

IKEv2 مادختساب DMVPN ل 3 ةلحرمل نيوكت ةداهشلا ةقداصمب

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[ةكبشلال ليطي طيختلا مسرلا](#)

[تانوكتلا](#)

[ةداهشلل ةيساسالا ةينبلا دادعا](#)

[Crypto IKEv2 و IPSec نيوكت](#)

[قفللا نيوكت](#)

[ةحصللا نمققحتلا](#)

[اهجالصا وءاطخاللا فاشكتسا](#)

ةمدقملا

Dynamic Multipoint VPN نم 3 ةلحرمل نيوكت ةيفيك لوح تامولعم دنتسمل اذه فصى
IKEv2 مادختساب ةداهشلا ةقداصم عم (DMVPN).

ةيساسالا تابلطتملا

تابلطتملا

عوضوم نم ةفرعم ىقلتى يصوي cisco:

- DMVPN ب ةيساسا ةفرعم
- EIGRP ب ةيساسا ةفرعم
- (PKI) ماعلا حاتفملا ةيساسالا ةينبالاب ةيساسا ةفرعم

ةمدختسملا تانوكملا

ةغيص ةيجرمب اذه ىلع ةقيثو اذه يف ةمولعمل تسسأ:

- Cisco C8000v (VXE) ضكري Cisco IOS® رادصلا 17.3.8a.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراولا تامولعمل عاشنإ مت
تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجالا عيمج تأدب
رمأ يال لم تحملا ريثاتلل كمهف نم دكأتف ، ليغشتلا ديق كتكبش

ةيساساً تامولعم

ربع رشابملا لاصتالا ةيناكم | Dynamic Multipoint VPN (DMVPN) نم 3 ةلحرملا رفوت لوصولا ةحول زواجت لالخ نم ةءافك رثكأ لكشب لمعلم VPN تاكبشل حيتي امم ،تنرتنالا لوصولا نمز ليلقت ىلع ميمصتلا اذه لمعي .تانايبل رورم ةكرح تاراسم مطعمب ةصاخلا (Hop) ةوطخل ليلحت لوكوتورب مادختسا حمسي .دراوملا مادختسا نيسحتو ىندال دحل ىل قافنا عاشن او ضعبلا اهضعب ىلع يكيما نيد لكشب فرع تلاب تاراسم لل (NHRP) ةيلاتلا ةدقعملاو ةريبكلا ةكبشل تاططخم معددي امم ،ةرشابم

ةنم قافنا عاشن ةيساسالا ةيلالا (IKEv2) تنرتنالا حاتفم لدابت نم 2 رادصالا رفوي ةمدقتم نامأ رييعام IKEv2 رادصالا رفوي ،ةقباسلا تالوكوتورب لابت ةنراقم .ةئيبل هذه يف ةددعتملا تالاصتالاو لقنتلا تالاصتلا نم لكل انسحم امعدو عرسأ ةغايص ةداعا تاي لمعو نمأ لكشب حيتافملا ةراداو قفنلا دادعا ةجلاعم DMVPN نم 3 ةلحرملا عم هلمكت نمضيو لالعفو .

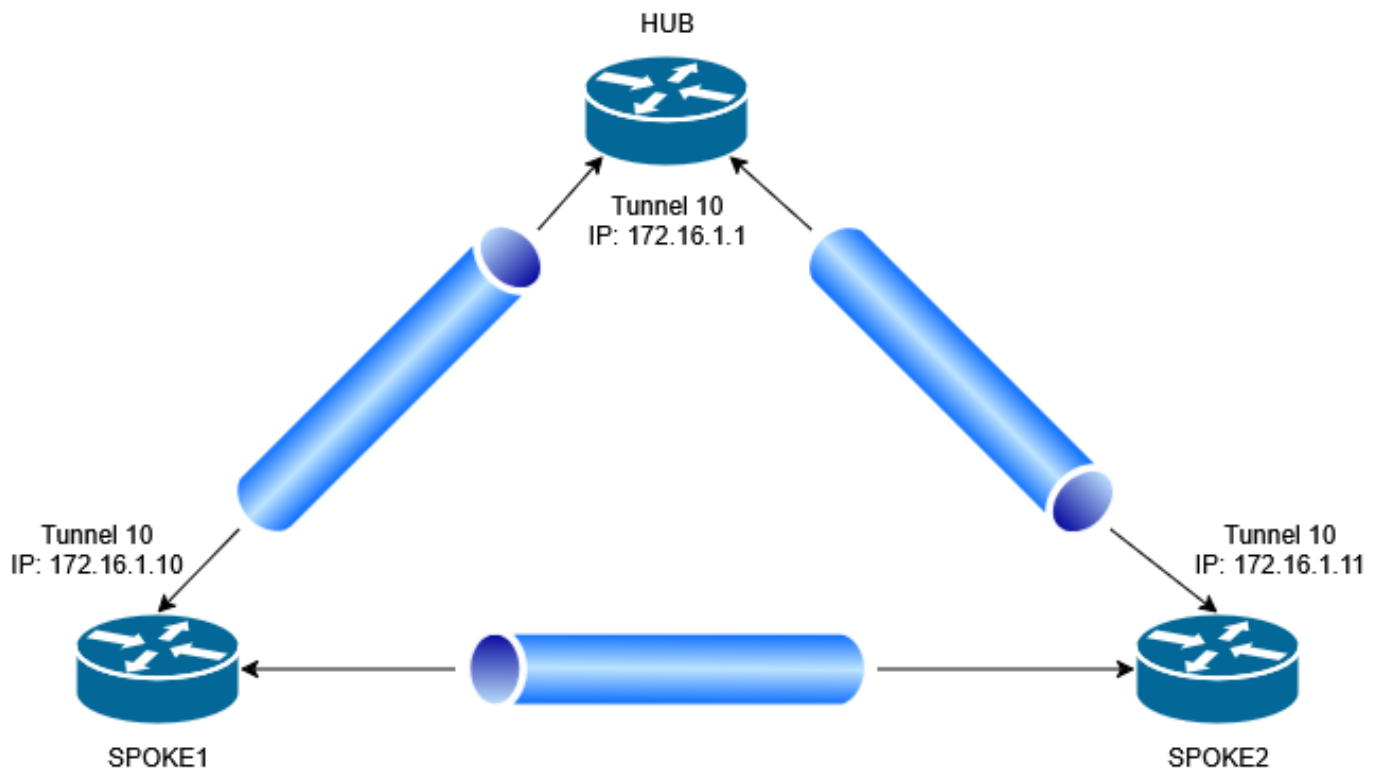
بولسالا اذه حيتي .ةيمقرلا ةداهشلا ةقداصم IKEv2 معددي ،ةكبشل نامأ زيزعت ةدايزلو ةرادالا طسبي امم ،صيخارثلا مادختساب ضعبلا اهضعب نيب تايوهلا نم ققحتلا ةزهجالل ةديفم ةداهشلا ىلع ةمئاقلا ةقثلا دعت .ةكرتشملا رارسال ةقفارملا رطاخملا نم للقيو ايدحت ةيدرفلا حيتافملا ةرادا لثمت ثيح قاطنلا ةعساو رشنلا تاي لمع يف صاخ لكشب اريبك .

ةقداصم IKEv2 لوكوتورب نم يثالثا رادصالا DMVPN نم ةثلاثلا ةلحرملا رفوت ،الامجا تابلطتم ةيبلت ىلع لحلا اذه لمعي .ايوق (VPN) ةيرهاظ ةصاخ ةكبش لمع راطا تاداهشلا تانايبلل ةيوقلا ةيامحل او ةنرملا لاصتالا ةيناكم نامض لالخ نم ةثيدحل تاسسؤملا ةطسبملا تاي لمعل او

نيوكتلا

IKEv2 مادختساب DMVPN نم 3 ةلحرملا نيوكتل ةوطخب ةوطخ تاداشرا مسقلا اذه رفوي نمأ VPN لاصتلا نيكمتل تاوطخل هذه لمكأ .ةداهشلا ىل ةدنتسملا ةقداصملا مادختساب ةربكملاو ةيروحملا تاهجوملا نيب ريوطتل لباقو .

ةكبشلل يطيختلا مسرلا



تاني وكتال

ةداهش لل ةيساس ال ةينبل دادعإ

ةمزالل ةيمقرل تاداهشل تيبتت مت (تاونقلاو عيزوتل تاحول) ةزهجال عي م نأ نم دكأت زاهج لك ىلع حيحص لكشب اهليجستو ةقث قدصم عجرم نم تاداهشل هذه رادصا بجي ةنمأل IKEv2 ةداهش ةقداصم نيكم تل ةيلاتل تاوطخل لمكأ ،ةهجوملاو ةيروحمل تاهجوملا ىلع ةداهش ليجستل

1. crypto pki رمال مادختساب ةبولطملا تامولعمل مادختساب لاصتا ةطقن نيوكتب مق .
trustPoint <TrustPoint Name>.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki trustpoint myCertificate
```

```
Hub(ca-trustpoint)# enrollment terminal
```

```
Hub(ca-trustpoint)# ip-address 10.10.1.2
```

```
Hub(ca-trustpoint)# subject-name cn=Hub, o=cisco
```

```
Hub(ca-trustpoint)# revocation-check none
```

2. <TrustPoint Name> ىلع قداصملا crypto pki رمال مادختساب TrustPoint ةقداصم .

```
<#root>
```

```
Hub(config)#
```

```
crypto pki authenticate myCertificate
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

 عجم ال نم ةداهش ال قصل لئيلع بجي crypto pki authenticate رمال رادصا دعب :ةظحال م
ءاشنال ةي رورض ةوطخال هذه .زاهال تاداهش عي قوتل اهم ادختسا متي يتال (CA) ق دصم ال
ةرصل تاهوم نم لك ىلع ةداهش ال لي جست ةعباتم لبق CA و زاهال ني ب ةقث
م لك تال او

3. crypto pki login رمال مادختساب (CSR) ةداهش ال عي قوت بلطو صاخال حاتفم ال ءاشنال مق
<TrustPoint Name>.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki enroll myCertificate
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will include: cn=Hub, o=cisco
```

```
% The subject name in the certificate will include: Hub
```

```
% Include the router serial number in the subject name? [yes/no]: n
```

```
% The IP address in the certificate is 10.10.1.2
```

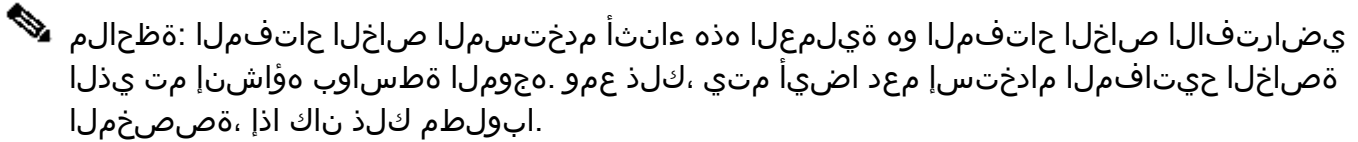
```
Display Certificate Request to terminal? [yes/no]: yes
```

```
Certificate Request follows:
```

```
MIICsDCCAZgCAQAwSjE0MAwGA1UEChMFY2l2Y28xDDAKBgNVBAMTA0hVQjEgMBAG  
CSqGSIb3DQEJAhYDSFVCMBYGCSqGSIb3DQEJCBMjMTAuMTAuMS4yMIIBIjANBgkq  
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo/M40+ivsqJhpF0PRUxdCGSUVgLUHzQ  
cwnuMtSbfn5fMKIj7w06Qa7Gvx2rjrdoyxH9JgXjTEMzMv6HP9/EuN2o+qKzR/+  
CNzMUDJobb01BNbe0WKL4IAQjbvNT0yA5iuUzHZCgMrCFG3oU7v+a2tMiSZihvdu  
+m2JSDNXn5cXyewQbQsEaELA00yosi2t6BQyzM3FRU23dCwnFVwY1VAADC7CrNh3  
o44SiFY5HtWq1tU1cLTY4sjNf6XJQxjmHPudbUp164RDFUSo37Zjvt7S800oLU  
+XUBRE3aRDlwJ+Ug2D031ZWzfc+rBZ1BsKW1YFB1Lk3mL9RA1nf3eQIDAQABoCEw  
HwYJKoZIhvcNAQkOMRIwEDA0BgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD  
ggEBAEKUURWZ+YeCx9T7kuzIaDwJ53vMqq6rITDJcNF9FJ4IgJ7PsxF0cWxm7MM  
030i1yq1K/4X7Mb5Iz6CjtdyXVqakgcEPY7W9No03Xo8Nxb4pFfe19E02Xuj8fxm  
GTqi7UAw8Zs1zJ2jrS7bXasVMb5jjr39cqQkrXfNIAwF1Sw6IA3oKfTelq8/iCJu  
TEjF0D8Si2PWziuxJVS4Adjg5GxbJpd/tDKrKUuvqD2z4HD3M40oGVvoBWQ0tjhB  
4gx1q2D209K0nMCvZr0fp/PFd6+cYc57E73ZPVSGQpHIiWcytuRKdKArN6vRcP  
iiugceU2F3L14CI7wXMYqCxQOGU=
```

```
---End - This line not part of the certificate request---
```

```
Redisplay enrollment request? [yes/no]:
```



4. عي قوتلل (CA) قدصملا عجرملا إله سرأ، CSR عاشنإ دعب .

5. crypto pki رمل ال داري تسإ <TrustPoint Name> ةداهش مدختسأ ، ةداهش ال عي قوت درجم ب. اوؤاشنإ متي ال TrustPoint ب ةطبترم ال ةعقوم ال ةداهش ال داري تسإ ال.

<#root>

```
Hub(config)#
```

```
crypto pki import myCertificate certificate
```

```
% You must authenticate the Certificate Authority before
you can import the router's certificate.
```

6. PEM. قيسننتب قدصملا عجرملا لبق نم ةعقوملا ةداهشلا قصل.

IPSec و Crypto IKEv2 نیوكت

كل ذو. عزم لاولي روحم ل ن م لك ىلع هسفن وه IPsec و Crypto IKEv2 ل نيوكتال نوكي نأ نكمي
 ةزهجال عي مج ربع امئاد قباطت نأ بجي ةمدختسم ل تارفشل ل و تاحارتقال لثم رصانع نأ ل
 يني بل ليغشت ل ةيناكمي قسانت ل اذه نمضي . حاجنب قفن ل عاشن ل ةيناكمي نامضل
 DMVPN ل 3 ةلحرمل ةئي ي لخاد نمآل لاصلتال و

1. IKEv2 حترقم نيوكت

```
crypto ikev2 proposal ikev2
encryption aes-cbc-256
integrity sha256
group 14
```

2. IKEv2 فی رعت فلم نیوكت

<#root>

```
crypto ikev2 profile ikev2Profile
match identity remote address 0.0.0.0
identity local address 10.10.1.2
```

```
authentication remote rsa-sig
```

```
authentication local rsa-sig
```

pki trustpoint

myCertificate



مَدْخُت سَمَلَا قُتْلَا طِقْ نَو PKI ةداهش قِداصم فيرعت متي شيح انه :ةظحال م
ة قِداصم لل

3. لي وحت ةعوم حم و IPsec فيرعت فلم ني وكت .

```
crypto ipsec transform-set ipsec esp-aes 256 esp-sha256-hmac
mode tunnel
crypto ipsec profile ipsec
set transform-set ipsec
set ikev2-profile ikev2Profile
```

ق فن لل ني وكت

لك شب زي كرتللا عم ،ة عرفللا وة سيئرللا تالو حم لل نم لك قافنأ ني وكت مسقلا اذه ي طغي
DMVPN دادعإ نم 3 ةل حرملا ىل ع صاخ

1. روم لل ق فن ني وكت .

```
interface Tunnel10
ip address 172.16.1.1 255.255.255.0
no ip redirects
no ip split-horizon eigrp 10
ip nhrp authentication cisco123
ip nhrp network-id 10
ip nhrp redirect
tunnel source GigabitEthernet1
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

2. Talk1 ق فن ني وكت .

```
interface Tunnel10
ip address 172.16.1.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet2
```

```
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

3. TALK2 قف ننيوكت .

```
interface Tunnel10
ip address 172.16.1.11 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

ةحصلا نم ققحتلا

:ةيلاتلا رماوأل مدختسأ ،حيحص لكشب 3 ةلحرمل DMVPN ةكبش لمع ديكتأل

- <قفنل مسا> show dmvpn interface
- show crypto ikev2 sa
- show crypto ipSec sa peer <peer ip>

نيب ةطشنل تاسللجلا ىرت نأ كنكمي ، show dmvpn interface <tunnel name> رملأل مادختساب ةمئاقلا تالاصتالا هذه جتانلل سكعي نأ كنكمي ، Talk1 روظنم نم .تاببقملاو ةرصللا

<#root>

SPOKE1#

show dmvpn interface tunnel10

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

N - NATed, L - Local, X - No Socket

T1 - Route Installed, T2 - Nexthop-override, B - BGP

C - CTS Capable, I2 - Temporary

Ent --> Number of NHRP entries with same NBMA peer

NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting

UpDn Time --> Up or Down Time for a Tunnel

=====

Interface: Tunnel10, IPv4 NHRP Details

Type:Spoke, NHRP Peers:2,

Ent Peer NBMA Addr Peer Tunnel Add

State

UpDn	Tm	Attrb
1	10.10.1.2	172.16.1.1

UP

1w6d	S
1	10.10.3.2
	172.16.1.11

UP

00:00:04 D

امم، روحمل او عورفل نيب اهنيوكت مت يتل IKEv2 قافنأ show crypto ikev2 sa رملأل ضرعي
ةحجانل ىلوالأ ةلحرمل تاضوافم دكؤي.

<#root>

SPOKE1#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/f/ivrf
-----------	-------	--------	------------

Status

1	10.10.2.2/500	10.10.3.2/500	none/none
---	---------------	---------------	-----------

READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:

RSA

Life/Active Time: 86400/184 sec

Tunnel-id	Local	Remote	fvr/f/ivrf
-----------	-------	--------	------------

Status

2	10.10.2.2/500	10.10.1.2/500	none/none
---	---------------	---------------	-----------

READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:

RSA

Life/Active Time: 86400/37495 sec

IPv6 Crypto IKEv2 SA

يتم ال IPsec قافناً من قحت ال كنكمي، show crypto ipsec sa peer <peer ip> رم ال مادت ساب
DMVPN. كبش ل خاد ن م ال تاناي ب ال لقن ن مضي امم، هجوم ل او م داوخل ن ي ب اه وشن ا مت

<#root>

SPOKE1#show

crypto ipsec sa peer 10.10.3.2

interface: Tunnel10

Crypto map tag: Tunnel10-head-0, local addr 10.10.2.2

protected vrf: (none)

local ident (addr/mask/prot/port): (10.10.2.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.10.3.2/255.255.255.255/47/0)

current_peer 10.10.3.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.10.2.2, remote crypto endpt.: 10.10.3.2

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2

current outbound spi: 0xF341E02E(4081180718)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x8ED55E26(2396347942)

transform: esp-256-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2701, flow_id: CSR:701, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0

sa timing: remaining key lifetime (k/sec): (4607999/3188)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0xF341E02E(4081180718)

transform: esp-256-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2702, flow_id: CSR:702, sibling_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0

sa timing: remaining key lifetime (k/sec): (4607999/3188)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcsp sas:

اه حال صا و عا طخا ل فاشكتسا

دەيلىتىلارمىۋالما دىخسى كنىكى، اھالى صاواظى الى فاشكتى سال:

- `debug dmvpn condition peer [nbma/tunnelIP]`، عيّن حالة لمراقبة DMVPN، على وجه التحديد، لمراقبة DMVPN التي تتضمن NBMA أو IP. يُمكن تشغيل `debug dmvpn` على جميع الواجهات التي تدعم DMVPN. يُمكن أيضًا تشغيل `debug dmvpn` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN. يُمكن أيضًا تشغيل `debug dmvpn` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN.
- `debug dmvpn all`، عيّن حالة لمراقبة DMVPN، على وجه التحديد، لمراقبة DMVPN التي تتضمن NBMA أو IP. يُمكن تشغيل `debug dmvpn` على جميع الواجهات التي تدعم DMVPN. يُمكن أيضًا تشغيل `debug dmvpn` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN.
- `show dmvpn`، عيّن حالة لمراقبة DMVPN، على وجه التحديد، لمراقبة DMVPN التي تتضمن NBMA أو IP. يُمكن تشغيل `show dmvpn` على جميع الواجهات التي تدعم DMVPN. يُمكن أيضًا تشغيل `show dmvpn` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN.
- `show crypto ikev2 sa`، عيّن حالة لمراقبة DMVPN، على وجه التحديد، لمراقبة DMVPN التي تتضمن NBMA أو IP. يُمكن تشغيل `show crypto ikev2 sa` على جميع الواجهات التي تدعم DMVPN. يُمكن أيضًا تشغيل `show crypto ikev2 sa` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN.
- `show crypto ipsec`، عيّن حالة لمراقبة DMVPN، على وجه التحديد، لمراقبة DMVPN التي تتضمن NBMA أو IP. يُمكن تشغيل `show crypto ipsec` على جميع الواجهات التي تدعم DMVPN. يُمكن أيضًا تشغيل `show crypto ipsec` على واجهة محددة باستخدام `condition`، على سبيل المثال، `condition peer [nbma/tunnelIP]`، حيث `nbma` هي واجهة NBMA، و `tunnelIP` هي عنوان IP للواجهة التي يتم استخدامها لإنشاء DMVPN.

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 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 م ا ة 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