

HTTP راسم ةبقارم مادختساب PBR نيوكت FMC ىلع

تايوتحملا

[ةمدقملا](#)

[ةيساسالاب تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[ةكبش ليل طي طختلا مسرلا](#)

[HTTP راسم ةبقارم PBR نيوكت](#)

[\(ECMP\) ةفلكتلا يواستم تاراسملا ددعت م راسم نيوكت](#)

[نمآلا FTD ل هب قوئوملا DNS نيوكت](#)

[راسملا ةبقارم نيوكتم](#)

[ةبقارملا تامولعم ةحول ةفاضلا](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او عا طخألا فاشكتسا](#)

[ةلص تاذ تامولعم](#)

ةمدقملا

مادختساب (PBR) ةسايسلا ىلإ دنتسملا هيچوتلا نيوكت ةيفيك دنتسملا اذه فصبي Cisco نم (FMC) نمآلا ةياملحلا رادج ةرادا زكرم ىلع HTTP راسم ةبقارم.

ةيساسالاب تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت نأب Cisco يوصوت:

- لمعلا ىلع ةردقلا لاجم ي ةيساسالاب فراعملا
- Cisco نم ةيساسالاب ةنمآلا ةرادلا زكرم ةبرجت
- Cisco نم يساسالاب (FTD) نمآلا ةياملحلا رادج ديدعت دض عافدلا

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربل تارادصا ىلإ دنتسملا اذه ي ةدراولا تامولعملا دنتست:

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware يذلي 7.4 رادصإلا لغشي
- Cisco (FTDv) VMware نمآلا ةياملحلا رادج ديدعت ن عافدلل يرهاظلا زاوجل

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشن ا مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عيمج تأدب رمل يال لمحتمل ريثأتلل كمهف نم دكأتف ،ليغشتل دي قكتكبش

ةيساسا تامولعمل

نم ،كلذعمو ،ةهوجل IP ناو نع ل ا ادانتسا مزحلل هي جوت متي ،يديلقتل هي جوتل ي كحنمي .ةهوجل ا ل دنتسمل هي جوتل ماظن ي ف رورمل ةكرح ديدحت هي جوت رييغت بعصلل اهرفوت يتل ةدوجومل تايال ال عيسوت لال خ نم هي جوتل ي ف م كحتل نم ديزمل PBR اهلالمك او هي جوتل تالوكوتورب

لثم ،ةني عم رورم ةكرحل راسم ديدحتب حمست اهنأ امك . IP ةي قسبأ نييغت ب PBR حمسي ىرخأ ريياعم لىل هي جوتل دمتعي ،PBR عم .ةفلكتل يلاع طابترا ربع ةيولوال رورم ةكرح تاقيبطت وأ ةهوجل ذفنم وأ ةهوجل ناو نع وأ ردصلل ذفنم لثم ةهوجل ةكبش ريغ ةكبشل رورم ةكرح فينصلت PBR مادختسا نكمي .تانئال هذه نم ةعومجم وأ لوكوتورب نكمي .نامال ةعومجم نارثقاو ةعومجمل ةيوضعو مدختسمل مساو قيبطتل ل ا ادانتسا لىل لوصولاب ةديدع ةزهجأ اهي ف موقت يتل تالاحل ي ف هذه هي جوتل ةقيرط قيبطت رشنل تاي لمعم نمضتت ،يديلقت لكشبو .ريبك ةكبش رشن ي ف تانايبلل تاقيبطتل ةرفشم رورم ةكرحك زكرم لىل لمالكالب ةكبشل رورم ةكرح لقن لىل لمعت تاططخم ةريبكلك شودح لىل ابلاغ تاططخم هذه يدؤت .هجوم لىل ةمئاق (VPN) ةيرهظ ةصاخ ةكبش ي ف مزحلل طاقساو ي ددرتل قاطنل ضافخناو مزحلل لوصو نمز لثم تالكشم

تالاصتال لىل هقيبطت متي الو هجومل ةيامل رادج عضو لىل طقف PBR معد متي ذفنمل ةانقو ةي دامل تاهجاول لىل HTTP لىل دنتسمل قيبطتل معد متي .ةيني نجل ةعومجمل ماظن ةزهجأ لىل دمتعم ريغ وهو .ةلاحل ةانقو ةي عرفل تاهجاولو

طسوتمو هوشتلل او (RTT) ةلوجل تقول لثم ةقتشم سيي اقم لال خ نم تاهجاول نيوكت دنع هي جوتل لصفال راسمل ديدحتل مدختست اهنأ ف ،ةهجاو لكل ةمزحلل نادقفو (MOS) يارل ةجرد لكل دعب نع ءارظنل نم ددعل ةنرم سيي اقم باسحب راسمل ةبقارم موقت .PBR رورم ةكرح لىل ةدوجومل ةسايس لال خ نم ةددعتم تاقيبطتل راسمل لصفأ ديدحتو ةبقارم لجأ نم .ةهجاو بابسأل هذهل ICMP لىل HTTP ليضفت متي ،يعرف ةيامل رادج

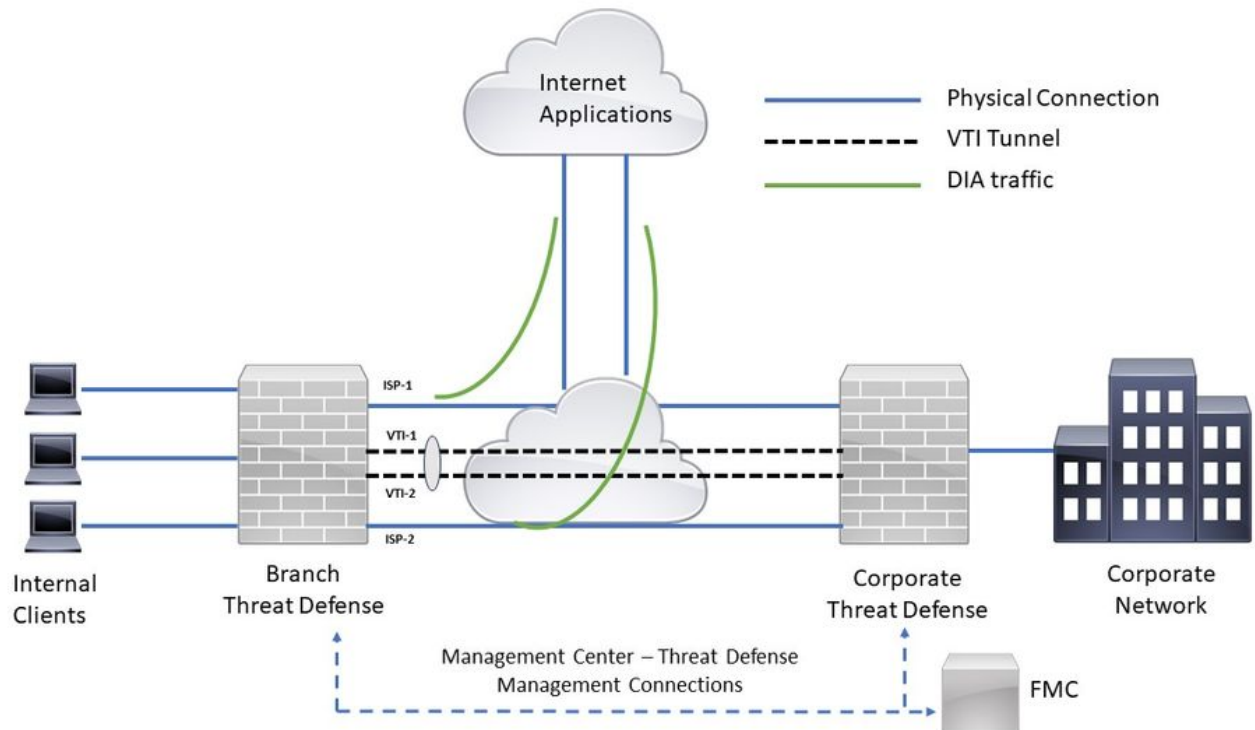
- قيبطت ةقبط ىتح راسملل ءادأل سيي اقم HTTP لاصتال رابتخا جرتسي نأ نكمي . قيبطتل ةفاضتسا متت شيح ،مخال
- مداخل IP ناو نع رييغت متامل ك ةيامل رادج نيوكت رييغت لىل ةجالح ةلازا تمت . IP ناو نع نم ال دب قيبطتل لاجم بقعت متي شيح قيبطتل

نيوكتل

ةكبشلل يطيختل مسرل

رورم ةكرح عيمج لاسرا متي شيح يجذومن ةسسؤم ةكبش وي رانيس رابتعال ي ف عض متي و ةكرشلل ةكبشل راسمل لىل ةدنتسمل VPN ةكبشل لال خ نم ةي عرفل ةكبشلل قلصتم ةي عرفل ةكبش يلاتل ططخم ضرعي .اهبلط دنع ةيجراخلل ةكبشل لىل اهليوحت

متمت، يدي لقت لكشبو. هي جوت الى الى عدنتسم ال VPN ككبش لال خ نم ككرش ال ككبش ب
 عي ج راخ ال او عي ل خ ا د ال رورم ال كرح نم لك عم لماعت لل ككرش ال تادي دت نع عاف دل ما ظن عئي هت
 عرف ال دي دت دض عاف دل ني وكت متي، PBR عسايس مادخت ساب. يعرف ال بتكم ال ي
 عي ره ا ظ ال قافن ال نم ال دب WAN ككبش الى الى عني عم رورم كرح هي جوت ب موقت عسايس ب
 دات عملاك، راسم ال الى الى عدنتسم ال VPN ككبش لال خ نم قفدت رورم ال كرح عي قب



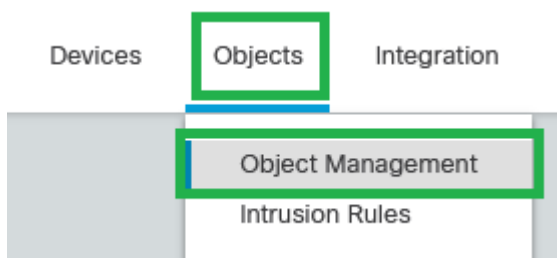
ككبش ال اي ج ول و ب و ط

عرف ال دي دت نع عاف دل ل عاف لاب امن وكت مت VTI و ISP تاه جاو ن ني وكت ال مسق ضررت في
 نم ال FMC في.

HTTP راسم عبقارم ل PBR ني وكت

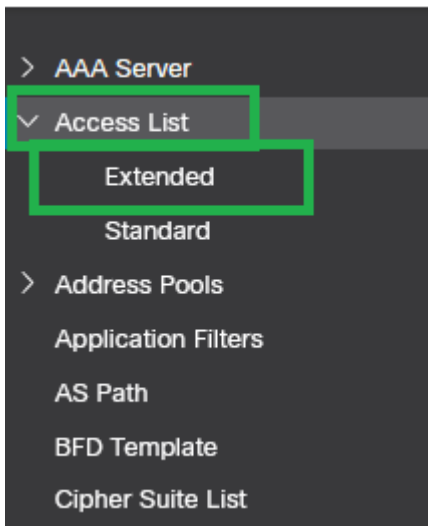
ISP-1 و ISP-2 تاه جاو الى ع راسم ال عبقارم ني وكت اذه ني وكت ال مسق حضوي

Objects > الى لقتنا. عبقارم ال تاق ي ب ط لل ع س و م ال ل و ص و ل ع م ئ ا ق ع ا ش ن ا ب م ق 1. ع و ط خ ل
 Object Management



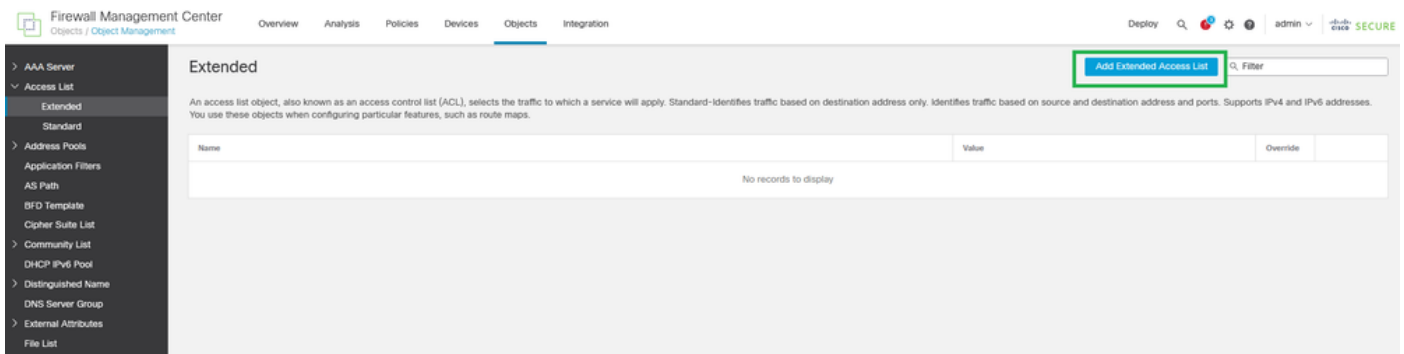
ت ا ن ئ ا ك ل ع ر ا د - ت ا ن ئ ا ك ل

ي ر س ي ال Access-list > Extended ع م ئ ا ق ال الى لقتنا 2. ع و ط خ ل



ةعسومل - لوصول ةمئاق

رقن 3. ةوطخل Add Extended Access List.



ةعسومل لوصول ةمئاق ةفاض

رقن 4. ةوطخل Add. ةعسومل لوصول ةمئاق يف مسا دادعاب مق.

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

ديدل ةعسومل لوصول ةمئاق نئاك

اذل Cisco تاقيفبطت ضع ب راي تخا مت ةبولطمل تاقيفبطتال رتخاو Application رقن 5. ةوطخل Add. رقن 4. ةوطخل.

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

Available Applications (4)

Search by name

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

- 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

ةعسوملا لوصول ةمئاق لاخدا ةفاض



ذفانملاو IP نيوانع مادختساب ةعسوملا لوصول ةمئاق نيوكت نكمي :ةظحالم كنكمي .ةبولطملا تاقيبطتلا الى ةنيعم رورم ةكرح ةقباطملا ةهول/ردصملا PBR. نيوكت الى ةهقيبطتلا ةعسوملا لوصول في مكحتلا مئاقو نم ديدعلا عاشن

Save. قوف رقناو ةعسوملا لوصول ةمئاق نيوكت نم ققحت .6 ةوطخل

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		

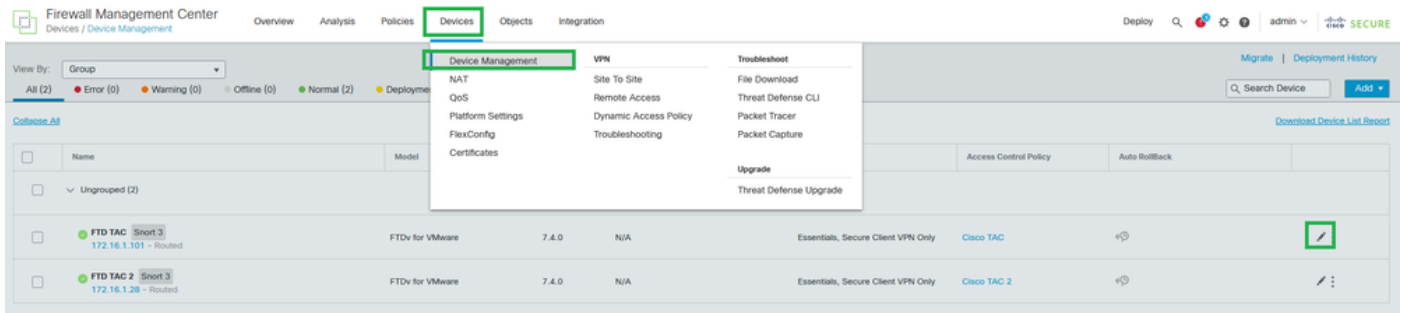
☐ Allow Overrides

Cancel

Save

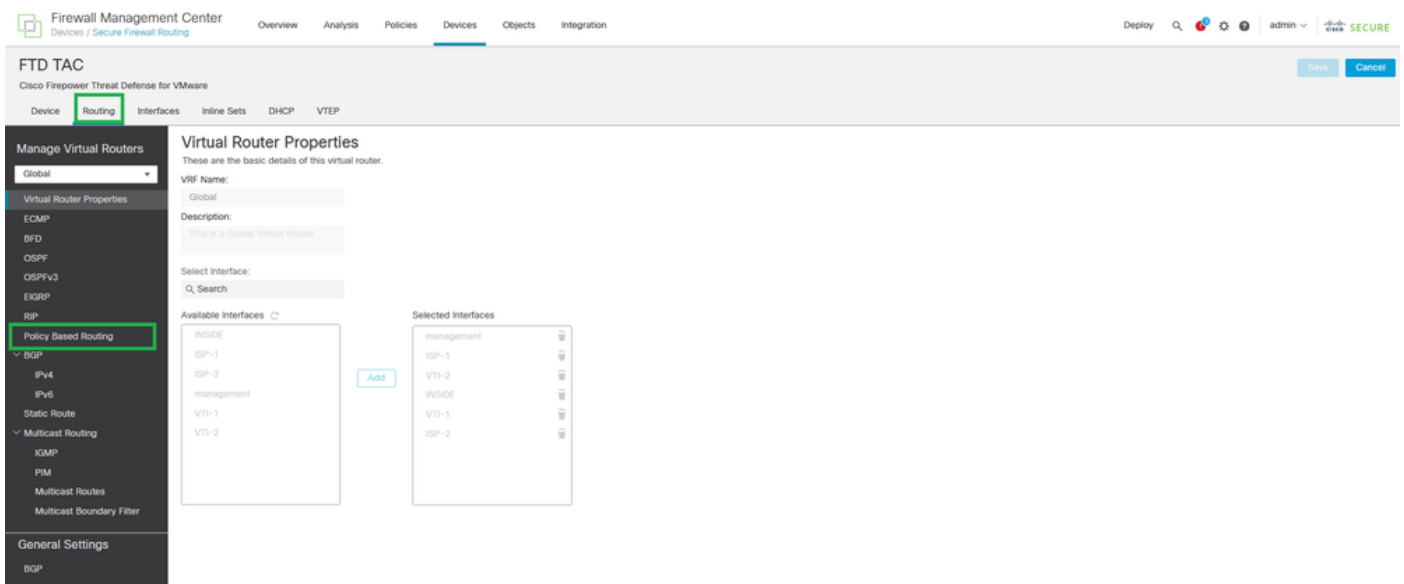
ةعسوملا لوصول ةمئاق نئاك ظفح

هريحتب مقو Devices > Device Management عافد ىلإ لقتنا 7. ةوطخل



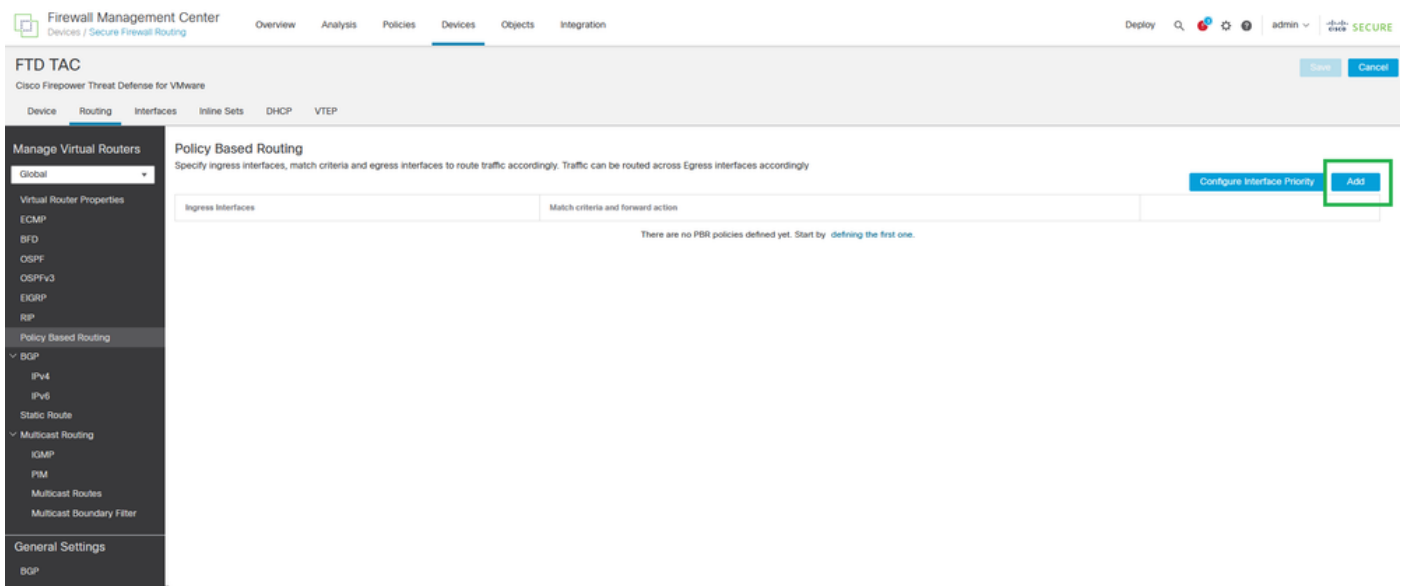
زاهجلا ةرادا

Routing > Policy-Based Routing ىلإ لقتنا 8. ةوطخل



ةسايسلا ىلع مئاقلا هيحوتلا - هيحوتلا

Add. رقنا 9. ةوطخل



ةسايسلا ىلإ دنتسملا هيحوتلا ةفاضإ

Add. رققنا مٲ ، (لاٲملا اذه ف لآاد) PBR نڤوكتل لوآدلا ةهآاو فاضاً 10. ةوطآلا

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

ةسائسلا ىل دنٲسم راسم ةفاضل

تاوطآلا ف اهؤاشنل مٲ ٲل ةسسوملا لوصولل ةمئاق عم) ةقباطملا رڤياعم ددآ. 11. ةوطآلا ةهآاولا بٲٲرتو ،آورآلا تاهآاو ،(ةقباسلا

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

هتي جوتال ةداع | تاءارج | ةفاض |



[PBR قئاثو](#) نم ققحت . اذه نيوكتال ليلدل هراي تخا مت Minimal Jitter Egress Interfaces: ةظحال م
ىخأل تاراخيال لوح دي زملا ةفر عمل [قي مسرلا](#).

Save. رقنا م ث ، (لا ثمل اذهل ISP-1 و ISP-2) جورخال تاهجاو رتخا . 12 ةوطخال

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

دەدەمەلە جۆرەلە تەجەو

Save. رەقەنە PBR نە قەقەتە 13. قەوغلە

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

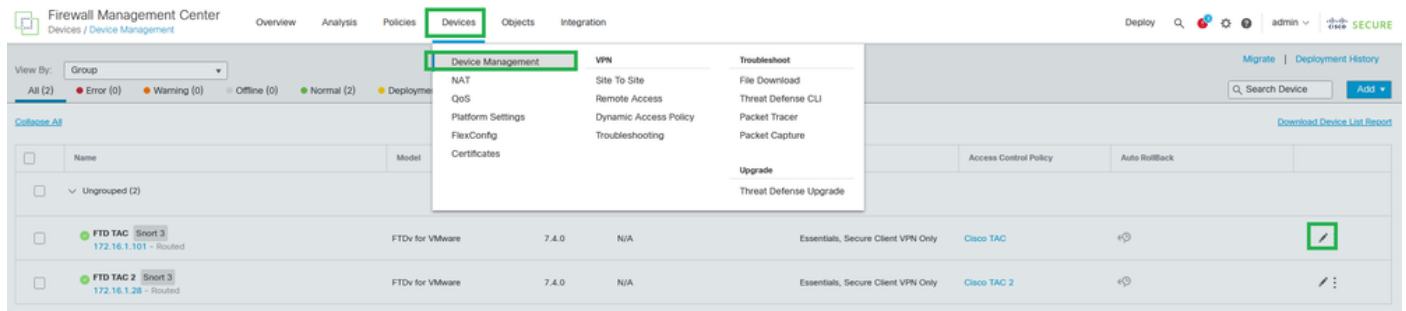
ةساي سلا ىل دنستسملا هيچوتلا ةحص نم ققحتلا

مكحتلا مئاقو نم ديزملا عاشن مت اذا 13 و 12 و 11 و 10 و 9 تاوطخل ررك (يراي تخا). 14 ةوطخل نيوكت قيبطت بجي شي رصملا تاهجاو نم ديزملا كانه ناك اذا و اةعسوملا لوصولا يف PBR.

FMC. نم اهرشنو تاريغي تالظا 15 ةوطخل

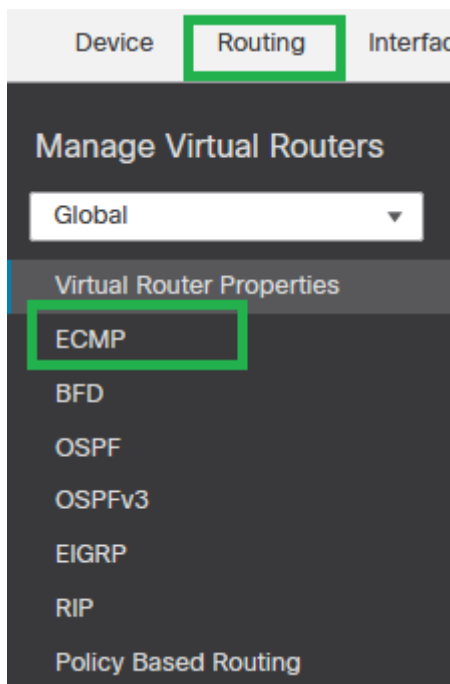
(ECMP) ةفلكتلا يواسم تاراسملا ددعتم راسم نيوكت

عافدلا اذه ررحو ديدهتلا عافد Devices > Device Management ىل لقنتا 1. ةوطخل



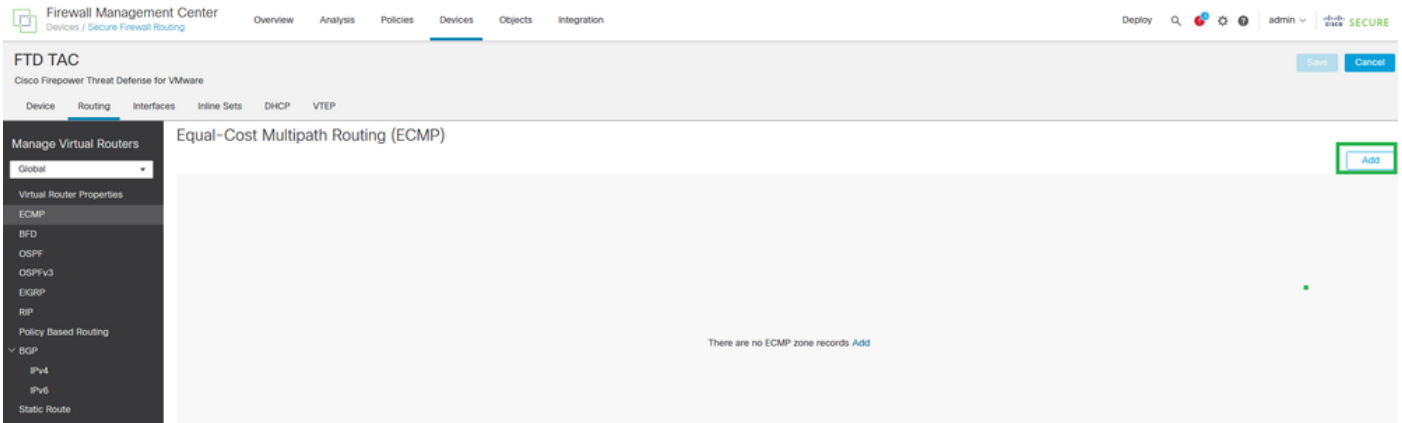
زاهجلا ةرادا

Routing > ECMP ىل لقنتا 2. ةوطخل



ECMP - هيچوتلا

نيوكتلا لي لذل ISP-1 و ISP-2) WAN و VTIs تاهجاو ني ب ECMP عاشن ا قوف Add رقنا 3. ةوطخل اذه).



ECMP) ةفلكتل ةيواستم تاراسم لدعتم هيچوتل

Add. رقنا م ث VTIs، تاهجاو عي م رتخاو ECMP لوكوتورب مسا دادعاب مق 4. ةوطخل

Add ECMP

Name

Available Interfaces

INSIDE
ISP-1
ISP-2

Selected Interfaces

VTI-1
VTI-2

Add

Cancel

OK

ECMP J VTIs

نيوكتل ليلدل ISP-2 و ISP-1) WAN تاهجاو ني ب ECMP عاشنال 4 و 3 تاوطخل ررك 5. ةوطخل اذه).

Add ECMP

Name

ISP-ECMP

Available Interfaces

INSIDE
VTI-1
VTI-2

Add

Selected Interfaces

ISP-2
ISP-1

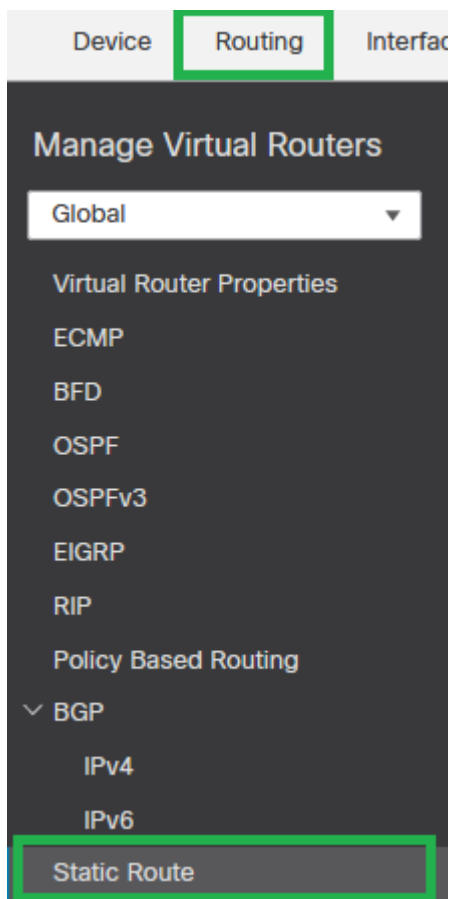
Cancel

OK

ISP تاهجاول ECMP

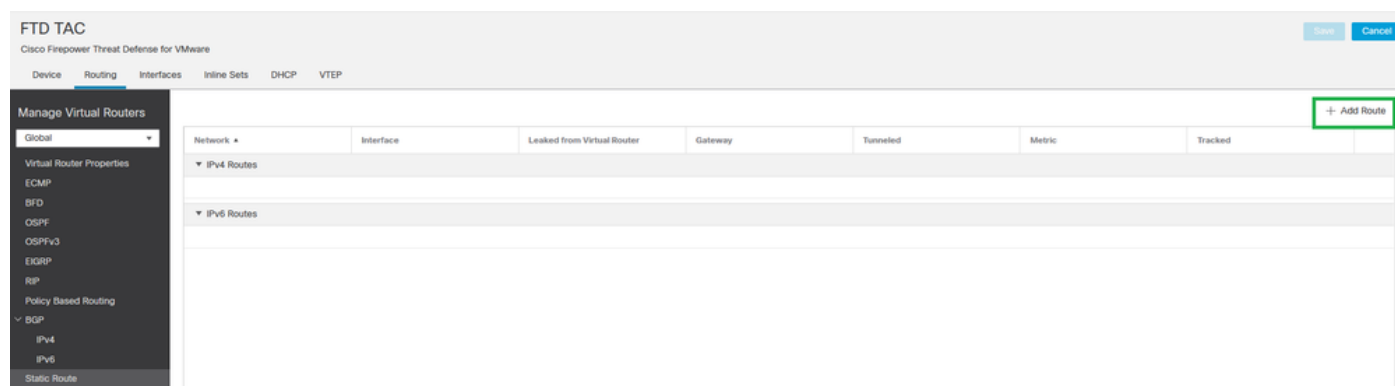
ECMP نيوكت ظفح. 6 ةوطخل

ىل لقتنا. لامأل ةنزاوم لجأ نم ةقطنملا تاهجاول ةتباثل تاراسملا نيوكتب مق. 7 ةوطخل
Routing > Static Route.



تباثال راسم ال - هيجوتال

لليدل (VTI-1) VTI (تاهجاو) ههجاو ليضارتفا يكيئاتاسإ نكاس راسم عاشنإب مق 9. ةوطخل



راسم ةفاضإ +

لليدل (VTI-1) VTI (تاهجاو) ههجاو ليضارتفا يكيئاتاسإ نكاس راسم عاشنإب مق 9. ةوطخل
OK. راقنا مٲ، يرت مةمي قك 1 عم (اذه نيوكتال

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 ل يضا رت ف ا ل ا ت با ث ل ا ر ا س م ل ا

ا ه ن ي و ك ت م ت ي ت ل ا VTI ت ا ه ج ا و ن م د ي ز م ل ا ك ا ن ه ن ا ك ا ذ ا 8. ة و ط خ ل ا ر ر ك 10. ة و ط خ ل ا



ا ه ن ي و ك ت م ت VTI ة ه ج ا و ل ل ك ل ي ض ا ر ت ف ا ر ا س م ا ش ن ا ب م ق : ة ط خ ا ل م

ل ي ل د ل (ISP-1) WAN/ISP (ت ا ه ج ا و) ة ه ج ا و ل ي ض ا ر ت ف ا ت با ث ر ا س م ا ش ن ا ب م ق 11. ة و ط خ ل ا
OK ر ق ن ا م ت ، VTI ن م ر ب ك ا س ا ي ق ة م ي ق ب (ا ذ ه ن ي و ك ت ل ا

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 ل يضارثفالا تباطال راسملا

اهنيوكت مت يثلا WAN/ISP تاهجاو نم ديزملا كانه ناك اذا 10 ةوطخلا ررك 12 ةوطخلا



اهنيوكت مت WAN/ISP ةهجاو لك ل يضارثفلا راسملا عاشنإ: ةطخال

OK. ررقناو ةيضارثفالا تاهجوملا نيوكت نم ققحت 13 ةوطخلا

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							

تباثال راسم ال نيوكت

نمآل FTD ل هب قوٹوم ال DNS نيوكت

Devices > Platform Settings. إلى ل قتنا 1. ةوطخل

Devices

Objects

Device Management

NAT

QoS

Platform Settings

FlexConfig

Certificates

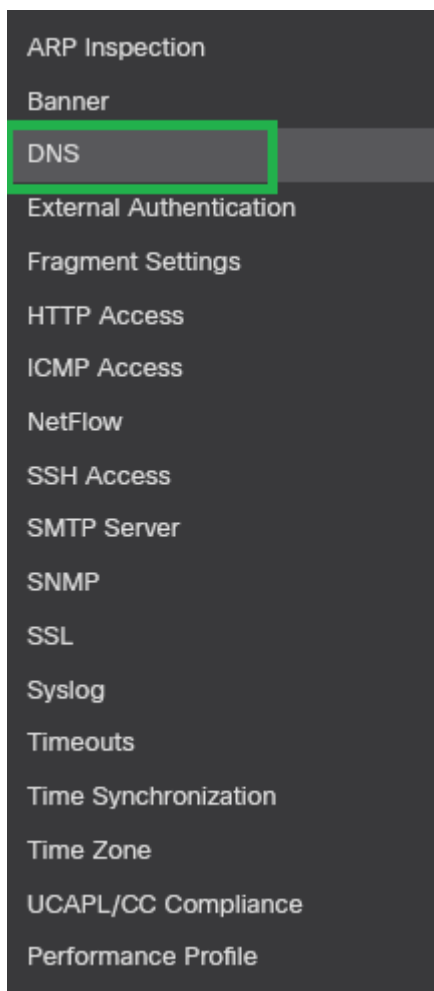
يساسأل ماظنل تاداعل - ةزهأل

هريحت وأ يلحال يساسأل ماظنل تاداعل جهن عاشن. 2. ةوطخل



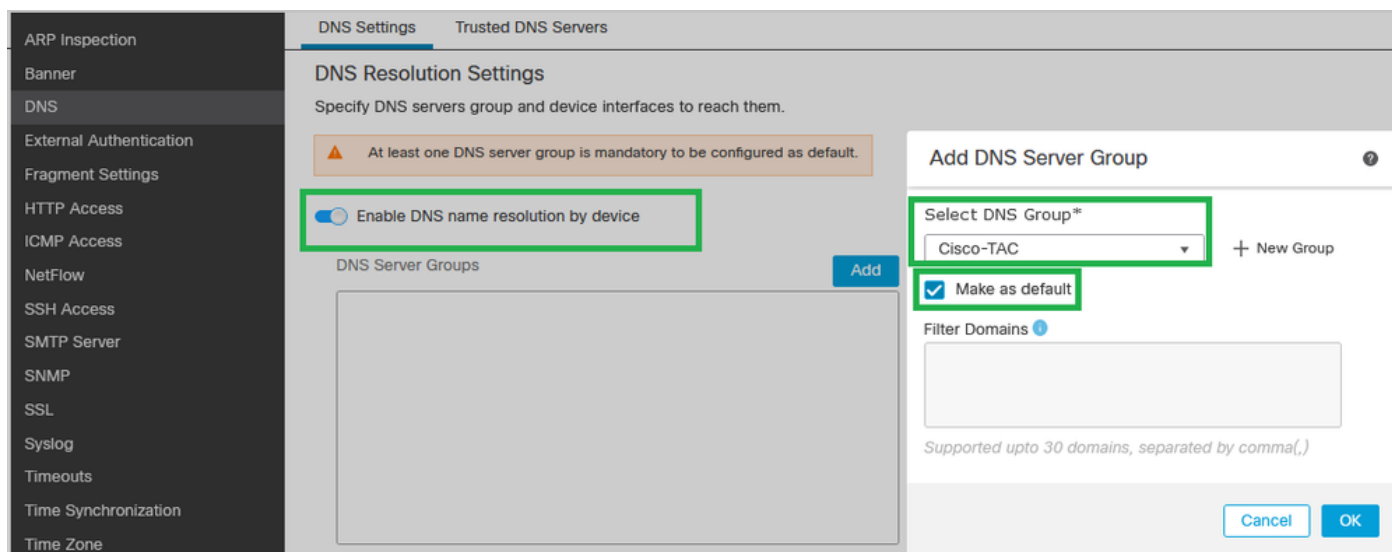
نع عافدل ةزهأ نيماأل يساسأل ماظنل تاداعل ةسايس قيبطت نم دكأت :ةظحال مديهتال.

DNS. رقنا 3. ةوطخل



يَسَّاسُ الْمَظَنِّ اِتَادَعِ DNS

Make as default، رتخأ. ةدوجوم DNS ةعومجم رتخأ وأ Add قوف رقن او DNS name resolution by device نكم. 4. ةوطخل OK. رقنا م



DNS م داوخ ةعومجم ةفاض



يَسَّاسُ الْمَظَنِّ اِتَادَعِ DNS نيوكت لوح ديزملا ةفرعم تدراً اذا: ةطخال م

ةيسرللايساسألا ماضنللا تادادعلا قئاثو نم ققحتف

مسقلالInterface Objectsنمض WAN/ISP تاهجاو رتخأ 5. ةوطخل

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:
1Range: 1-65535 minutes

Poll Timer:
240Range: 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

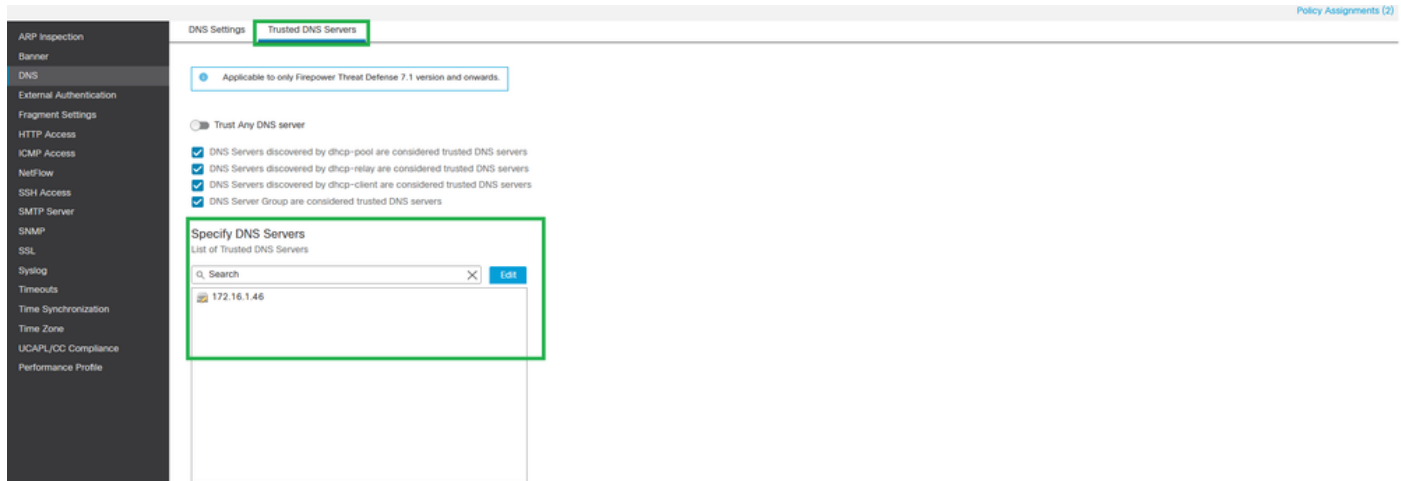
ISP-2

☐ Enable DNS Lookup via diagnostic/Management interface also.

DNS ةهجاو نيوكت

تاريغتلا ظفح 6. ةوطخل

مداوخل هذه دجواهب قوئومال DNS مداوخل Trusted DNS Serversإلى لقئنا 7. ةوطخل

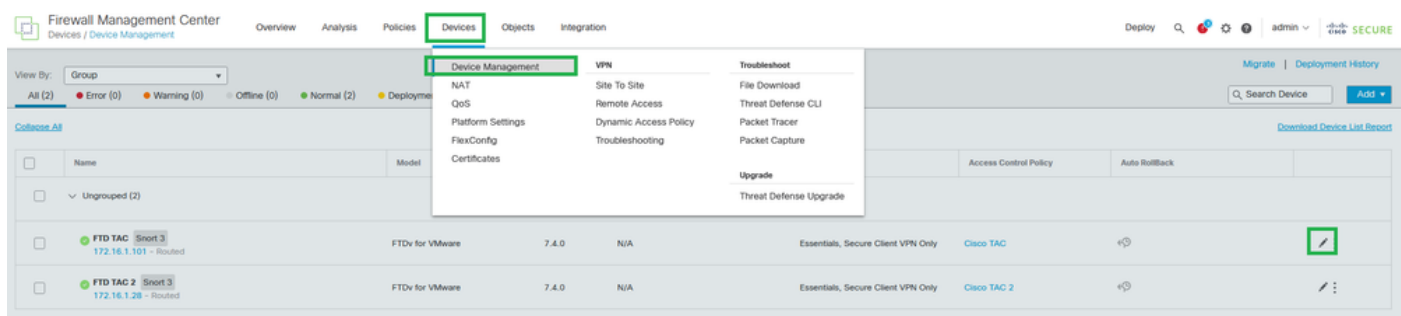


اهب قوٹومل DNS مداوخ

اھرشنب مقو تاريغيغتال Savel قوف رقنا 8. ةوطخل

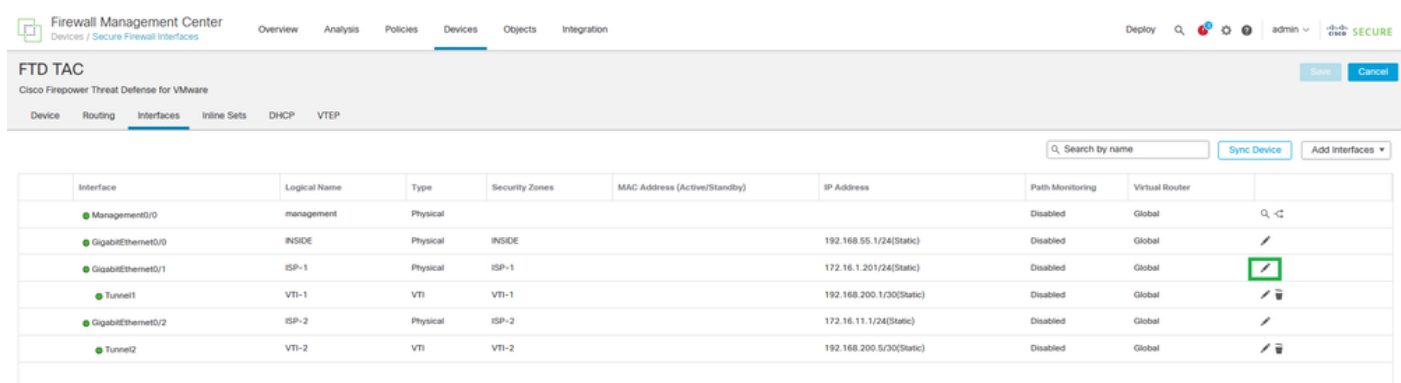
راسمل ةبقارم نيكم

عافدل اذه ررحو ديدهتال عافد Devices > Device Management لقنتا 1. ةوطخل



زاجال ةرادا

لليدل (ISP-1 و ISP-2) WAN/ISP تاجاو ريرحتب مق، بيوبتال ةمالع Interfaces تحت 2. ةوطخل (اذه نيوكتال).



ةجاولا نيوكت

HTTP-based Application ةناخ Enable IP Monitoring رتخاو، بيوبتال Path Monitoring ةمالع قوف رقنا 3. ةوطخل Monitoring رايخال. ننيكم توارياخال Save. رقنا م.

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

ههجاوول راسم ةبقارم نيوكت



قبااسل نيوكتل مسق ي ف اهنويوكت مت ي تل تاقيبطتل جارد ا بجي :ريذحت



ةبقارم تادادع نم ققحت . اذه نيوكتل ليلدل "ةبقارمل عون" رايتخ ا مت :ةطحال م
ىرخأل تارايل ل و ح ديزمل ةفرعمل [ي مسرل نيوكتل ليلدل](#) ىلع راسمل

اهنيوكت مت ي تل WAN/ISP تاهجاو عيمل 3 و 2 تاوطخل ررك 4. ةوطخل

اهرش ن ب مقو تاريغت ل Savel قوف رقنا 5. ةوطخل

ةبقارمل تامولعم ةحول ةفاض ا

System > Health > Monitor. ا لقتنا 1. ةوطخل

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

راسم ال سي ياقم بة دي دج تامول عم ةحول ةفاض

ةحصل نم ققحتال

تائالكال ةعومجم و ECMP و ةمئاعال ةتباثال تاراسمال نم ققحتال ةي فيك مسقلا اذه حضوي
PBR. تانيوكتو تاقيبطتال عم

ةيضا رتفالال تاهجومال او ةمئاعال ةتباثال تاراسمال نيوكت نم ققحتال:

```
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 نيوكت نم ققحتال:

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

هيچوتال لودج موق ي نأ بجي .هيچوتال لودج ىلع ،ECMP ةطساوب رورمال ةكرح ةنزاوم نم ققحت
نم آل FTD هيچوت لودج ي ف ني هجومال الك تي ب ثب

```
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: راسم ةطيرخ نيوكت نم ققحتال

```
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
!
```

مسا نم ققحت) PBR نيوكتل اهنبيعت متي التال (ACL) لوصولو في مكحتال ةمئاق نم ققحت
(راسم ال ةطيرخ نيوكت لىل (ACL) لوصولو في مكحتال ةمئاق

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

نم ققحت) لوصولو ةمئاق لىل ةنعمل تاقيبطتال مادختساب تانئالك ال ةومجم نم ققحت
(ACL)) لوصولاب مكحتال ةمئاق نيوكت في تانئالك ال ةومجم مسا

```
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"
```

PBR: نيوكت لىل ةمدختسمال تانايابل تاهاول نيعمل جهنل راسم نم ققحت

```

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
!

```

ةلوج تقوو MOS نافجر نم ققحتلاو HTTP راسم ةبقارم تامولعم ةحول تامولعم نم ققحت ةمزل نادقف تاءاصحاو ةلحرلا



HTTP راسم ةبقارم تامولعم ةحول نم ققحتلا

اهحالصاوا عاطاخال افاشكتسا

ةبقارملا نيكمت عم WAN/ISP تاهجاو نيوكت متي ،راسملا ةبقارم لشف ةلاحي فو تاراسملا يلع اهنوكت متي تال ةباوبلا ال ICMP قيقحت مزح لاسرال IP ال ةدنتسملا ICMP لمع نم ققحتلل WAN/ISP تاهجاو يلع جرخملا/لخدملا طاقتل نيوكتب مق .ةتباثل

جرحم و لخدم طاق تال:

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

لخدم رسأ:

```
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
```

جرحم لال رسأ:

```
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
```



نأل هه جولاو ردصم لل IP نيوان ع مادختساب طاقتلال تاي لمع ني وكت نم دكأت :ريذحت
عبرملا ىلع ظوحلم لكشب عادأل دي زت نأ نكمي طاقتلال تاي لمع.



لخدم ريصقتلا عم رشابملا ليصوتلا ىرحتي ،زي زأة لمع لمعي ال نا :حيملت
cisco TAC ب لصتا وأ ،ةلواط ARP لا تصحف.

رورم ةكره هجوت نامضل مزحلل عبتتت ةادأ مادختسا كنكمي ،لمعي PBR ناك اذا امم ققحتلل
PBR مادختساب قيبتلل.

```
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
```



متي تال ةكبشلا ةمدخل قيبتلل ابصاخلا IP نيوان ع لوح دي زملا ةفرعمل :ةظحال
show object-group network-service detail رمأل مدختسا ،تائال تاعومجم ىلع اهني وكت.

ەلص تاذا تامولعم

انە HTTP راسم ەبقارم عم PBR ب ەقلعتم ەيفاضا تادنتسم ىلع روثلعل نكمي

- [يرانلا رادجلا ەرادا زكرم زاھ نيوكت ليلد ىلع ەسايسلا ىلع مئاقلا ەيچوتلا نيوكت نملآا](#)
- [زاھ نيوكت ليلد ىلع ەسايسلا ىلا دنتسملا ەيچوتلا نيوكت ىلع راسملا ەبقارم نملآا ەيامجللا رادج ەرادا زكرم](#)
- [ەسايسلا ىلا دنتسملا ەيچوتلا ەن نيوكت](#)
- [ەسايسلا ىلا دنتسملا ەيچوتلا نيوكتلا لاثم](#)
- [PBR راسم ەبقارم لاثم نيوكت](#)
- [راسملا ەبقارم تامولعم ەحول ەفاضلا](#)
- [ەيامجللا رادج ەرادا زكرم زاھ نيوكت ليلد ىلع DNS ىساسلا ماظنلا تاداعلا نيوكت نملآا](#)
- [Cisco نم تاليزنتلا و ىنفلا معدلا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا