

FMCのHTTP Path Monitorを使用したPBRの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[HTTPパスモニタリング用のPBRの設定](#)

[等コストマルチパス\(ECMP\)の設定](#)

[セキュアFTDのための信頼できるDNSの設定](#)

[パスモニタリングの有効化](#)

[監視ダッシュボードの追加](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Secure Firewall Management Center(FMC)でHTTPパスモニタリングを使用してポリシーベースルーティング(PBR)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- PBRの基礎知識
- Cisco Secure Management Centerの基本的なエクスペリエンス
- 基本的なCisco Secure Firewall Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 7.4リリースを実行するCisco Secure Firewall Management Center Virtual(FMCv)VMware
- 7.4リリースを実行するCisco Secure Firewall Threat Defense Virtual Appliance(FTDv)VMware

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

従来のルーティングでは、パケットは宛先IPアドレスに基づいてルーティングされますが、宛先ベースのルーティングシステムでトラフィックを指定するルーティングを変更することは困難です。PBRを使用すると、ルーティングプロトコルによって提供される既存のメカニズムを拡張および補完することによって、ルーティングをより詳細に制御できます。

PBRでは、IP優先順位を設定できます。また、高コストリンク上のプライオリティトラフィックなど、特定のトラフィックのパスを指定することもできます。PBRでは、ルーティングは宛先ネットワーク以外の基準（送信元ポート、宛先アドレス、宛先ポート、プロトコルアプリケーション、これらのオブジェクトの組み合わせなど）に基づいて行われます。PBRを使用すると、アプリケーション、ユーザ名、グループメンバーシップ、およびセキュリティグループアソシエーションに基づいてネットワークトラフィックを分類できます。このルーティング方式は、大規模なネットワーク展開で多数のデバイスがアプリケーションやデータにアクセスする状況に適用できます。従来、大規模な導入では、すべてのネットワークトラフィックをハブにルーテッドベースのVPN内の暗号化トラフィックとしてバックホールするトポロジが採用されていました。これらのトポロジでは、パケット遅延、帯域幅の減少、パケットのドロップなどの問題が頻繁に発生します。

PBRはルーテッドファイアウォールモードでのみサポートされ、初期接続には適用されません。HTTPベースのアプリケーションは、物理、ポートチャネル、サブインターフェイス、およびステータストンネルインターフェイスでサポートされます。クラスタデバイスではサポートされません。

設定されたインターフェイスが、ラウンドトリップ時間(RTT)、ジッター、平均オピニオン評点(MOS)、インターフェイスごとのパケット損失などのメトリックを導出する場合、PBRトラフィックをルーティングするためのベストパスを決定するために使用されます。パスモニタリングは、インターフェイスごとに複数のリモートピアの柔軟なメトリックを計算します。ブランチファイアウォール上のポリシーを通過する複数のアプリケーションのベストパスを監視および決定するには、次の理由から、ICMPよりもHTTPの方が優先されます。

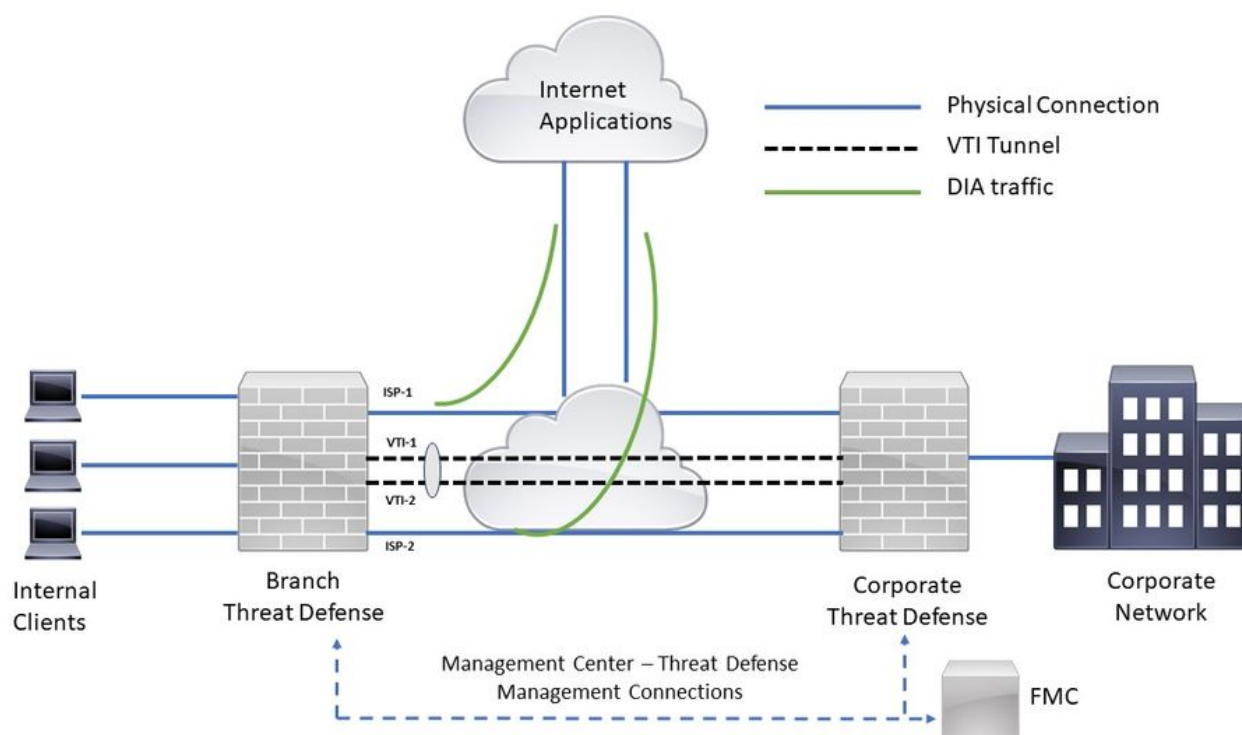
- HTTP-pingを使用すると、アプリケーションがホストされているサーバのアプリケーション層までのパスのパフォーマンスメトリックを取得できます。
- アプリケーションドメインはIPアドレスではなく追跡されるため、アプリケーションサーバのIPアドレスが変更されるたびにファイアウォール設定を変更する必要がなくなります。

設定

ネットワーク図

すべてのブランチネットワークトラフィックが企業ネットワークのルートベースのVPNを介して

送信され、必要に応じてエクストラネットに転送される、一般的な企業ネットワークのシナリオを考えてみます。次のトポロジは、ルートベースのVPNを介して企業ネットワークに接続されたブランチネットワークを示しています。従来、企業の脅威対策は、ブランチオフィスの内部トラフィックと外部トラフィックの両方を処理するように設定されています。PBRポリシーを使用すると、ブランチの脅威に対する防御は、仮想トンネルではなくWANネットワークに特定のトラフィックをルーティングするポリシーで設定されます。その他のトラフィックは、通常どおり、ルートベースのVPNを通過します。



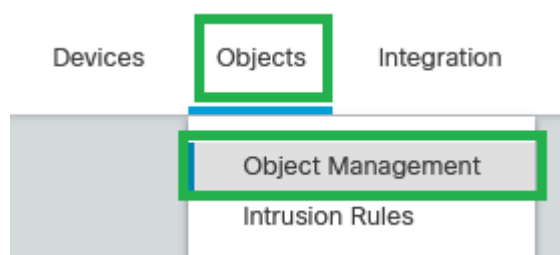
ネットワーク トポロジ

「設定」セクションでは、ISPおよびVTIインターフェイスがSecure FMCのブランチ脅威対策にすでに設定されていることを前提としています。

HTTPパスモニタリング用のPBRの設定

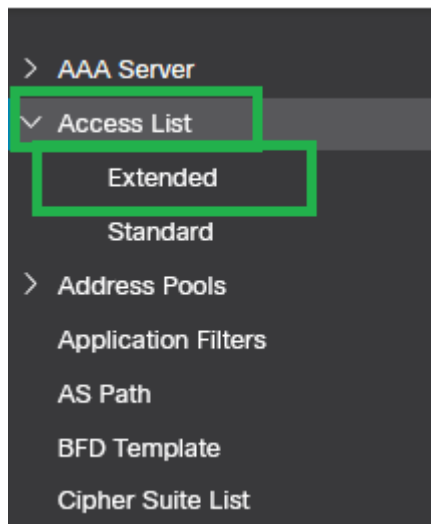
この設定セクションでは、ISP-1およびISP-2インターフェイスでのパスモニタリングの設定を示しています。

ステップ 1：監視対象アプリケーションの拡張アクセスリストを作成します。Objects > Object Managementの順に移動します。



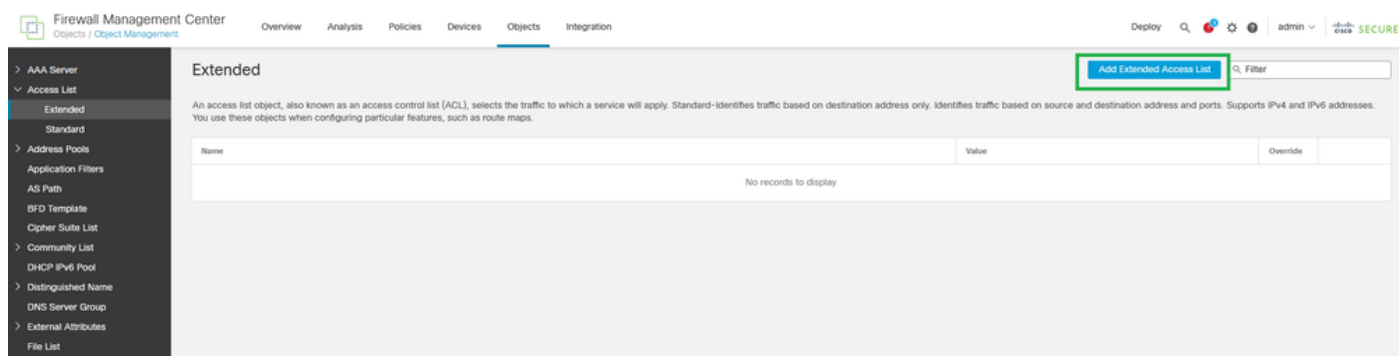
オブジェクト - オブジェクト管理

ステップ 2：左側のメニューで、Access-list > Extended の順に選択します。



アクセスリスト：拡張

ステップ 3：Add Extended Access List をクリックします。



拡張アクセスリストの追加

ステップ 4：Extended Access List で名前を設定して、Add をクリックします。

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

新しい拡張アクセスリストオブジェクト

ステップ 5：Application をクリックして、目的のアプリケーションを選択します（この例では、一部

のシスコアプリケーションが選択されています)。次にAddをクリックします。

Add Extended Access List Entry

Action:
Allow

Logging:
Default

Log Level:
Informational

Log Interval:
300 Sec.

NetworkPortApplicationUsersSecurity Group Tag

Application Filters Clear All Filters

Search by name

Risks (Any Selected)

Very Low730

Low622

Medium734

High1556

Very High577

Business Relevance (Any Selected)

Very Low885

Available Applications (4)

Search cisco

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

拡張アクセスリストエントリの追加

注：拡張アクセスリストでは、特定のトラフィックを目的のアプリケーションに一致させるために、送信元/宛先IPとポートを設定できます。PBR設定に適用するために、複数の拡張アクセスコントロールリスト(ACL)を作成できます。

手順 6：拡張アクセスリストの設定を確認し、Saveをクリックします。

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

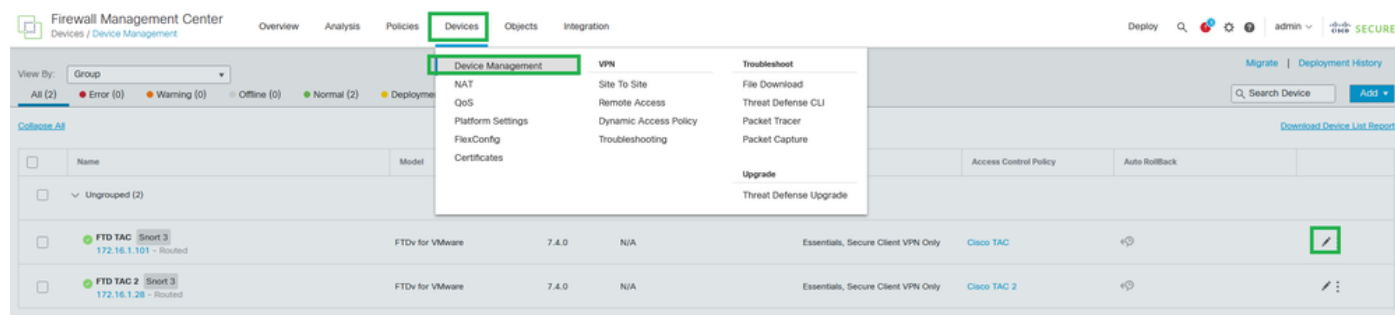
Allow Overrides

Cancel

Save

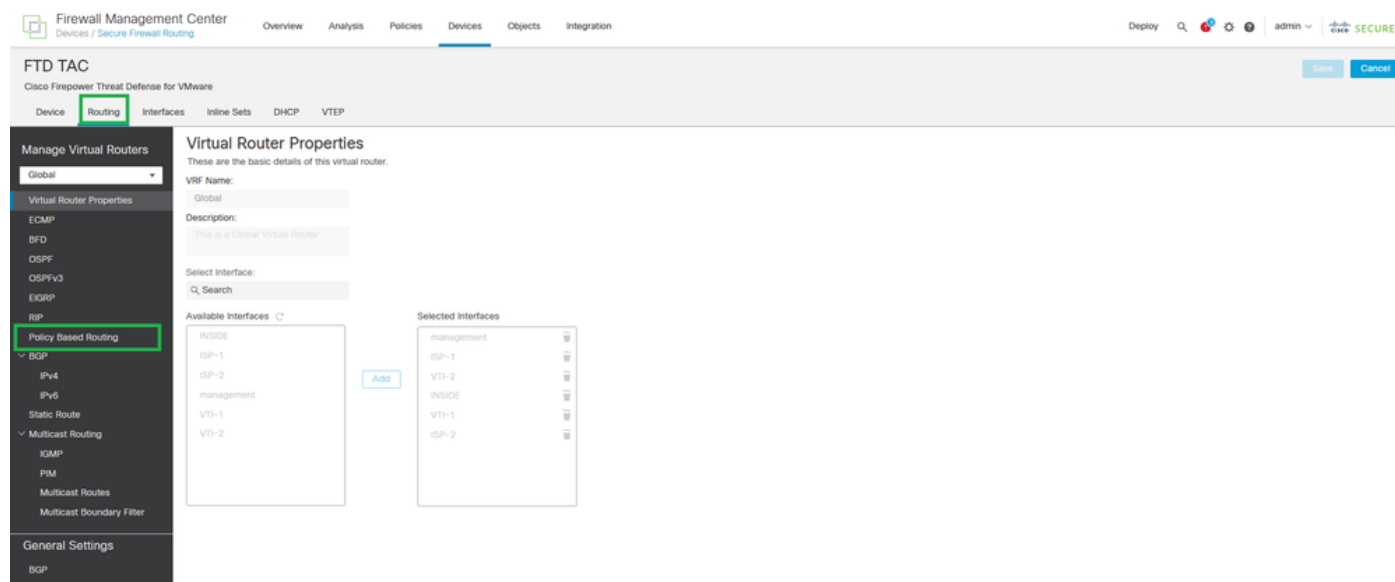
拡張アクセスリストオブジェクトの保存

ステップ7: Devices > Device Managementの順に移動し、脅威対策を編集します。



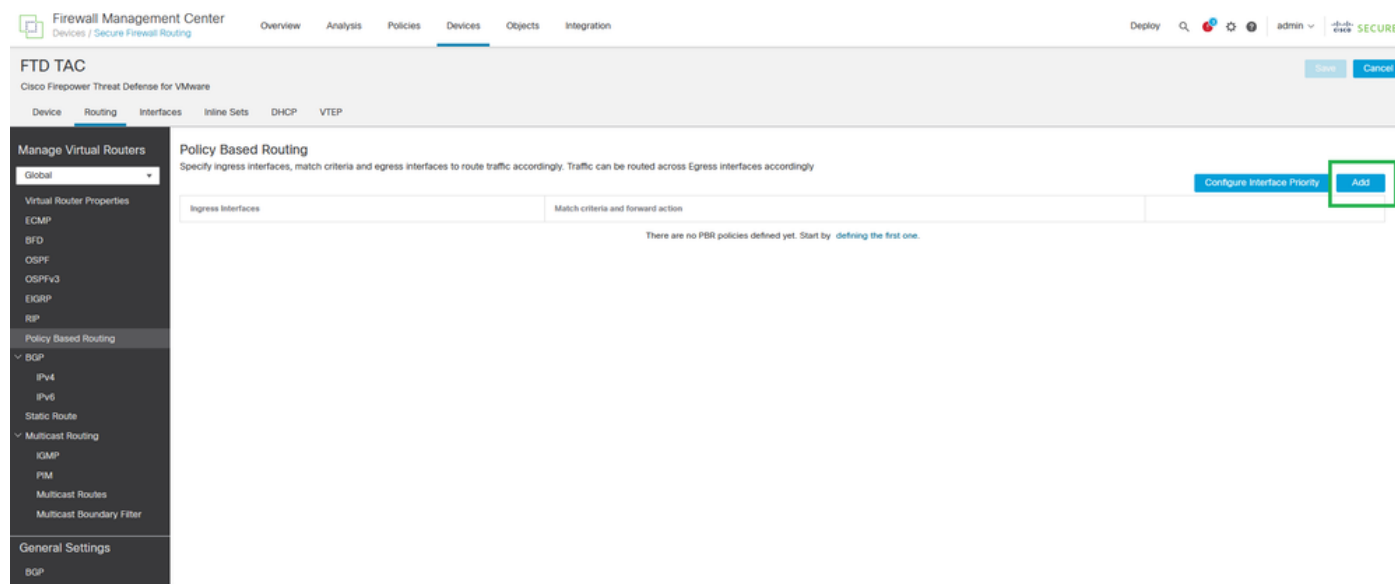
デバイス - デバイス管理

ステップ8: Routing > Policy-Based Routingの順に選択します。



ルーティング - ポリシーベースルーティング

ステップ9: [Add] をクリックします。



ステップ 10 : PBR設定用の入カインターフェイス (この例ではINSIDE) を追加してから、Addをクリックします。

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*

Select...

INSIDE

ISP-1

ISP-2

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

ステップ 11 : 一致基準 (前の手順で作成した拡張アクセスリストを使用) 、出カインターフェイス、およびインターフェイスの順序を定義します。

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

転送アクションの追加



注：この設定ガイドでは、出カインターフェイスと最小ジッタが選択されました。他のオプションの詳細については、[公式のPBRドキュメント](#)を参照してください。

ステップ 12 : Egress Interfaces (この例ではISP-1とISP-2) を選択してから、Saveをクリックします。

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

選択された出カインターフェイス

ステップ 13 : PBRの設定を確認し、Saveをクリックします。

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

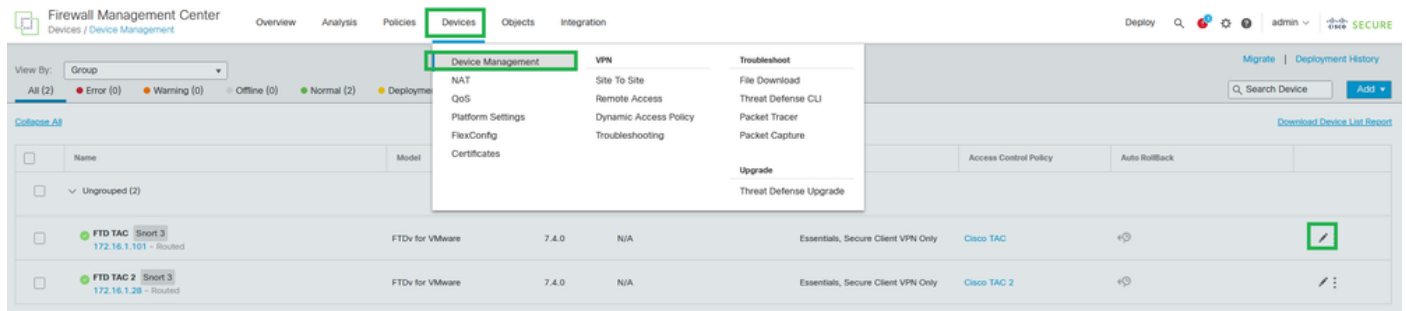
Save

ステップ14: (オプション) さらに拡張アクセスコントロールリスト(ACL)が作成された場合、またはPBR設定を適用する必要がある送信元インターフェイスが複数ある場合は、ステップ9、10、11、12、および13を繰り返します。

ステップ 15 : FMCからの変更の保存と展開

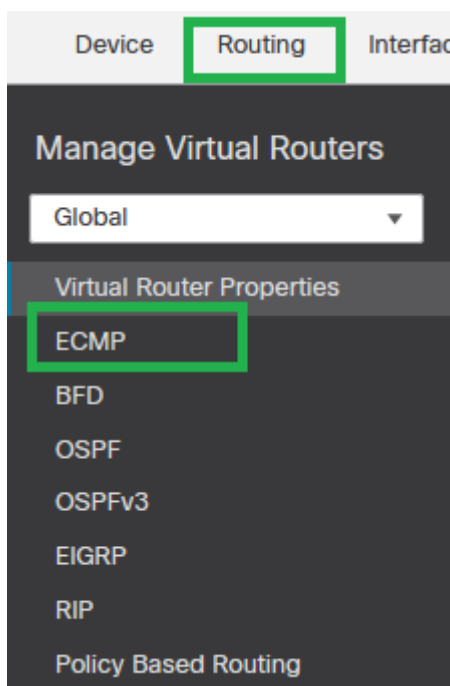
等コストマルチパス(ECMP)の設定

ステップ 1 : Devices > Device Managementに移動し、脅威対策を編集します。



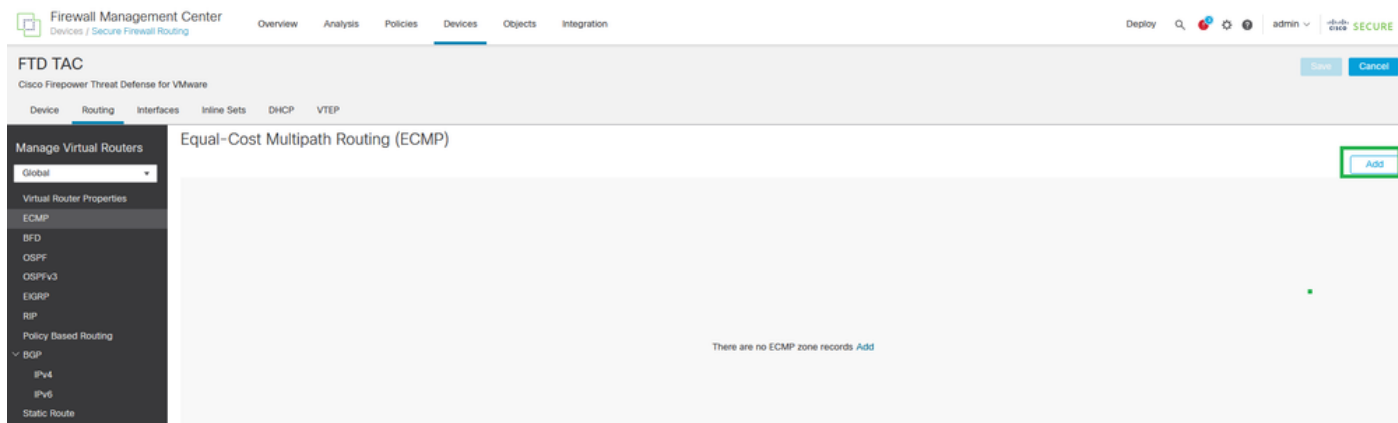
デバイス - デバイス管理

ステップ 2 : Routing > ECMPの順に選択します。



ルーティング : ECMP

ステップ 3 : Addをクリックして、VTIとWANインターフェイス (この設定ガイドではISP-1とISP-2) の間にECMPを作成します。



等コストマルチパスルーティング(ECMP)

ステップ 4 : ECMP名を設定し、すべてのVTIインターフェイスを選択してから、Addをクリックします。

Add ECMP ? ×

Name

VTI-ECMP

Available Interfaces

INSIDE

ISP-1

ISP-2

Selected Interfaces

VTI-1

VTI-2

Add

Cancel OK

VTI用のECMP

ステップ 5 : ステップ3と4を繰り返して、WANインターフェイス間にECMPを作成します (この設定ガイドではISP-1とISP-2) 。

Add ECMP

?

×

Name

ISP-ECMP

Available Interfaces

INSIDE

VTI-1

VTI-2

Add

Selected Interfaces

ISP-2

🗑

ISP-1

🗑

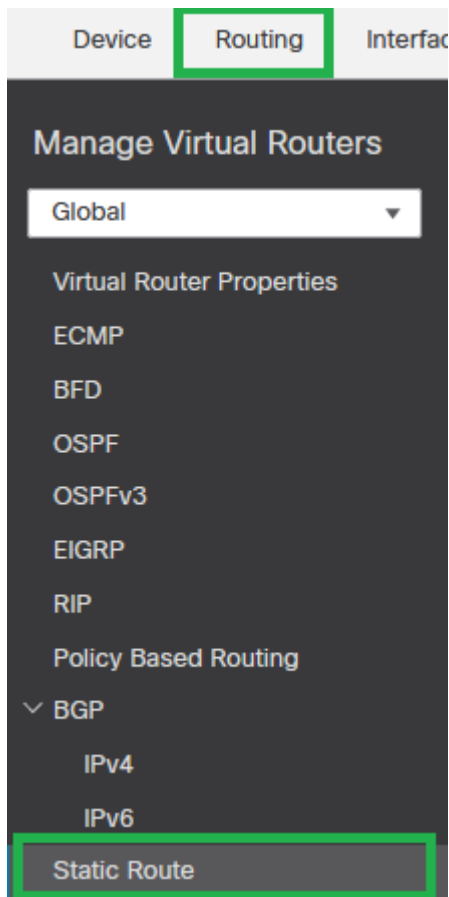
Cancel

OK

ISPインターフェイス用ECMP

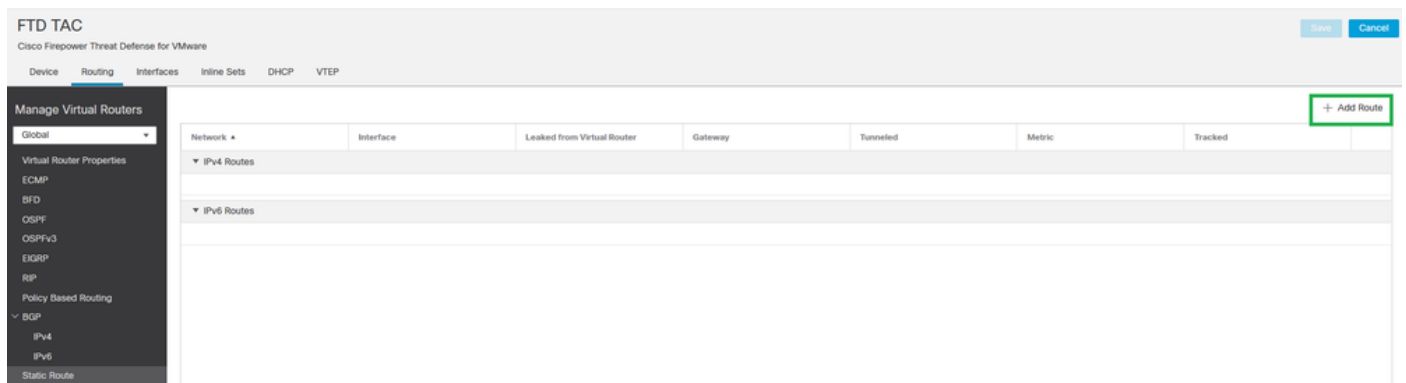
手順 6 : ECMP設定を保存します。

手順 7 : ロードバランスを行うために、ゾーンインターフェイスのスタティックルートを設定します。 Routing > Static Route の順に選択します。



ルーティング – スタティックルート

ステップ 8 : +ルートの追加をクリックします。



+ルートの追加

ステップ 9 : VTIインターフェイス (このコンフィギュレーションガイドではVTI-1) のデフォルトスタティックルートをメトリック値1で作成し、OKをクリックします。

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

VTI-1のデフォルトスタティックルート

ステップ 10 : さらに多くのVTIインターフェイスが設定されている場合は、ステップ8を繰り返します。



注 : 設定されたVTIインターフェイスごとにデフォルトルートを作成します。

ステップ 11 : WAN/ISPインターフェイス (この設定ガイドではISP-1) のデフォルトスタティックルートを、VTIよりも大きいメトリック値で作成し、OKをクリックします。

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

ISP-1のデフォルトスタティックルート

ステップ 12 : さらに多くのWAN/ISPインターフェイスが設定されている場合は、ステップ10を繰り返します。



注 : 設定されたWAN/ISPインターフェイスごとにデフォルトルートを作成してください。

ステップ 13 : デフォルトルートを確認し、OKをクリックします。

FTD TAC

Cisco Firepower Threat Defense for VMware

DeviceRoutingInterfacesInline SetsDHCPVTEP

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

You have unsaved changes

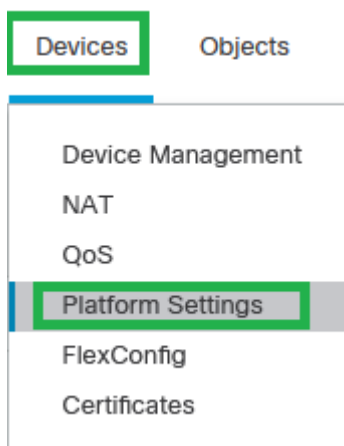
Save

Cancel

スタティックルートの設定

セキュアFTDのための信頼できるDNSの設定

ステップ 1：Devices > Platform Settingsの順に移動します。



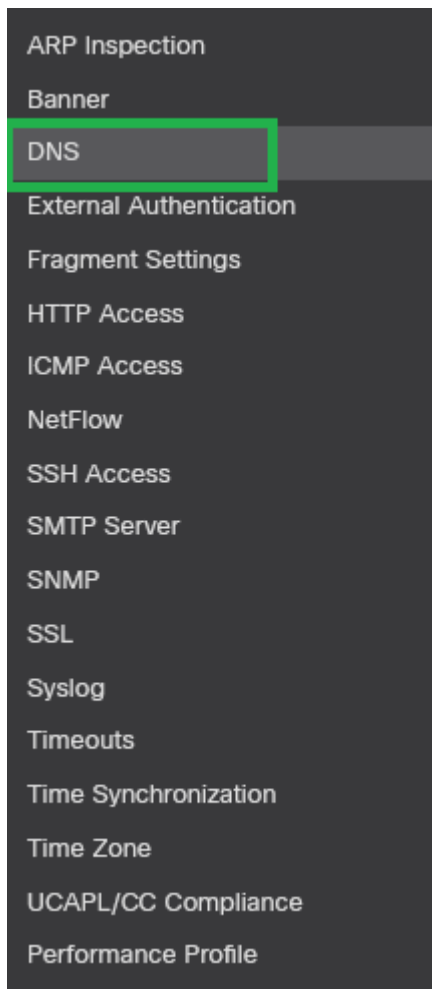
デバイス－プラットフォームの設定

ステップ 2：既存のプラットフォーム設定ポリシーを作成または編集します。



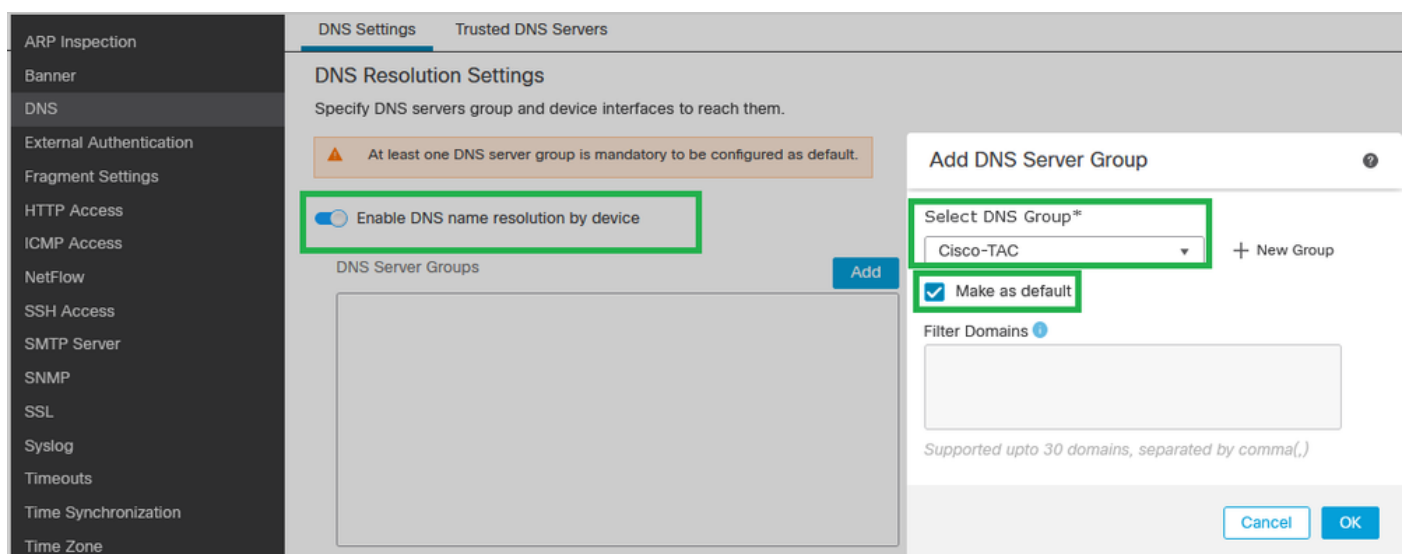
注：プラットフォーム設定ポリシーがセキュアな脅威対策デバイスに適用されていることを確認してください。

ステップ 3：DNSをクリックします。



DNSプラットフォームの設定

ステップ 4：デバイスによるDNS名前解決を有効にする Add をクリックするか、既存のDNSグループを選択します。Make as default を選択し、OK をクリックする。



DNSサーバグループの追加



注：プラットフォーム設定ポリシーに関するDNS設定の詳細については、[公式のプラッ](#)

[トフォーム設定](#)ドキュメントを参照してください。

ステップ 5 : Interface Objects セクションでWAN/ISPインターフェイスを選択します。

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

Q Search

INSIDE

ISP-1

ISP-2

VTI-1

VTI-11

VTI-2

Add

Selected Interface Objects

ISP-1

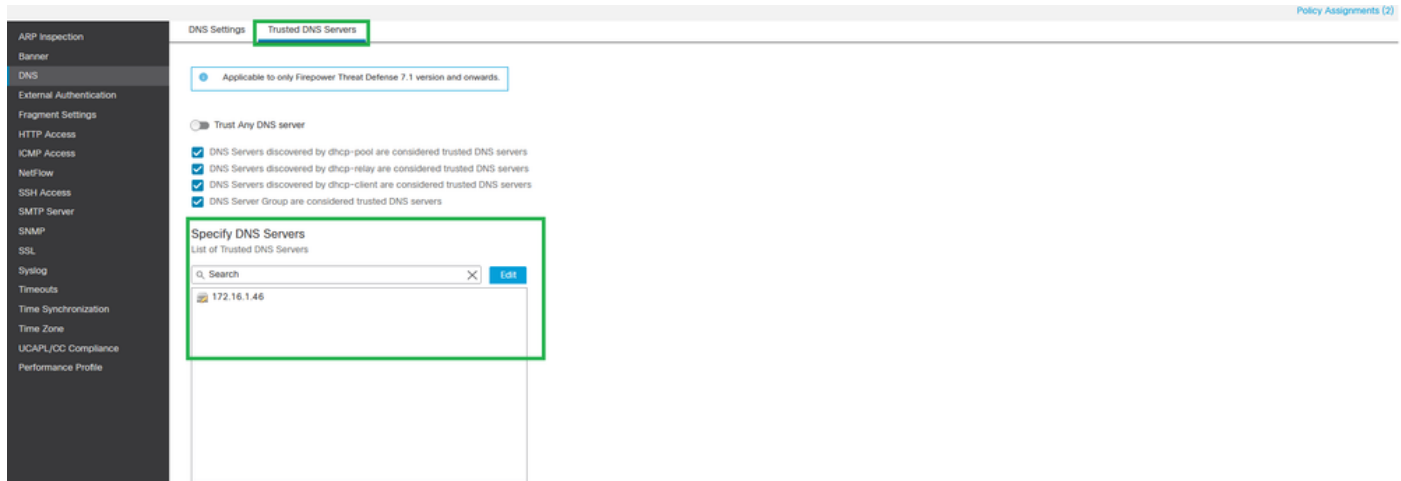
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

DNSインターフェイスの設定

手順 6 : 変更を保存します。

手順 7 : Trusted DNS Servers に移動し、信頼できるDNSサーバを指定します。

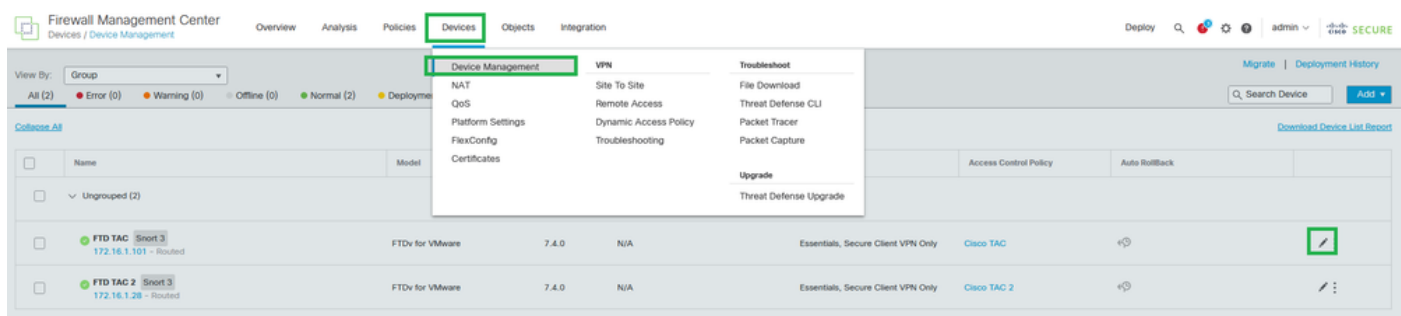


信頼されたDNSサーバ

ステップ 8：Save をクリックして、変更を展開します。

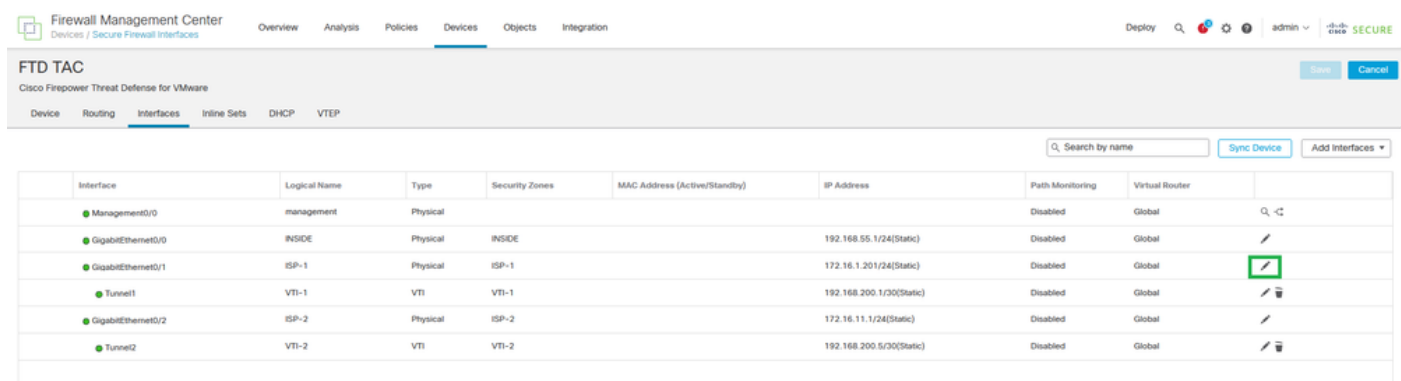
パスモニタリングの有効化

ステップ 1：Devices > Device Management に移動し、脅威対策を編集します。



デバイス - デバイス管理

ステップ 2：Interfaces タブで、インターフェイス WAN/ISP インターフェイス (この設定ガイドでは ISP-1 と ISP-2) を編集します。



インターフェイス設定

ステップ 3：Path Monitoring タブをクリックし、Enable IP Monitoring チェックボックスを選択して、HTTP-based Application Monitoring チェックボックスをオンにします。次に [Save] をクリックします。

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

インターフェイスパスモニタリングの設定



注意：前の設定セクションで設定したアプリケーションがリストされている必要があります。



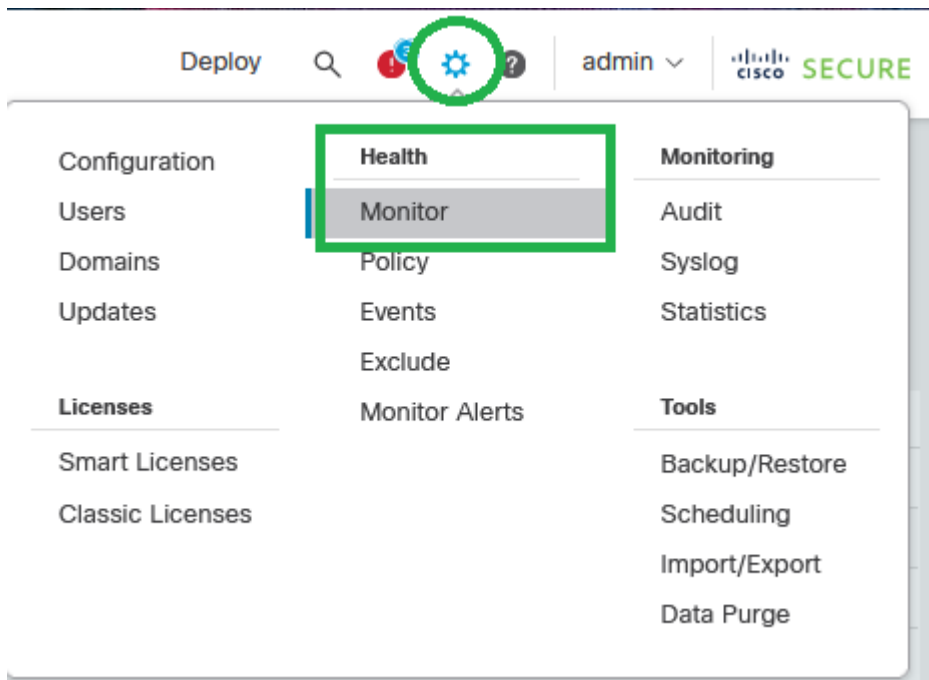
注：この設定ガイドでは、「Monitoring Type」が選択されています。その他のオプションの詳細については、[公式のコンフィギュレーションガイド](#)の「パスモニタリングの設定」を参照してください。

ステップ 4：設定されたすべてのWAN/ISPインターフェイスに対して、ステップ2と3を繰り返します。

ステップ 5：Saveをクリックして、変更を展開します。

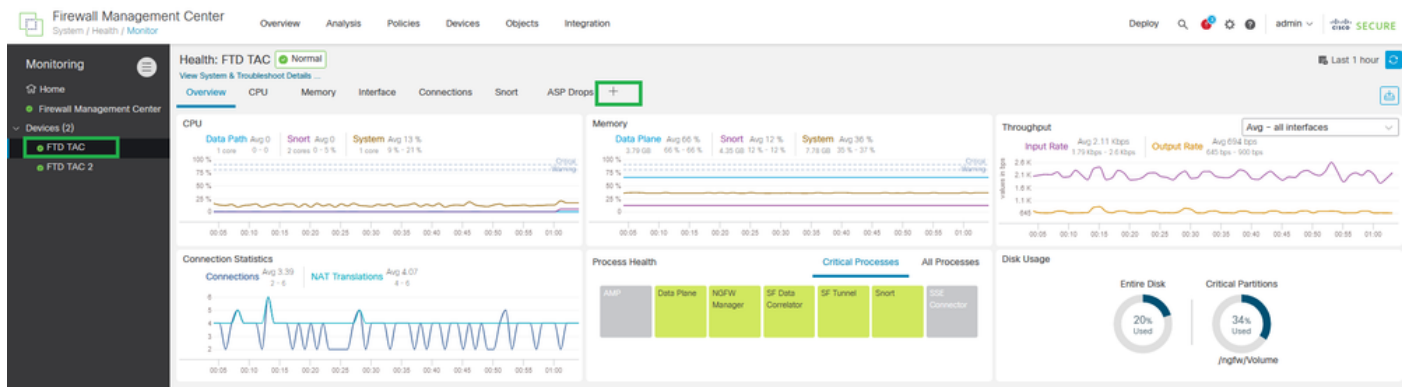
監視ダッシュボードの追加

ステップ 1：System > Health > Monitorの順に選択します。



システム - ヘルス - モニタ

ステップ2:セキュアFTDデバイスを選択し、Add New Dashboardをクリックします。



新しいダッシュボードの追加

ステップ 3 : ダッシュボード名を設定し、Correlate Metricsダイアログボックスで、ドロップダウンリストからInterface - Path Metricsを選択します。次に、Add Dashboardをクリックします。

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

パスメトリックを使用した新しいダッシュボードの追加

確認

このセクションでは、フローティングスタティックルート、ECMP、アプリケーションを使用したオブジェクトグループ、およびPBR設定を確認する方法について説明します。

デフォルトルートとフローティングスタティックルートの設定を確認します。

```
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
```

ECMP設定を確認します。

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

ルーティングテーブルで、トラフィックがECMPによってバランシングされているかどうかを確認します。ルーティングテーブルでは、両方のルートをSecure FTDルーティングテーブルにイン

ストールする必要があります。

```
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
```

PBRルートマップ設定を確認します。

```
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
!
```

PBR設定に割り当てられているACLを確認します (ルートマップ設定のACL名を確認します)。

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

アクセスリストに割り当てられているアプリケーションを使用して、オブジェクトグループを確認します (ACL設定でオブジェクトグループ名を確認します)。

```
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"
```

PBR設定で使用されているデータインターフェイスに割り当てられているポリシールートを確認します。

```
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
!
```

HTTPパスモニタリングダッシュボードの情報から、ジッタ、MOS、ラウンドトリップ時間、およびパケット損失の統計情報を確認して確認します。



HTTPパスモニタリングダッシュボードの確認

トラブルシューティング

パスモニタリングが失敗し、IPベースのモニタリングが有効になっている場合、WAN/ISPインターフェイスは、スタティックルート上に設定されたゲートウェイにICMPプローブパケットを送信するように設定されます。ICMPが機能するかどうかを確認するために、WAN/ISPインターフェイスで入力/出力キャプチャを設定します。

入力および出力キャプチャ：

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

入力キャプチャ：

```
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
```

出力キャプチャ：

```
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
```



注意：キャプチャではボックスのパフォーマンスが大幅に向上する可能性があるため、送信元と宛先のIPアドレスを使用してキャプチャを設定してください。



ヒント: pingが機能しない場合は、デフォルトゲートウェイとの直接接続をトラブルシューティングし、ARPテーブルを確認するか、Cisco TACに問い合わせてください。

PBRが機能しているかどうかを確認するには、パケットトレーサツールを使用して、アプリケーショントラフィックがPBRでルーティングされていることを確認します。

```
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



注：オブジェクトグループで設定されているネットワークサービスのアプリケーション IPアドレスを調べるには、`show object-group network-service detail`コマンドを使用します。

関連情報

HTTPパスモニタリングを使用したPBRに関連するその他のドキュメントについては、次のリンクを参照してください。

- [『Secure Firewall Management Centerデバイス設定ガイドでのポリシーベースルーティングの設定』](#)
- [Secure Firewall Management Centerデバイスでのポリシーベースルーティング設定に関するパスモニタリング設定ガイド](#)
- [ポリシーベースルーティングポリシーの設定](#)
- [ポリシーベースルーティングの設定例](#)
- [PBRパスモニタリングの設定例](#)
- [パスモニタリングダッシュボードの追加](#)
- [セキュアファイアウォール管理センターでのDNSプラットフォーム設定のデバイスコンフィギュレーションガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。