

Azure عقوم ىلإ عقوم نم VPN ةكبش نيوكت ةيامحل رادج نيماآل vWAN

تايوتحمل

[قم دقمل](#)

[ةيساسال تابلطمل](#)

[تابلطمل](#)

[قم دختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[يطي طختل مسرل](#)

[\(باركتل Azure لمج قنزاوم\) FTD و Azure نيبي دلاخ vWAN DIA Link لاصتا](#)

[نيوكتل](#)

[Azure vWAN/Hub نيوكت: ىلوالا قلخرمل](#)

[vWAN ةكبش عاشنا: 1 ةوطخل](#)

[vWAN عزوم عاشنا: 2 ةوطخل](#)

[Azure vWAN نم VPN عقوم نيوكت: ةيناثلا قلخرمل](#)

[\(دعب نع FTD زاوج\) Azure vWAN VPN عقوم عاشنا: 1 ةوطخل](#)

[Azure vWAN عقومل VPN تامولعم نيوكت: 2 ةوطخل](#)

[Azure vWAN عقوم قفن نيوكت ليزنت: 3 ةوطخل](#)

[FTD نيوكت: ةثلاثلا قلخرمل](#)

[Azure VPN نيوكت لىلخت: 1 ةوطخل](#)

[عاجرتسال نيوكت: 2 ةوطخل](#)

[2 قلخرمل/1 قلخرمل جهن تانئاك نيوكت: 3 ةوطخل](#)

[Azure ب نم آلا لاصتال نيوكت: 4 ةوطخل](#)

[Azure ب ىلوالا لاصتال نم ققختلا: 5 ةوطخل](#)

[Azure Instance1 ىلإ ىناثلا قفنتلا ةياهن ةطقن نيوكت: 6 ةوطخل](#)

[ECMP نيوكت: 7 ةوطخل](#)

[ةصاخلا IPS ةلثم ىلإ ةتباثلا تامولعم نيوكت: 8 ةوطخل](#)

[BGP نيوكت: 9 ةوطخل](#)

[تاراسمل ددعت BGP نيوكت: 10 ةوطخل](#)

[ققصل نم ققختلا](#)

[ىرخأ تارابتعا](#)

[AS راسم ديمت](#)

[امجالص او عا طخال فاشكتسا](#)

[قلص تاذا تامولعم](#)

قم دقمل

ىلإ عقوم نم (vWAN) Microsoft Azure Virtual WAN نم VPN لاصتا نيوكت دنتسمل اذه فصى
Cisco Secure Firewall ب عقوم

سياسات التابلطتم

تابلطتم

التي تعلقها تاعوضوم الة فرع م Cisco صوت

- Microsoft Azure (vWAN) لة ره اظلا عساو الة قطنم الة كبش
- Cisco نم (FMC) نم الة امحل راج عراا زكرم
- Cisco نم (FTD) الة امحل راج ديدهت نع نم الة افدل

م دختسم الة انوكم

التي تعلقها الة انوكم او جمارب الة ارادصا الة دننسم الة اذ في ة دراو الة امولعمل دننست

- Cisco Secure FTD، رادصا الة 10.0
- Cisco Secure FMC، رادصا الة 10.0

صاخ الة لمعم ةئي ب في ة دوجوم الة زهجال نم دننسم الة اذ في ة دراو الة امولعمل عاشن م تناك اذا. (يضا رتفا) حوسم نم نيوك تب دننسم الة اذ في م دختسم الة زهجال عي مج تادب رمأ الة لم تحم الة ري ثأ لل كم هف نم دكأ تف، لي غشت الة دي ق ك تكبش

سياسات امولعمل

تاكبش الة تاي ناكم نم دي دعل ني ب Microsoft Azure نم (vWAN) الة ره اظلا WAN ة كبش عمجت ة باوب vWAN عروم لك في ضتسي نأ نكمي. دحاو زكرم نيوك تفلخ Azure نم هي جوتل او نام الة او زهجال اهم دختست ي تل او عقوم الة عقوم نم اهت راد م متو Microsoft لبق نم ة رادم VPN ة ين الة انب الة رارطضال نو د Azure الة لوصول، نم الة امحل راج لثم، ة دي عبال اهت نا ي صو ة رابعلل ة سياسات

Azure نم VPN ة باوب رشن م تي، IPsec نم ني تطقن تاذ ة دي لقت VPN ة كبش س ك ع الة اهنم لكل، (Instance0 و Instance1) تال ي ثم الة نم طشن-طشن جوزك عقوم الة عقوم نم vWAN نم ة داف تسال. (BGP) ة دي دوجل ة رابعل لوكوتورب بناجت ناو نعو اب صاخ الة ماع ال IP ناو نع لاسر الة جم انرب موق ي، ة فياض الة ة ل عمل ة عسو راركت لال قلعتي امي في ني تل لال اتلك لوكوتورب م ادختساو لي ثم لكل (IPsec) IP ناما ق فن عاشن اب ي عرف ال (FTD) عرسال قئاف ي كي ماني د لكشب اه بحسو تاراسم الة الة فرعتل، ه دجو تبا ثل هي جوتل نم الة ب BGP و (ECMP) تاراسم الة ددعتم هي جوتل لمعي، كلذ دعب. اه رفوت مدع و ا ة لثم الة رفوت درج م ني ق فن الة الة الة ظافحل الة ف TD الة تاراسم الة ددعت BGP راسم و ة واسم الة ة لكتل

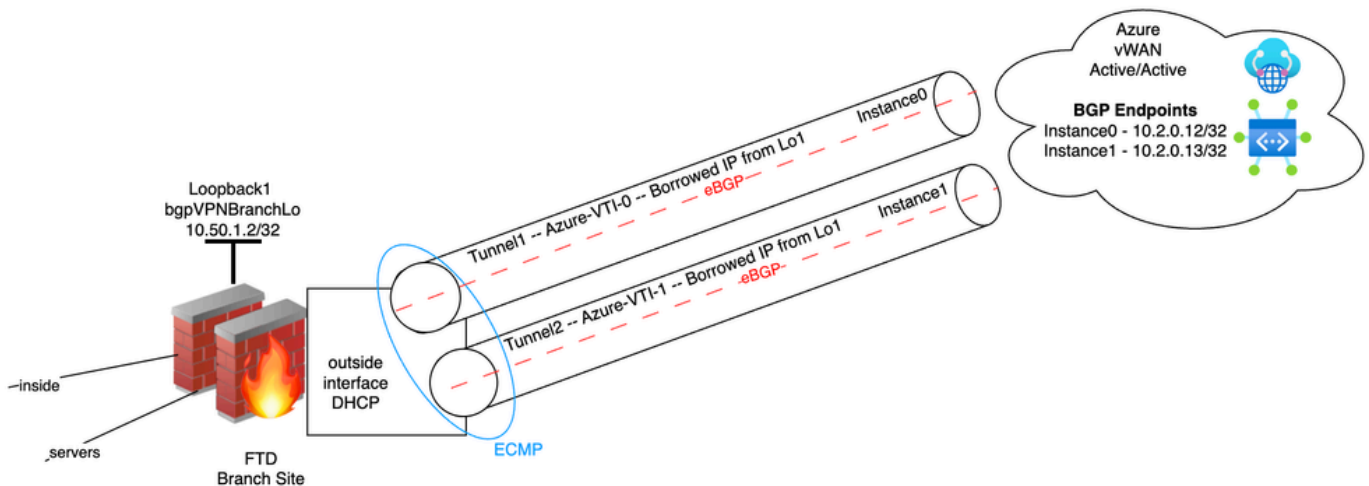
يېلېس دادعتسك امه دجأ ةجلالعم نم الدب ،تقول س فن في ني طشن

vWAN روحم تانئاك عاشنإ م تي :لحارم ثالث ىل عمي مصتلا اذه نيوكتب دنتسملا اذه موقى
سفن مادختسا م تي م ث ،ةجتانل لاصتالا تاملعم ليزنت م تي و ،الو Azure نم VPN عقوم و
رادصلال Internet Key Exchange و (VTIs) ةقباطملا ةيرهاظلا قفنل تاهجاو نيوكتل تاملعمل
FMC لالخم نم FTD ىل ريظن BGP و ،ECMP و ،ةتباتل تاراسملاو ،جهنل IKEv2/IPsec 2

ي طي طختلا مسرلا

لوصول ديحول ريغتمل ردصي و .ةلاقملا هذه في حضومل نيوكتل ططخم ططخملا حضوي
FTD ىل ةيجراخ ةهجاو نم Azure قافنأ (DIA) تنرتنالا ىل رشابملا

(راركتل/Azure لمحنزاوم) FTD و Azure نيبي داحأ vWAN DIA Link لاصتا



نيوكتل

اهؤاشنإ م تي ال Azure بناج ىل ةدوجومل تانئاكل جتنت .ببترتلاب ثالثال لحارملا لمكأ
حاتملاو (AS) BGP ل ي تاذلا ماطنلا ماقراو ريظنل IP نيوانع 2 ةلحرملو 1 ةلحرمل في
FTD ىل كلذ دعب 3 ةلحرمل هيلع قبطنت يذلا اقبس م كرتشملا

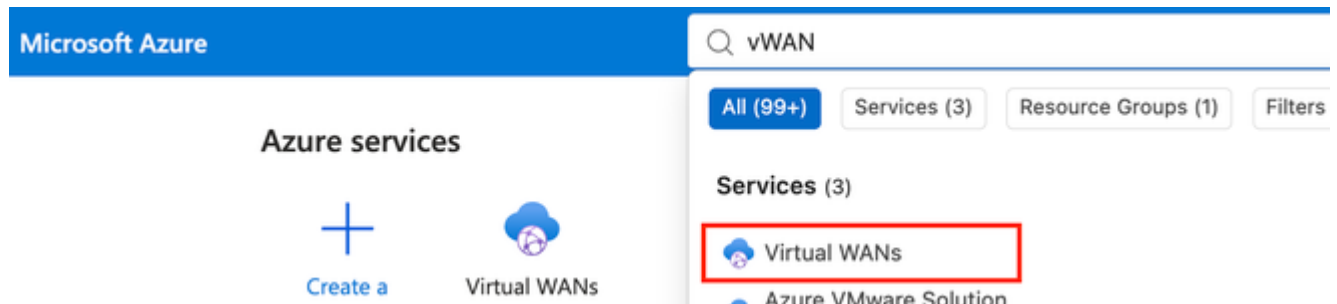
Azure vWAN/Hub نيوكت :ىلوالا ةلحرمل



تاوطلخال رفوتو ىوتسملا ةللا دنتسملا اذه في ةدراول نيوكتلا تاوطلخ: ةطلخال
Microsoft نم Azure vWAN قئاثو ىلا عجار. Azure vWAN ب FTD ليصوتل ةيرورضل
ىخأ قئاثوو [Azure Virtual WAN؟ وه ام](#) عجار. تانيوكتلا ةيمهأ مهفل

vWAN ةكبش عاشنإ: 1 ةوطخل

ةيرهاظلا WAN تاكبش قوف رقنا، Azure شحبلا عبرم في WAN ةكبش نع شحب أ)



عاشنإ + قوف رقنا ب)



ةحفص ىل عاشنإ قوف رقناو، عاشنإ + ةعجارم قوف رقناو، ديذل vWAN ليثمل مسا لخدأ ج)
جلعمل لخد عاشنإ + ةعجارم

Create WAN ...

Basics Review + create

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#) 

Project details

Subscription *

Resource group * [Create new](#)

Virtual WAN details

Region *

Name * 

Type ⓘ

Review + create

Previous

Next : Review + create >

نوكت روصال في ةفلتخم لوقح في ميقل يطغت يتل اءاضيبل ةحاسملا :ةظالم
دننسملا اذه رشنل ةدوصقم

دروملا إلالاقتنا قوف رقنا د)



VirtualWanDeployment | Overview

Deployment



Delete



Cancel



Redeploy



Download



Refresh

Overview

Inputs

Outputs

Template



Your deployment is complete



Deployment name : VirtualWanDeployment

Subscription :

Resource group :



Deployment details



Next steps

Go to resource

vWAN عزوم عاشنإ: 2 ةوطخل

ةديج لصوةحول + رقناو عيزوتلا تاحول > لاصتالا ىلإ لقتنا أ)



CX-vWAN | Hubs



Virtual WAN



New Hub



Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Properties

Locks

Connectivity

Hubs



VPN sites

User VPN configurations

ExpressRoute circuits

Clear all filters

Add filter

Hub

Hub status

Region

No results

نأ ن م دكأت .يفاضإلإ نيوكتلال لوح يفاضإ قاي س ىل ع لوصحلل Azure قئاثو ىلإ عجرا (ب) صاخلا ةيلخادلل نيوانعلا تاحاسم نم ي أ عم لخادتت ال صصخمل صاخلا Hub ناو نع ةحاسم عقوم : كلذ دعب تقطقط .عزومال هيحوت ليضفت ،يرهاظلا عزومال ،مسالال نيوكتب مق .كب >.عقوم ىلإ

Home > CX-vWAN | Hubs

Create virtual hub

Basics Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpsite). [Learn more](#)

Project details

The hub will be created under the same subscription and resource group as the vWAN. ⓘ

Subscription

Resource group

Virtual Hub Details

Region *

Name * ✓

Hub private address space * ⓘ ✓

Virtual hub capacity * ⓘ

Hub routing preference * ⓘ

Creating a hub with a gateway will take 30 minutes.

[Review + create](#) [Previous](#) [Next : Site to site >](#)

لوقحلال لوح تامولعم ىل ع لوصحلل Microsoft Azure vWAN Hub قئاثو ىلإ كلذك عجرا (ج) BGP ل يئاذل ماطنل مقرر نوكي . (VPN ةبابو) عقوم ىلإ عقوم عاشنإل م عن لي دبت . ةمدقمال ةسدنه لمع قيرف لبق نم هصي صخت مت امك ، 65515 وه صصخمل يضا رتفال (AS) زجحك صاخلا مادختسال ددحي يذلا 6996 (RFC) تاقيلعتال بلطي ف (IETF) تنرتنإل

دحو ىل ع ةيلبقتسمال نيوكتلال تاوطلخ BGP AS لوكوتورب ليحستب مق : ةظالم (FMC) . ةيساسألأ ةرادإل ي ف مكحتال

Create virtual hub ...

Basics Site to site Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

☒ Yes☐ No

Copied

AS Number

65515

Gateway scale units

Routing preference



Microsoft network



Internet

Creating a hub with a gateway will take 30 minutes.

[Review + create](#)[Previous](#)[Next : Point to site >](#)

تادادعإل نيوك تل > ع قوم إل إل ع ج ر : ل ل ل قوف ر ق ن أ ، ء ا ش ن إ + ة ع ج ا ر م قوف ر ق ن ا
ة ر ا ي ت خ ل ا

ء ا ش ن إ قوف ر ق ن ا ، ص خ ل م ل ا ة ح ص ن م ق ق ح ت ل ا د ع ب د)

ة ق ي ق د 30 ة ر ص ل ا ء ا ش ن إ ق ر غ ت س ي ، Azure ر ك ذ ت ا م ك : ة ط ح ا ل م

Home > CX-vWAN | Hubs

Create virtual hub

✓ Validation passed

Basics Site to site Point to site ExpressRoute Tags **Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	
Name	CX-vWAN-Hub
Hub private address space	10.2.0.0/16
Virtual hub capacity	
Hub routing preference	

Site to site

Site to site (VPN gateway)	Enabled
AS Number	65515
Gateway scale units	

Point to site

Point to site (VPN gateway)

ExpressRoute

ExpressRoute gateway

Tags

Creating a hub with a gateway will take 30 minutes.

[Create](#) [Previous](#) [Next](#) [Download a template for automation](#)

ثحب ال قاطن قبيضتل .كب صاخل ي لصلأل vWAN دروم مسا نع ثحبا ،رشنل لامتكا دعب ه) دراومل قوف رقنا ،ربكأ لكشب

Home

VirtualHubDeployment | Overview

Deployment

Search [x] [y] [z]

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name : VirtualHubDeployment

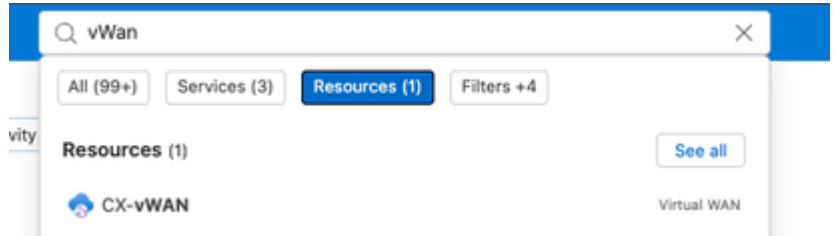
Subscription :

Resource group :

> Deployment details

✓ Next steps

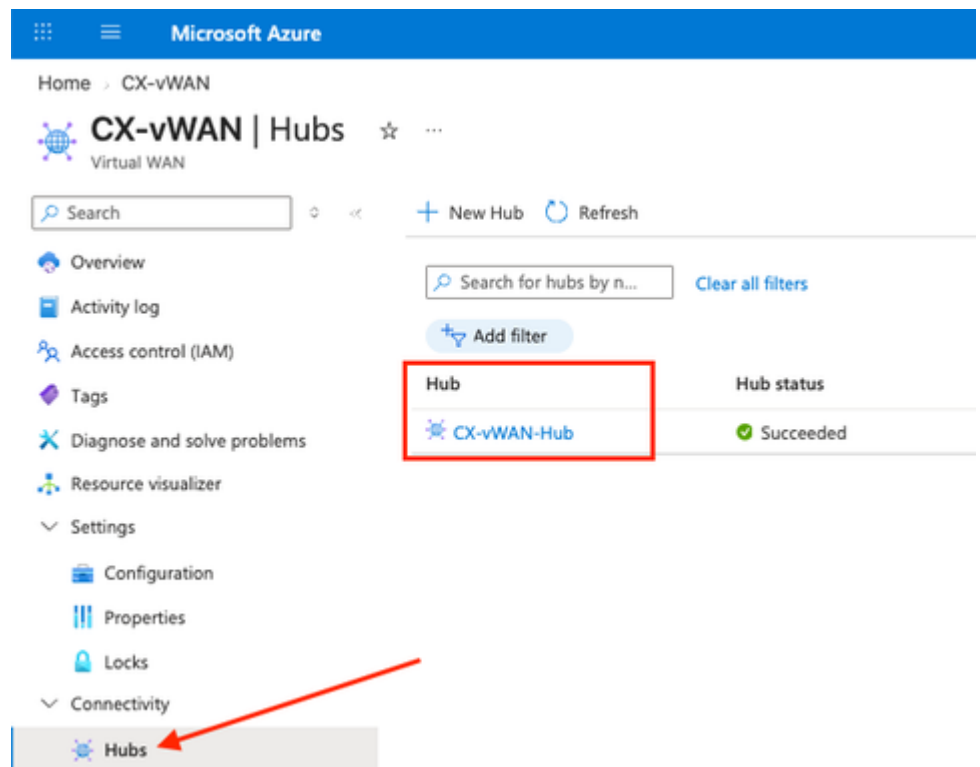
[Go to resource](#)



Azure vWAN نم VPN عقوم نيوكت :ةيناثلا ةلحرمل

(دعب نع FTD زاھج) Azure vWAN VPN عقوم ءاشنإ :1 ةوطخل

ةرصلال ىلع رقناو عيزوتلا تاحول > لاصتالا قيرط نع اهؤاشنإ مت يتلا ةرصلال ىلإ لخدأ أ) ةقباسلا تاوطخلال في اهؤاشنإ مت يتلا



ديج عقوم VPN قلخي + ةقطقو (عقوم ىلا عقوم) VPN >ةيلوصوم ةقطق (ب)

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ⓘ

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

Site name	Location	Cloud
No results		

امدق يضل لل > طباورلا :يلاتلا رقنا ،ءاهتناال دنع .ةبولطملا لوقحللا يف ميقلا لخدأ (ج)

Create VPN site ...

Basics Links Review + create

Project details

Subscription

Resource group *

Instance details

Region *

Name *

Device vendor *

Private address space

At least one address space is required if BGP isn't configured. To configure BGP, please go to Links tab.

 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Links >

ناونع طبارلل ASN لقحو طبارلل BGP ناونع سكهي .ةبولطملا طابترالا تامولعم لخدأ (د) نيوكت متي عرفال عقوم يف مقرك BGP لثمي وي لخدال قفنلل 3 ةقبطلا نم BGP ةهجو ةيعرف ةكبش ناونع وه طبارلل BGP ناونع .عقوم ىلإ عقوم نم قافناً ربع Azure عم راولا اهنىوكت متي تال روحملل صاخلا ناونع بة صاخلا ةيعرفال ةكبشال جراخ (/32) لخداتم ريغ IP ناونع نإ .BGP راجك اهلا لوصولل 32/ راسمك اهتيبثت Azure موقى يتلاو ،اقباس لقتنت يتلا رورملا ةكرحل يجرال سارلل 3 ةقبطلا نم ةهجولل IP ناونع وه FQDN/طابترال IPsec/IKEv2 لاصتا ريفوتل يرورضل عرفال عقوم ىلإ

169.254.22.255 ىلإ 169.254.21.0 نم حوارتت نيوانع مدختست تنك اذا :ةطحال م ةيبلتل [Azure VPN](#) ةرابعل BGP نيوكت ةيفيك ةعجارم نم دكأتف ،قافنأل نيوانعل .ةدحمتابلطتم

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

Link name	Link speed	Link provider name	Link IP address / FQDN	Link BGP address	Link ASN	
single-dia-link ✓	1000 ✓	provider ✓	✓	10.50.1.2 ✓	65500 ✓	...

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Review + create >

عاشنإ ىلع رقنا ،تادادعإلأ ةحص نم دكأتلا دعب ه)

Create VPN site ...

✓ Validation passed

Basics Links **Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region

Name

VPN-Site

Device vendor

Cisco

Private address space

Links

Link name	single-dia-link
Link provider name	provider
Link speed	1000
Link IP address / FQDN	
Link ASN	65500
Link BGP address	169.254.10.2

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Create

Previous

Next

ةكبش روحم نيوكت ىلإ عجرا ، (VPN) ةيرهاظلا ةصاخلا ةكبشلل عقوم رشن لامتكأ درجمب (و
WAN v.

Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

- Overview
- Inputs
- Outputs
- Template

✓ Your deployment is complete

Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

[Go to resource](#)

Search vWan

All (99+) Services (3) **Resources (1)** Filters +4

Resources (1) [See all](#)

 CX-vWAN Virtual WAN

Azure vWAN VPN عمل تام نيوكت 2: ةوطخل

ةرصل ال عل رقن او ع يزوتل ااحول > لاصل ال قيرط نع اهؤاشن م ت ال ةرصل ال إل لخدأ أ)
ةقباسل ااوطخل ال ف اهؤاشن م ت ال

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search New Hub Refresh

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Configuration
Properties
Locks
Connectivity
Hubs

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

نارتقا حسمل X قوف روناو (عقوم ىلا عقوم نم) VPN > لاصتالا ىلا ىرخأ قرم لقتنا ب)
اهلاصتا عطق مت يلا عقاوملا ضرعل قلصتملا ةيفصتلا: عزوملا

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview
Connectivity
VPN (Site to site)
ExpressRoute
User VPN (Point to site)
Routing
Security
Third party providers
Monitor

Essentials
Gateway configuration
NAT Rules

VPN Sites Metrics

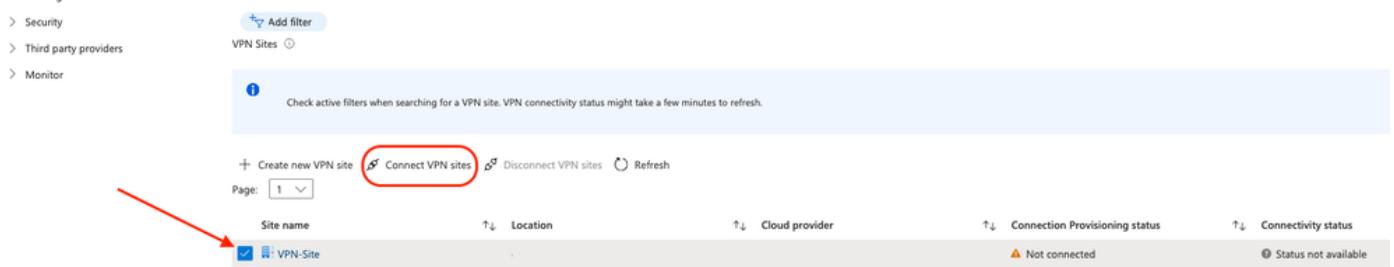
Search this page Clear all filters

Hub association : Connected Add filter

VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

لي صوت قوف رونا م، اقبسم هنيوكت مت يذال VPN عقوم راجب دوجومال ع برمل ددح c)
عقومال ديدحت دعب هنيوكت مت يذال او، VPN عقاوم



مقو (PSK) اقبسم كرتشم حاتفم لخدأ. Connect عقومب ةصاخلا ةيبناجال جردلا ةحول رهظت د)
ةمئاقلا نم صصخم رايتخا دنع. ةبولطمال IPsec 2 ةلجرمل او IKEv2 1 ةلجرمل تادادعلا نيوكتب
يف قباطت نا بجي شيح، ميقل هذه ظحال؛ ايئاقلا ميقلل ميمعت متي، IPsec ةلدسنملا
ارظنو. ةبولطم (PFS) ةلمالكلا هيحوتلا ةداعا ةيرس تناك اذا ام راتخت نا اضيا كيلى بجي. FTD.
لي صوت قوف رونا. كلذل اقوفو تادادعلا نيوكتب مق، راسملا الى دنسسي قفن اذه نال
نيوكتلا ظفحل اهلامتكا درجمب

[Azure vWAN](#) ةصصخملا IPsec تاسايس لباقم ةيضا رتفال تاسايسلا عجار: ةظحالم
تامولعمل نم ديزم يلى لوصحلل

Connect sites

Virtual HUB

Security settings

Pre-shared key (PSK) ⓘ

Protocol

IPsec ⓘ

SA Lifetime in seconds * ⓘ

IKE Phase 1 ⓘ

IKE Phase 2(ipsec) ⓘ

Propagate Default Route ⓘ

Use policy based traffic selector ⓘ

Configure traffic selector?

Connection Mode ⓘ

.....

IKEv2 IKEv1

Default Custom

i When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

27000

Encryption *

GCM AES256

Integrity/PRF *

SHA384

DH Group *

DHGroup24

IPsec Encryption *

GCM AES256

IPsec Integrity *

GCM AES256

PFS Group *

NONE

Enable Disable

Enable Disable

Yes No

Default Initiator Only Responder Only

These sites will be connected to the [CX-vWAN-Hub] hub.

Site name

↑↓

Region

↑↓

VPN-Site

eastus

Connect

أهتال ردقمل تقولا عم ،ةباوبل شيدحت متي هنا إلى ريشت تامولعم ضرع متي (ه)

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site) ⓘ ...
Virtual HUB

Search

Download VPN Config

Packet Capture

Delete gateway

Reset gateway

Monitor Gateway

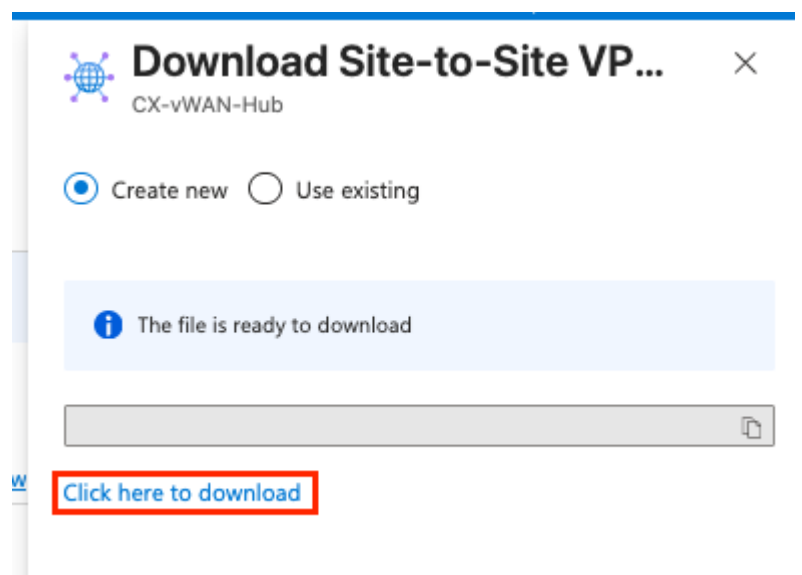
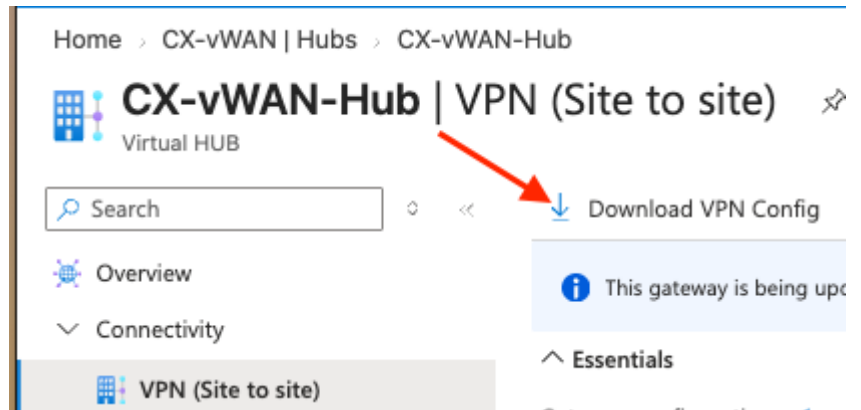
Overview

Connectivity

i This gateway is being updated. It may take upto 30 minutes for the update

Azure vWAN عقوم قفني وكت لي زنت : 3 ةوطخلا

VPN. نيوكت لي زنت كنكمي، ةبوابل شي دحت ءانثأ أ)



BGP و ريظنل نيوانع) هب ةصاخلا لاصتالا تاملعمو هؤاشنإ مت يذلا VPN عقوم لي زنت عم
في FTD لىل عىب اطملا رصانعلا نيوكتل اهسفن ميقل مادختسإ متي، (PSK و ماقراك
3. ةلحرملا

FTD نيوكت :ةثلاثلا ةلحرملا

Azure VPN نيوكت لي لحت :1 ةوطخلا

ةفثكملا جتاوئلل ةهباشم و دبت اهنإ. Azure نم هلي زنت مت يذلا VPN نيوكت فلم حتفا أ)
ةديفم تامولعم رفوتو ةضورعملا

جاوزأو ةلصللا تاذ ريغ تانئاكلال نم ديدعلال ميقلت متي، زيكرتلال نيسحتلو :ةطحال

زاجي إالا لجأ نم ميقلل/حي تافملا

```
[
  {
    "configurationVersion": {
      "LastUpdatedTime": "

    },
    "Version": "

    ",
    "BgpSetting": {
      "Asn": 65500,
      "BgpPeeringAddress": "10.50.1.2"
    },
    "LinkName": "single-dia-link"
  },
  "vpnSiteConnections": [
    {
      "hubConfiguration": {
        "AddressSpace": "10.2.0.0/16",
        "Region": "

      "
    },
    "gatewayConfiguration": {
      "IpAddresses": {
        "Instance0": "57.x.x.x",
        "Instance1": "52.x.x.x"
      },
      "BgpSetting": {
        "Asn": 65515,
        "BgpPeeringAddresses": {
          "Instance0": "10.2.0.12",
          "Instance1": "10.2.0.13"
        }
      }
    },
    "connectionConfiguration": {
      "IsBgpEnabled": true,
      "PSK": "

    ",
    "IPsecParameters": {
      "IPsecEncryption": "GCMAES256",
      "IPsecIntegrity": "GCMAES256",
      "IKEEncryption": "GCMAES256",
      "IKEIntegrity": "SHA384",
      "PfsGroup": "None",
      "DhGroup": "DHGroup14",
```

```

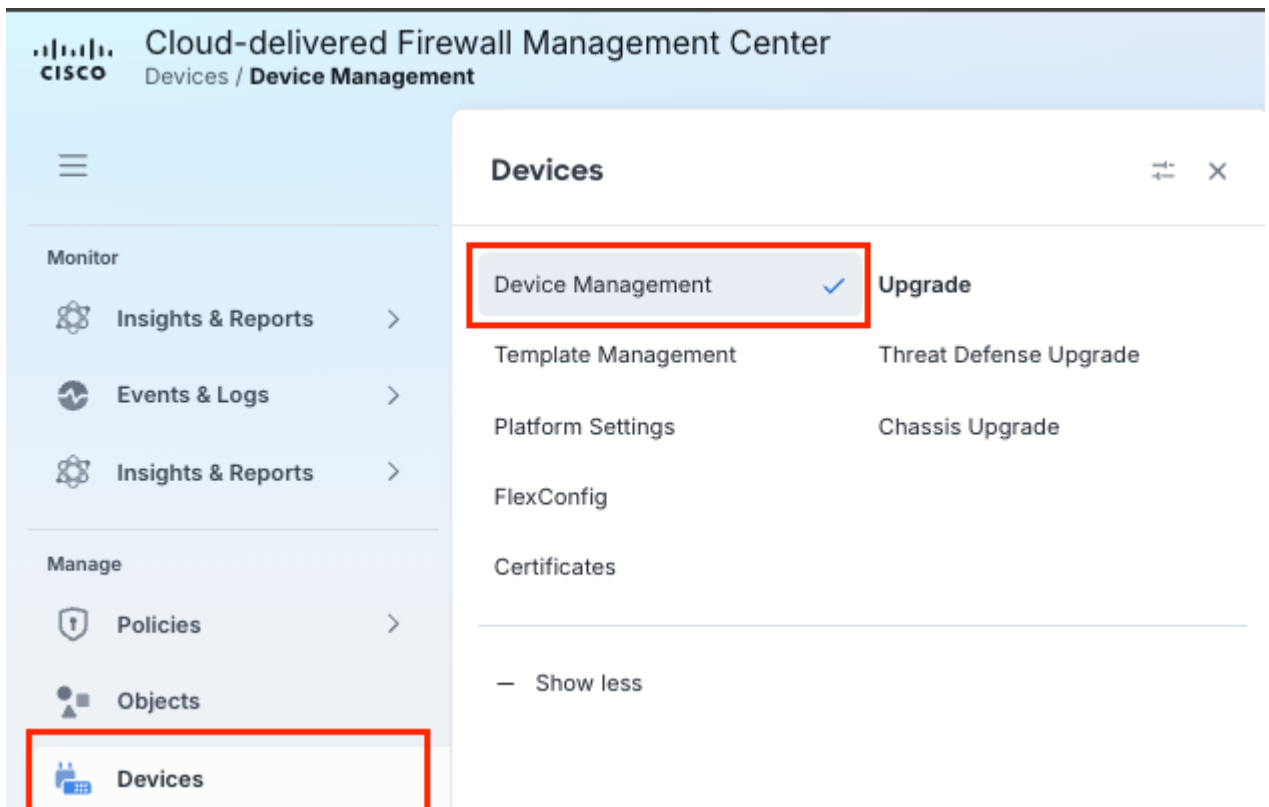
"SADataSizeInKilobytes": 0,
"SALifeTimeInSeconds": 27000
}
}
}
]
}
]

```

عاجرتسالا نيوكت 2: ةوطخلا

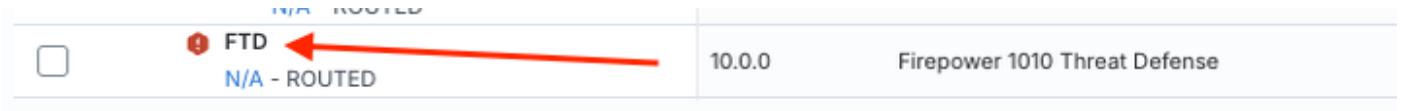
الوأ نراق عاجرتسالا ت لكش ك لذل ،تبات ق فن رصم ىلإ دعب امي ف لكشي VTI لك جاتي

ةزهجال ةرادا > ةزهجال ىلإ لقتنا أ)

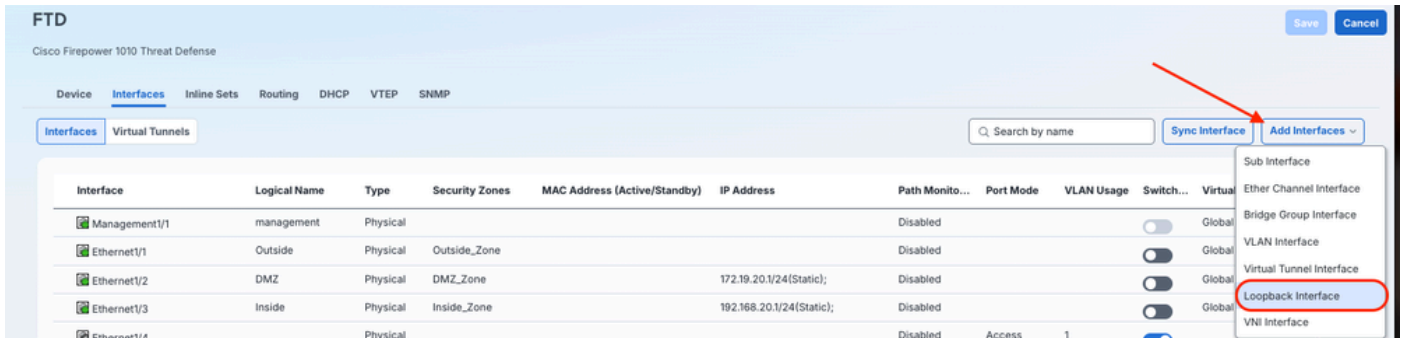


ةباحسالا ربع هليصوت مت يذلا ةيامحال رادج ةرادا زكرم ربتخملا اذه مدختسي :ةظحالم ةرادا ي ف مكحتلا ةدحول ةبسنلاب اهسفن يه تاوطخلا يقبت ،كلذ عمو ؛(CDfmc) اقبسم ةدوجوملا (FMC) ةيساسالا ةحوللا

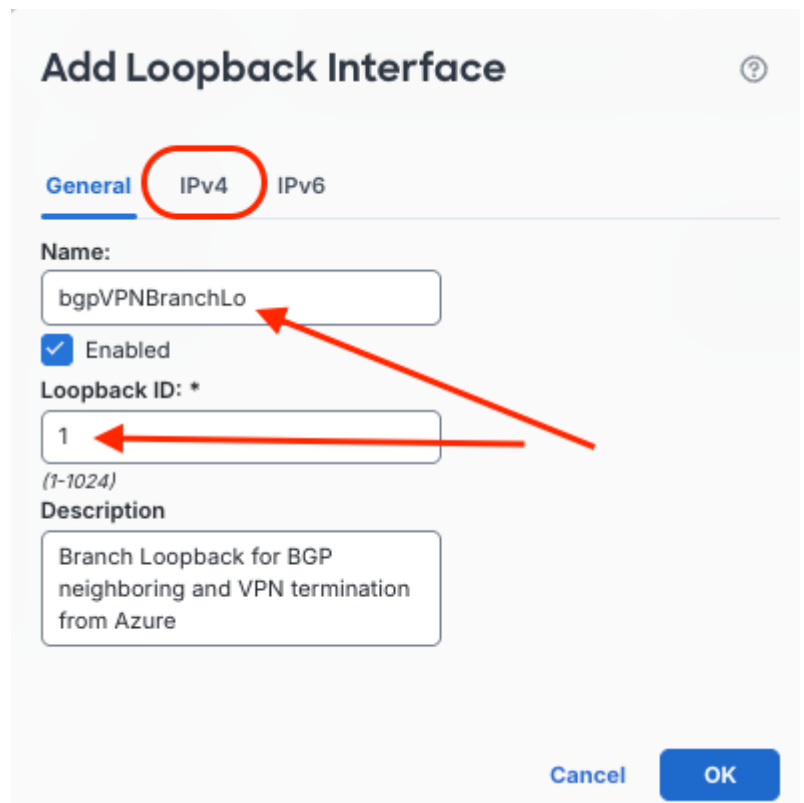
عق و م ل / ع ر ف ل ل VPN ز ا ح ك ه ن ي و ك ت ب م و ق ت ي ذ ل ا FTD د د ح (ب)



ع ا ج ر ت س ا ل ا ه ج ا و ق و ف ر ق ن ا و ، ت ا ه ج ا و ف ا ض ا ة ل د س ن م ل ا ة م ئ ا ق ل ا ق و ف ر ق ن ا (ج)



IPv4 ق و ف ر ق ن ا . ر م ا ل ا م ز ل ا ذ ا ف ص و ل ا و ، ع ا ج ر ت س ا ل ا ف ر ع م ، ا ه م س ا ع ا ج ر ت س ا ل ا ه ج ا و ا ط ا ع (د)



م ت ا م ك ط ا ب ت ر ا ل ل BGP ن ا و ن ع ل خ د ا ، ت ب ا ث IP م ا د خ ت س ا ه ن ا ة ل ع ف ر ع م IP ع و ن ن ا ن م د ك ا ت (ه)
ي ف ا ق ب س م ا ه ف ي ر ع ت م ت ي ت ل ا ة م ي ق ل ا ل ا ة و ج ر ل ا ك ن ك م ي . 1d ة و ط خ ل ، 2 ة ل ح ر م ل ا ي ف ه ن ي و ك ت
VPN config JSON م ت ي ذ ل ا vpnSiteConfiguration.BgpSetting.BgpPeeringAddress ن م ض ه ل ي ز ن ت م ت

RFC 1918 ب ة ص ا خ ل ا ن ا و ن ع ل ا ح ا س م ن م ض و /32 ع ا ن ق ب ن ا و ن ع ل ا د د ح : ة ط ح ا ل م

Add Loopback Interface ?

General
IPv4
IPv6

IP Type:

Use Static IP
▼

IP Address:

10.50.1.2/32

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel
OK

ظفح ىل ع رقنا و)

🔍

Deploy
🌐
🔔
2
?

You have unsaved changes
Save

2 ةلحرم ل/1 ةلحرم ل جهن تانئاك نيوك ت: 3 ةوطخل

ب ةصاغل VPN تاططخم يف قيبطتلل FMC ىل ع قباطم ال IKEv2/IPsec نيوك ت نيوك ت ل (أ) عسوت و VPN ىل ل ىرسل ال ةمئاكل يف لفسأ ىل ل لقتناو، تانئاك > ةراد ىل ل لقتنا، FTD، ةمئاكل يف IKEv2 جهن رايتخاب IKEv2 ل 1 ةلحرم ل جهن نيوك ت ب مق. ةيعرف ال ةمئاكل IKEv2 جهن ةفاضل قوف رقنل او

Policy List

Port

> Prefix List

Route Map

> Security Intelligence

Sinkhole

SLA Monitor

Time Range

Time Zone

Tunnel Zone

URL

Variable

Variable Set

VLAN Tag

VPN

Certificate Map

Custom Attribute

Group Policy

IKEv1 IPsec Proposal

IKEv1 Policy

IKEv2 IPsec Proposal

IKEv2 Policy

Secure Client Customization

Secure Client File

IKEv2 Policy

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

Add IKEv2 Policy

Filter

Name	
AES-GCM-NUL- SHA	Q ☐ ⚙
AES-GCM-NUL- SHA-LATEST	Q ☐ ⚙
AES- SHA-SHA	Q ☐ ⚙
AES- SHA-SHA-LATEST	Q ☐ ⚙
DES- SHA-SHA	Q ☐ ⚙
DES- SHA-SHA-LATEST	Q ☐ ⚙
Umbrella-AES-GCM-256	Q ☐ ⚙

Displaying 1 - 7 of 7 rows | < > Page 1 of 1 >

ةساي سلا قباطت نم دكأت .ةايحل اى دم وأ/و ةيولوالا رتخاو ،ديدل IKEv2 جهنل امسا لخدأ (ب
 Diffie-hellman وPRF وري فشلالاو لماكلال ةومجمل قلع تي امي ف قفنل ايفرط الك لىل
 رقن او ، Azure نيوكت عم قباطتل اه اذاحم تمت يتلل ةومجمل رصانع/ةيمزراوخلال رتخأ (DH).
 ةفاضل قوف

هليزنت مت يذل نيوكتل فلم لخد اة قيقدلل ميقلل هذو لىل اةراشلال كنكمي :ةطحال م
 vpnSiteConnections[0].connectionConfiguration.IPsecParameters لىل

New IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
-
- SHA384
- NULL

Selected Algorithms

SHA256

ظافح تق طوط ،للكشلال مكي نإ ام (ج).

Edit IKEv2 Policy ?

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

1

2

5

14

15

16

19

20

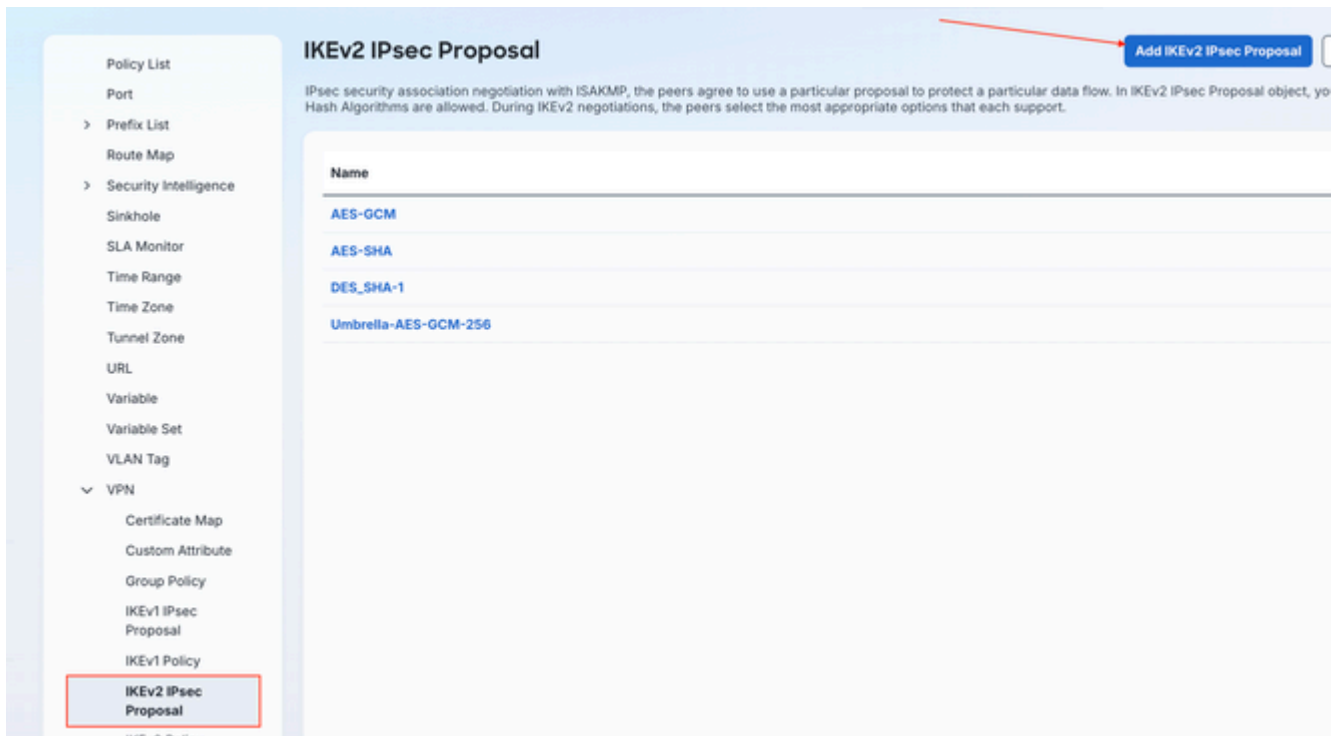
...

Add

14

[Cancel](#) [Save](#)

رقن او IKEv2 IPsec حرت قمل ة يعرف ال ةمئاق ال ي ف IPsec/2 ةل حرم ال تامل عم ني وكتب مق (د
IKEv2 IPsec حرت قمل ة فاضا قوف



رقنا، عاتن ال درج م. تادادع ال س فن ةاذاح م نم دكأتو IKEv2 IPsec حارتقا ةيمستب مق (ه) ظفح قوف.

هليزنت مت يذل نيوكتل فلم نمض ميقل هذه إلى ةراش ال كنكمي: ةظحال م
vpnSiteConnections[0].connectionConfiguration.IPsecParameters

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256

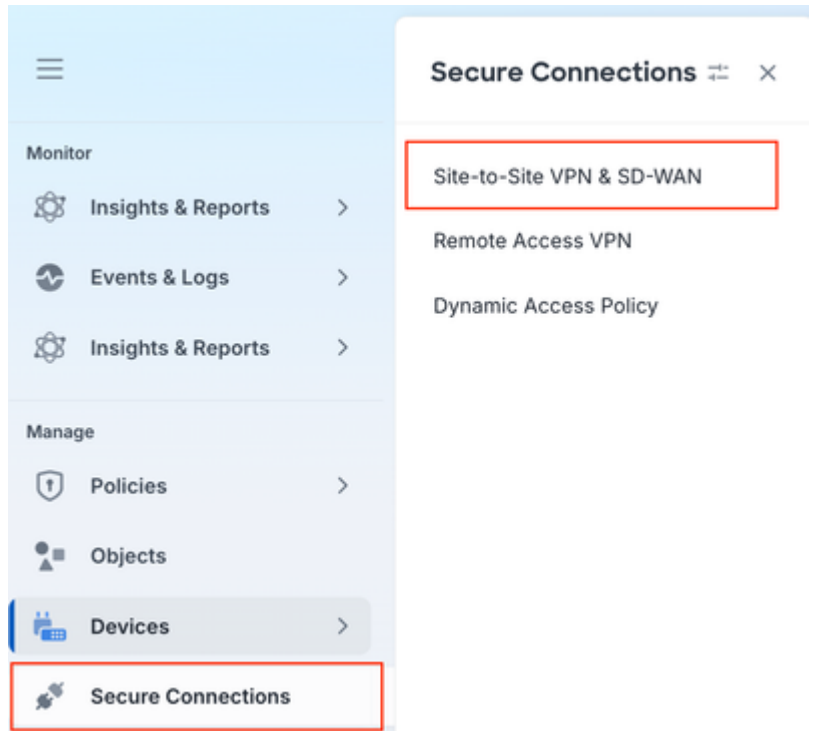


Cancel

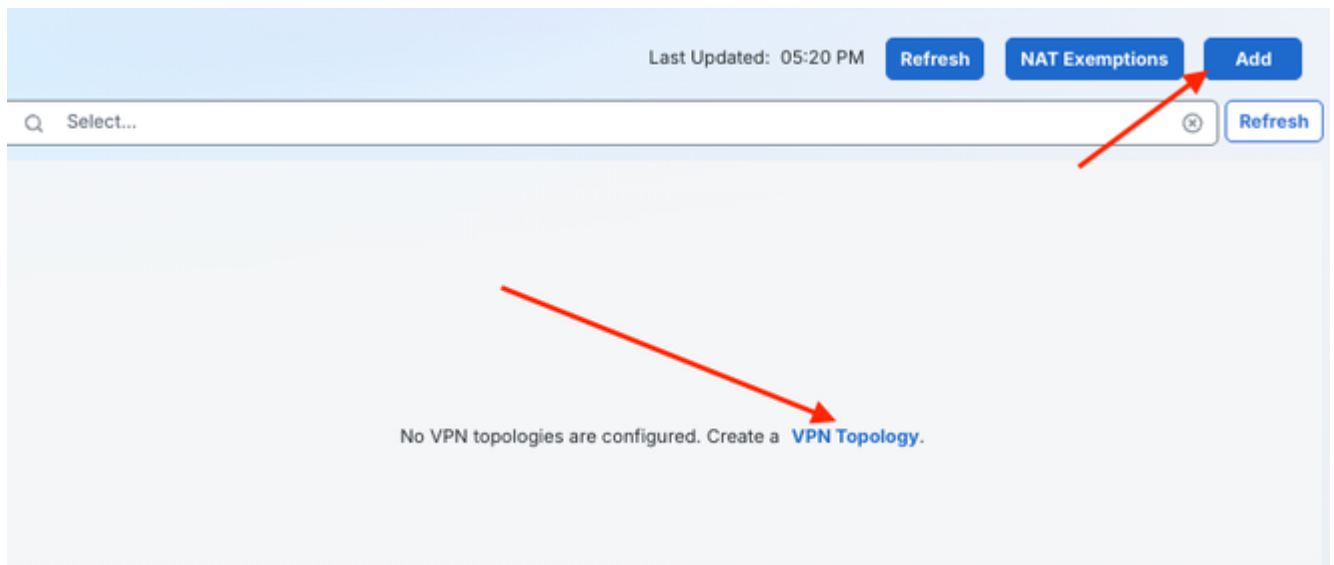
Save

Azure ب نم آلا لاصتال نيوكت 4: ةوطخلا

SD-WAN و عقوم ىلإ عقوم نم VPN ةكبش > نم آلا تالاصتال > ةرادإ ىلإ لقتنا أ)



قوف رقنا وأ، فصتنملا يف يلولال VPN ططخم نيوكتل يبعشتلا طابترالا ىلع ام رقنا (ب) ةفاضإ.



دنتسملا VPN وي دار رز قوف رقناو، Azure0 ليثم ىلإ لولال قفنلل ايچولوبط مسالخدأ c) قوف رقنا، لامتكالا درجمب. ريظنلا ىلإ ريظنلا VPN ايچولوبط عون قوف رقناو، راسملا ىلإ عاشنإ.

Create VPN Topology

Topology name *

Azure-VTI-Instance0

VPN Type

SD-WAN Topology
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☐ Hub and Spoke
Prerequisites

Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☒ Peer to Peer

Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh

SASE Topology
SASE topology cannot be selected because Secure Access and Umbrella are not configured.
Prerequisites
Refresh

Cancel Create

رادم ال HA-pair جوز مسا رتخاو زاهجلا ةلدسننملا ةمئاقلا قوف رقنا A، ةدقعلل ةبسننلاب د) نم ديعبل فرطلا وه نأل، ب ةدقعل ل ترتخأ. هيلع نيوكتلل رشن متي يذل FTD/FTD ةمئاق ةادأل نم تنارتسك، لاثم Azure vWAN ىلع يهن ي ايجولوبطال ي لىصوتلا ةهجاو ةلدسننملا ةمئاقلل رواجمل + زمرلا قوف رقنا A، ةدقعلل ةبسننلاب، كلذ دع ب. ةلدسننم (VTI). ةيرهاظلا قفنلا

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

+ Edit VTI

☐ Tunnel Source IP is Private

☐ Send Local Identity to Peers

+ Add Backup VTI (optional)

> Advanced Settings

Node B

Device:*

Extranet

Device Name:*

Endpoint IP Address:*

Primary IP*, [Backup Peer IPs]

Cancel Save

تني ع VTI، لى إة قطنم نم أ دوجوم وأ ديدج تني ع .هنكمت نم دكأتو، VTI، لو أةيمستب مق (ه)
ةلدسنم ةمئاق رواجم ناوعال نم ip ناوعال ترتخاو، ردصم قفنل

Add Virtual Tunnel Interface

Tunnel Type
☒ Static ☐ Dynamic

Name:*
Azure-VTI-0

☒ Enabled

Description:

Security Zone:
Azure-Spoke-Zone

Priority:
0 (0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*
1 (0 - 10413)

Tunnel Source:*
Ethernet1/1 (Outside) Dynamic

نم عاجرتسال س فن رتخأ م ث، (مقرم ال ريغ IP) IP ضارتقا رز ديدجت نم دكأت، كلذ دعب (و)
م تي نإ ام ok ةق طقط .ينمي ال ةلدسنم ال ةمئاق ال

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*
 (0 - 10413)

Tunnel Source:*

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☐ Configure IP ⓘ
☒ Borrow IP (IP unnumbered) +



لصاً نإ ايئاقلت علمي وه) ناونع ردصم قفنل ايودي تديش، تقبطو VTI ل تلکش نإ ام g) لئثمل as well as، مسإ تلکش ةادأ b ةدقعل نأ تنمضو، DHCP نم ناونع تلمعتسا نراق IKE بويوبتل ةمالع قوف رقنا، اهلامتكا درجمب. ناونع ةياهن ةطقن

يذل نيوكتل فلم ي ف ةياهنل ةطقنل IP ناونع ةميقي لىل ةراشإل كنكمي: ةطحال م
 vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0 لىل هليزنت مت

Edit VPN Topology

Topology Name:*

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source IP is Dynamic (DHCP) [Edit VTI](#)

Tunnel Source IP Address:* ?

☐ Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional

Node B

Device:*

Device Name*:

Endpoint IP Address*:

[Cancel](#) [Save](#)

حالات فم ال ىلع ةقداصلال عون نني عت نم دكأتو IKEv2 تادادعإ ىلإ لفسأل ريرمتلاب مق (ح) مق .ةقباسللا تاوطخلال في Azure في هنيوكت مت يذل PSK لخدأو ،اقبسم كرتشملا يوديلا ريرحتل صاصرلا ملقلا زمر قوف رقنلاب IKEv2 نم ىلوالا ةلحرملا تاسايس نيوكتب .ةرفتوملا IKEv2 تاسايس

نيوكتلا فلم في اقبسم كرتشملا حالات فم ال ىلإ عوچرلا كنكمي :ةطحال م :ةطحال م
 vpnSiteConnections[0].connectionConfiguration.IPSecParameters.PSK ىلع هليزنت مت يذل

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policies:* AES-GCM-NUL-**SHA-LATEST**

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

3. قوطخال في ايئدبم اهنويوكت متي الت IKEv2 نم ىلوالا قلحرملا ةسايس ةفاضإ i)

IKEv2 Policy



Available IKEv2 Policy  

 Search

AES-GCM-NULL-SHA
AES-GCM-NULL-SHA-LAT...
AES-SHA-SHA
AES-SHA-SHA-LATEST
Azure_IKEv2
DES-SHA-SHA
DES-SHA-SHA-LATEST

Add

Selected IKEv2 Policy

Azure_IKEv2 

Cancel

OK

IPsec پي وپتال ءمال ع ددح (ج)

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐

IKEv1

☒

IKEv2

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Azure_IKEv2

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

☐

Enforce hex-based pre-shared key only

ملقاة ونوقية أوف رقتنلاب ليوحتالتاعومجم نمض IKEv2 IPsec حرتقم ريرحتب مق (ك)
صاصرللا

Edit VPN Topology

Topology Name:*

Azure-VTI-Instance0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

AES-GCM

☐ Enable Security Association (SA) Strength Enforcement

تفضل أو، أيضا ارتفال AES-GCM لي وحتة ومجم الازال تالمهم الة لسة نوقيا قوف رقنا ل) نم يثا ال فصننل في اهواشن مت يثا ال IKEv2 IPsec /ة صصخم ال Azure_IPsec لي وحتة ومجم قف اوم قوف رقنا 3. ةوطخل

IKEv2 IPsec Proposal

Available Transform Sets +

Search

AES-GCM

AES-SHA

Azure_IPsec

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

Azure_IPsec

Cancel

OK

مق. Azure. تامل علم قباطت يتي التال رمع الة قرت ف لاوط 27000 لخدأو لفسأل ريرمتلاب مق m) ظفح قوف رقنا .نكم أن PFS ةومجم نيكم تب

م تيذلا نيوكتال فلم يي فيضارتفالال رمع الة ميق يلا عوجرلا كنكمي :ةظحال م
vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds يلع هليزنت

Edit VPN Topology

Topology Name:*
Azure-VTI-Instance0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE **IPsec** Advanced

Lifetime Duration*: 27000 Seconds (Range 120-2147483647)

Lifetime Size: Unlimited Kbytes (Range 10-2147483647)

> ESPv3 Settings

Cancel Save

تاريغتلال رشن (ن)

Search Deploy

Search Device Advanced Deploy Deploy All

FTD

In Progress... (83%)
Applying updated policy configurat

ةيرهاظلا ةصاخلا ةكبشلا > ةنمآلا تالاصتالا > ةرادإ تحت ققحت ،رشنلا ءاهتنا درجمب o)
حجانلا لاصتالا سكعي ؛قننلا ةلاح عيزوت نمض SD-WAN ةكبشو عقوم يلا عقوم نم (VPN)
(UP) رضألا نوللا

Last Updated: 11:11 PM Refresh NAT Exemptions Add					
Q Select... Refresh					
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	✎ ✕

BGP و IKE/IPsec تاقبب نم لك ىلع حاجنب هؤاشنإ متي هنأ نم دكأت، لوألا قفنللا رشن عم راركتلل يناتلل قفنللا نيوكت لب ق

Azure ب يلوألا لاصتالا نم ققحتلا 5: ةوطخلا

ىلع ةم لك نم ام كانه نأ ام ب، لخدي طغضاو، en بتك، system support diagnostic-cli، فداو FTD ي SSH إ) طقف ةعارقلل FTD ل CLI

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftd>
```

```
en
```

```
Password:
ftd#
```

قفنللا ةلاح نم 2 ةلحرمل/1 ةلحرمللا صحف ب)

```
<#root>
```

```
ftd#
```

```
show crypto isakmp sa | i Status:
```

```
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
ftd#
ftd#
ftd#
```

```
show crypto ipsec sa | i State|spi
```

```
current outbound spi: 5E83023A
current inbound spi : 62BC7C9E
spi: 0x62BC7C9E (0x00010B45)
SA State: active
spi: 0x5E83023A (0x0002029B)
SA State: active
ftd#
```

Azure نم ملتسي (TCP) لاسرالا في مكحتلا لوكوتورب ثب BGP ل صحفي نأ ضبطق تزجنا (ج)
لوكوتورب تانايب ططخم لمعتسم (NAT-T) عطاقتم - عمجرت ناونع ةكبش اما قفنلا في
instance-0 نم ماع IP ل نم يجرخ طاقتلالا لعل رورم ةكرح 500 ءانيم 4500/UDP ءانيم (UDP)
قفن Azure.

<#root>

ftd#

capture out-instance-0 trace interface Outside match ip host

any

ftd#

capture tun-vti-0 interface Azure-VTI-0 trace match ip host

any

ftd#

show cap tun-vti-0

3 packets captured

1: 03:23:43.510074 10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240

2: 03:23:44.511204 10.2.0.12.62061 > 10.50.1.2.179: SWE 2114095813:2114095813(0) win 64240

3: 03:23:46.512211 10.2.0.12.62061 > 10.50.1.2.179: S 2114095813:2114095813(0) win 64240

ftd#

نوكي يتح 1 ليثمل لل VPN و VTI ايجولوبط نيوكت سفن ررك، Instance0 ب لاصتال ديكأت عم لوصول لباق Azure ةرابع تاليثم نم الك

Azure Instance1 الى يناثال قفنللا ةياهن ةطقن نيوكت 6 ةوطخللا

(b-f 3 ةوطخللا) عاچرتسالال سفن نم ضارتقا (Azure-VTI-1) ناث VTI عاشنإ (أ)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

Ethernet1/1 (Outside)

Dynamic

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4

☐ IPv6

IP Address:*

☐ Configure IP

i

☒ Borrow IP (IP unnumbered)

Loopback1 (bgpVPNBranchLo)

+

VPN Topology Usage

Azure-VTI-Instance1 (Tunnel Destination IP -

(g-n 4 ةوطخللا) يناثال ليثمل لل VPN ةكبش ططخم نيوكت (ب)

نيوكتال فلم ي ف 1 ةياهنللا ةطقنل IP ناوع ةميق الى ةراشلال كنكمي: ةطخالمل
vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1 الى هليزنت مت يذلا

Edit VPN Topology

Topology Name:*

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** **IPsec** **Advanced**

Node A

Device:*

Virtual Tunnel Interface:*
 +

Tunnel Source IP is Dynamic (DHCP) [Edit VTI](#)

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

Node B

Device:*

Device Name*:

Endpoint IP Address*:

+ Add Backup VTI (optional)

Additional

[Cancel](#) [Save](#)

قفننلا ةلاح نم ققحتلاو، نيوكتلا تاريغت رشن ج)

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
> Azure-VTI-Instance0	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	
> Azure-VTI-Instance1	Route Based (VTI)	Point-to-Point	1- Tunnels	✓	

Instance0 و Instance1 نم لكل لصتم، Azure لوصح م دوجو نم ققحتلا د)

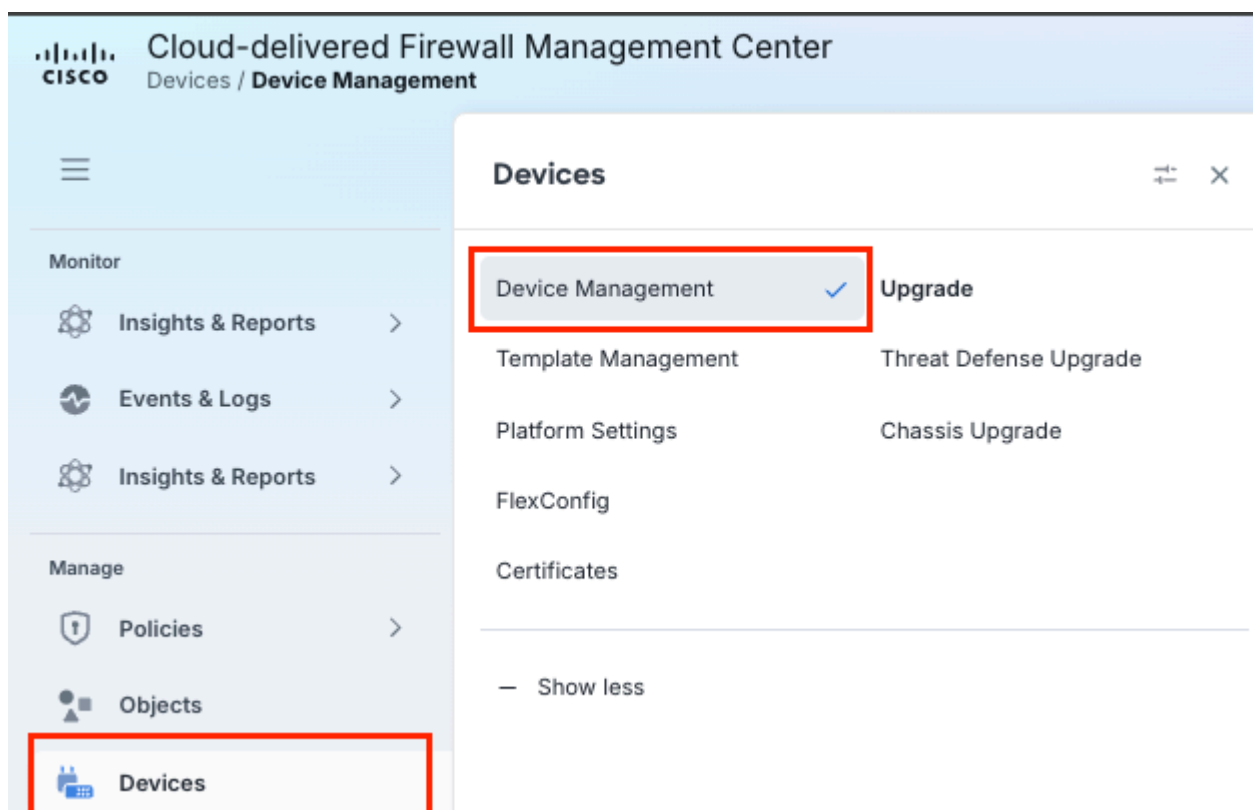
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ single-dia-link	provider	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

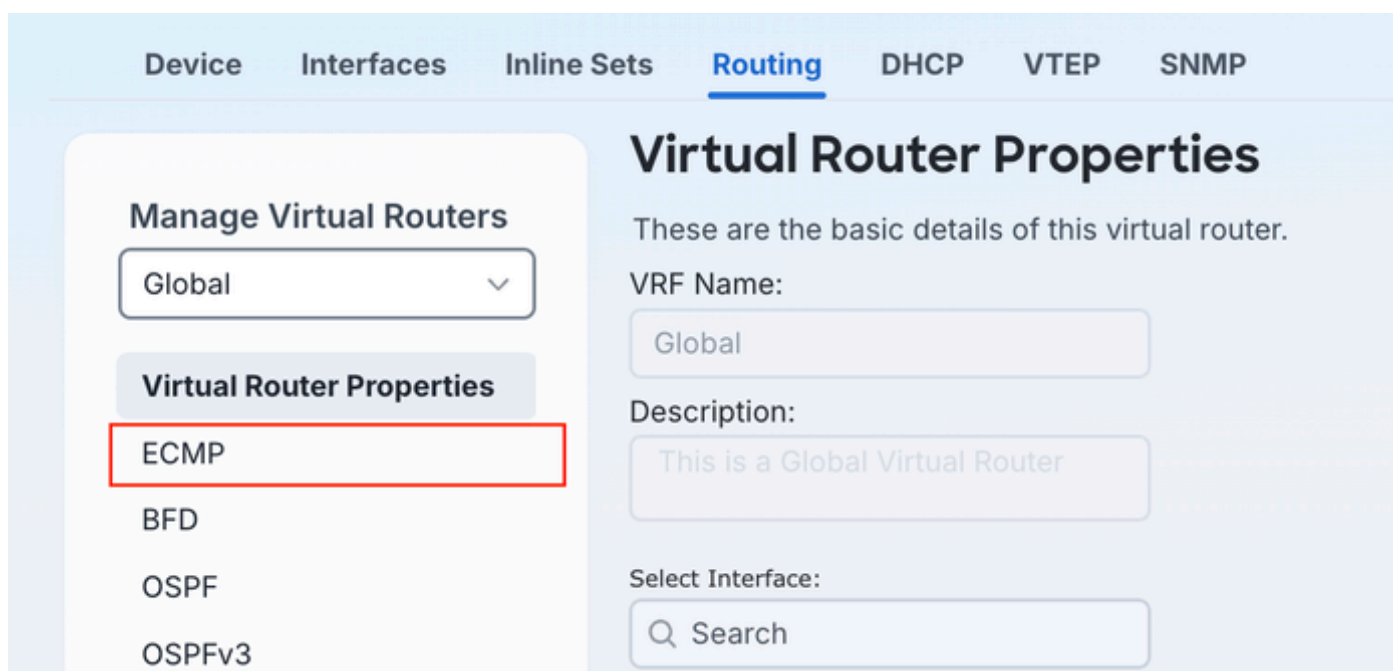
مادختسا رورملا ةكرحل نكمي ىتح ECMP هيجوت ىلى FTD جاتحي، طشن نيقفننلا الك دوجو عم يبللس دادعتساك يثالثا قففننلا ةجلاعم نم الدب، تقولا سفن في نيراسملا الك

ECMP نيوكت 7: ةوطخل

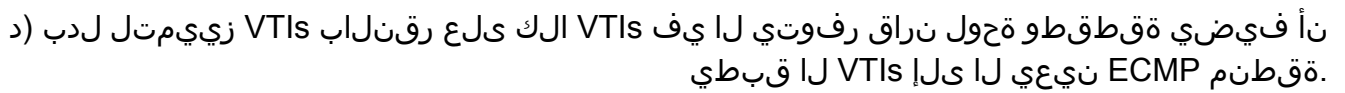
VPN تاكل بش مادختساب هنيوكت مت يذال FTD دحو ةزهجال ةرادا > ةزهجا > ةرادا الى لقتنا ا) الى Azure.



ECMP رتخاو هيچوتال بيوبتال ةمالع قوف رقنا ب)



ةديج ECMP ةقطنم عاشنال ةفاضل قوف رقنا ج)



ظفح ىلع رقنا ،تادادعإل ةحص نم دكأتلا دعب هـ



قيبطتل لباقلا FTD زاهج رتخاو ةزهجألا ةرادا > ةزهجأ > ةرادا ىلإ لقتنا (أ)

CISCO

Cloud-delivered Firewall Management Center

Devices / Device Management

Monitor

Insights & Reports

Events & Logs

Insights & Reports

Manage

Policies

Objects

Devices

Devices

Device Management

Template Management

Platform Settings

FlexConfig

Certificates

Upgrade

Threat Defense Upgrade

Chassis Upgrade

Show less

تېاٲ راسم > هچوٲ ىلا لقاٲنا (ب

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

Enable BGP: ☒

AS Number*

65500

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-id

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH attr

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EBC

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

Default local preference

رايتخالا قناخ نم ققحتال قيرط نع AS 65500/ IPv4 BGP هيجوت نيكمتب مق (ب)
BGP. ناريج نيوكتل رواجمل قوف رقناو IPv4 نيكمت ةرواجمل

FTD

Cisco Firepower 1010 Threat Defense

Device Interfaces Inline Sets **Routing** DHCP VTEP SNMP

Enable IPv4: ☒ AS Number 65500

General

Neighbor

Add Aggregate Address

Filtering

Networks

Redis

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

Setting

Learned Route Map

فيضي + عو قوط (ج)

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
---------	------------------	----------------	--------------------------	-------------

No records to display

+ Add

زاهجك هلخدأو vWAN روحم نم هيلا راشم لال BGP AS عجراو، Instance0 BGP ريشجت تامولعم لخدأ (د) عم دقتم تاراخي قوف رقنا. ابولطم كلذ ناك اذا افصو فضاو، Neighbor Remote AS.

تاهجاو نم لكل عاجرتسالا لصأ ىلا ةراشلال BGP شي دجت ردصم رييغت نم دكأت :ماه
FTD ىلع VTI.

Add Neighbor

IP Address*

10.2.0.12

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Instance0 Azure BGP Peering

Update Source:

bgpVPNBranchLo

Filtering Routes

Routes

Timers

Advanced

Migration

نم TTL تالقن ددع رييغت كنكمي، FTD ىلع BGP راج نيوكتل عم دقتم تاراخي عمئاق نمض (ه)

Azure BGP ةياهن طاقن نوكت ال .ريغتم مقرىل ةدحاو ةوطخ نم يضارتف ال eBGP دادعإ
ديزمل اانه نوكتي نأىل ليميو ،ةيساسأل Azure ةينب لخاد قفنل ربع ةرشابم ةلصتم
1. ل يضارتف ال eBGP TTL حيرصت نم ةياهنل ةطقن لىل تالقنل نم

☐ Disable Connection verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

f) Azure Instance1 BGP ريظنل امسفن تاوطخل ررك

Add Neighbor



IP Address*

10.2.0.13

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Instance1 Azure BGP Peering

Update Source:

bgpVPNBranchLo

Filtering Routes

Routes

Timers

Advanced

Migration

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

50

(1-255)

اهلامتكا درجمب تاريغيغتلا ظفح نم دكأت ز)

ets

Routing

DHCP

VTEP

SNMP

Enable IPv4: ☒

AS Number 65500

General

Neighbor

Add Aggregate Address

Filtering

Networks

Redistribution

Route Injection

You have unsaved changes

Save

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
10.2.0.12	65515	Enabled		Instance0 Azure BGP Peering
10.2.0.13	65515	Enabled		Instance1 Azure BGP Peering

يحتج، هي جوتال لودج في طقف لضألا وه دحاو راسم تي بثت ب BGP موقفي، يضارتفا لكشبو و BGP تاراسم ني كم ت بجي. احاتم ت باث دي دخت جاحس مل الك لعجي ECMP نأ نم مغرلا لىل ع في امه اذختساو ني مل علمال ني راسم الك تي بثت متي تحت لصف نم لكشبو ددعت مل ا تقولا سفن.

تاراسم ل ددعتم BGP ني وكت :10 ةوطخل

ةنوقيأ قوف رقناو ، General بي وبتال ةمالع قوف رقناو ، IPv4 > BGP > هي جوت لىل لقتنا ا) أ ددعتم تاراسم ربع ةي مأل مزحلل ةرواچم ل صا صرلا ملق

Device Interfaces Inline Sets **Routing** DHCP VTEP SNMP

Enable IPv4: ☒ AS Number 65500

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

General Neighbor Add Aggregate Address Filtering Networks Redistribution Rout

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP (Use filtering to limit the number of prefixes that are redistributed)	No

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

2. إلى 1 نم تاراسملا ددق لقحل ةيضا رتفال ةم ي قلا ريغت (ب)

Edit Forward packets Over Multiple Paths ?

Number of Paths

2

IBGP Number of Paths

1

Cancel OK

اشرشنو تاريغيغتلا ظفح نم دكأت (ج)

ةحصللا نم ققحتلا

هنأ كلذ دعب دكأت Azure. تاليثم نم لك عم رواجت لكشي BGP نأ نم دكأت، رشننلا لامتكأ دعب تاكبش نم الك مدختست رورملا ةكرح نأو، نيقيفننلا الك ربع تاراسملا ىلع فرعتلا مت دق 3، ةلحرملا يف ددحملا يصيخششلا (CLI) رمأوالا رطس ةهجاو لوصو سفن مادختساب، VTI، 5. ةوطخلا

FTD. يف رمأوالا رطس ةهجاو system support diagnostic-cli ىلى لقتنا

يقلت متيو (BGP) دودحلا ةباوب لوكونورب ناريج رهظت نأ عقوتملا نم، رشننلا دنع (أ) تائداپلا.

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftd#

ftd#

show bgp summary

BGP router identifier 10.50.1.2, local AS number 65500
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
2 multipath network entries and 4 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 952 total bytes of memory
BGP activity 2/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.2.0.12		4	65515	5	3		5	0	0 00:01:02 2
10.2.0.13		4	65515	3	4		5	0	0 00:00:55 2

ftd#

تاراسملا ةددعتم تاراسم اهنأ ىلع رهظت Azure نم ةدراولا تاراسملا نأ نم دكأت (ب)

<#root>

ftd#

show bgp

BGP table version is 7, local router ID is 10.50.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	10.2.0.12	0	65515	i	

```
*> 10.2.0.13 0 65515 i
*m 172.27.0.0 10.2.0.12 0 65515 i
*> 10.2.0.13 0 65515 i
ftd#
```

VTI مزج ددع نم ققحت ج)

```
<#root>

ftd#

show interface Tunnel1 | i packets

118 packets input, 31385 bytes
134 packets output, 8780 bytes
0 packets dropped
ftd#

show interface Tunnel2 | i packets

127 packets input, 33629 bytes
230 packets output, 15119 bytes
0 packets dropped
ftd#
```

BGP تاراجل ةتباثل تاراسملا ديكأت د)

```
<#root>

ftd#

show running-config route

route Azure-VTI-0 10.2.0.12 255.255.255.255 10.2.0.12 1
route Azure-VTI-1 10.2.0.13 255.255.255.255 10.2.0.13 1
ftd#
```

(ECMP) تنرتنإلا يف مكحتلا لئاسر لوكوتورب قطانم ديكأت ه)

```
<#root>

ftd#

show zone

Zone: Azure-VTI-ECMP-Zone ecmp
Security-level: 0
Zone member(s): 2
Azure-VTI-1 Tunnel2
Azure-VTI-0 Tunnel1

ftd#
```

BGP. نيوكت ديكات (و)

<#root>

ftd#

show running-config router bgp

```
router bgp 65500
  bgp log-neighbor-changes
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.2.0.12 remote-as 65515
neighbor 10.2.0.12 description Instance0 Azure BGP Peering
  neighbor 10.2.0.12 ebgp-multihop 50
neighbor 10.2.0.12 transport path-mtu-discovery disable
  neighbor 10.2.0.12 update-source bgpVPNBranchLo
    neighbor 10.2.0.12 activate
  neighbor 10.2.0.13 remote-as 65515
neighbor 10.2.0.13 description Instance1 Azure BGP Peering
  neighbor 10.2.0.13 ebgp-multihop 50
neighbor 10.2.0.13 transport path-mtu-discovery disable
  neighbor 10.2.0.13 update-source bgpVPNBranchLo
    neighbor 10.2.0.13 activate
    no auto-summary
  no synchronization
exit-address-family
ftd#
```

هيجوتل لودج ديكات (ز)

<#root>

ftd#

show route bgp

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 10.0.0.1 to network 0.0.0.0

```

B          10.2.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
          [20/0] via 10.2.0.12, 15:50:50
B          172.27.0.0 255.255.0.0 [20/0] via 10.2.0.13, 15:50:50
          [20/0] via 10.2.0.12, 15:50:50
```

يرخأ تارابتعا

يف دحاو ISP لصومو دحاو دهي جراخ دهجاو دوجو دنتسمل اذه يف يساسأل نيوكتل ضررت في ميمصتل كلد عسوت تارابتعالا هذه .يعرفال FTD

AS راسم ديهمت

الدب ،يساسأ راسمك FTD وأ Azure لصفنت نيقفنل نم يا يلع ريثأتل الى عجاجب تنك اذا AS حيجرتب مقف ،تاراسمل ددعتم BGP و ECMP لالخنم يواستللاب لمحلل اكراشم نم .يوناث راسمك هعم لماعتل متي ل BGP راج يلع عيفاضل تارمل نم رثكأ وأ دحاو مقري لملل ديدحت اناثأ راسمك هل قبسمل او لوطأل راسمل يا ذ رواجمل راسملل عيولوالا حنم متي لملللاب ECMP عطقنم نم رواجمل كلد اناثا الى عجاجل نود ،يسايلق ل BGP راسم لصفأ

اهحالصاو عاطخال افاشكتسا

- حاتفمل قباطت نم دكأت :ةيناثل اءلحرمل/يلوالا ءلحرمل قفن عاشن متي ال PRF و ءهزنل او ريفشتل) IKEv2/IPsec جهنب ءصال تامل عمل او اقبسمل كرتشم ال مكحتل ءدحوب صاخل IKEv2/IPsec ءسايس ضرع ني ب امامت (ةايحل ءرودو DH ءعومجمو show و مءدختسال .هليننت مت يذل Azure VPN نيوكتل فلم يف ءدوجومل ميقلل او FMC 5. ءوطخل ،3 ءلحرمل يف حضوم وه امك ،
`crypto isakmp sa show crypto ipsec sa`
- الى ل BGP تثبث نا تققد :update-source نونوكتل ال BGP ناريج نكلو ،قوف قفنل امب ءيلال ءمقي عم تلكش نوكل ebgp-multihop نا ،هسفن VTI ل سيل ،نراق عاچرتسال FTD ل الى ءرشابم تطبر سيل يا ،ناونع ريلظن Azure BGP غلبي نا يفكي
- سفن نم ءاضعأ VTIs ال كن نا نم دكأت :رورم ءكرح لمحي طقف ادحاو اقفن نكل ،BGP چدامن اهتبيثت مت Azure ليثلمل BGP يناونع ال الى ءتباتل تاراسمل نا ،ECMP عطقنم وه امك ،نيراسمل هنيوكتل مت تاراسمل ددعتم BGP نا ،ةيرادلل ءفاسمل سفن عم 10. ءوطخل ،3 ءلحرمل يف حضوم
- نع Azure vWAN نالعال ارظن :Azure الى لاثامتم ريغ هيچوت وأ ،ةعچرم رورم ءكرح دچوت ال يف رخأ ناكم يف ECMP لي طعت مدع نم دكأت ،نيقفنل ال ك ربع عزومل ناونع ءحاسم يذل ءسايسل الى دنتسمل هيچوتل وأ راسمل طئارخ نم ققحتو ،هيچوتل نيوكتل دحاو راسم الى تانايلبال رورم ءكرح تثبثي نا نكمي
- دكأت :رورم ءكرح رطح مت هنا ودي نكلو ،تاراسمل تيبتت مت وليغشتل دي ق BGP نامأل عطقنم مءدختساب هنيوكتل مت يتل لوصولل يف مكحتل ءعاوق كي دل نا نم چورخلل لوخللاب رورم ءكرحل حمست يتل VTI تاكلش الى ءنيعمل

ءلص تاذا تاملولعم

- [Azure Virtual WAN؟ وه ام](#)
- [Azure VPN ءرابعل BGP نيوكتل ءيفيك](#)
- [ءصصخملل IPsec جهن لباقم يضايرتفال Azure vWAN جهن](#)
- [Azure VPN ءرابعل اهلصال BGP عاطخال افاشكتسا](#)
- [طشنل اعضولل VPN تاباوب لوج](#)

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 ج 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 ج 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 ج 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 ج 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 ج 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