

Configurer PBR avec HTTP Path Monitor sur FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer PBR pour la surveillance du chemin HTTP](#)

[Configurer le protocole ECMP \(Equal-cost-multi-path\)](#)

[Configurer le DNS sécurisé pour le FTD sécurisé](#)

[Activer la surveillance des chemins](#)

[Ajouter un tableau de bord Surveillance](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le routage basé sur des politiques (PBR) avec la surveillance du chemin HTTP sur le Cisco Secure Firewall Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- connaissances de base de PBR
- Expérience de base de Cisco Secure Management Center
- Cisco Secure Firewall Threat Defense (FTD) de base

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware version 7.4

- Appliance virtuel Cisco Secure Firewall Threat Defense (FTDv) VMware version 7.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans le routage traditionnel, les paquets sont routés en fonction de l'adresse IP de destination. Toutefois, il est difficile de modifier le routage de la spécification du trafic dans un système de routage basé sur la destination. PBR vous offre un meilleur contrôle du routage en étendant et en complétant les mécanismes existants fournis par les protocoles de routage.

PBR permet de définir la priorité IP. Elle permet également de spécifier un chemin pour un certain trafic, tel que le trafic prioritaire sur une liaison à coût élevé. Avec PBR, le routage est basé sur des critères autres que le réseau de destination, tels que le port source, l'adresse de destination, le port de destination, les applications de protocole ou une combinaison de ces objets. PBR peut être utilisé pour classer le trafic réseau en fonction de l'application, du nom d'utilisateur, de l'appartenance au groupe et de l'association au groupe de sécurité. Cette méthode de routage est applicable dans les situations où de nombreux périphériques accèdent à des applications et à des données dans un déploiement de réseau étendu. Traditionnellement, les grands déploiements ont des topologies qui acheminent tout le trafic réseau vers un concentrateur en tant que trafic chiffré dans un VPN basé sur le routage. Ces topologies entraînent souvent des problèmes tels que la latence des paquets, la réduction de la bande passante et la perte de paquets.

PBR est pris en charge uniquement en mode pare-feu routé et n'est pas appliqué aux connexions Embryonic. L'application basée sur HTTP est prise en charge sur les interfaces physiques, de canal de port, de sous-interfaces et de tunnel d'état. Il n'est pas pris en charge sur les périphériques de cluster.

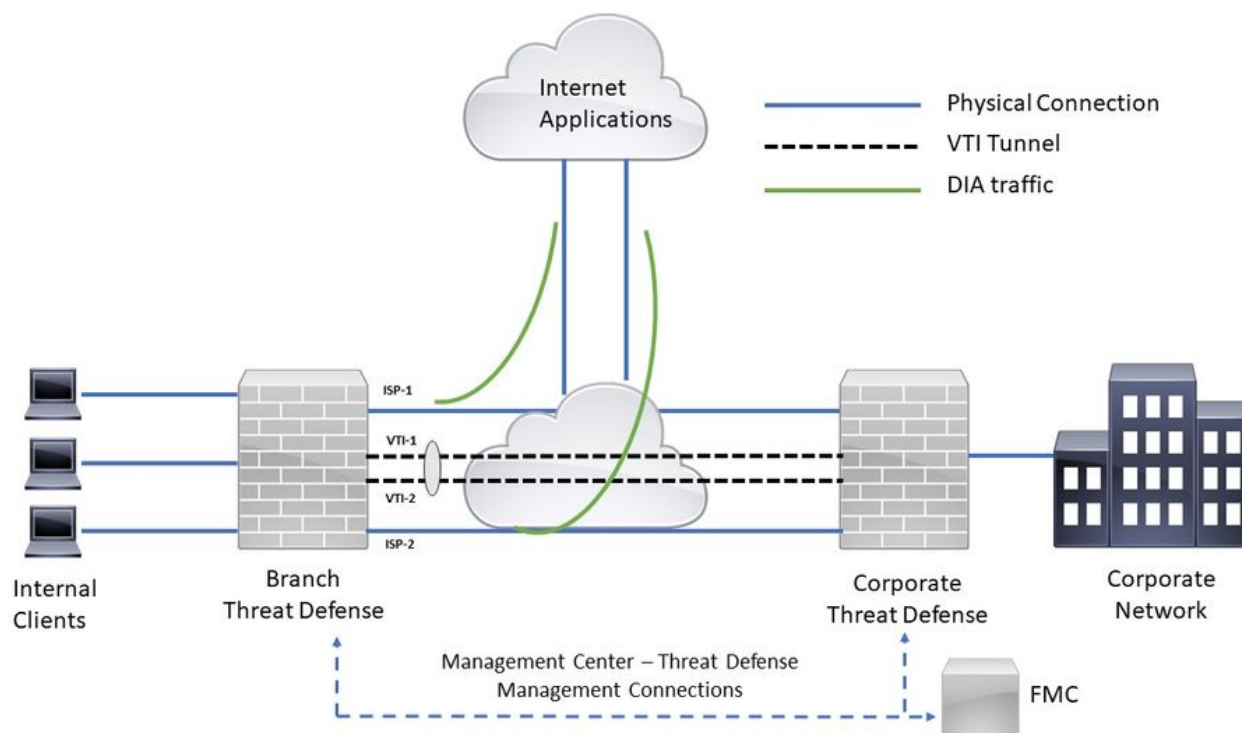
Lorsque des interfaces configurées dérivent des métriques telles que le temps de parcours aller-retour (RTT), la gigue, le score d'opinion moyen (MOS) et la perte de paquets par interface, elles sont utilisées pour déterminer le meilleur chemin pour le routage du trafic PBR. Path Monitoring calcule des métriques flexibles pour plusieurs homologues distants par interface. Afin de surveiller et de déterminer le meilleur chemin pour plusieurs applications via une stratégie sur un pare-feu de filiale, HTTP est préféré à ICMP pour les raisons suivantes :

- HTTP-ping peut dériver les mesures de performances du chemin jusqu'à la couche application du serveur, où l'application est hébergée.
- La nécessité de modifier la configuration du pare-feu chaque fois que l'adresse IP du serveur d'applications est modifiée est supprimée lorsque le domaine d'application est suivi au lieu de l'adresse IP.

Configurer

Diagramme du réseau

Imaginez un scénario de réseau d'entreprise typique dans lequel tout le trafic du réseau de filiale est envoyé via un VPN basé sur la route du réseau d'entreprise et diverge vers l'extranet lorsque cela est nécessaire. La topologie suivante montre un réseau de filiale connecté au réseau d'entreprise via un VPN basé sur la route. Traditionnellement, la protection de l'entreprise contre les menaces est configurée pour gérer le trafic interne et externe de la filiale. Avec la stratégie PBR, la défense contre les menaces des filiales est configurée avec une stratégie qui achemine un trafic spécifique vers le réseau WAN au lieu des tunnels virtuels. Le reste du trafic passe par le VPN basé sur la route, comme d'habitude.



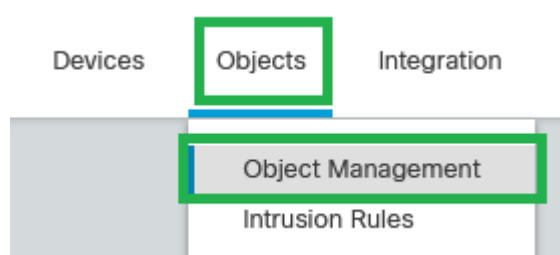
Topologie du réseau

La section de configuration suppose que les interfaces ISP et VTI sont déjà configurées pour la défense contre les menaces des filiales dans le FMC sécurisé.

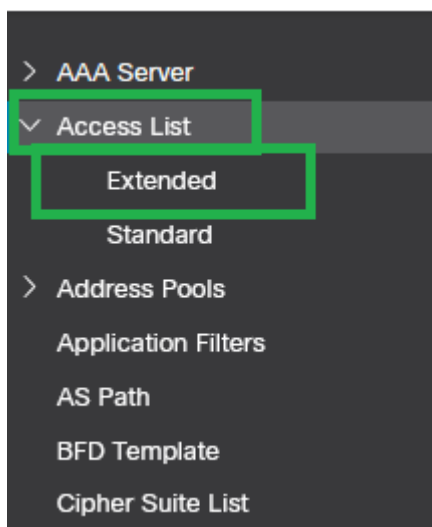
Configurer PBR pour la surveillance du chemin HTTP

Cette section de configuration présente la configuration Path Monitoring sur les interfaces ISP-1 et ISP-2.

Étape 1 : création d'une liste d'accès étendue pour les applications surveillées Accédez à **Objects > Object Management**.

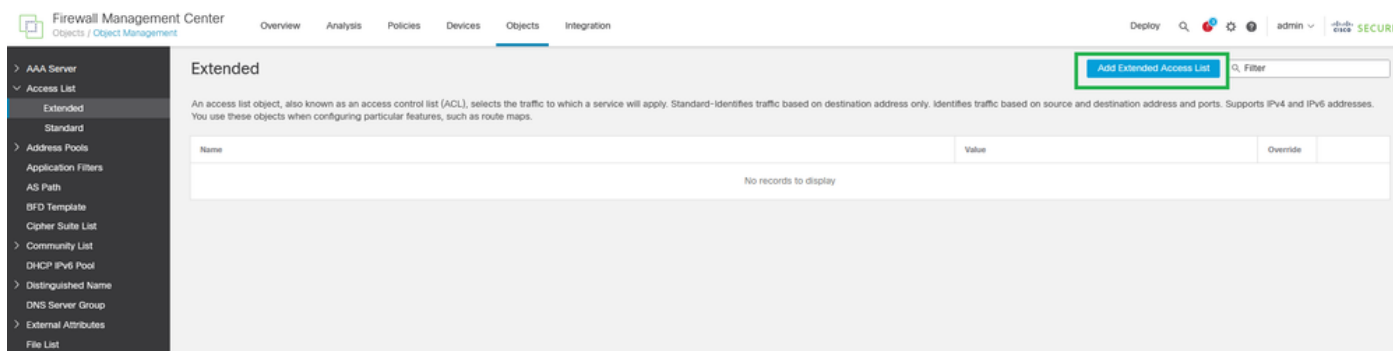


Étape 2. Accédez à Access-list > Extended dans le menu de gauche.



Liste d'accès - Étendue

Étape 3. Cliquez sur Add Extended Access List.



Ajouter une liste d'accès étendue

Étape 4. Configurez un nom dans la liste de contrôle d'accès étendue et cliquez sur Add.

New Extended Access List Object

Name
Applications

Entries (0)

Add

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

☐ Allow Overrides

Cancel Save

Nouvel objet de liste d'accès étendue

Étape 5. Cliquez sur **Application** et choisissez les applications souhaitées (certaines applications Cisco ont été choisies pour cet exemple). Cliquez ensuite sur **Add**.

Add Extended Access List Entry ?

Action:
Allow

Logging:
Default

Log Level:
Informational

Log Interval:
300 Sec.

Network Port **Application** Users Security Group Tag

Application Filters Clear All Filters

Search by name

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)

Search by name

- 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

Ajouter une entrée de liste d'accès étendue



Remarque : La liste de contrôle d'accès étendue peut être configurée avec les adresses IP et les ports source/de destination afin de faire correspondre le trafic spécifique aux applications souhaitées. Vous pouvez créer plusieurs listes de contrôle d'accès étendues afin de les appliquer à la configuration PBR.

Étape 6. Validez la configuration de la liste de contrôle d'accès étendue et cliquez sur **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

Enregistrer l'objet de liste de contrôle d'accès étendu

Étape 7. Naviguez jusqu'à **Devices > Device Management** la défense contre les menaces et modifiez-la.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployed (0)

Collapsible All

Device Management

NAT
QoS
Platform Settings
FlexConfig
Certificates

VPN
Site To Site
Remote Access
Dynamic Access Policy
Troubleshooting

Troubleshoot
File Download
Threat Defense CLI
Packet Tracer
Packet Capture

Upgrade
Threat Defense Upgrade

Access Control Policy Auto Rollback

Download Device List Report

FTD TAC 172.16.1.101 - Routed FTDv for VMware 7.4.0 N/A Essentials, Secure Client VPN Only Cisco TAC

FTD TAC 2 172.16.1.28 - Routed FTDv for VMware 7.4.0 N/A Essentials, Secure Client VPN Only Cisco TAC 2

Périphérique - Gestion des périphériques

Étape 8. Accédez à **Routing > Policy-Based Routing**.

Firewall Management Center
Devices / Secure Firewall Routing

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
EIGRP
RIP
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

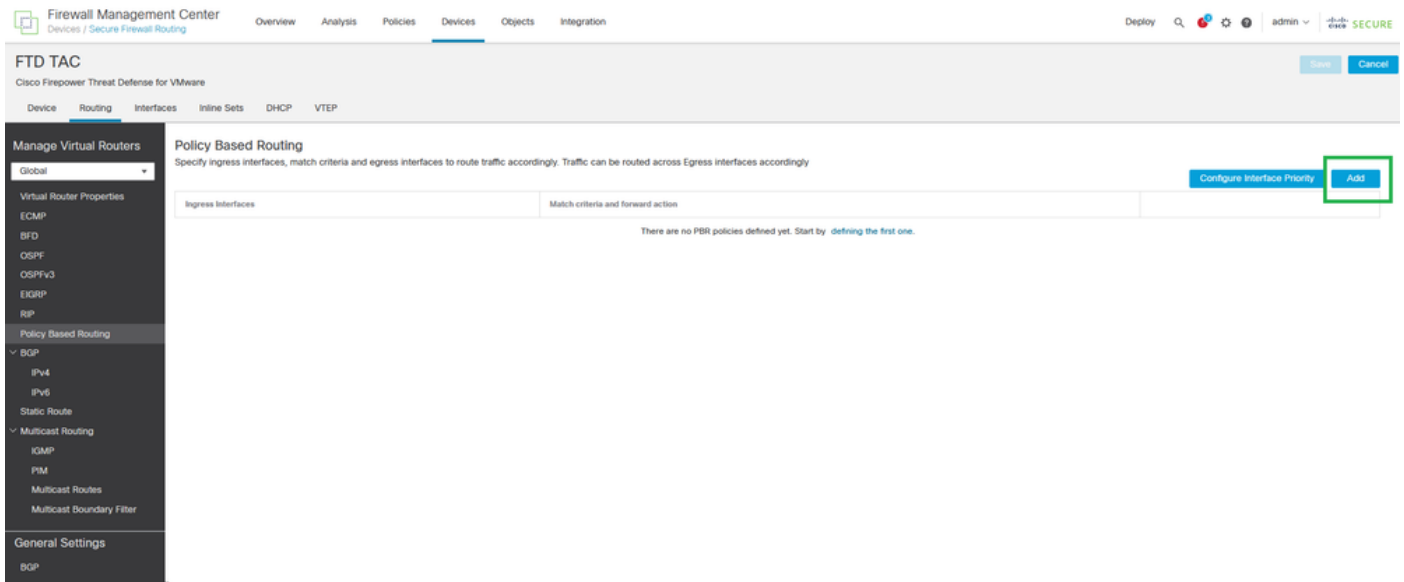
management
VTI-1
VTI-2

Selected Interfaces

management
ISP-1
VTI-2
INSIDE
VTI-1
ISP-2

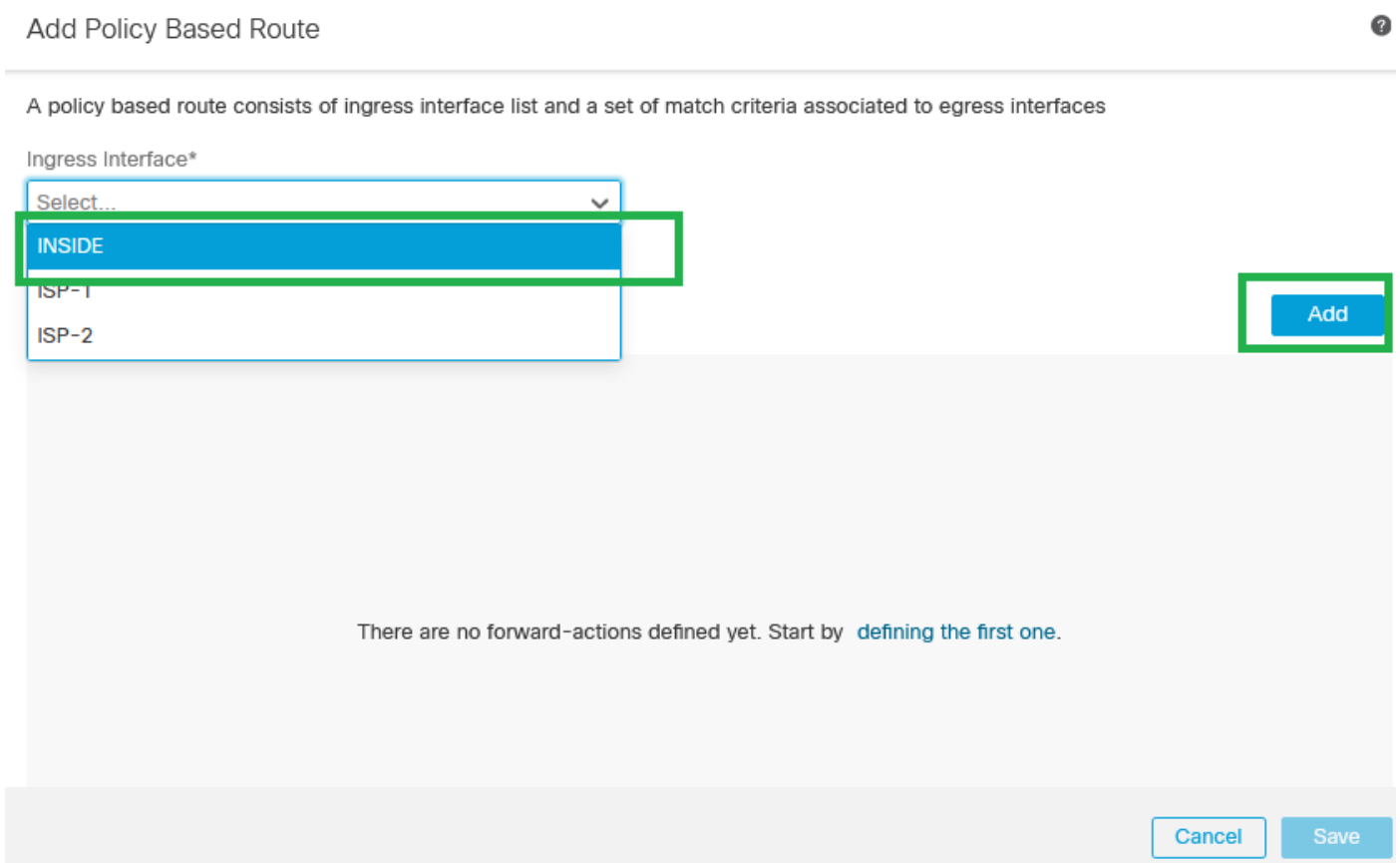
Routeur - Routage basé sur des politiques

Étape 9. Cliquez sur **Add**.



Ajouter un routage basé sur des stratégies

Étape 10. Ajoutez l'interface d'entrée pour la configuration PBR (INSIDE dans cet exemple), puis cliquez sur Add.



Ajouter une route basée sur une stratégie

Étape 11. Définissez les critères de correspondance (avec la liste de contrôle d'accès étendue créée aux étapes précédentes), les interfaces de sortie et le classement des interfaces.

Add Forwarding Actions



Match ACL:* Applications +

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter i

Available Interfaces

Search by interface name

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

Selected Egress Interfaces*

No interfaces selected

Cancel

Save

Ajouter des actions de transfert



Remarque : Egress Interfaces et ont Minimal Jitter été choisis pour ce guide de configuration. Consultez la [documentation PBR officielle](#) afin d'en savoir plus sur les autres options.

Étape 12. Choisissez les interfaces de sortie (ISP-1 et ISP-2 dans cet exemple), puis cliquez sur Save.

Add Forwarding Actions



Match ACL:* Applications

Send To:* Egress Interfaces

Interface Ordering:* Minimal Jitter

Available Interfaces

Search by interface name



Interface	
INSIDE	+
VTI-1	+
VTI-2	+

Selected Egress Interfaces*

Interface	
ISP-1	
ISP-2	

Cancel

Save

Interfaces de sortie sélectionnées

Étape 13. Validez la configuration PBR et cliquez sur 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



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

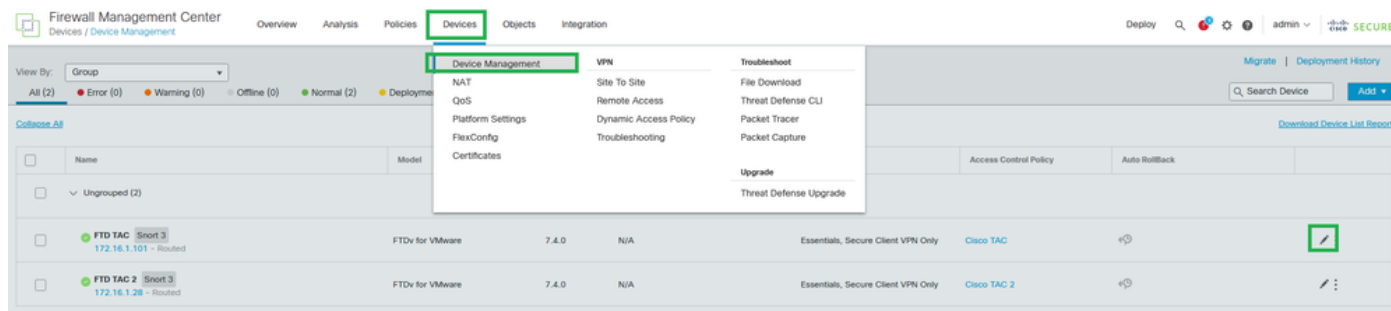
Save

Étape 14. (Facultatif) Répétez les étapes 9, 10, 11, 12 et 13 si d'autres listes de contrôle d'accès étendues ont été créées ou s'il existe d'autres interfaces source où la configuration PBR doit être appliquée.

Étape 15. Enregistrement et déploiement des modifications depuis FMC

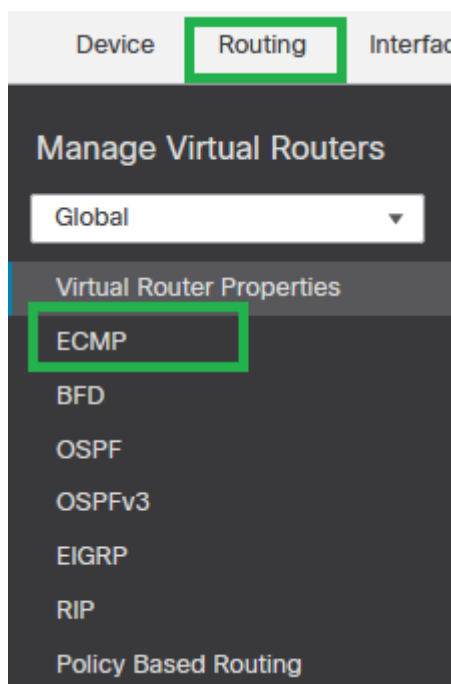
Configurer le protocole ECMP (Equal-cost-multi-path)

Étape 1. Accédez à la défense contre les menaces **Devices > Device Management** et modifiez-la.



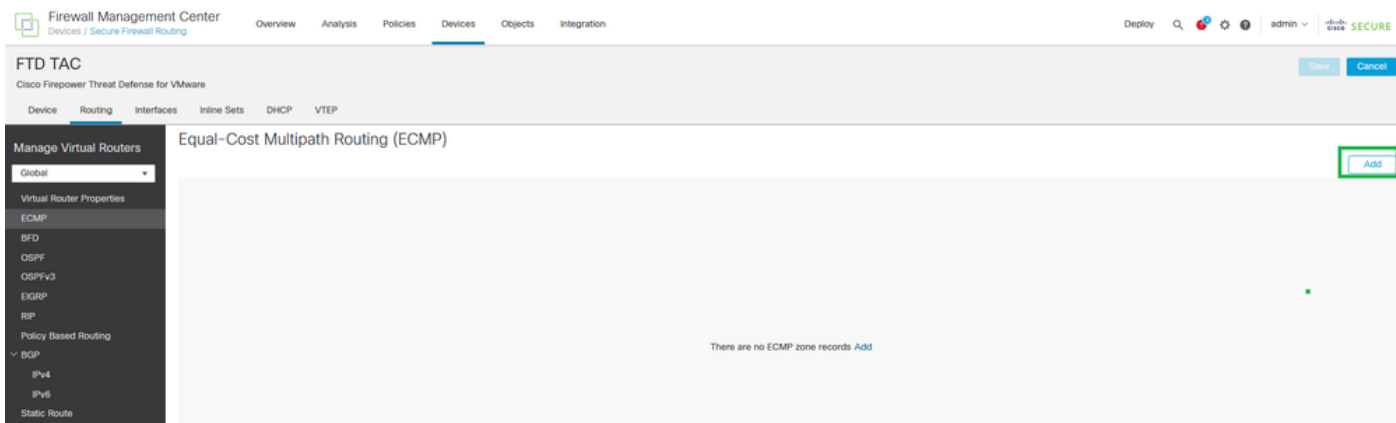
Périphérique - Gestion des périphériques

Étape 2. Accédez à **Routing > ECMP**.



Routage - ECMP

Étape 3. Cliquez sur **Add** afin de créer un ECMP entre les interfaces VTI et WAN (ISP-1 et ISP-2 pour ce guide de configuration).



Routage par trajets multiples à coût égal (ECMP)

Étape 4. Configurez le nom ECMP et sélectionnez toutes les interfaces VTI, puis cliquez sur Add.

Add ECMP

Name

VTI-ECMP

Available Interfaces

INSIDE
ISP-1
ISP-2

Selected Interfaces

VTI-1
VTI-2

Add

Cancel

OK

ECMP pour VTI

Étape 5. Répétez les étapes 3 et 4 afin de créer un ECMP entre les interfaces WAN (ISP-1 et ISP-2 pour ce guide de configuration).

Add ECMP

?

×

Name

ISP-ECMP

Available Interfaces

INSIDE
VTI-1
VTI-2

Add

Selected Interfaces

ISP-2
ISP-1

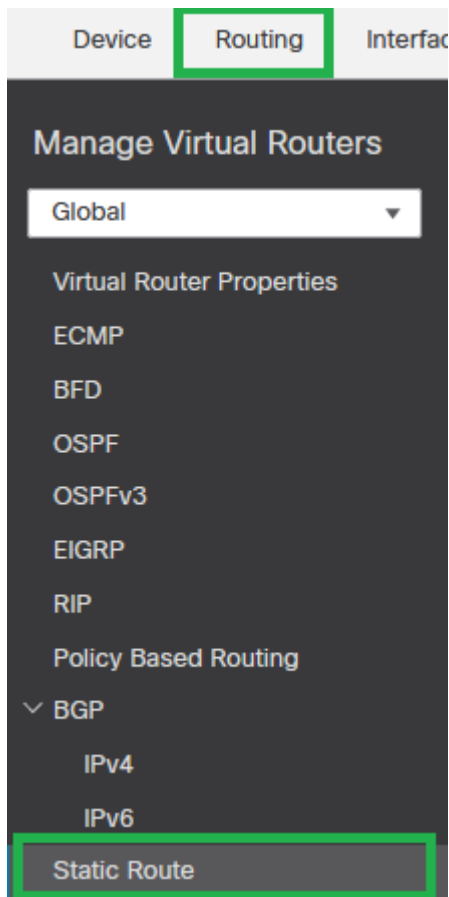
Cancel

OK

ECMP pour les interfaces ISP

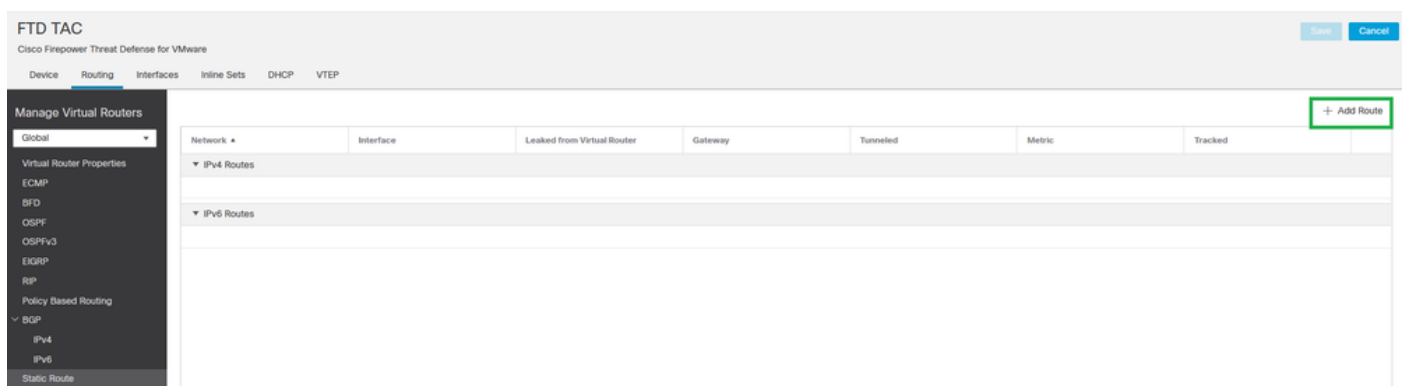
Étape 6 : enregistrement de la configuration ECMP

Étape 7 : configuration des routes statiques pour les interfaces de zone afin d'équilibrer la charge
Naviguez jusqu'à Routing > Static Route.



Routeage - Route statique

Étape 8. Cliquez sur + Add Route.



+ Ajouter une route

Étape 9. Créez une route statique par défaut pour la ou les interfaces VTI (VTI-1 pour ce guide de configuration) avec 1 comme valeur de mesure, puis cliquez sur 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

any-ipv4

IPv6-to-IPv4-Relay-Anycast

Selected Network

any-ipv4



Gateway*

VTI-Tunnel1-FPR2



Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:



Cancel

OK

Route statique par défaut pour VTI-1

Étape 10. Répétez l'étape 8. si d'autres interfaces VTI sont configurées.



Remarque : Créez une route par défaut pour chaque interface VTI configurée.

Étape 11. Créez une route statique par défaut pour la ou les interfaces WAN/ISP (ISP-1 pour ce guide de configuration) avec une valeur métrique supérieure à VTI, puis cliquez sur 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 statique par défaut pour ISP-1

Étape 12. Répétez l'étape 10. si d'autres interfaces WAN/ISP sont configurées.



Remarque : Créez une route par défaut pour chaque interface WAN/ISP configurée.

Étape 13. Validez la configuration des routes par défaut et cliquez sur OK.

FTD TAC
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

RFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

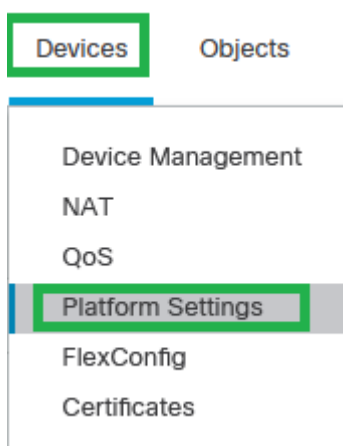
Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
IPv4 Routes							
any-ipv4	ISP-2	Global	172.16.11.254-GW-24	false	10		
any-ipv4	ISP-1	Global	172.16.1.254GW-24	false	10		
any-ipv4	VTI-2	Global	VTI-Tunnel2-FPR2	false	1		
any-ipv4	VTI-1	Global	VTI-Tunnel1-FPR2	false	1		
IPv6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

+ Add Route

Configuration de route statique

Configurer le DNS sécurisé pour le FTD sécurisé

Étape 1. Accédez à **Devices > Platform Settings**.



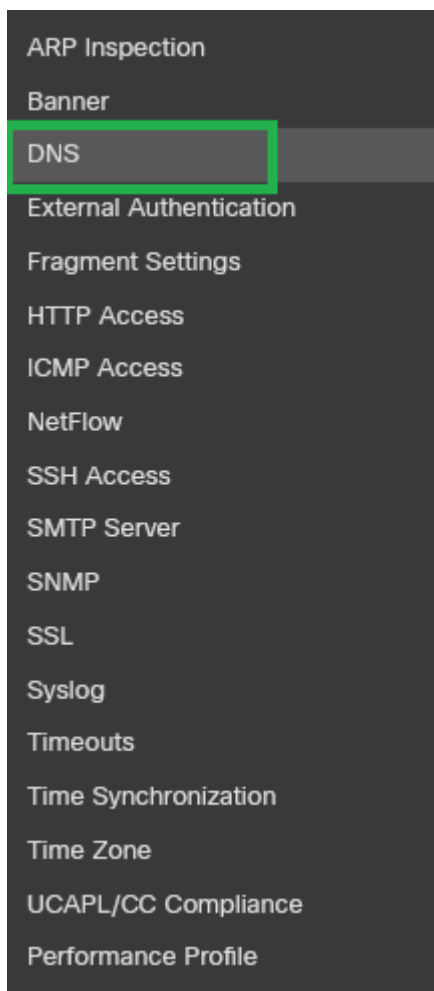
Périphériques - Paramètres de plateforme

Étape 2 : création ou modification d'une stratégie de paramètres de plate-forme existante



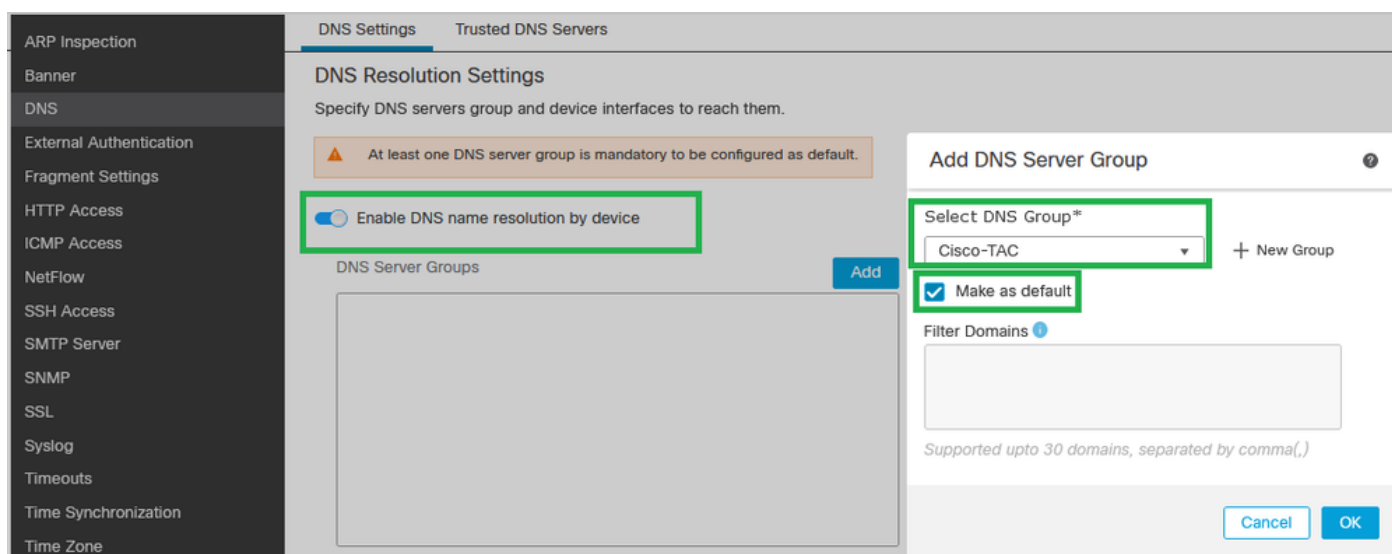
Remarque : Assurez-vous que la stratégie des paramètres de plate-forme est appliquée aux périphériques Secure Threat Defense.

Étape 3. Cliquez sur **DNS**.



Paramètres de plateforme DNS

Étape 4. Activez DNS name resolution by device et cliquez sur Add ou sélectionnez un groupe DNS existant. Choisissez Make as default, puis cliquez sur OK.



Ajouter un groupe de serveurs DNS



Remarque : Si vous voulez en savoir plus sur la configuration DNS sur la stratégie des

paramètres de plateforme, consultez la documentation [officielle des paramètres de plateforme](#).

Étape 5. Choisissez les interfaces WAN/ISP sous la section Interface Objects.

The screenshot displays the configuration page for DNS. On the left is a dark sidebar with a list of settings: ARP Inspection, Banner, DNS (highlighted), External Authentication, Fragment Settings, HTTP Access, ICMP Access, NetFlow, SSH Access, SMTP Server, SNMP, SSL, Syslog, Timeouts, Time Synchronization, Time Zone, UCAPL/CC Compliance, and Performance Profile.

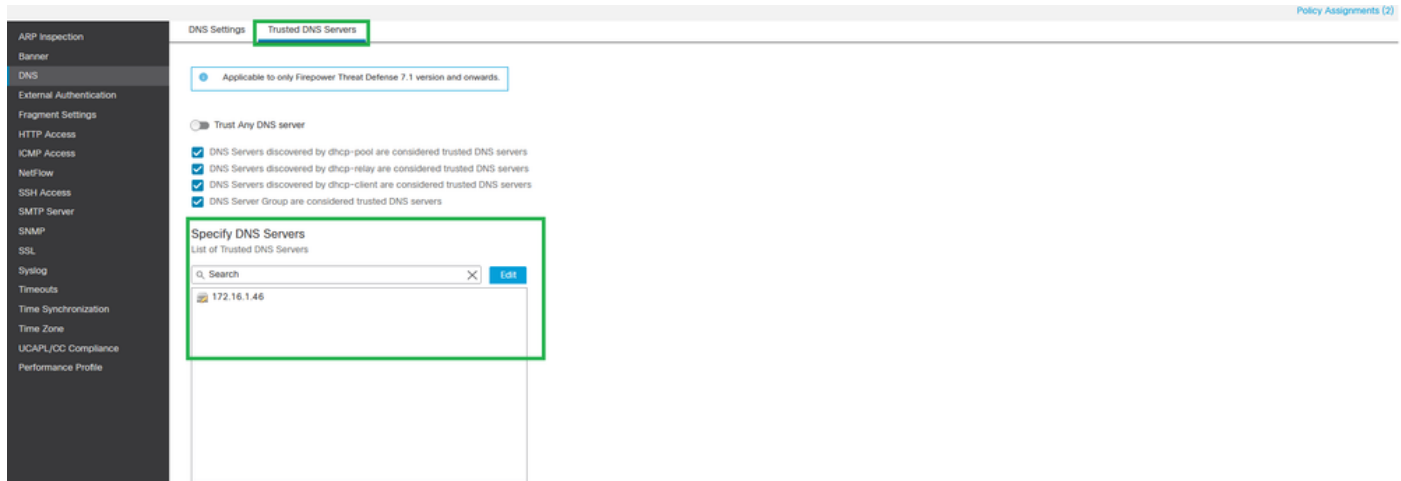
The main content area is divided into several sections:

- Expiry Entry Timer:** A text input field containing the value '1', with a range of 1-65535 minutes.
- Poll Timer:** A text input field containing the value '240', with a range of 1-65535 minutes.
- Interface Objects:** This section is highlighted with a green box. It contains the text: "Devices will use specified interface objects for connecting with DNS Servers." Below this text are two panels:
 - Available Interface Objects:** A list with a search bar. The items are INSIDE, ISP-1, ISP-2 (highlighted in blue), VTI-1, VTI-11, and VTI-2. An 'Add' button is located to the right of this list.
 - Selected Interface Objects:** A list containing ISP-1 and ISP-2, each with a trash icon to its right. This panel is also highlighted with a green box.
- Enable DNS Lookup via diagnostic/Management interface also:** A checkbox that is currently unchecked.

Configuration de l'interface DNS

Étape 6 : enregistrement des modifications

Étape 7. Accédez à l' Trusted DNS Servers et spécifiez les serveurs DNS approuvés.

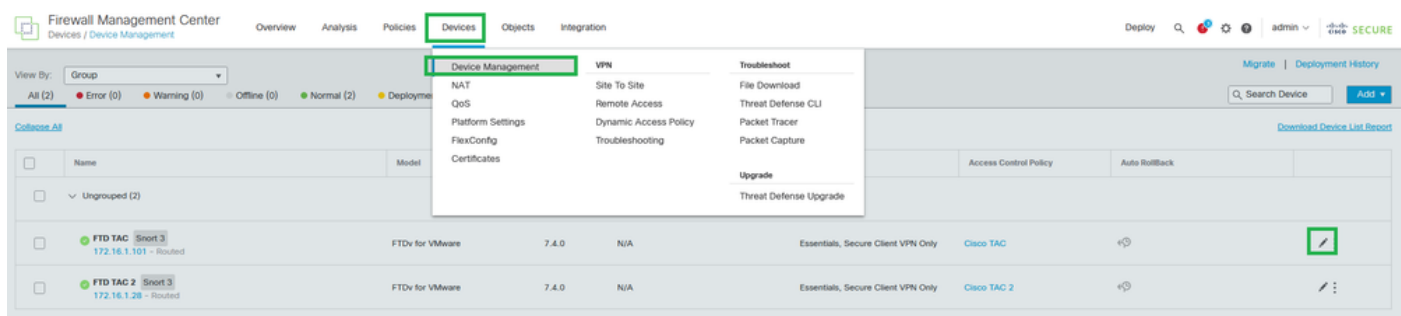


Serveurs DNS approuvés

Étape 8. Cliquez sur **Save** et déployez les modifications.

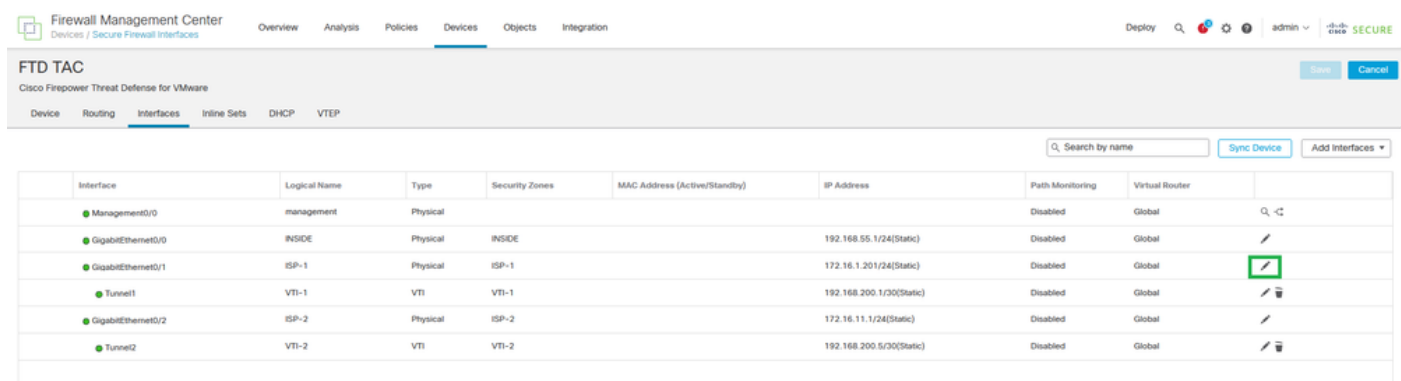
Activer la surveillance des chemins

Étape 1. Accédez à la défense contre les menaces **Devices > Device Management** et modifiez-la.



Périphérique - Gestion des périphériques

Étape 2. Sous l' **Interfaces** onglet , modifiez les interfaces WAN/ISP (ISP-1 et ISP-2 pour ce guide de configuration).



Configuration de l'interface

Étape 3. Cliquez sur l' **Path Monitoring** onglet, sélectionnez l' **Enable IP Monitoring** et activez la case à cocher **HTTP-based Application Monitoring**. Cliquez ensuite sur **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

Configuration du contrôle du chemin d'interface



Mise en garde : Les applications configurées dans la section de configuration précédente doivent être répertoriées.



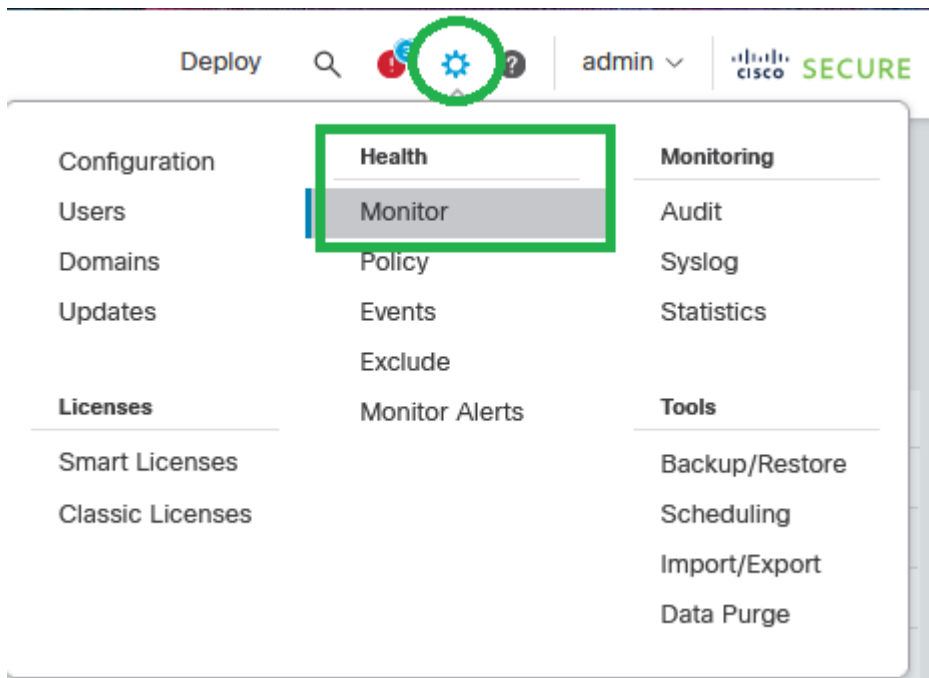
Remarque : 'Type de surveillance' a été choisi pour ce guide de configuration. Consultez les paramètres de surveillance du chemin dans le [guide de configuration officiel](#) afin d'en savoir plus sur les autres options.

Étape 4. Répétez les étapes 2 et 3 pour toutes les interfaces WAN/ISP configurées.

Étape 5. Cliquez sur **Save** et déployez les modifications.

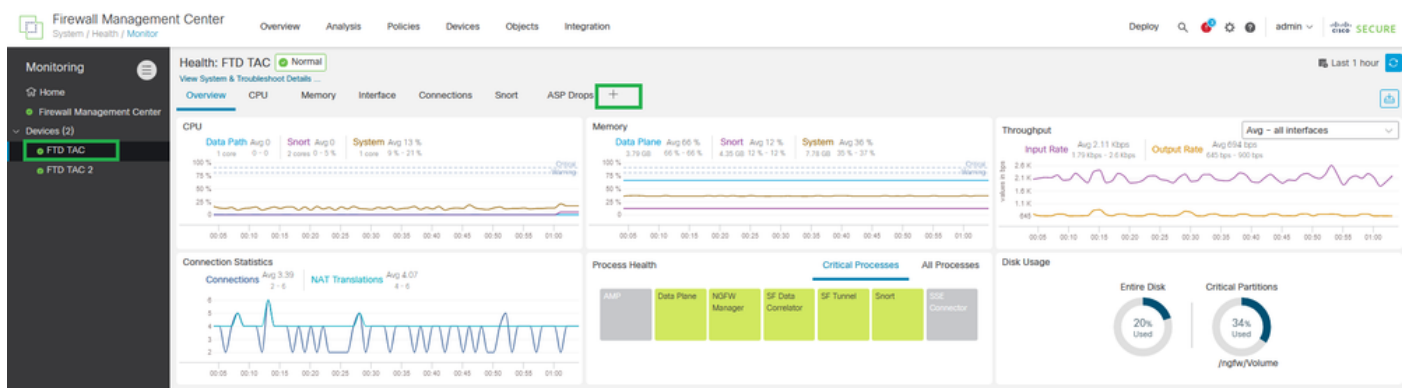
Ajouter un tableau de bord Surveillance

Étape 1. Accédez à **System > Health > Monitor**.



Système - État - Moniteur

Étape 2. Choisissez le périphérique Secure FTD, puis cliquez sur Add New Dashboard.



Ajouter un nouveau tableau de bord

Étape 3. Configurez le nom du tableau de bord et, dans la boîte de dialogue, Correlate Metrics dans la liste déroulante, sélectionnez Interface - Path Metrics. Cliquez ensuite sur 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

Ajouter un nouveau tableau de bord avec des métriques de chemin

Vérifier

Cette section décrit comment vérifier les routes statiques flottantes, ECMP, le groupe d'objets avec les applications et les configurations PBR.

Vérifiez la configuration des routes par défaut et des routes statiques flottantes :

```
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
```

Vérifiez la configuration ECMP :

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

Vérifiez si le trafic est équilibré par le protocole ECMP, dans la table de routage. La table de routage doit installer les deux routes sur la table de routage Secure FTD.

```
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
```

Vérifiez la configuration de la carte de routage 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
!
```

Vérifiez la liste de contrôle d'accès attribuée à la configuration PBR (vérifiez le nom de la liste de contrôle d'accès dans la configuration route-map) :

```
firepower# show run access-list | i Applications
access-list Applications extended permit ip any object-group-network-service FMC_NSQ_639950173988
```

Vérifiez le groupe d'objets avec les applications affectées à la liste d'accès (vérifiez le nom du groupe d'objets dans la configuration de la liste de contrôle d'accès) :

```
firepower# show run object-group
object-group network-service FMC_NSQ_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"
```

Vérifiez la route de stratégie attribuée aux interfaces de données utilisées dans la configuration 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
!

```

Vérifiez les statistiques de gigue, de MOS, de temps de parcours aller-retour et de perte de paquets à partir des informations du tableau de bord de surveillance du chemin HTTP.



Vérification du tableau de bord de surveillance du chemin HTTP

Dépannage

En cas d'échec de la surveillance du chemin, lorsque la surveillance basée sur IP est activée, les interfaces WAN/ISP sont configurées pour envoyer des paquets de sonde ICMP à la passerelle

configurée sur les routes statiques. Configurez les captures d'entrée/sortie sur les interfaces WAN/ISP afin de vérifier si le protocole ICMP fonctionne.

Capture d'entrée et de sortie :

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

Capture d'entrée :

```
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
```

Capture de sortie :

```
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
```



Mise en garde : Assurez-vous de configurer les captures avec les adresses IP source et de destination, car les captures peuvent considérablement améliorer les performances de la boîte.



Conseil : Si la commande ping ne fonctionne pas, dépannez la connexion directe avec la passerelle par défaut, consultez la table ARP ou contactez le centre d'assistance technique Cisco.

Afin de vérifier si PBR fonctionne, vous pouvez utiliser l'outil Packet Tracer pour vous assurer que le trafic d'application est routé avec 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
```



Remarque : Afin d'en savoir plus sur les adresses IP d'application pour le service réseau configuré sur les groupes d'objets, utilisez la commande `show object-group network-service detail`.

Informations connexes

D'autres documents relatifs à PBR avec HTTP Path Monitoring sont disponibles ici :

- [Guide de configuration du routage basé sur des politiques sur le périphérique Secure Firewall Management Center](#)
- [Guide de configuration du périphérique Path Monitoring on Policy-Based Routing Configuration on Secure Firewall Management Center](#)
- [Configurer une politique de routage basée sur des politiques](#)
- [Exemple de configuration du routage basé sur des stratégies](#)
- [Exemple de configuration de la surveillance du chemin PBR](#)
- [Ajouter un tableau de bord de surveillance des chemins](#)
- [Guide de configuration des paramètres de la plate-forme DNS sur le périphérique Secure Firewall Management Center](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.