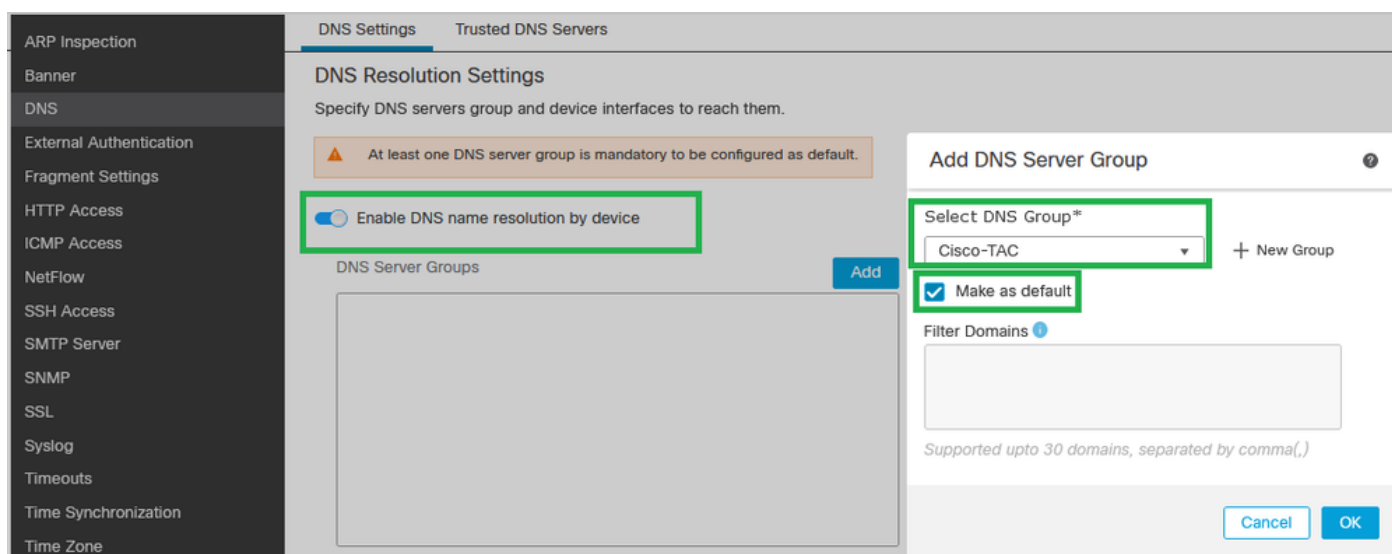
Nota: Accertarsi che il criterio Impostazioni piattaforma sia applicato ai dispositivi di difesa da minacce sicure.

Passaggio 3. Fare clic su **DNS**.



Impostazioni piattaforma DNS

Passaggio 4. Abilitare DNS name resolution by device e fare clic su Add o scegliere un gruppo DNS esistente. Scegliere Make as default, quindi fare clic su OK.



Aggiungi gruppo di server DNS



Nota: Per ulteriori informazioni sulla configurazione DNS nel criterio Impostazioni

piattaforma, vedere la documentazione [ufficiale](#) relativa a [Impostazioni piattaforma](#).

Passaggio 5. Selezionare le interfacce WAN/ISP nella Interface Objects sezione.

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Expiry Entry Timer:

1 Range: 1-65535 minutes

Poll Timer:

240 Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Search

INSIDE

ISP-1

ISP-2

VTI-1

VTI-11

VTI-2

Add

Selected Interface Objects

ISP-1

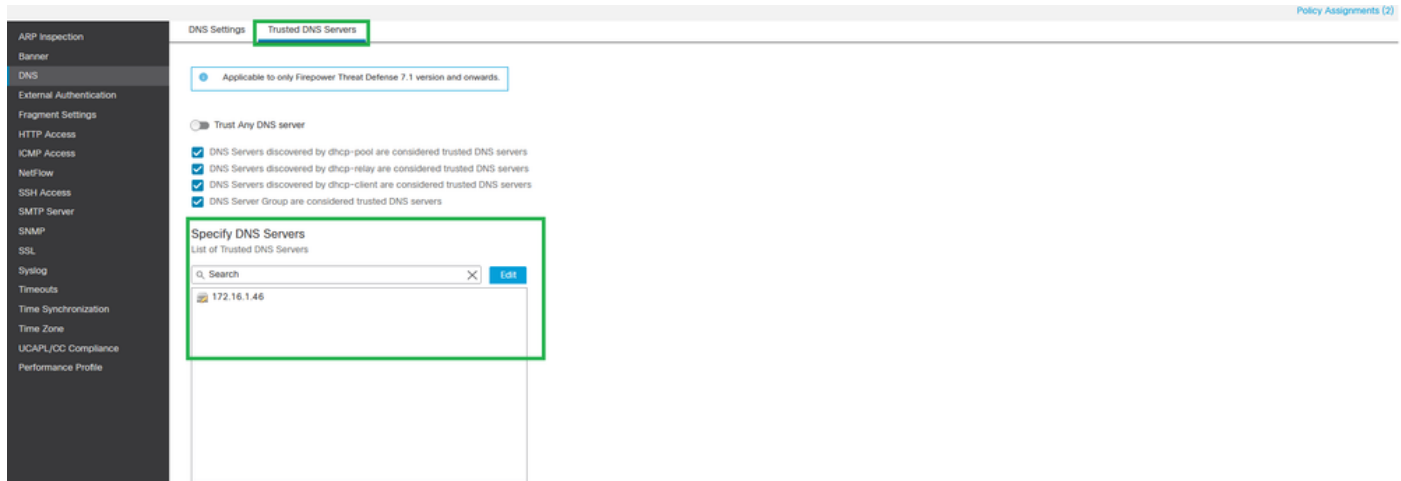
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

Configurazione interfaccia DNS

Passaggio 6. Salvare le modifiche.

Passaggio 7. Passare alla pagina Trusted DNS Servers e specificare i server DNS trusted.

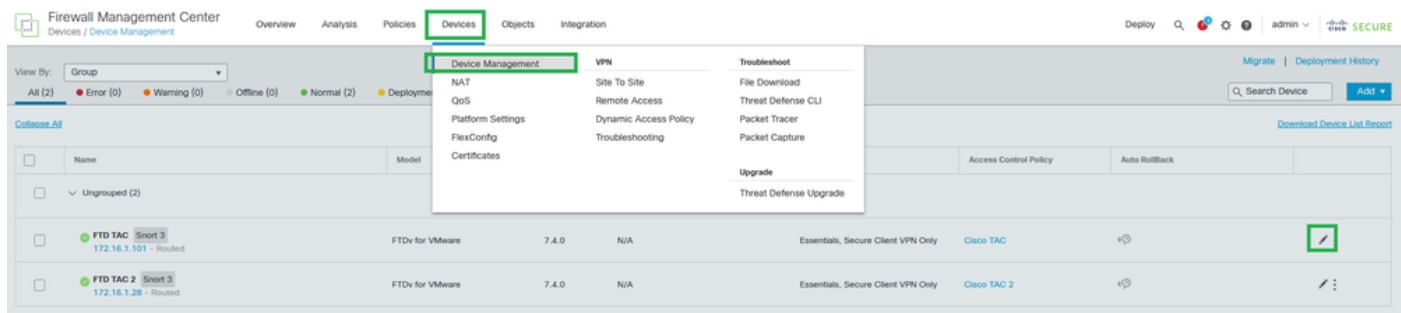


Server DNS trusted

Passaggio 8. Fare clic su **Save** e distribuire le modifiche.

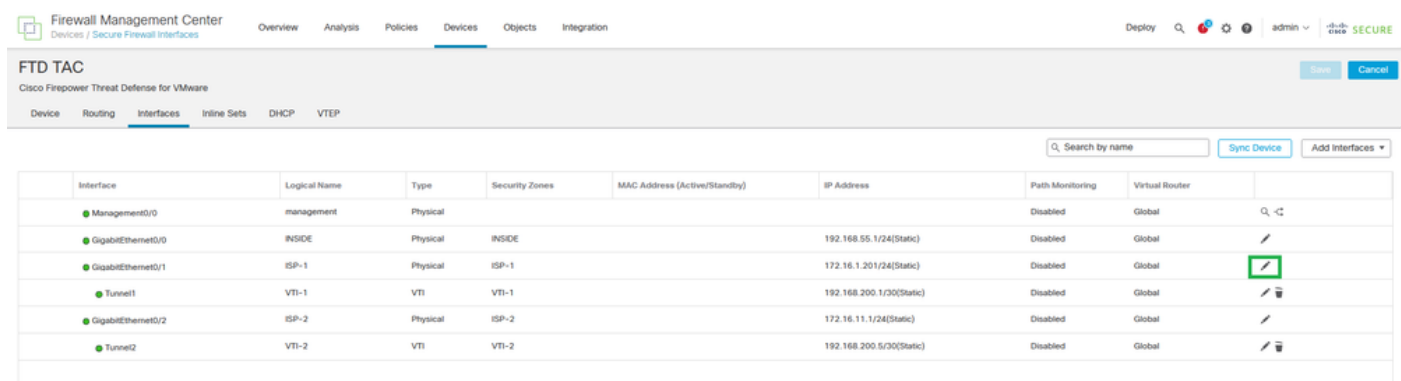
Abilita monitoraggio percorso

Passaggio 1. Passare alla difesa della minaccia e modificarla **Devices > Device Management**.



Dispositivo - Gestione dispositivi

Passaggio 2. Sotto la **Interfaces** scheda, modificare l'interfaccia WAN/ISP (ISP-1 e ISP-2 per questa guida alla configurazione).



Configurazione dell'interfaccia

Passaggio 3. Fare clic sulla **Path Monitoring** scheda, scegliere **Enable IP Monitoring** e abilitare la casella di controllo **HTTP-based Application Monitoring**. Quindi fate clic su **Save**.

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

☒ Enable IP based Monitoring

Select to monitor jitter, round trip time, packet-lost & mean opinion score of each interface.

Monitoring Type:

Next-hop of default route out of interface (Auto) ▼

System monitors the next hop of the interface. Tries IPv4 and then IPv6.
If the peer is unavailable, monitoring is not done.

☒ Enable HTTP based Application Monitoring

By enabling application monitoring you are allowing all the applications configured in Extended ACLs used in policy based routing with this interface as egress interface to be monitored automatically.

Applications

Cisco Jabber

Cisco Secure Endpoint

Cisco Webex Assistant

WebEx

WebEx Connect

Cancel

OK

Configurazione monitoraggio percorso interfaccia



Attenzione: È necessario elencare le applicazioni configurate nella sezione di configurazione precedente.



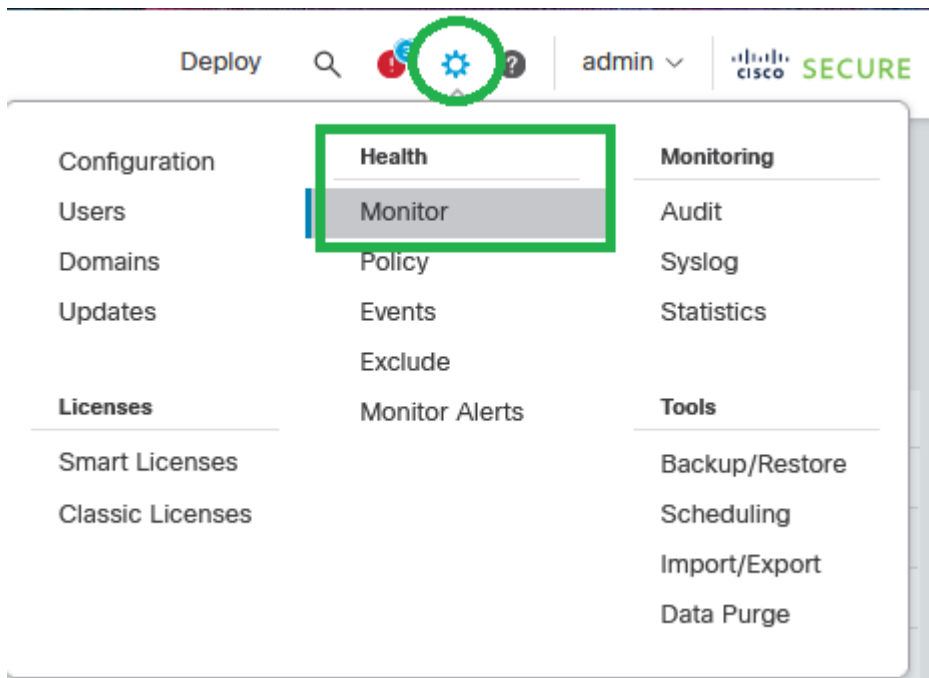
Nota: Per questa guida alla configurazione è stato scelto "Tipo di monitoraggio". Per ulteriori informazioni sulle altre opzioni, consultare la sezione Path Monitoring Settings della [guida ufficiale](#) alla [configurazione](#).

Passaggio 4. Ripetere i passaggi 2 e 3 per tutte le interfacce WAN/ISP configurate.

Passaggio 5. Fare clic su **Save** e distribuire le modifiche.

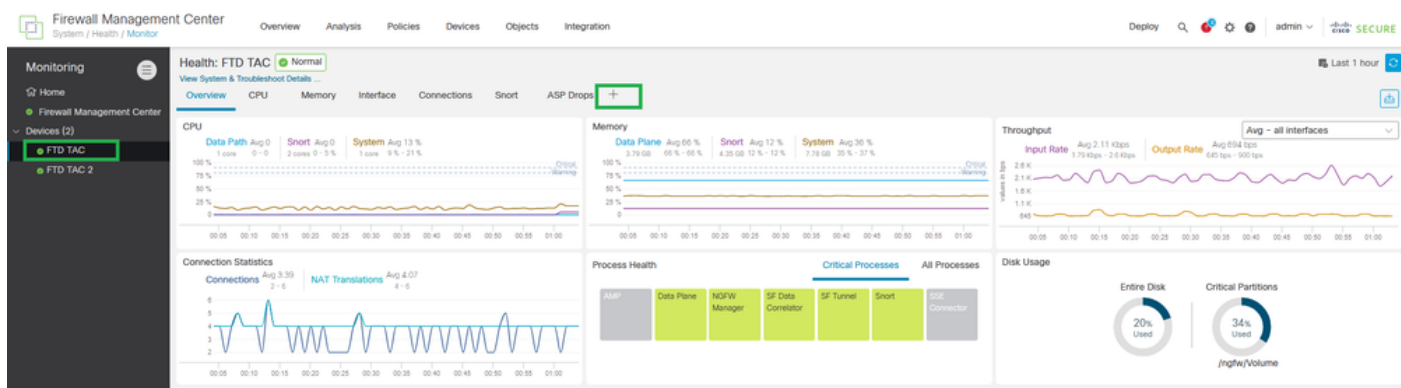
Aggiungi dashboard di controllo

Passaggio 1. Passare a **System > Health > Monitor**.



Sistema - Integrità - Monitor

Passaggio 2. Scegliere il dispositivo Secure FTD e fare clic su Add New Dashboard.



Aggiungi nuovo dashboard

Passaggio 3. Impostare il nome del dashboard e nella Correlate Metrics finestra di dialogo scegliere Interface - Path Metrics dall'elenco a discesa. Quindi fate clic su Add Dashboard.

Add New Dashboard



Name*

FTD HTTP Path Monitoring

Metrics*

Metrics can be chosen from pre-defined correlation groups or/and metrics of your choice. Related metrics are grouped together, select a group and then the metrics.

Interface

Jitter x

x

v



Interface

Mean Opinion Score (MOS) x

x

v



Interface

Round Trip Time x

x

v



Interface

Packet Loss x

x

v



Add Metrics

Add from Predefined Correlations v

Clear All

Cancel

Add Dashboard

Aggiungi nuovo dashboard con metriche dei percorsi

Verifica

Questa sezione descrive come verificare le route statiche mobili, ECMP, il gruppo di oggetti con applicazioni e le configurazioni PBR.

Verificare la configurazione delle route predefinite e delle route statiche mobili:

```
firepower# show run route
route VTI-1 0.0.0.0 0.0.0.0 192.168.200.1 1
route VTI-2 0.0.0.0 0.0.0.0 192.168.200.5 1
route ISP-1 0.0.0.0 0.0.0.0 172.16.1.254 10
route ISP-2 0.0.0.0 0.0.0.0 172.16.11.254 10
```

Verificare la configurazione ECMP:

```
firepower# sh run | i ecmp
zone ECMP-VTI ecmp
zone ECMP-ISP ecmp
```

Verificare che il traffico venga bilanciato dall'ECMP nella tabella di routing. La tabella di routing deve installare entrambe le route nella tabella di routing FTD sicuro.

```
firepower# show route static
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 172.16.11.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.200.5, VTI-2
[1/0] via 192.168.200.1, VTI-1
```

Verificare la configurazione della route-map PBR:

```
firepower# show run route-map
!
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set adaptive-interface cost ISP-1 ISP-2
!
```

Verificare l'ACL assegnato alla configurazione PBR (controllare il nome ACL nella configurazione route-map):

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSG_639950173988
```

Verificare il gruppo di oggetti con le applicazioni assegnate all'elenco degli accessi (controllare il nome del gruppo di oggetti nella configurazione ACL):

```
firepower# show run object-group
object-group network-service FMC_NSG_639950173988
network-service-member "Cisco Jabber"
network-service-member "Cisco Secure Endpoint"
network-service-member "Cisco Webex Assistant"
network-service-member "WebEx"
network-service-member "WebEx Connect"
network-service-member "Webex Teams"
```

Verificare il percorso dei criteri assegnato alle interfacce dati utilizzate nella configurazione PBR:

```

interface GigabitEthernet0/0
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.35.1 255.255.255.0
policy-route route-map FMC_GENERATED_PBR_1694885402369
!
interface GigabitEthernet0/1
nameif ISP-1
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
zone-member ECMP-ISP
ip address 172.16.1.202 255.255.255.0
policy-route path-monitoring auto
!
interface GigabitEthernet0/2
nameif ISP-2
security-level 0
zone-member ECMP-ISP
ip address 172.16.11.2 255.255.255.0
policy-route path-monitoring auto
!

```

Verificare e controllare le statistiche Jitter, MOS, Round Trip Time e Packet Loss dalle informazioni del dashboard di monitoraggio del percorso HTTP.



Verifica dashboard monitoraggio percorso HTTP

Risoluzione dei problemi

In caso di errore nel monitoraggio del percorso, con il monitoraggio basato su IP abilitato, le interfacce WAN/ISP sono configurate per inviare i pacchetti di richieste ICMP al gateway configurato sulle route statiche. Configurare le acquisizioni in entrata/uscita sulle interfacce

WAN/ISP per controllare se l'ICMP funziona.

Acquisizione in ingresso e in uscita:

```
firepower# cap in interface ISP-1 trace match icmp any any
firepower# cap in2 interface isP-2 trace match icmp any any
```

Acquisizione in ingresso:

```
firepower# show cap in
```

12 packets captured

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

```
1: 00:08:28.073604 172.16.1.202 > 172.16.1.254 icmp: echo request
2: 00:08:28.074672 172.16.1.254 > 172.16.1.202 icmp: echo reply
3: 00:08:29.150871 172.16.1.202 > 172.16.1.254 icmp: echo request
4: 00:08:29.151832 172.16.1.254 > 172.16.1.202 icmp: echo reply
5: 00:08:30.217701 172.16.1.202 > 172.16.1.254 icmp: echo request
6: 00:08:30.218876 172.16.1.254 > 172.16.1.202 icmp: echo reply
7: 00:08:31.247728 172.16.1.202 > 172.16.1.254 icmp: echo request
8: 00:08:31.248980 172.16.1.254 > 172.16.1.202 icmp: echo reply
9: 00:08:32.309005 172.16.1.202 > 172.16.1.254 icmp: echo request
10: 00:08:32.310317 172.16.1.254 > 172.16.1.202 icmp: echo reply
11: 00:08:33.386622 172.16.1.202 > 172.16.1.254 icmp: echo request
12: 00:08:33.387751 172.16.1.254 > 172.16.1.202 icmp: echo reply
```

12 packets shown

Acquisizione in uscita:

```
firepower# show cap in2
```

12 packets captured

```
1: 00:08:28.073543 172.16.11.2 > 172.16.11.254 icmp: echo request
2: 00:08:28.074764 172.16.11.254 > 172.16.11.2 icmp: echo reply
3: 00:08:29.150810 172.16.11.2 > 172.16.11.254 icmp: echo request
4: 00:08:29.151954 172.16.11.254 > 172.16.11.2 icmp: echo reply
5: 00:08:30.217640 172.16.11.2 > 172.16.11.254 icmp: echo request
```

```
6: 00:08:30.218799 172.16.11.254 > 172.16.11.2 icmp: echo reply
7: 00:08:31.247667 172.16.11.2 > 172.16.11.254 icmp: echo request
8: 00:08:31.248888 172.16.11.254 > 172.16.11.2 icmp: echo reply
9: 00:08:32.308913 172.16.11.2 > 172.16.11.254 icmp: echo request
10: 00:08:32.310012 172.16.11.254 > 172.16.11.2 icmp: echo reply
11: 00:08:33.386576 172.16.11.2 > 172.16.11.254 icmp: echo request
12: 00:08:33.387888 172.16.11.254 > 172.16.11.2 icmp: echo reply
12 packets captured
```



Attenzione: Assicurarsi di configurare le acquisizioni con gli indirizzi IP di origine e di destinazione, in quanto le acquisizioni possono migliorare notevolmente le prestazioni nella confezione.



Suggerimento: Se il ping non funziona, risolvere i problemi di connessione diretta al gateway predefinito, controllare la tabella ARP o contattare Cisco TAC.

Per verificare se il PBR funziona, è possibile utilizzare lo strumento di traccia dei pacchetti per verificare che il traffico dell'applicazione venga instradato con il PBR.

```
firepower# packet-tracer input insIDE tcp 172.16.35.2 54352 'PUBLIC-IP-ADDRESS-FOR-WEBEX' $
---
[Output omitted]
---
Phase: 3
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Config:
route-map FMC_GENERATED_PBR_1694885402369 permit 5
match ip address Applications
set ip next-hop 172.16.1.254
Additional Information:
Matched route-map FMC_GENERATED_PBR_1694885402369, sequence 5, permit
Found next-hop 172.16.1.254 using egress ifc ISP-1
---
[Output omitted]
---
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: ISP-1
output-status: up
output-line-status: up
Action: allow
```



Nota: Per informazioni sugli indirizzi IP delle applicazioni per il servizio di rete configurato sui gruppi di oggetti, utilizzare il comando `show object-group network-service detail`.

Informazioni correlate

Ulteriori documenti relativi al PBR con monitoraggio del percorso HTTP sono disponibili qui:

- [Guida alla configurazione dei dispositivi con routing basato su criteri nel centro di gestione del firewall protetto](#)
- [Guida alla configurazione del monitoraggio dei percorsi sulla configurazione del routing basato su criteri nel centro di gestione del firewall protetto](#)
- [Configura criteri di routing basati su criteri](#)
- [Esempio di configurazione per il routing basato su criteri](#)
- [Configurare l'esempio per il monitoraggio del percorso PBR](#)
- [Aggiungi Dashboard Di Monitoraggio Del Percorso](#)
- [Guida alla configurazione delle impostazioni della piattaforma DNS nel centro di gestione Secure Firewall](#)
- [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).