

Konfiguration von PBR mit HTTP Path Monitor auf FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[PBR für HTTP-Pfadüberwachung konfigurieren](#)

[Konfigurieren von Equal-Cost-Multi-Path \(ECMP\)](#)

[Vertrauenswürdige DNS für sichere FTD konfigurieren](#)

[Pfadüberwachung aktivieren](#)

[Überwachungskonsole hinzufügen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie richtlinienbasiertes Routing (Policy-Based Routing, PBR) mit HTTP-Pfadüberwachung auf dem Cisco Secure Firewall Management Center (FMC) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- PBR Basiswissen
- Grundlegende Erfahrung mit Cisco Secure Management Center
- Grundlegender Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware mit Version 7.4
- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware mit Version 7.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Beim herkömmlichen Routing werden Pakete basierend auf der Ziel-IP-Adresse geroutet. Es ist jedoch schwierig, das Routing des spezifizierten Datenverkehrs in einem zielbasierten Routing-System zu ändern. PBR bietet Ihnen mehr Kontrolle über das Routing, indem die vorhandenen Mechanismen der Routing-Protokolle erweitert und ergänzt werden.

Mit PBR kann die IP-Rangfolge festgelegt werden. Darüber hinaus können Sie einen Pfad für bestimmten Datenverkehr festlegen, z. B. für Prioritätsdatenverkehr über eine teure Verbindung. Beim PBR basiert das Routing auf anderen Kriterien als dem Zielnetzwerk, wie Quellport, Zieladresse, Zielport, Protokollanwendungen oder einer Kombination dieser Objekte. PBR kann verwendet werden, um den Netzwerkverkehr basierend auf Anwendung, Benutzername, Gruppenmitgliedschaft und Sicherheitsgruppenzuordnung zu klassifizieren. Diese Routing-Methode eignet sich in Situationen, in denen eine Vielzahl von Geräten in einer umfangreichen Netzwerkbereitstellung auf Anwendungen und Daten zugreift. Traditionell weisen große Bereitstellungen Topologien auf, bei denen der gesamte Netzwerkverkehr als verschlüsselter Datenverkehr in einem gerouteten VPN auf einen Hub zurücktransportiert wird. Diese Topologien führen häufig zu Problemen wie Paketlatenz, reduzierter Bandbreite und Paketverlusten.

PBR wird nur im Routing-Firewall-Modus unterstützt und nicht für embryonale Verbindungen. HTTP-basierte Anwendungen werden auf physischen Schnittstellen, Port-Channels, Subschnittstellen und Statustunnel-Schnittstellen unterstützt. Es wird nicht auf Clustergeräten unterstützt.

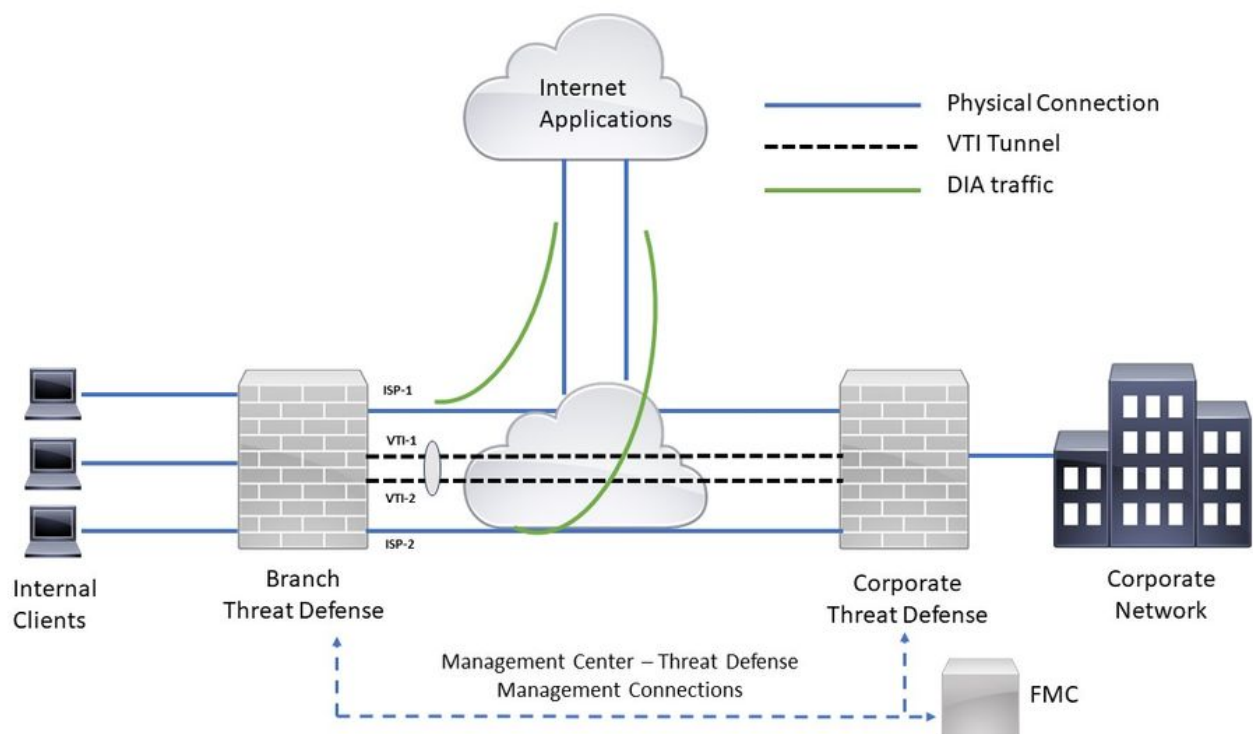
Wenn konfigurierte Schnittstellen Metriken wie Round-Trip Time (RTT), Jitter, Mean Opinion Score (MOS) und Paketverluste pro Schnittstelle ableiten, werden diese verwendet, um den besten Pfad für das Routing des PBR-Datenverkehrs zu bestimmen. Path Monitoring berechnet flexible Metriken für mehrere Remote-Peers pro Schnittstelle. Um den besten Pfad für mehrere Anwendungen über eine Richtlinie auf einer Firewall in einer Zweigstelle zu überwachen und zu bestimmen, wird HTTP aus den folgenden Gründen gegenüber ICMP bevorzugt:

- HTTP-Ping kann die Leistungsmetriken des Pfads bis zur Anwendungsebene des Servers ableiten, auf dem die Anwendung gehostet wird.
- Die Notwendigkeit, die Firewall-Konfiguration bei jeder Änderung der IP-Adresse des Anwendungsservers zu ändern, entfällt, wenn die Anwendungsdomäne anstatt der IP-Adresse verfolgt wird.

Konfigurieren

Netzwerkdiagramm

Ein typisches Szenario für Unternehmensnetzwerke sieht vor, dass der gesamte Netzwerkverkehr der Außenstelle über ein routenbasiertes VPN des Unternehmensnetzwerks gesendet wird und bei Bedarf zum Extranet ausweicht. Die nächste Topologie zeigt ein Zweigstellennetzwerk, das über ein routenbasiertes VPN mit dem Unternehmensnetzwerk verbunden ist. Bisher wurde der unternehmensinterne Bedrohungsschutz so konfiguriert, dass er sowohl den internen als auch den externen Datenverkehr der Zweigstelle verarbeitet. Mit der PBR-Richtlinie wird der Bedrohungsschutz für die Außenstelle mit einer Richtlinie konfiguriert, die bestimmten Datenverkehr an das WAN-Netzwerk und nicht an die virtuellen Tunnel weiterleitet. Der restliche Datenverkehr fließt wie gewohnt über das routenbasierte VPN.



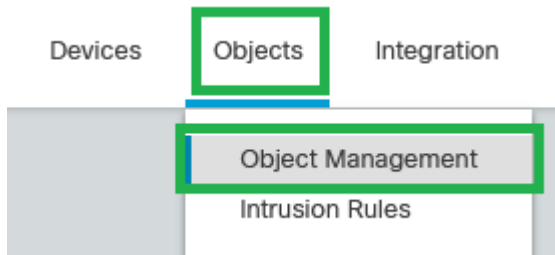
Netzwerktopologie

Im Abschnitt `configure` wird davon ausgegangen, dass die ISP- und VTI-Schnittstellen bereits für den Schutz vor Bedrohungen in der Außenstelle im Secure FMC konfiguriert sind.

PBR für HTTP-Pfadüberwachung konfigurieren

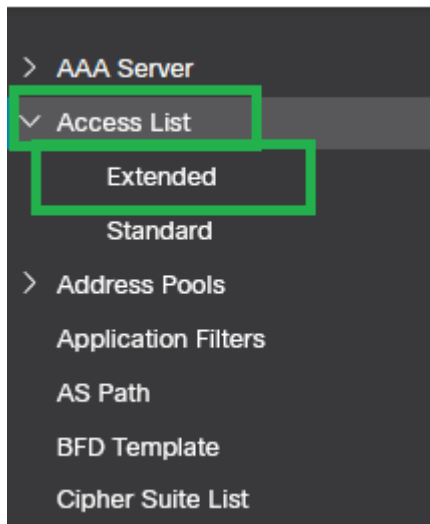
Dieser Konfigurationsabschnitt zeigt die Pfadüberwachungskonfiguration für ISP-1- und ISP-2-Schnittstellen.

Schritt 1: Erstellen einer erweiterten Zugriffsliste für überwachte Anwendungen Navigieren Sie zu `.Objects > Object Management`



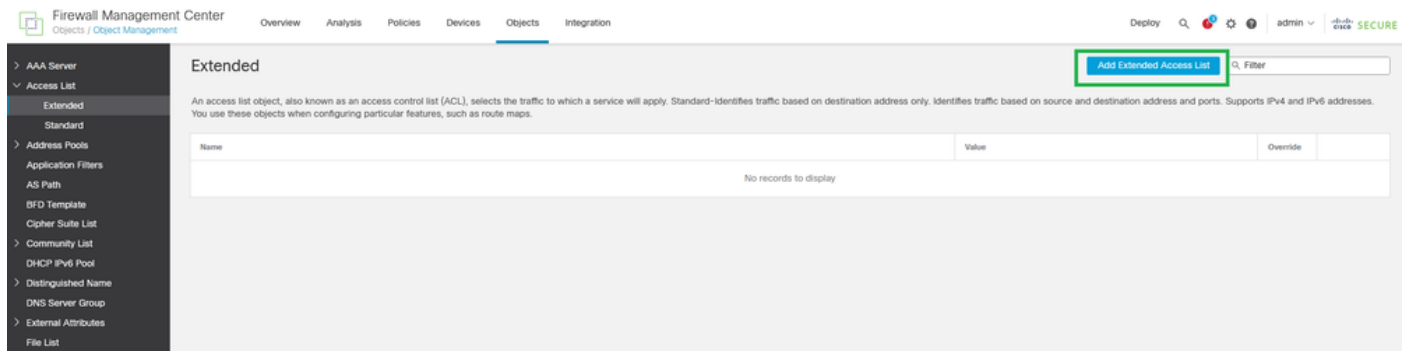
Objekte - Objektmanagement

Schritt 2. Navigieren Sie im Menü links zu Access-list > Extended .



Zugriffsliste - Erweitert

Schritt 3. Klicken Sie auf Add Extended Access List.



Erweiterte Zugriffsliste hinzufügen

Schritt 4: Richten Sie einen Namen in der erweiterten Zugriffsliste ein, und klicken Sie auf 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

Neues erweitertes Zugriffslistenobjekt

Schritt 5: Klicken Sie auf **Application** , und wählen Sie die gewünschten Anwendungen aus (für dieses Beispiel wurden einige Cisco Anwendungen ausgewählt). Klicken Sie dann auf **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

Erweiterten Zugriffslisteneintrag hinzufügen



Anmerkung: Die erweiterte Zugriffsliste kann mit Quell-/Ziel-IPs und Ports konfiguriert werden, um den spezifischen Datenverkehr den gewünschten Anwendungen zuzuordnen. Sie können mehrere erweiterte Zugriffskontrolllisten erstellen, um diese auf die PBR-Konfiguration anzuwenden.

Schritt 6: Validieren Sie die Konfiguration der erweiterten Zugriffsliste, und klicken Sie auf **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

Objekt der erweiterten Zugriffsliste speichern

Schritt 7. Navigieren Sie zum **Devices > Device Management** Threat Defence, und bearbeiten Sie ihn.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

View By: Group

Device Management

Name	Model	Version	Location	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		

Gerät - Gerätemanagement

Schritt 8: Navigieren Sie zu **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

VTI-1

VTI-2

Selected Interfaces

management

ISP-1

VTI-2

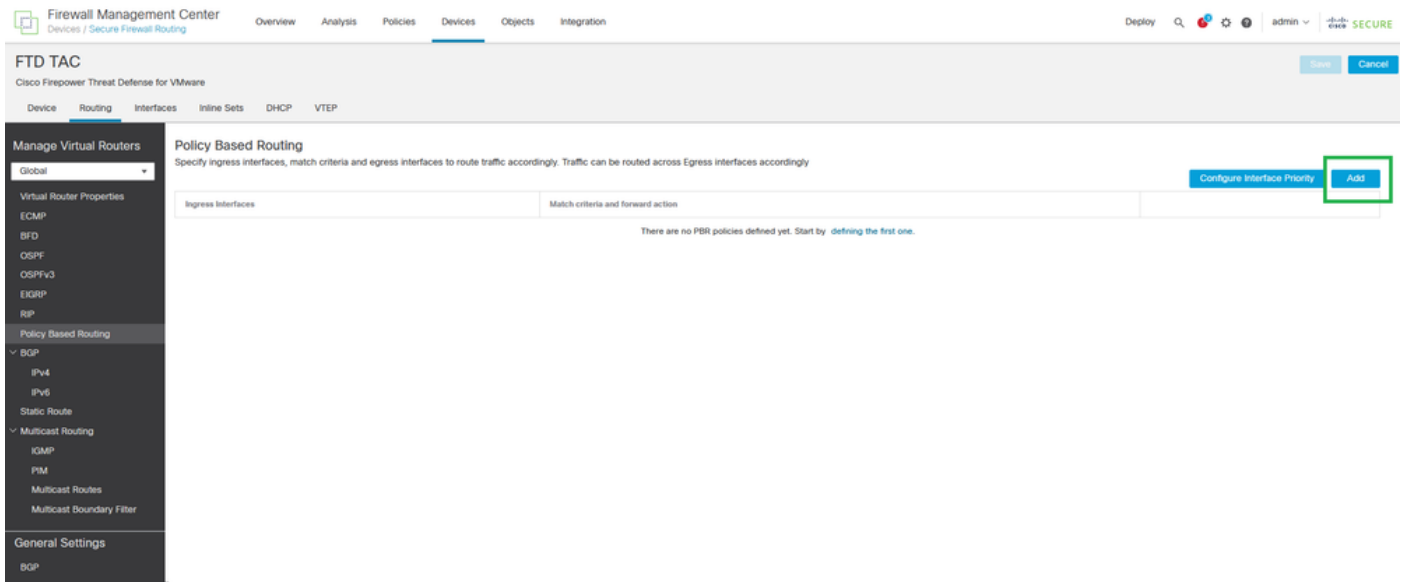
INSIDE

VTI-1

ISP-2

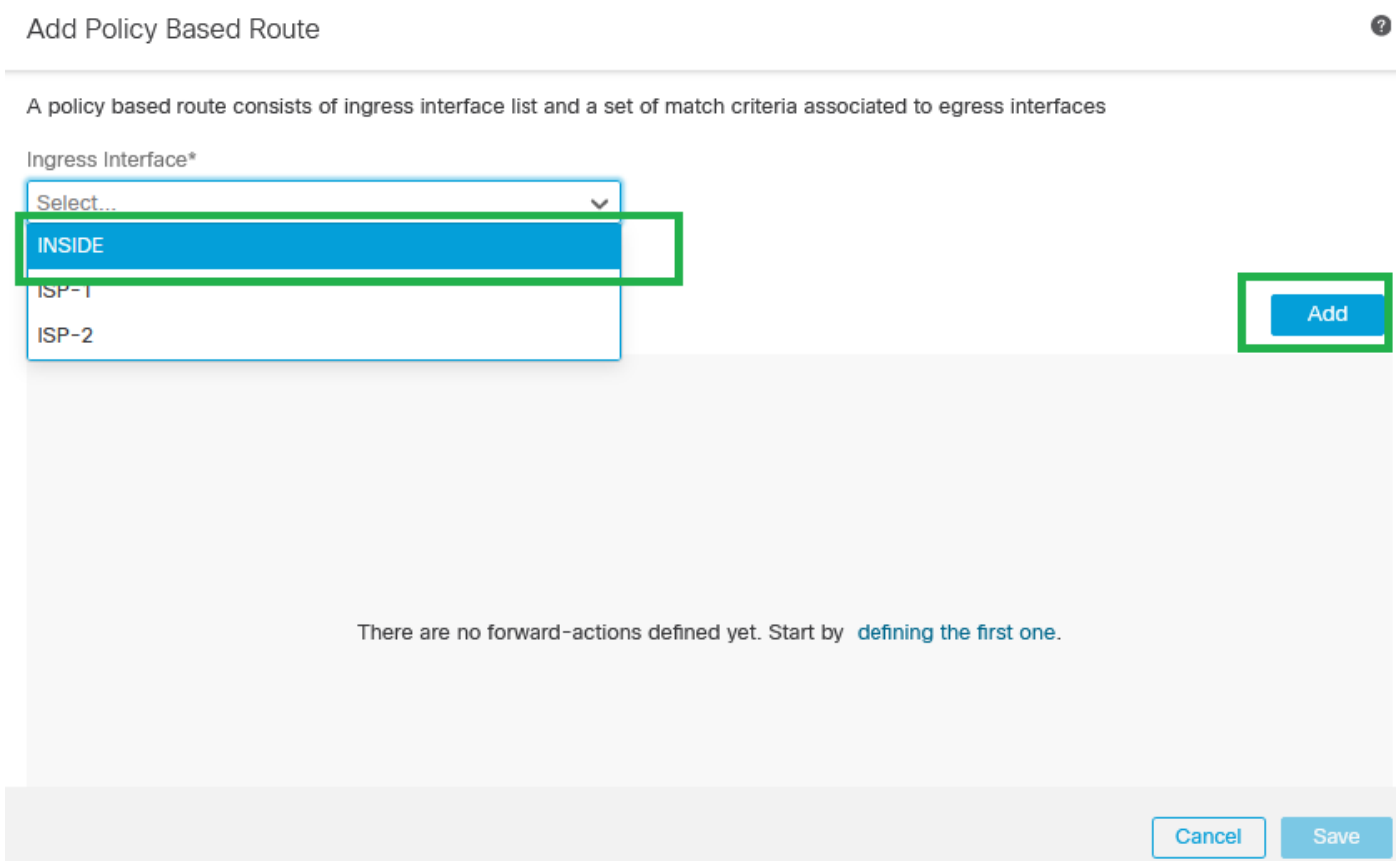
Routing - Richtlinienbasiertes Routing

Schritt 9: Klicken Sie auf **Add**.



Richtlinienbasiertes Routing hinzufügen

Schritt 10: Fügen Sie die Eingangsschnittstelle für die PBR-Konfiguration hinzu (in diesem Beispiel INSIDE), und klicken Sie dann auf Add.



Richtlinienbasierte Route hinzufügen

Schritt 11: Definieren der Zuordnungskriterien (wobei die erweiterte Zugriffsliste in den vorherigen Schritten erstellt wurde), der Ausgangsschnittstellen und der Schnittstellenbestellung.

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

Weiterleitungsaktionen hinzufügen



Hinweis: Egress Interfaces und Minimal Jitter wurden für diesen Konfigurationsleitfaden ausgewählt. Weitere Informationen zu den anderen Optionen finden Sie in der [offiziellen PBR-Dokumentation](#).

Schritt 12: Wählen Sie die Ausgangsschnittstellen (in diesem Beispiel ISP-1 und ISP-2) aus, und klicken Sie dann auf **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

Ausgewählte Ausgangsschnittstellen

Schritt 13: Validieren Sie die PBR-Konfiguration, und klicken Sie auf **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

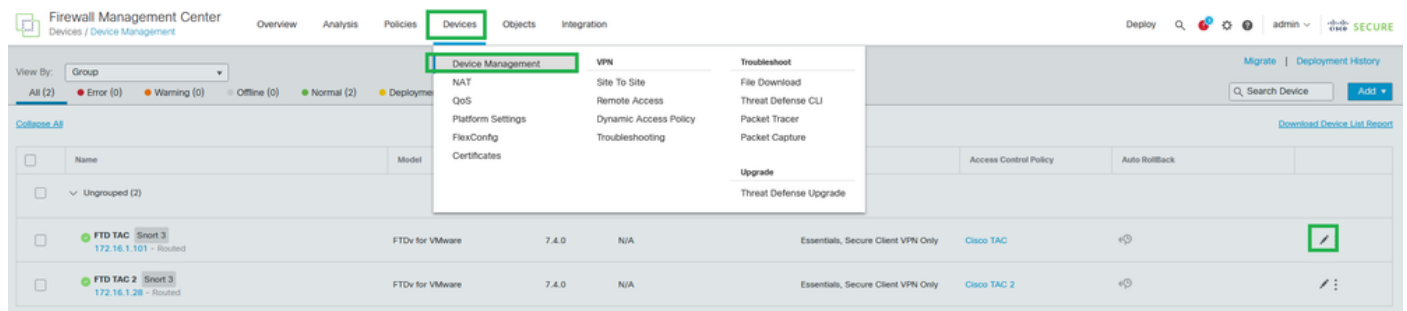
Save

Schritt 14: Wiederholen Sie optional die Schritte 9, 10, 11, 12 und 13, wenn weitere erweiterte Zugriffskontrolllisten erstellt wurden oder wenn mehrere Quellschnittstellen vorhanden sind, auf die die PBR-Konfiguration angewendet werden muss.

Schritt 15: Speichern und Bereitstellen von Änderungen vom FMC.

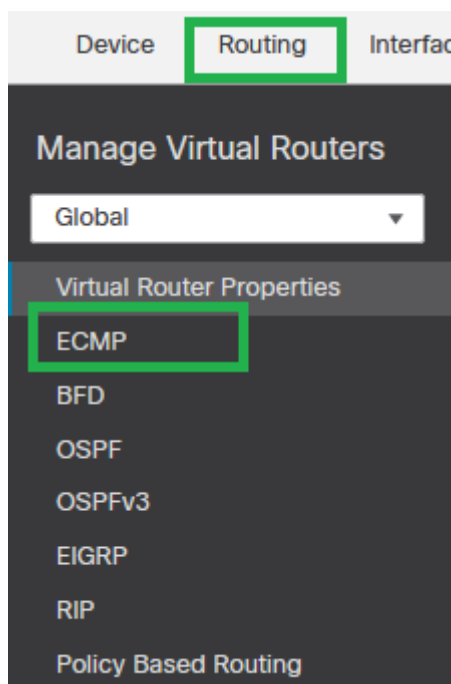
Konfigurieren von Equal-Cost-Multi-Path (ECMP)

Schritt 1: Navigieren Sie zu **Devices > Device Management** Threat Defence, und bearbeiten Sie diese.



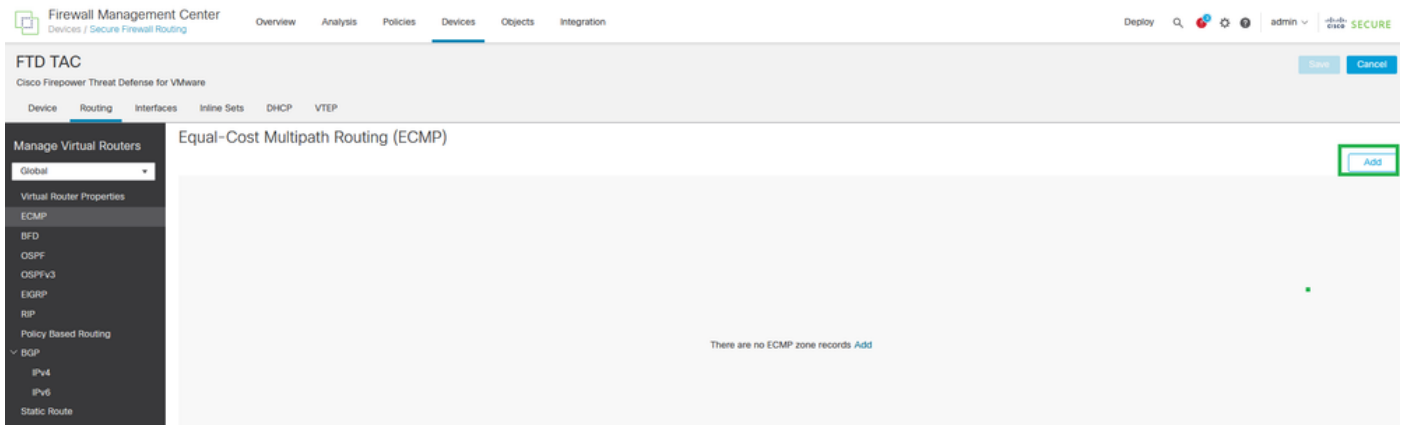
Gerät - Gerätemanagement

Schritt 2. Navigieren Sie zu **Routing > ECMP**.



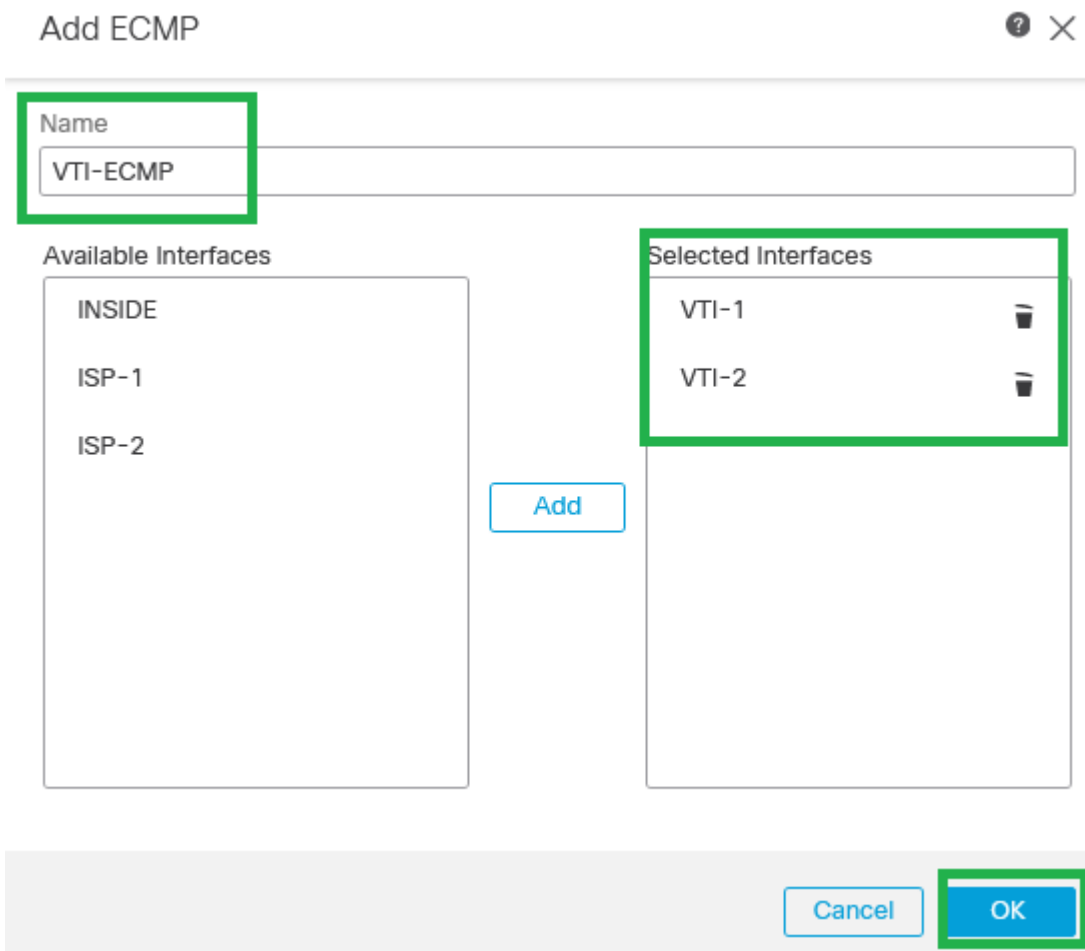
Routing - ECMP

Schritt 3: Klicken Sie hier **Add**, um ECMP zwischen den VTIs und den WAN-Schnittstellen zu erstellen (ISP-1 und ISP-2 für diese Konfigurationsanleitung).



Equal-Cost Multipath Routing (ECMP)

Schritt 4: Richten Sie den ECMP-Namen ein, und wählen Sie alle VTIs-Schnittstellen aus. Klicken Sie anschließend auf Add.



ECMP für VTIs

Schritt 5: Wiederholen Sie die Schritte 3 und 4, um ECMP zwischen WAN-Schnittstellen (ISP-1 und ISP-2 für diese Konfigurationsanleitung) zu erstellen.

Add ECMP? ×

Name

ISP-ECMP

Available Interfaces

INSIDE

VTI-1

VTI-2

Add

Selected Interfaces

ISP-2

ISP-1

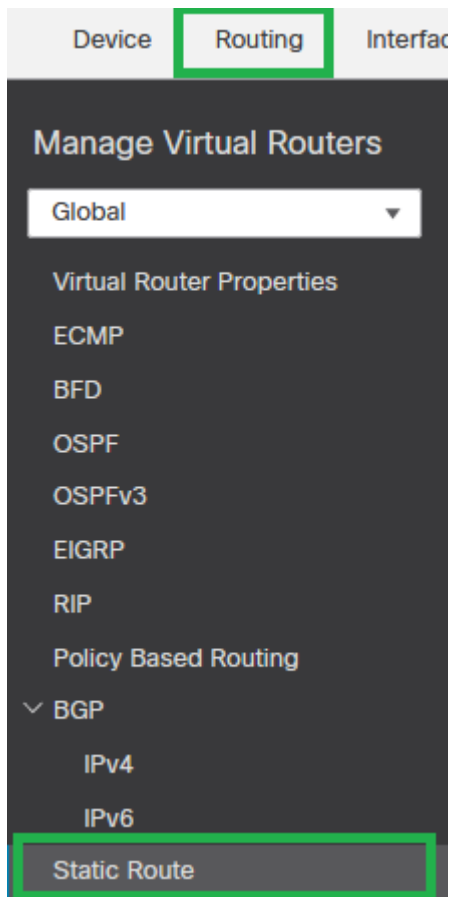
Cancel

OK

ECMP für ISP-Schnittstellen

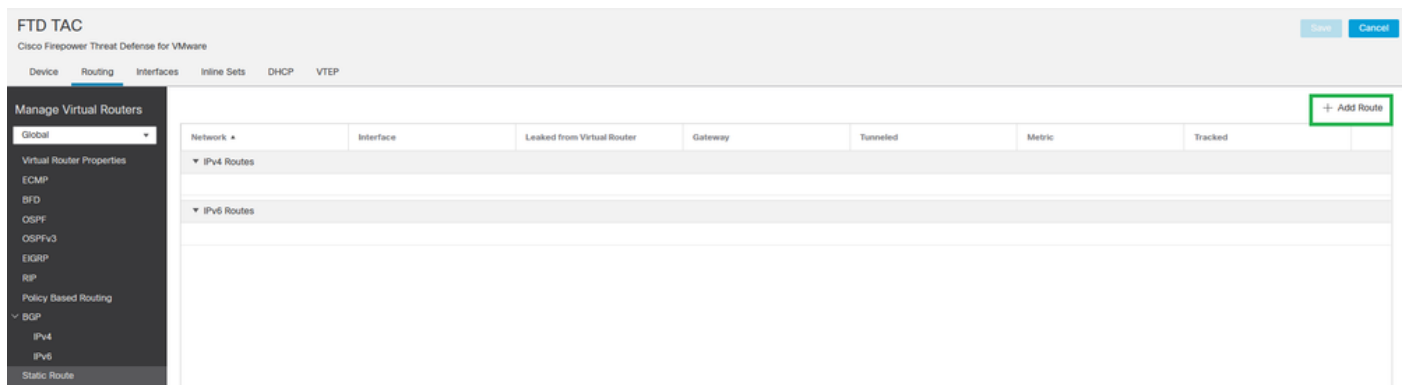
Schritt 6: Speichern der ECMP-Konfiguration

Schritt 7: Konfigurieren Sie die statischen Routen für die Zonenschnittstellen, um den Lastenausgleich zu erreichen. Navigieren Sie zu [Routing > Static Route](#).



Routing - Statische Route

Schritt 8: Klicken Sie auf + Add Route.



+ Route hinzufügen

Schritt 9: Erstellen Sie eine statische Standardroute für die VTI-Schnittstelle(n) (VTI-1 für diesen Konfigurationsleitfaden) mit 1 als Metrikwert, und klicken Sie dann auf 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

Standardmäßige statische Route für VTI-1

Schritt 10: Wiederholen Sie Schritt 8, wenn mehr VTI-Schnittstellen konfiguriert sind.



Anmerkung: Erstellen Sie eine Standardroute für jede konfigurierte VTI-Schnittstelle.

Schritt 11: Erstellen Sie eine statische Standardroute für die WAN/ISP-Schnittstelle(n) (ISP-1 für diesen Konfigurationsleitfaden) mit einem größeren metrischen Wert als VTI, und klicken Sie dann auf 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

Standardmäßige statische Route für ISP-1

Schritt 12: Wiederholen Sie Schritt 10, wenn mehr WAN/ISP-Schnittstellen konfiguriert sind.



Anmerkung: Erstellen Sie eine Standardroute für jede konfigurierte WAN/ISP-Schnittstelle.

Schritt 13: Validieren Sie die Konfiguration der Standardrouten, und klicken Sie auf 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

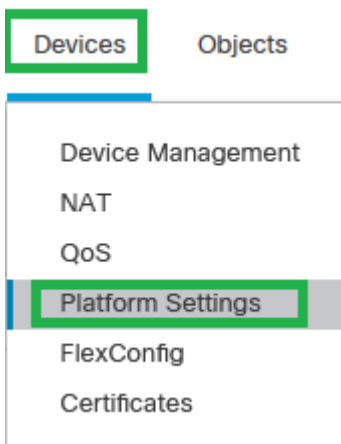
Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
IPv4 Routes							
any-ipv4	ISP-2	Global	172.16.11.254-GW-24	false	10		
any-ipv4	ISP-1	Global	172.16.1.254GW-24	false	10		
any-ipv4	VTI-2	Global	VTI-Tunnel2-FPR2	false	1		
any-ipv4	VTI-1	Global	VTI-Tunnel1-FPR2	false	1		
IPv6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

+ Add Route

Statische Routenkonfiguration

Vertrauenswürdige DNS für sichere FTD konfigurieren

Schritt 1. Navigieren Sie zu **Devices > Platform Settings**.



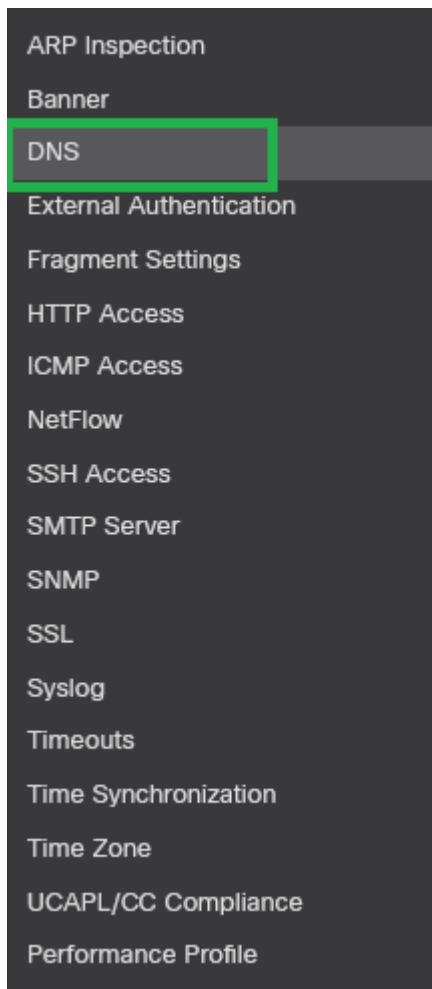
Geräte - Platformeinstellungen

Schritt 2: Erstellen oder bearbeiten Sie eine vorhandene Richtlinie für Platformeinstellungen.



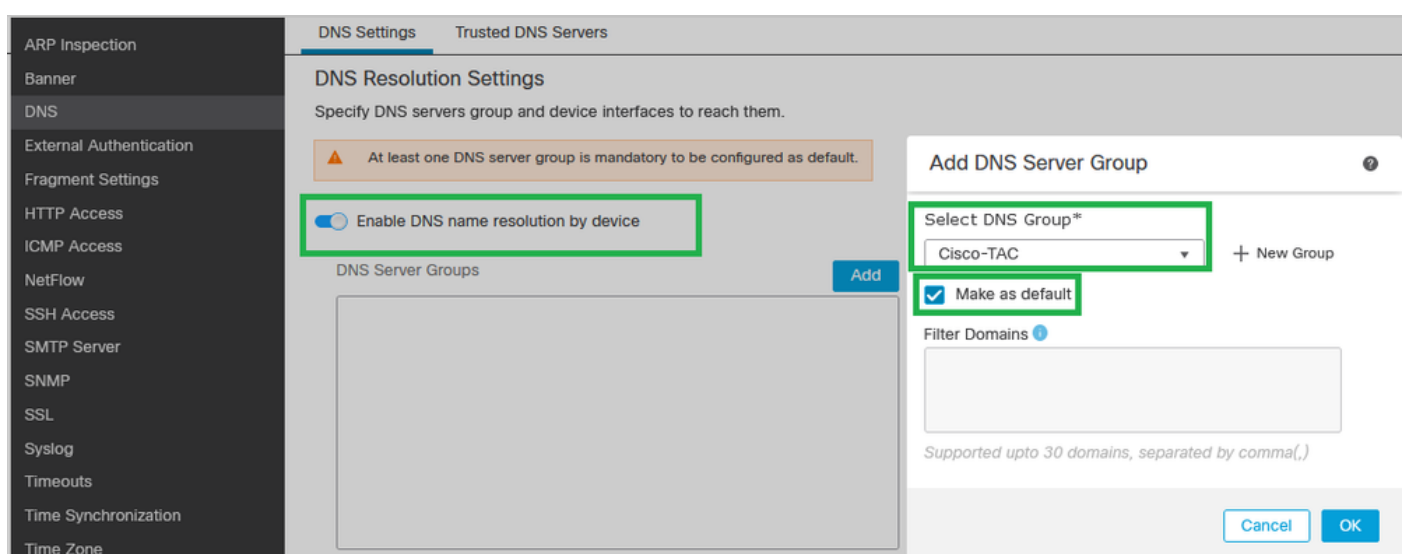
Anmerkung: Stellen Sie sicher, dass die Richtlinie für die Platformeinstellungen auf Geräte zum Schutz vor Bedrohungen angewendet wird.

Schritt 3. Klicken Sie auf **DNS**.



DNS-Plattformeinstellungen

Schritt 4: Aktivieren Sie die Option, DNS name resolution by device und klicken Sie auf eine vorhandene DNS-Gruppe, oder wählen Sie eine solche aus Add. Wählen Sie Make as default aus, und klicken Sie dann auf OK.



DNS-Servergruppe hinzufügen



Anmerkung: Weitere Informationen zur DNS-Konfiguration finden Sie in der [offiziellen Dokumentation](#) zu den [Plattformeneinstellungen](#).

Schritt 5: Wählen Sie im Abschnitt die WAN-/ISP-Schnittstellen aus Interface Objects.

The screenshot displays the DNS configuration page. 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 has a large empty box at the top. Below it are two input fields: 'Expiry Entry Timer:' with a value of '1' and 'Poll Timer:' with a value of '240', both with a range of 1-65535 minutes. The 'Interface Objects' section is highlighted with a green box. It contains the text 'Devices will use specified interface objects for connecting with DNS Servers.' Below this is a list of 'Available Interface Objects' (INSIDE, ISP-1, ISP-2, VTI-1, VTI-11, VTI-2) with a search bar and a refresh icon. A blue 'Add' button is next to the list. To the right, the 'Selected Interface Objects' box (also highlighted with a green box) contains 'ISP-1' and 'ISP-2', each with a trash icon. At the bottom, there is a checkbox labeled 'Enable DNS Lookup via diagnostic/Management interface also.'.

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

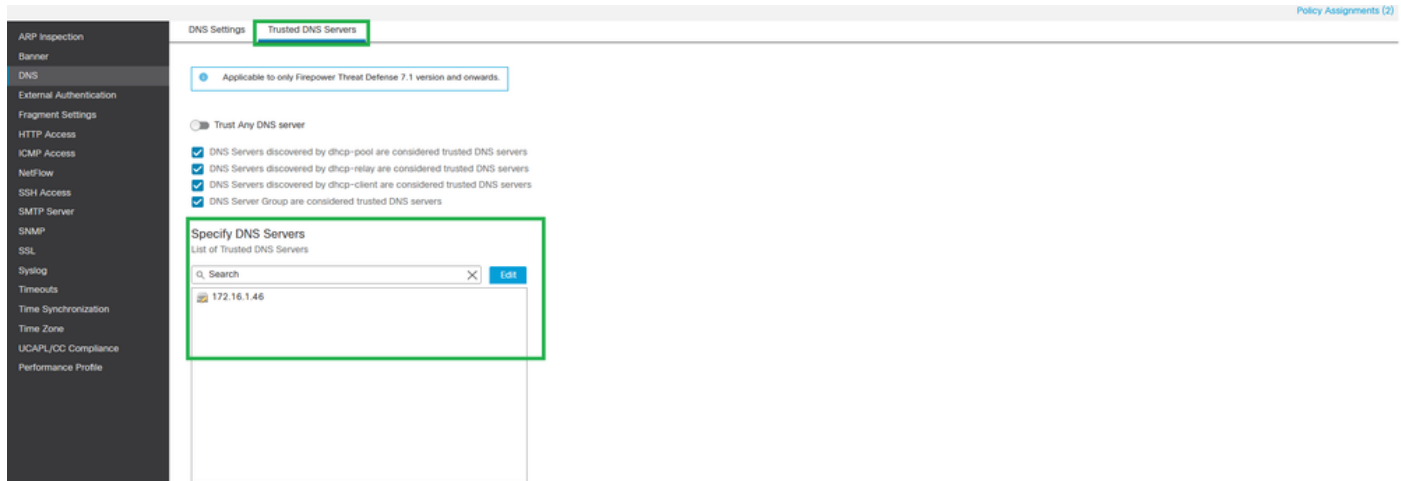
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

DNS-Schnittstellenkonfiguration

Schritt 6: Speichern der Änderungen

Schritt 7: Navigieren Sie zum , und geben Sie die Trusted DNS Servers vertrauenswürdigen DNS-Server an.

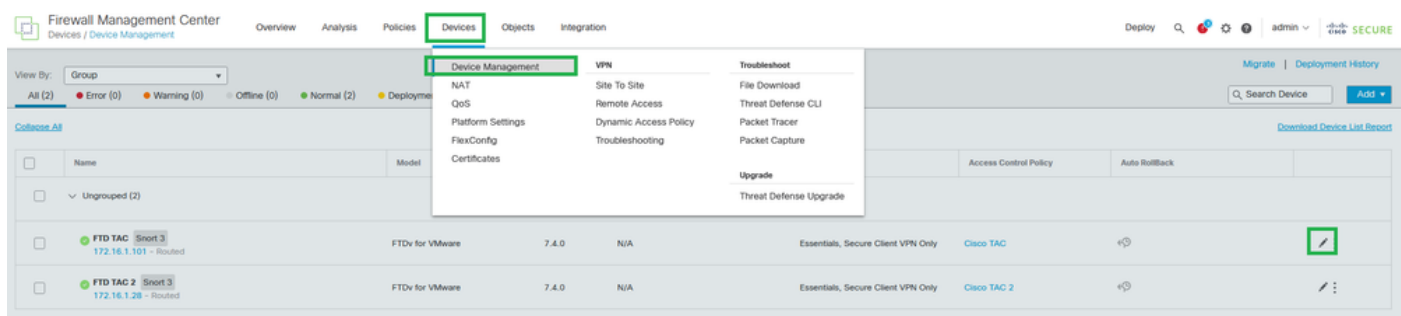


Trusted DNS Server

Schritt 8: Klicken Sie auf **Save**, und stellen Sie die Änderungen bereit.

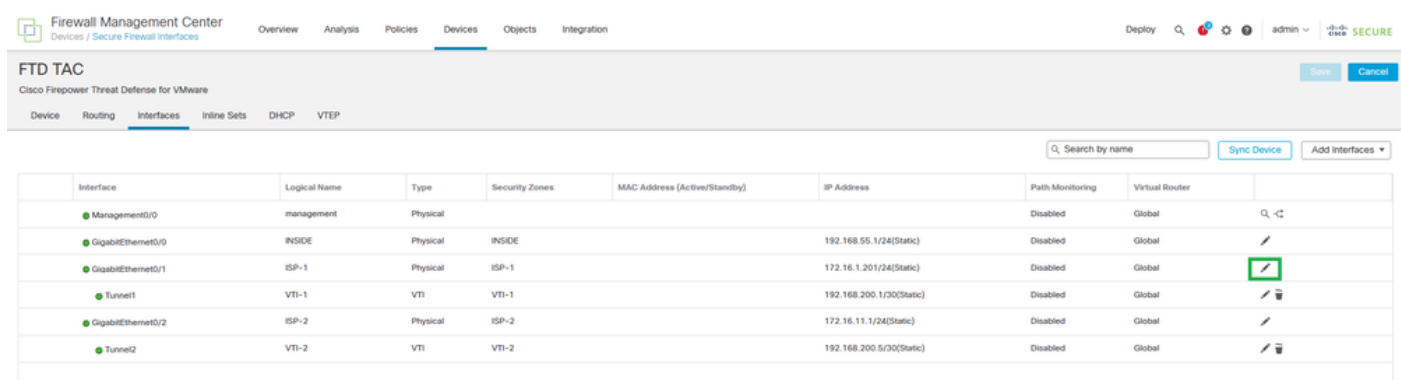
Pfadüberwachung aktivieren

Schritt 1: Navigieren Sie zu **Devices > Device Management** Threat Defence, und bearbeiten Sie diese.



Gerät - Gerätemanagement

Schritt 2: Bearbeiten Sie auf der **Interfaces** Registerkarte die WAN/ISP-Schnittstellen der Schnittstelle (ISP-1 und ISP-2 für diese Konfigurationsanleitung).



Schnittstellenkonfiguration

Schritt 3. Klicken Sie auf die **Path Monitoring** Registerkarte, wählen Sie die **Enable IP Monitoring** und aktivieren Sie das **HTTP-based Application Monitoring** Kontrollkästchen. Klicken Sie dann auf **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

Konfiguration der Schnittstellenpfadüberwachung



Vorsicht: Die Anwendungen, die im vorherigen Konfigurationsabschnitt konfiguriert wurden, müssen aufgeführt werden.



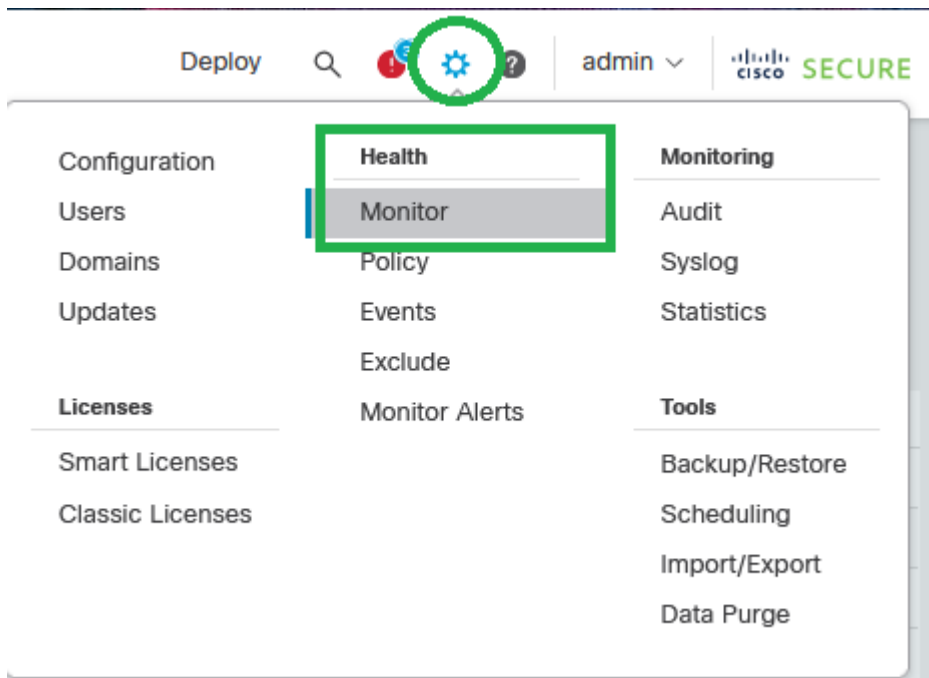
Anmerkung: 'Überwachungstyp' wurde für diesen Konfigurationsleitfaden ausgewählt. Überprüfen Sie die Pfadüberwachungseinstellungen im [offiziellen Konfigurationsleitfaden](#), um mehr über andere Optionen zu erfahren.

Schritt 4: Wiederholen Sie die Schritte 2 und 3 für alle konfigurierten WAN/ISP-Schnittstellen.

Schritt 5: Klicken Sie auf **Save**, und stellen Sie die Änderungen bereit.

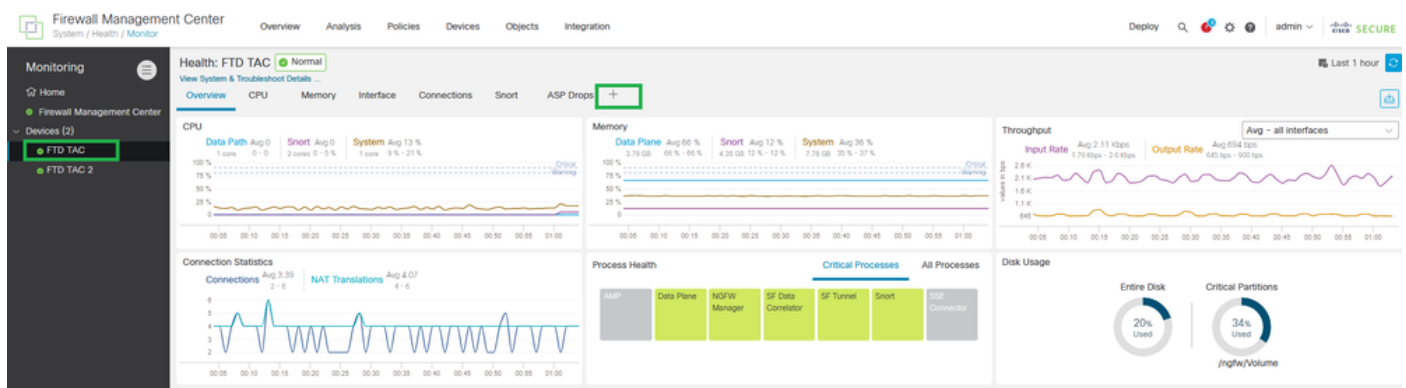
Überwachungskonsole hinzufügen

Schritt 1. Navigieren Sie zu **System > Health > Monitor**.



System - Zustand - Monitor

Schritt 2. Wählen Sie das sichere FTD-Gerät, und klicken Sie auf Add New Dashboard.



Neues Dashboard hinzufügen

Schritt 3: Richten Sie den Dashboard-Namen ein, und wählen Sie im Correlate Metrics Dialogfeld aus der Dropdown-Liste die Option Interface - Path Metrics. Klicken Sie dann auf 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



Interface

Mean Opinion Score (MOS) x



Interface

Round Trip Time x



Interface

Packet Loss x



Add Metrics

Add from Predefined Correlations



Clear All

Cancel

Add Dashboard

Neues Dashboard mit Pfadmetriken hinzufügen

Überprüfung

In diesem Abschnitt wird beschrieben, wie schwebende statische Routen, ECMP, Objektgruppen mit Anwendungen und PBR-Konfigurationen überprüft werden.

Überprüfen Sie die Konfiguration der Standardrouten und statischen Floating-Routen:

```
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
```

Überprüfen Sie die ECMP-Konfiguration:

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

Überprüfen Sie in der Routing-Tabelle, ob für den Datenverkehr ein Ausgleich durch den ECMP besteht. In der Routing-Tabelle müssen beide Routen in der Secure FTD-Routing-Tabelle

installiert werden.

```
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
```

Überprüfen der PBR-Routing-Map-Konfiguration:

```
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  
!
```

Überprüfen Sie die der PBR-Konfiguration zugewiesene ACL (überprüfen Sie den ACL-Namen in der Routing-Map-Konfiguration):

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

Überprüfen Sie die Objektgruppe mit Anwendungen, die der Zugriffsliste zugewiesen sind (überprüfen Sie den Namen der Objektgruppe in der ACL-Konfiguration):

```
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"
```

Überprüfen Sie die Richtlinienroute, die den auf der PBR-Konfiguration verwendeten Datenschnittstellen zugewiesen ist:

```
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
!
```

Überprüfen und überprüfen Sie die Statistiken zu Jitter, MOS, Round Trip Time und Paketverlusten in den HTTP Path Monitoring Dashboard-Informationen.



HTTP-Pfadüberwachungs-Dashboard überprüfen

Fehlerbehebung

Bei einem Ausfall der Pfadüberwachung, bei dem die IP-basierte Überwachung aktiviert ist, sind die WAN/ISP-Schnittstellen so konfiguriert, dass sie ICMP-Prüfpakete an das auf statischen Routen konfigurierte Gateway senden. Konfigurieren Sie Eingangs-/Ausgangserfassungen an WAN-/ISP-Schnittstellen, um zu überprüfen, ob ICMP funktioniert.

Erfassung von Ein- und Ausgängen:

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

Erfassung des Eingangs:

```
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
```

Erfassung am Ausgang:

```
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
```



Vorsicht: Stellen Sie sicher, dass die Erfassungen mit Quell- und Ziel-IP-Adressen konfiguriert werden, da Erfassungen die Leistung auf dem Gerät erheblich steigern können.



Tipp: Wenn der Ping-Befehl nicht funktioniert, beheben Sie die direkte Verbindung mit dem Standard-Gateway, überprüfen Sie die ARP-Tabelle, oder wenden Sie sich an das Cisco TAC.

Um zu überprüfen, ob PBR funktioniert, können Sie das Paket-Tracer-Tool verwenden, um sicherzustellen, dass der Anwendungsdatenverkehr mit PBR geroutet wird.

```
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
```



Anmerkung: Um mehr über die IP-Adressen der Anwendungen für den Netzwerkdienst zu erfahren, der für Objektgruppen konfiguriert wurde, verwenden Sie den Befehl `show object-group network-service detail`.

Zugehörige Informationen

Weitere Dokumente zu PBR mit HTTP Path Monitoring finden Sie hier:

- [Richtlinienbasierte Routing-Konfiguration in Secure Firewall Management Center - Gerätekonfigurationsleitfaden](#)
- [Path Monitoring on Policy-Based Routing Configuration on Secure Firewall Management Center Device Configuration Guide](#)
- [Konfigurieren einer richtlinienbasierten Routingrichtlinie](#)
- [Konfigurationsbeispiel für richtlinienbasiertes Routing](#)
- [Beispiel für PBR-Pfadüberwachung konfigurieren](#)
- [Pfadüberwachungs-Dashboard hinzufügen](#)
- [Konfiguration der DNS-Plattformeinstellungen im Konfigurationsleitfaden für Secure Firewall Management Center-Geräte](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.