

حياتافم مداوخ مادختساب GETvpn نيوكت ةداهشلا ةقداصم و COOP

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[ةكبشلالبيطي طختلا مسرلا](#)

[تانويوكتلا](#)

[ةقداصملا PKI](#)

[GETVPN نيوكت](#)

[COOP نيوكت](#)

[ةحصللا نم ققحتلا](#)

[اوخالص او عاخذالا فاشكتسا](#)

ةمدقملا

ةداهش لمعتسي نأ VPN (GETVPN) لقن رفشي ةعومجم لكشي نأ فيك ةقيثو اذه فصي لدان حاتفم COOP و ةقداصملا يمقر.

ةيساسالاب تابلطتملا

تابلطتملا

ةيلالاي عيضاوملاب ةفرعم لكي دل نوكت نأب Cisco ي صوت:

- Cisco Group Encrypted Transport VPN (GETVPN)

- (PKI) ماعلا حاتفملا ةيساسالاب ةينبلا -

- (CA) ةداهشلا حنم ةهج -

ةمدختسملا تانوكملا

ةيلالال جماربلا تارادصلا ىلا دنتسملا اذه في ةدراولا تامولعمل دنتست:

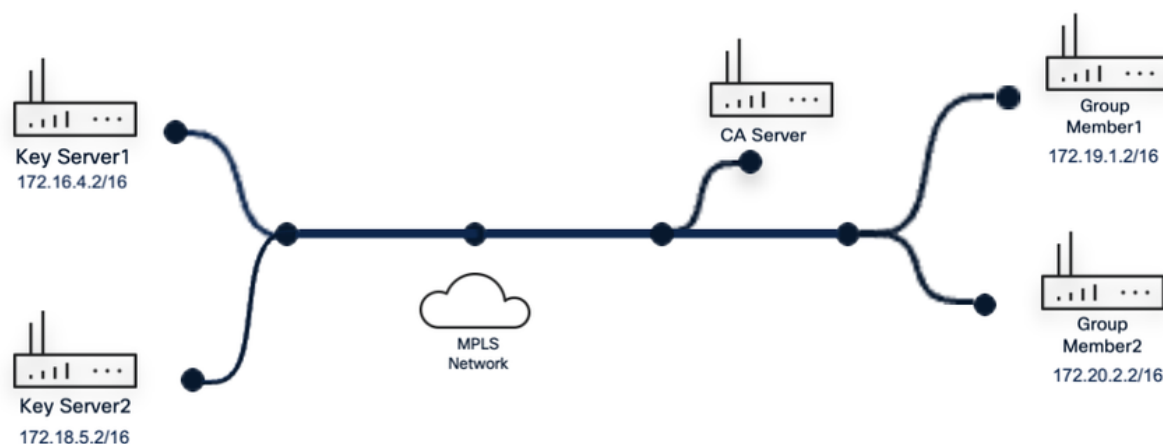
- CSR1000V - Cisco IOS® XE، رادصلا 16.12.03 - مداخلك - CA مداخلو ةعومجم.

ةيساساً تامولعم

ةينواعت ال KS م ست ةدعت م حيتافم مداوخ GETVPN م عدي ،وي راني س لا اذه لي لقت لو ن. كم ري غ حاتفم مداخ لي لا لوصول ا حبص ا اذا دادر تس لا او راركت ال رفوت ي ت لا (COOP)

نى وكىتلا

ةكبشلل یطىطختلا مسرلا



GetVPN ای جی وی پی

تانی وکٹالا

ةقداصم ل PKI

اههجاوت ييتلا ةيسيئرلا تابوعصلال يلعل بلغلل ةيساسأل اهتېنب PKI ءكرش مدختستو
ةينبلل ةيساسأل ةينبل لمعتو .ةيمومعلا حيتافملا قفارم مادختسا دنع ةرادإلا
عجرمك (CA) ةيساسأل ةينبلل ةيساسأل ةينبلل ةيساسأل ةينبلل ةيساسأل
ةيوهل تاداهش (ظفتحي مث) ردصي تاداهشلل

[illegible]



نيوكت متي، ليلدلا اذهل. ققصم عجرم ياً ةطساوب تاداهشلا رادصا نكمي: ةظحالم
ةقداصلم رشنلا يف ةزهجالا عيمج ىلا تاداهش رادصا CA ةئيه ىلع CSR1000V
اهتيوه.

مداخ CA# show crypto PKI

مداخ ca-server crypto PKI

تانايبل ةدعاق ىوتسم لامتك

1511021f07257a767b73 7 رورملا ةملك pkcs12 تانايبل ةدعاق فيشرا

name=Root-CA.cisco.com ou=lab رقصملا

SHA255 ةئجلتلا ةئجلتلا ديرجت

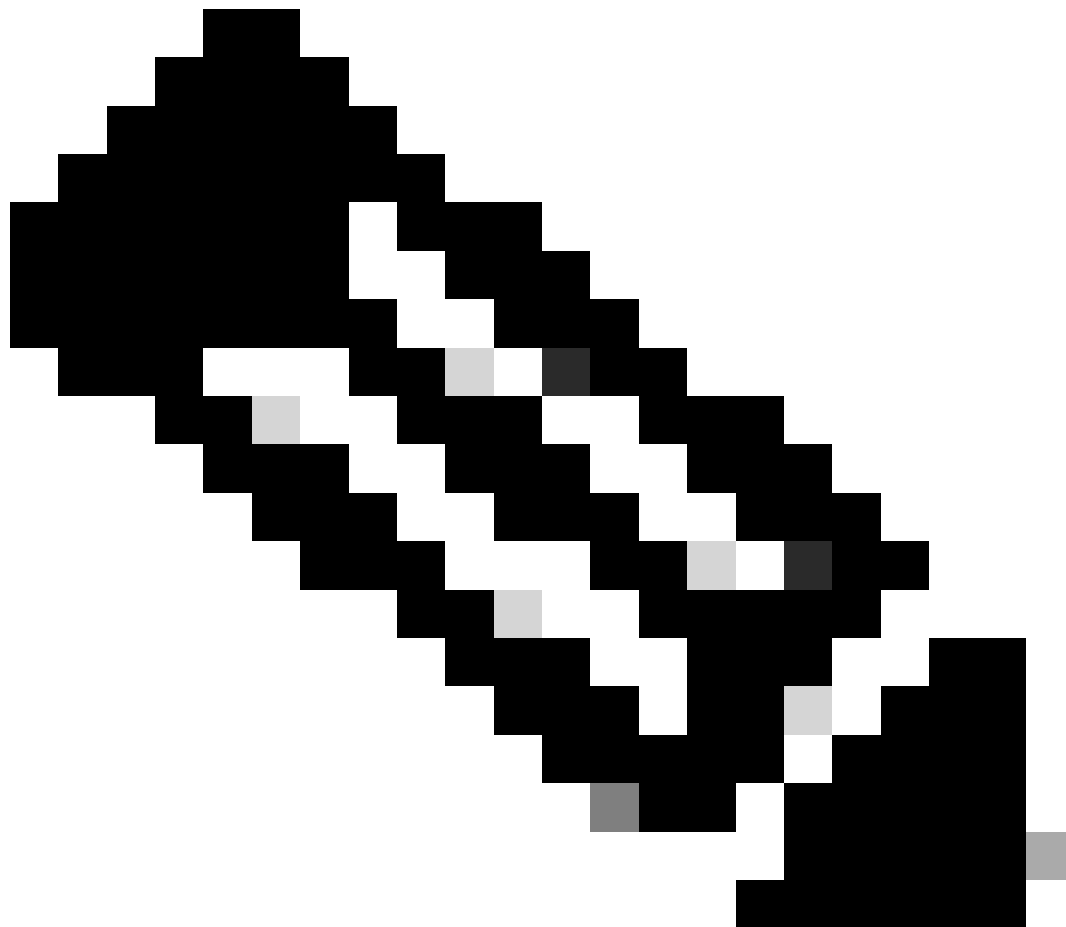
5000 يضارثفالا رمعل ةداهش

7300 ةايحل ىدم قدصملا عجرملا ةداهش

EKU ب صاخلا مداخلل لي م عمل ةق داصم

تانايبلا ةدعاق URL nvram

1.- (CA) قدصم عجرم نم ةي وه ةداهش ىلع لوصحل بجي، PKI ىلع ةمئاقلا رشنل تاي لمع يف .
م تي RSA حيتافم جوز عاشناب مق ، ةعومجملا ءاضعأو حيتافملا مداخل تاهجوم يف . زاهج لك
مهب ةصاخلا ةقثلا طاقن نيوكت يف همادختسا .



ءاضعأ تاهجومو ةيساسألا مداوخل عيمج كترتشت ، لي لدلا اذه ضرع ضارغلأو : ةطحال م
هسفن نيوكتلا يف طاخلما اذه يف ةعومجملا

يسئي رلا مداخل

KS(config)# crypto key generate rsa modulus 2049 general-keys label pkikey The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 0 seconds) KS(config)# crypto pki trustpoint GETVPN KS(config)# enrollment url <http://10.191.61.120:80> KS(config)# subject-name OU=GETVPN_KS KS(config)#

revocation-check none KS(config)# rsakeypair pkikey KS(config)# auto-enroll 70

ةومجمل وضع

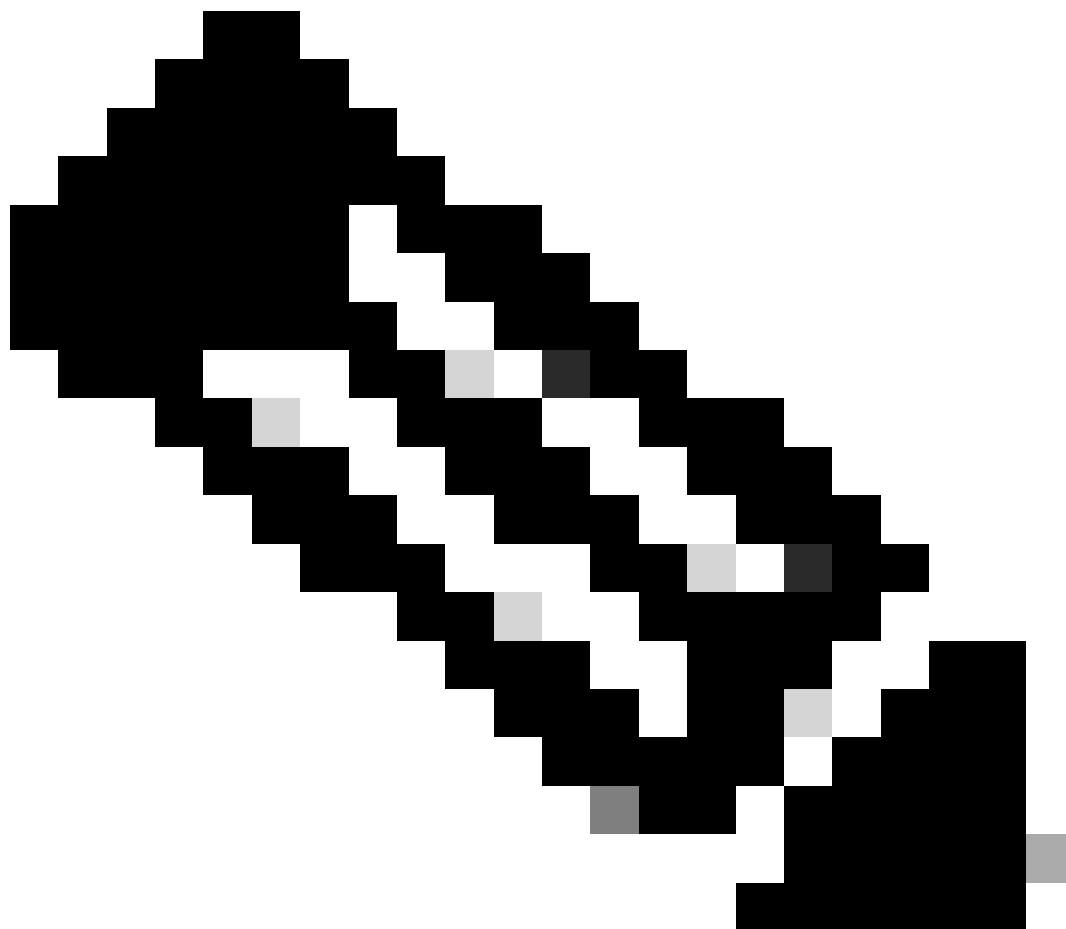
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)# **enrollment url <http://10.191.61.120:80>**

GM(ca-trustpoint)# **subject-name OU=GETVPN_GM**

GM(ca-trustpoint)# **revocation-check none**

GM(ca-trustpoint)# **rsakeypair pkikey**

GM(ca-trustpoint)# **auto-enroll 70**



ىلع ظافحلل ةزهجالا عيمج ىلع RSA حاتفم مسا مادختسا ةداعا متي :ةظحال م
هتميقي في ديرف RSA حاتفم لك نال ىرخال تاداعالا ىلع رثوي الو قسانتالا
ةيباسحالا.

نم اما كلذب مايقلل نكمي و TrustPoint، في الوا قدصم الم عجرم الم نم ةداهش الم تيبتت بجي -2.
ةتبتثم CA ةداهش دوجو مدعل ارطن .ةرشابم ليجستل و TrustPoint لعل ةقداصم الم لالخ
ال و TrustPoint ةقداصم عارج ليجشت متي ،اقبسم

يسيئرل مداخل

KS(config)# **crypto pki enroll GETVPN** % You must authenticate the Certificate Authority before

you can enroll with it. % Attempting authentication first.

Certificate has the following attributes: Fingerprint MD5: CD60821B 034ACFCF D1FD66D3 EA27D688 Fingerprint SHA1:
3F0C3A05 9BC786B4 8828007A 78A3973D B507F9C4 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. %
Start certificate enrollment .. % Create a challenge password. You need to verbally provide this password to the CA Administrator in order to
revoke your certificate. For security reasons your password is not saved in the configuration. Please make a note of it. Password: Re-enter
password: % The subject name in the certificate includes: OU=GETVPN_KS % The subject name in the certificate includes: get-KS % Include
the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Request certificate from CA?
[yes/no]: yes % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose GETVPN' command will show the
fingerprint.

ةومجم الم وضع

GM(config)# **crypto pki enroll GETVPN** % You must authenticate the Certificate Authority before

you can enroll with it. % Attempting authentication first.

Certificate has the following attributes: Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1:
A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E

% Do you accept this certificate? [yes/no]: y % Trustpoint CA certificate accepted. % Start certificate enrollment .. % Create a challenge
password. You need to verbally provide this

password to the CA Administrator in order to revoke your certificate.

For security reasons your password is not saved in the configuration.

Please make a note of it.

Password:

Re-enter password:

% The subject name in the certificate will include: OU=GETVPN % The subject name in the certificate will include: get_GM % Include the
router serial number in the subject name? [yes/no]: n % Include an IP address in the subject name? [no]: n Request certificate from CA?
[yes/no]: y % Certificate request sent to Certificate Authority % The 'show crypto pki certificate verbose GETVPN' command will show the
fingerprint.

ةقث الم طاقن في اءداريتس متي اءي ةرداص الم اءاهش الم نأ نيزاهج الم لك لعل ةقق د-3
'show crypto pki' رم الم اءءتساب (اضأ CA ةداهش ءاريءس بجي) اءب ةصاخ الم اءل لعل ةدصم الم

certificates verbose'.

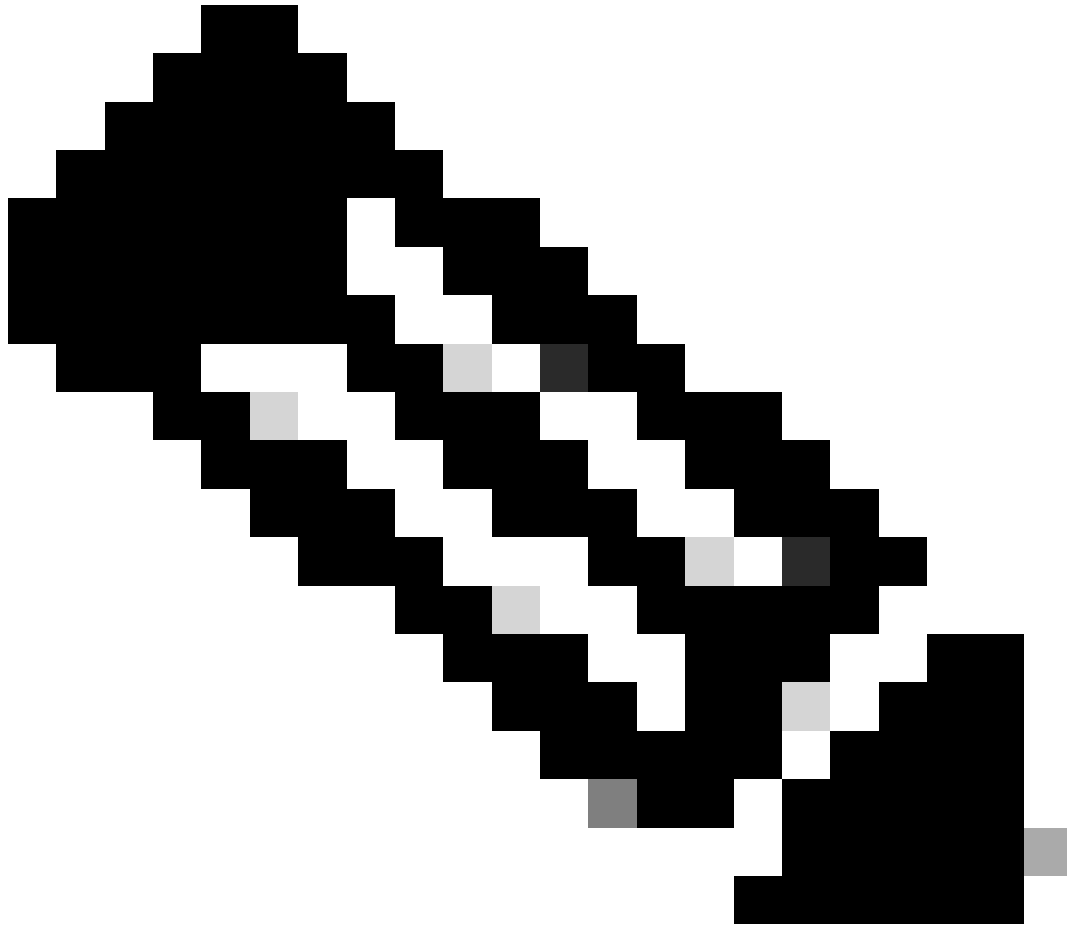
ي سي ئرل م داخ ل

KS# show crypto pki certificates verbose GETVPN

. **Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 05 Certificate Usage: General Purpose **Issuer:** cn=Root-CA.cisco.com OU=LAB **Subject:** Name: get-KS hostname=get-KS ou=GETVPN_KS **Validity Date:** start date: 11:58:27 UTC Sep 9 2025 end date: 11:58:27 UTC May 19 2039 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2049 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: 51576B28 1203C5EC 06FF408E F90B0E47 Fingerprint SHA1: 9D5B10E5 E9418C00 895E6DC7 9BE86624 B273CF15 X509v3 extensions: X509v3 Key Usage: A0000000 Digital Signature Key Encipherment X509v3 Subject Key ID: 3A1012CD 1FB41E07 5B64742B 778B1E24 E1F07A92 X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: **Extended Key Usage:** **Client Auth Server Auth** Cert install time: 11:58:28 UTC Sep 9 2025 **Associated Trustpoints:** GETVPN Storage: nvram:Root-CAcisco#5.cer **Key Label:** pkikey Key storage device: private config **CA Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature **Issuer:** cn=Root-CA.cisco.com OU=LAB **Subject:** cn=Root-CA.cisco.com OU=LAB **Validity Date:** start date: 11:28:11 UTC Sep 9 2025 end date: 11:28:11 UTC Sep 4 2045 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E X509v3 extensions: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F X509v3 Basic Constraints: **CA: TRUE** X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: Cert install time: 11:58:16 UTC Sep 9 2025 **Associated Trustpoints:** GETVPN Storage: nvram:Root-CAcisco#1CA.cer

ة و ع و م ج م ل ا و ض ع

GM# show crypto pki certificates verbose GETVPN **Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 08 Certificate Usage: General Purpose **Issuer:** cn=Root-CA.cisco.com OU=LAB **Subject:** Name: get_GM hostname=get_GM ou=GETVPN **Validity Date:** start date: 12:05:19 UTC Sep 9 2025 end date: 12:05:19 UTC May 19 2039 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2049 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: CA8AF53B B7424CD6 4C94F689 6FDD441F Fingerprint SHA1: 8ACE3BC0 5BC6BBF1 D9696805 2998AFDB 2A73A65E X509v3 extensions: X509v3 Key Usage: A0000000 Digital Signature Key Encipherment X509v3 Subject Key ID: F3C5E024 F93B09A0 4F99215E 34EB9C88 553C7CAD X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: **Extended Key Usage:** **Client Auth Server Auth Associated Trustpoints:** GETVPN Storage: nvram:Root-CAcisco#8.cer **Key Label:** pkikey **CA Certificate** Status: Available Version: 3 Certificate Serial Number (hex): 01 Certificate Usage: Signature **Issuer:** cn=Root-CA.cisco.com OU=LAB **Subject:** cn=Root-CA.cisco.com OU=LAB **Validity Date:** start date: 11:28:11 UTC Sep 9 2025 end date: 11:28:11 UTC Sep 4 2045 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Signature Algorithm: SHA256 with RSA Encryption Fingerprint MD5: E184D9EC 2D6499B3 D5D78E8A CD0B910C Fingerprint SHA1: A31EE77D A4FFA2B7 90F39933 00337A6D 46CBE32E X509v3 extensions: X509v3 Key Usage: 86000000 Digital Signature Key Cert Sign CRL Signature X509v3 Subject Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F X509v3 Basic Constraints: **CA: TRUE** X509v3 Authority Key ID: 4F0F7126 6D21324A 585A0BF3 652EB561 17D18B2F Authority Info Access: **Associated Trustpoints:** GETVPN Storage: nvram:Root-CAcisco#1CA.cer



ىلع يوتحت ةمدقملا ةداهشلا نأ نم دكأت ،ةداهشلا ةقداصل ةبسنلاب :ةظحالم
مادختساو (CN) عئاشلا مسالا لثم زاهجلا ةيوه نم ققحتلل ةححصلا تاملعمل
ةحاصللا خيراتو (EKU) عسوملا حاتفملا

GETVPN نيوكت

تازيم لبق هنيوكتب ىصوي يذلقباسلا نيوكتلا ىلع GETVPN ل ةماهلا تازيملا دمتعت
ISAKMP و GDOI.

ةيمستلا لمحي ري دصتلا لباق RSA حاتفم ءاشنإب مق ،ةيساسأل حاتفملا مداخي في 4.-
ةزيملا نإف ،لكذل . "حاتفملا مداخ" لك ىلع اقباطم حاتفملا اذه نوكي نأ بجي . "getKey"
ةيلاتلا تاوطخلل ةرورض ري دصتلا لباقلا

KS(config)# **crypto key generate rsa general-keys label getKey modulus 1024 exportable** The name for the keys will be: **getKey** % The key
modulus size is 1024 bits % Generating 1024 bit RSA keys, keys are exportable. .. [OK] (elapsed time was 0 seconds)

ىلع بجي يتلا ةديفملا رورملا ءكرح مادختساب ةعسوملا لوصول ةمئاق ديدحتب مق 5.-

مق، ةيوناثلل حيتافملا مداخ يف . اهربع رورملا دنع اهريفشت ةعومجملا عاضعأ تاهجوم
مسال س فن مادختساب لوصولا ةمئاق س فن ديدحتب

يساسال حاتفملا مداخ

```
KS(config)# ip access-list extended data_plane KS(config-ext-nacl)# 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 KS(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
```

يوناثلل حاتفملا مداخ

```
KS2(config)# ip access-list extended data_plane KS2(config-ext-nacl)# 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 KS2(config-ext-nacl)# 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
```

عاشنال مدختسملا IPsec فيرعت فلمو IPsec transform set و ISAKMP ةسايس نيوكتب مق 6-
GDOI. ةعومجم لئاسر لدابت عدبل GMS عم نمال لاصلال

```
KS(config)# crypto isakmp policy 10 KS(config-isakmp)# encryption aes 256 KS(config-isakmp)# hash sha256 KS(config-isakmp)# group 14 KS(config-isakmp)# lifetime 3600
```

```
KS(config)# crypto ipsec transform-set get-ts esp-aes esp-sha-hmac KS(config)# crypto ipsec profile gdoi-profile KS(ipsec-profile)# set security-association lifetime seconds 7200 KS(ipsec-profile)# set transform-set get-ts
```

نيوكت COOP

ةلثامتم ةليكشت ةينعمل ةيسيئرلا مداوخلل نوكت نأ بجي ،ينواعتلل ذيفنتللا يف 7-
حيتافملا مداخ نم اقبسم هؤاشنإ مت يذل ريصتلل لباقلا RSA حاتفم ريصتتب مق
(KS2). ةيوناثلل حيتافملا مداخ ىلا ةماعلاو ةصاخلا حيتافملا نم لك داريئساو يساسال
حيتافملا مداخ رمتسي ،بيجتسم ريغ ةيساسال حيتافملا مداخ هي فحبصي ويراني ي
ةعومجملا لخاد GM ةزهجأ ةفاك حاتفم يف مكحتللا يف ةيوناثلل

يساسال حاتفملا مداخ

```
KS(config)# crypto key export rsa getKey pem terminal 3des cisco123 % Key name: getKey Usage: General Purpose Key Key data: -----  
BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAAdGV3ZPaGQcsAqO  
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07  
5bOsrT7B2uOpCBmAJK9iiTsr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTTlLubxQIDAQAB -----END  
PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-  
CBC,AA98923B28E00DCCto1Wym6cRvqEXBl97UZdGyusf3cW/iumb7oD9/09q5if4ouoE
```

```
brPykL3No0WMI7h56WQPiaHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9
```

```
zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu
```

```
GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2
```

```
n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb
```

```
AI286GHqCOW2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C
```

```
2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuItpG+BpCty/XW99dvuhqh9hjyfy2sKqF4H
```

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

5Bu+jzxSeQAxbUAXGiIfp9hCL8jq4ac/g+OafCqyHETJd8m5Yr6W9/0bGLnsEzNLbhgPR7A==

-----END RSA PRIVATE KEY-----

يوناثلل حاتفملا م داخ

KS2(config)# **crypto key import rsa getKey pem exportable terminal cisco123**

% Enter PEM-formatted public General Purpose key or certificate.

% End with a blank line or "quit" on a line by itself. -----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcsAqO

1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07

5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGSz baErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END

PUBLIC KEY----- quit % Enter PEM-formatted encrypted private General Purpose key.

% End with "quit" on a line by itself. -----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,AA98923B28E00DCCto1Wym6cRvqEXBlr97UZdGysuf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAhZLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOW2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFr0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuItpG+BpCty/XW99dvuhqh9hjfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

5Bu+jzxSeQAxbUAXGiIfp9hCL8jq4ac/g+OafCqyHETJd8m5Yr6W9/0bGLnsEzNLbhgPR7A==

-----END RSA PRIVATE KEY-----

quit

% Key pair import succeeded.

ةيساسال KS ل نكمي ،ةقيرطلال هذهبو . COOP KSs لجأ نم يرودلل ISAKMP نيوكت بجي -8

ةيوناتال حيتافمالمداوخ ةبقارم

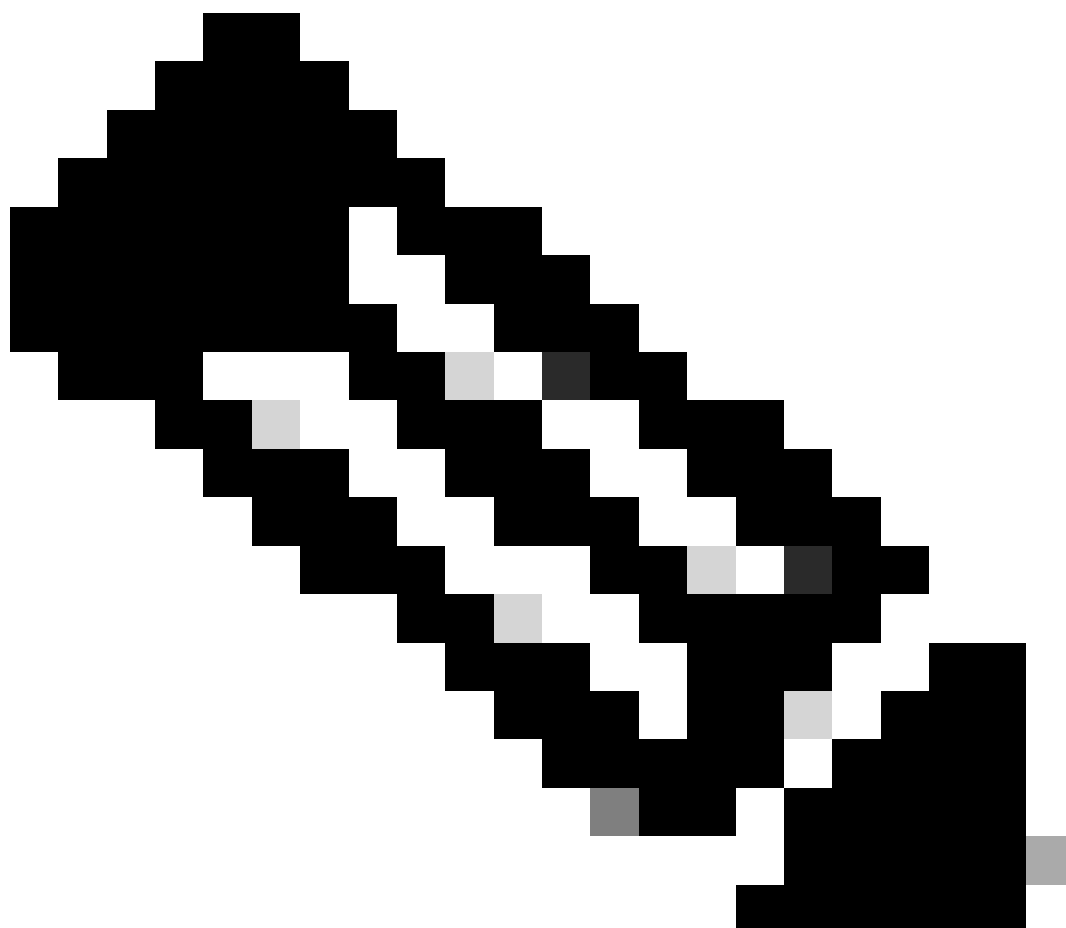
يساسألا حاتفمالمداوخ

KS(config)# crypto isakmp keepalive 15 periodic

ةيوناتال حيتافمالمداوخ

KS2(config)# crypto isakmp keepalive 15 periodic

متي مل اذا .يوناتال الى يساسألا نم دحاو هاجتإ في لاصتالا ةيساسألا COOP مداوخ لدابتت
يوناتال KS لواحي ،ةينات 30 اهتدم ةينمز ةرتف لالخ يساسألا KS نم يوناتال KS عامس
يساسألا KS نم يوناتال KS عمسي مل اذا .ةثدحم تامولعم بلطيوي يساسألا KS ب لاصتالا
يساسألا KS رايتخإ متي و COOP رايتخإ ةداعإ ةيلمع ليغشت متي ،ةينات 60 ةرتف ىدم ىلع
ديدج.



KS و GM نيب يروود DPD دوجو مزلي ال :ةظحالم

إذا. أهنيوكت مت يتل ايلعل الةيولوالا ةمي ق ىل اةيسيئرل مداول نيب رايخال دنتسي لك ىلعل GDOI ةومجم س فن نيوكتب مق IP. ناونع ىلعل دمتعي اذهف، ةهباشتم تناك ةعسومل لوصول مئاووقو ريفششال تاسايس س فن مادختساب حيتافم مداخل

يساسال حاتفمل مداخل

```
KS(config)# crypto gdoi group GETVPN KS(config-gkm-group)# identity number 484 KS(config-gkm-group)# server local KS(gkm-local-server)# rekey lifetime seconds 86400 KS(gkm-local-server)# rekey retransmit 40 number 2 KS(gkm-local-server)#rekey authentication mypubkey rsa getKey KS(gkm-local-server)# rekey transport unicast
```

ةكرحل ةصصخملم ريفششال تاسايس نيكمتب مق، يلحمل مداخل تاداعل س فن نمض 9.- اقبس م أهنيوكت مت يتل لوصول ةمئاقو تانايبال يوتسم رورم

```
KS(gkm-local-server)# sa ipsec 10 KS(gkm-sa-ipsec)# profile gdoi-profile KS(gkm-sa-ipsec)# match address ipv4 data_plane
```

حاتفم مداخل ةفيظو نيكمتب هي ف مت يذل نيوكتل يوتسم وه يلحمل مداخل تاداعل ىلعل ةيوناثال حيتافمل مداول نيوكتب جي. اذه حيتافمل مداخل رود ةدحمل ةيولوالا ددحت، COOP. ضعبال اهضعبب ةيارد ىلعل KS عيمج نوكت ىتح حيصر لكشب

```
KS(gkm-sa-ipsec)# exit KS(gkm-local-server)# redundancy KS(gdoi-coop-ks-config)# local priority 100 KS(gdoi-coop-ks-config)# peer address ipv4 172.18.5.2
```

حيتافمل ةمزحل ردصلم IP ناونع فيرعت وه يسيئرل COOP مداخل نيوكتب نم ريخال عزالو، حيتافمل مداخل هجوم تاهجاو ىدلح ي ف هنيوكت مت يذل IP ناونع وهو

```
KS(gdoi-coop-ks-config)# exit KS(gkm-local-server)# address ipv4 172.16.4.2
```

لقأ ةيولوالا نيوكتبو، ةيوناثال حيتافمل مداخل ىلعل اهس فن نيوكتل تاوطخ خسنب مق يساسال KS ناونع ليچستو يوناث مداخل هجومال ديدحتل

يوناثال حاتفمل مداخل

```
KS2(config)# crypto gdoi group GETVPN KS2(config-gkm-group)# identity number 484 KS2(config-gkm-group)# server local KS2(gkm-local-server)# rekey lifetime seconds 86400 KS2(gkm-local-server)# rekey retransmit 40 number 2 KS2(gkm-local-server)# rekey authentication mypubkey rsa getKey KS2(gkm-local-server)# rekey transport unicast KS2(gkm-local-server)# sa ipsec 10 KS2(gkm-sa-ipsec)# profile gdoi-profile KS2(gkm-sa-ipsec)# match address ipv4 data_plane KS2(gkm-sa-ipsec)# exit KS2(gkm-local-server)# redundancy KS2(gdoi-coop-ks-config)# local priority 78 KS2(gdoi-coop-ks-config)# peer address ipv4 172.16.4.2 KS2(gdoi-coop-ks-config)# exit KS2(gkm-local-server)# address ipv4 172.18.5.2
```

مداول ةنراقم لقأ نيوكتب نم GDOI ةومجم تاداعل نوكتت، ةومجم وضع هجوم لال خ نم 10.- س فن مادختساو، ISAKMP ةسايس نيوكتل طقف ةومجمال ي ف وضع دوجو مزلي. حيتافمل يتل ةيساسال مداول اب ةصخال IP نيوانع ىلعل لوصولالو، GDOI ةومجمو، ةقداصلم ةقيرط اهيل ليچستال GM هجوملل نكمي

ةومجم ال وضع

```
GM(config)# crypto isakmp policy 10 GM(config-isakmp)# encryption aes 256 GM(config-isakmp)# hash sha256 GM(config-isakmp)# group 14 GM(config-isakmp)# lifetime 3600
```

```
GM(config)# crypto gdoi group GETVPN GM(config-gkm-group)# identity number 484 GM(config-gkm-group)# server address ipv4 172.18.5.2
```

```
GM(config)# crypto map getvpn 10 gdoi GM(config-crypto-map)# set group GETVPN
```

```
GM(config)# interface GigabitEthernet1 GM(config-if)# crypto map getvpn
```

2 ةومجم ال وضع

```
GM2(config)# crypto isakmp policy 10 GM2(config-isakmp)# encryption aes 256 GM2(config-isakmp)# hash sha256 GM2(config-isakmp)# group 14 GM2(config-isakmp)# lifetime 3600 GM2(config)# crypto gdoi group GETVPN GM2(config-gkm-group)# identity number 484 GM2(config-gkm-group)# server address ipv4 172.16.4.2 GM2(config-gkm-group)# server address ipv4 172.18.5.2 GM2(config)# crypto map getvpn 10 gdoi GM2(config-crypto-map)# set group GETVPN GM2(config)# interface GigabitEthernet1 GM2(config-if)# crypto map getvpn
```

ةحصل ال نم ققحت ال

ي: لي امك لي كشت ال نم ةلحرم لك نم دادع اةي لمع ال تققد

ةيساس ال مداوخل ال ع تاناي بال يوتسم رورم ةكرحل لوصول ال ف مكحت ال مئوق

.ةدحمال مامته ال ةريثم ال رورم ال ةكرح عم ءاطخ اوجو مدع ديكا تل اذه ضرع ال رم امدختسا م تي

```
KS# show ip access-lists data_plane Extended IP access list data_plane 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 KS2# show ip access-lists data_plane Extended IP access list data_plane 10 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 20 permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255
```

ي: رايتخ ال لوكوتوربال ليحست ةلح

ال اريشم ،ةيساس ال مداوخل ال ني ب ةي لالح ال COOP ةلح 'show crypto gkm coop' رم ال ضرعي نارق ال او درف ال ةيولواو ،اهي ل يمتني ي تي ال GDOI ةومجمو ،يساس ال حي تافم ال مداخ وه نم نم اهل اسرا م تيس ي تي ال ةي لالح ال لئ اسرلاب قلعت ي امي ف تي قوت ال ةزهج او مهب ةصاخ ال ةي وناث ال مداوخل ال ال ةيساس ال مداوخل ال

يساس ال حات فم ال مداخ

```
KS# show crypto gkm ks coop Crypto Gdoi Group Name :GETVPN Group handle: 1073741826, Local Key Server handle: 1073741826 Local Address: 10.191.61.114 Local Priority: 100 Local KS Role: Primary , Local KS Status: Alive Local KS version: 1.0.27 Primary Timers: Primary Refresh Policy Time: 20 Remaining Time: 5 Per-user timer remaining time: 0 Antireplay Sequence Number: 63046 Peer Sessions: Session 1: Server handle: 1073741827 Peer Address: 10.191.61.115 Peer Version: 1.0.23 Peer Priority: 75 Peer KS Role: Secondary , Peer KS Status: Alive Antireplay Sequence Number: 0 IKE status: Established Counters: Ann msgs sent: 63040 Ann msgs sent with reply request: 3 Ann msgs rcv: 32 Ann msgs rcv with reply request: 4 Packet sent drops: 3 Packet Recv drops: 0 Total bytes sent: 42550002 Total bytes rcv: 22677
```

ي وناث ال حات فم ال مداخ

KS2# **show crypto gkm ks coop** Crypto Gdoi Group Name :GETVPN Group handle: 1073741829, Local Key Server handle: 1073741827
Local Address: 10.191.61.115 Local Priority: 75 Local KS Role: Secondary , Local KS Status: Alive Local KS version: 1.0.23 Secondary
Timers: Sec Primary Periodic Time: 30 Remaining Time: 11, Retries: 0 Invalid ANN PST recvd: 0 New GM Temporary Blocking Enforced?:
No Per-user timer remaining time: 0 Antireplay Sequence Number: 4 Peer Sessions: Session 1: Server handle: 1073741828 Peer Address:
10.191.61.114 Peer Version: 1.0.27 Peer Priority: 100 Peer KS Role: Primary , Peer KS Status: Alive Antireplay Sequence Number: 30 IKE
status: Established Counters: Ann msgs sent: 2 Ann msgs sent with reply request: 1 Ann msgs rcv: 28 Ann msgs rcv with reply request: 1
Packet sent drops: 1 Packet Recv drops: 0 Total bytes sent: 468 Total bytes rcv: 16913

ينواع الت حالات الم داخ لوح رادصإل تامولعمو ةومجم لل GETVPN تامولعم ضرع

KS# **show crypto gdoi group GETVPN ks coop version** Cooperative key server infra Version : 2.0.0 Client : KS_POLICY_CLIENT Version :
2.0.0 Client : GROUP_MEMBER_CLIENT Version : 2.0.1 Client : SID_CLIENT Version : 1.0.1

ةومجم الم وضع ليجست

GM# **show crypto gkm group GETVPN** Group Name : GETVPN Group Identity : 484 Group Type : GDOI (ISAKMP) Crypto Path : ipv4
Key Management Path : ipv4 Rekeys received : 0 IPsec SA Direction : Both Group Server list : 10.191.61.115 Group Member Information For
Group GETVPN: IPsec SA Direction : Both ACL Received From KS : gdoi_group_GETVPN_temp_acl Group member : 10.191.61.116 vrf:
None Local addr/port : 10.191.61.116/848 Remote addr/port : 10.191.61.115/848 fvrf/ivrf : None/None Version : 1.0.25 Registration status :
Registered Registered with : 10.191.61.115 Re-registers in : 5642 sec Succeeded registration: 1 Attempted registration: 1 Last rekey from :
UNKNOWN Last rekey seq num : 0 Unicast rekey received: 0 Rekey ACKs sent : 0 Rekey Received : never PFS Rekey received : 0 DP Error
Monitoring : OFF IPSEC init reg executed : 0 IPSEC init reg postponed : 0 Active TEK Number : 1 SA Track (OID/status) : disabled Fail-Close
Revert : Disabled allowable rekey cipher: any allowable rekey hash : any allowable transformtag: any ESP Rekeys cumulative Total received : 0
After latest register : 0 Rekey Acks sent : 0 ACL Downloaded From KS 10.191.61.115: access-list permit ip 10.0.0.0 0.0.0.255 172.16.0.0
0.0.255.255 access-list permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 KEK POLICY: Rekey Transport Type : Unicast Lifetime (secs) :
85185 Encrypt Algorithm : 3DES Key Size : 192 Sig Hash Algorithm : HMAC_AUTH_SHA Sig Key Length (bits) : 1296 TEK POLICY for
the current KS-Policy ACEs Downloaded: GigabitEthernet1: IPsec SA: spi: 0x535F673B(1398761275) transform: esp-aes esp-sha-hmac sa
timing:remaining key lifetime (sec): (5988) Anti-Replay(Counter Based) : 64 tag method : disabled alg key size: 16 (bytes) sig key size: 20
(bytes) encaps: ENCAPS_TUNNEL KGS POLICY: REG_GM: local_addr 10.191.61.116 overall check P2P POLICY: REG_GM: local_addr
10.191.61.116

اهحال صإو ءاطخأل فاشكتسا

يساسأل COOP مداخ رايتخإ

مق. اهدي دحتو COOP ةيلمعب ةقلعت الم تالكش الم بقعت يف syslog لئاسر دعاست نأ نكمي
هذه ةقلعت الم تامولعم ضرع COOP حيتافم مداوخ ىل ع GDOI ءاطخأ حيحصت ني كمتب
طقف ةيلمع الم

KS# **debug crypto gdoi ks coop**

ةيساسأل مداوخ لك ىل ع ةيلات syslog ةلئاسر رهظت ، COOP رايتخإ ةيلمع أدبت ام دنع

%GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GETVPN (Previous Primary = NONE)

لوح تامولعم COOP_KS_TRANS_TO_PRI ةلاسرلا ضرعت ،ةبختنال ةلمعل مامتإ دعبو .ةيوناثلاو ةسسال حيتافملا مداوخ ىلع ةلاسرلا دهاشتو ،ديجلال سسالأا حاتفملا مداخ ةلمعلل لولأا ةرملال في "ءش ال قبال لولأا ريرقتل رهظي نأ عقوتملا نمو .ةبختنال

%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 172.16.4.2 in group GETVPN transitioned to Primary (Previous Primary =

يسسالأا مداخلاب صاخلا IP ناو نع ةلاسرلا نمضتت ،Key Server رايتخإ ةداعإ ةلاح في قبال

%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 172.18.5.2 in group GETVPN transitioned to Primary (Previous Primary =

ةلاسر ضرع متي ،ةيوناثلا حيتافملا COOP مداوخب لاصتالا دقف متي ام دنع ةلاسرلا هذه مدختسيو ةيوناثلا KSs عيمج ةلاح يسسالأا KS عبتتتي .COOP_KS_UNREACH. KS ةلاح عبتتب طقف يوناثلا KS موقي .يوناثلا KS ب لاصتالا نادقف ىلإ ةراشلل KS ب لاصتالا نادقف ىلإ يوناثلا KS ىلع ةدوجوملا ةلاسرلا هذه ريشت .ةسسالأا يسسالأا

%GDOI-3-COOP_KS_UNREACH: Cooperative KS 172.18.5.2 Unreachable in group GETVPN

coop_KS_REACH". ةلاسر ضرع متي ،COOP KSs نيب لاصتالا ةداعتسإ متت ام دنع

%GDOI-5-COOP_KS_REACH: Reachability restored with Cooperative KS 172.18.5.2 in group GETVPN.

PKI ليچست لكاشم

PKI. ءاطخأ حيصت مدختسأ ،TrustPoint لكاشم ةقداصم وأ ليچست ءاطخأ حيصت دنع

debug crypto pki messages debug crypto pki transactions debug crypto pki validation debug crypto pki api debug crypto pki callback

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