COOP 키 서버 및 인증서 인증을 사용하여 GETVPN 구성

목차

소개

이 문서에서는 인증 및 COOP 키 서버에 디지털 인증서를 사용하도록 GETVPN(Group Encrypted Transport VPN)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 그룹 암호화 전송 VPN(GETVPN)

- PKI(Public Key Infrastructure)

- CA(인증 기관)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CSR1000V - Cisco IOS® XE, 버전 16.12.03 - Cisco IOS® XE 키 서버, 그룹 구성원 및 CA 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

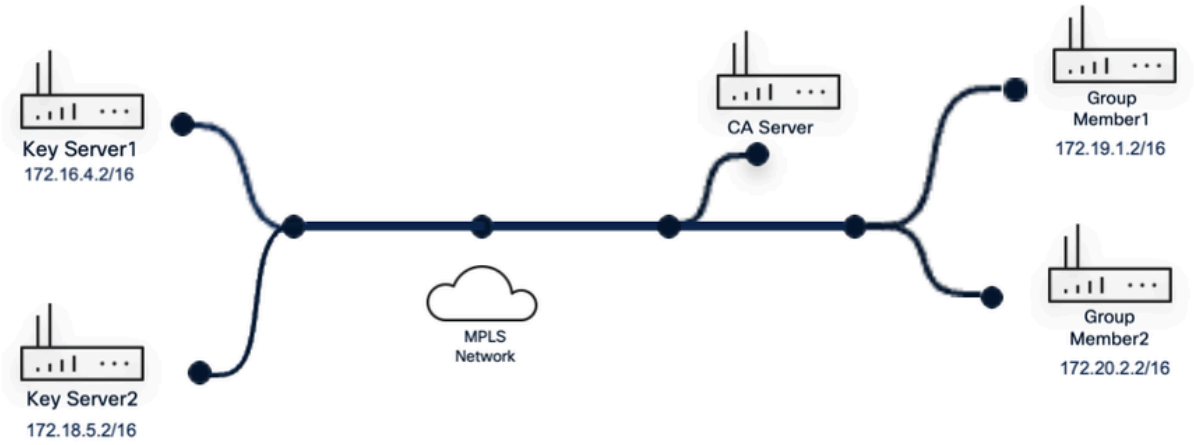
배경 정보

KS가 제어 평면을 유지하기 때문에 GETVPN 구축에서는 키 서버가 가장 중요한 엔티티입니다. 전체 GETVPN 그룹을 관리하는 단일 디바이스를 통해 단일 장애 지점이 생성됩니다.

이러한 상황을 완화하기 위해 GETVPN은 COOP(cooperative) KS라는 여러 키 서버를 지원하는데, 이 KS는 키 서버에 연결할 수 없는 경우 이중화 및 복구를 제공합니다.

구성

네트워크 다이어그램



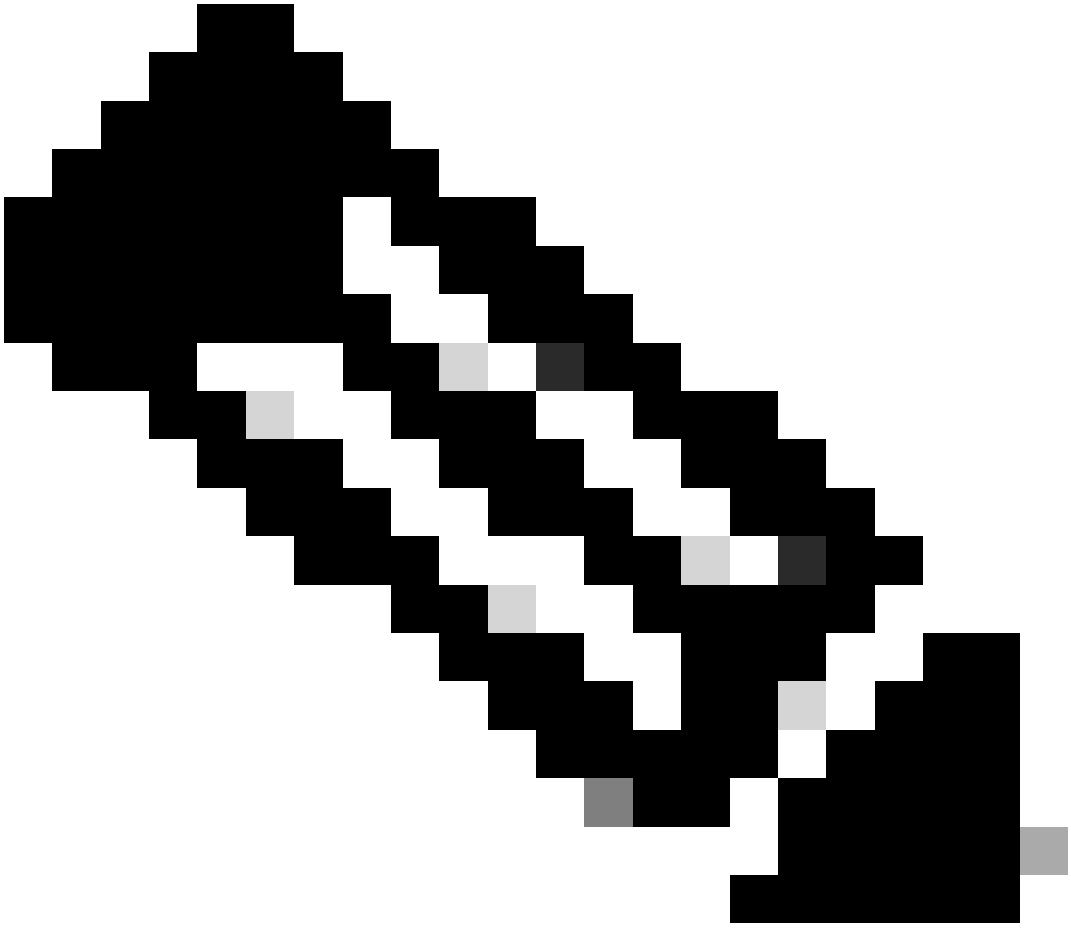
GETVPN 토폴로지

설정

인증용 PKI

PKI는 인프라를 사용하여 PSK 사용 시 발생하는 주요 관리 문제를 해결합니다. PKI 인프라는 ID 인증서를 발급(및 유지 관리)하는 CA(Certificate Authority) 역할을 합니다.

인증서 정보가 ISAKMP ID와 일치하는 모든 그룹 구성원 라우터는 권한이 부여되며 KS에 등록할 수 있습니다.



참고: 인증서는 모든 CA에서 발급할 수 있습니다. 이 설명서에서 CSR1000V는 ID를 인증하기 위해 구축의 모든 디바이스에 인증서를 발급하는 CA로 구성됩니다.

CA# show crypto pki server

crypto pki server ca-server

데이터베이스 수준 완료

데이터베이스 아카이브 pkcs12 비밀번호 7 1511021F07257A767B73

issuer-name CN=Root-CA.cisco.com OU=LAB

자동 해시 sha255 부여

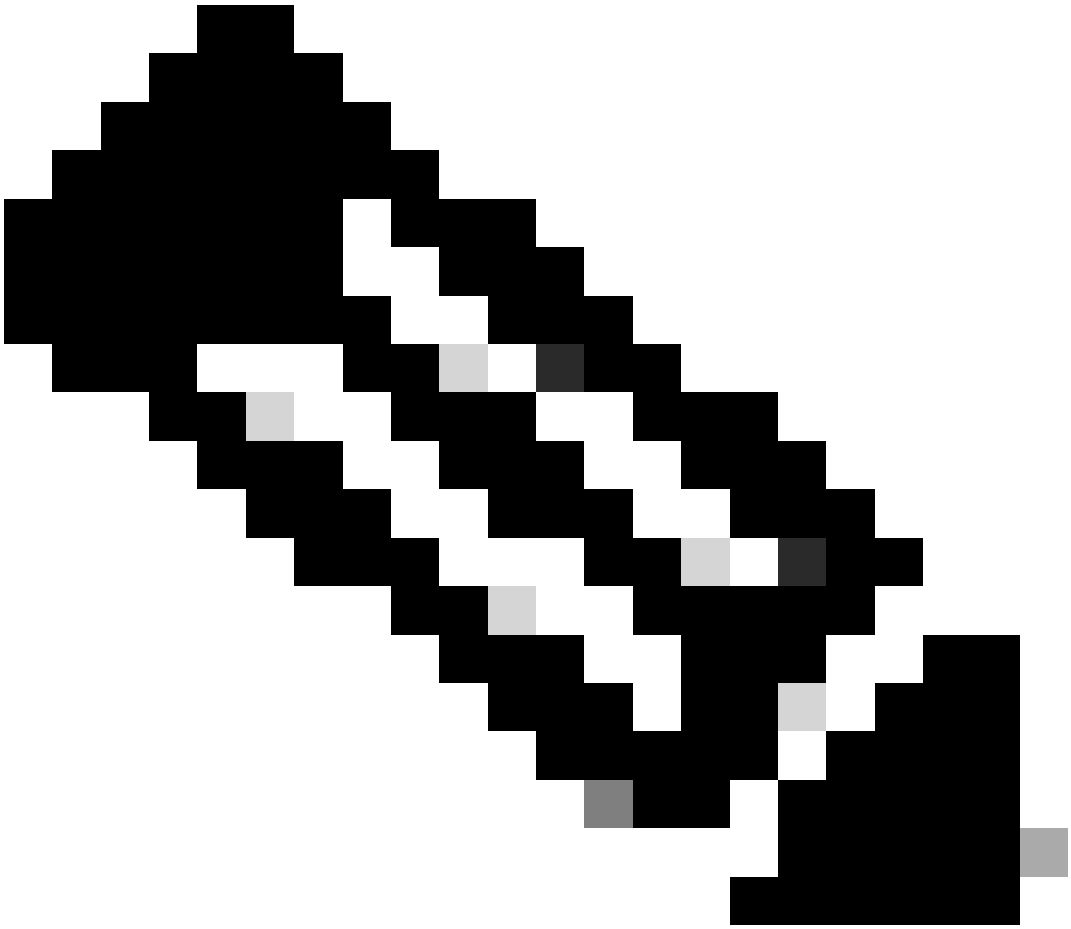
수명 인증서 5000

수명 ca 인증서 7300

eku server-auth client-auth

데이터베이스 url nvram

1.- PKI 기반 구축에서는 각 디바이스의 CA(Certificate Authority)에서 ID 인증서를 받아야 합니다. 키 서버 및 그룹 멤버 라우터에서 신뢰 지점 컨피그레이션에 사용되는 RSA 키 쌍을 생성합니다.



참고: 이 설명서의 데모를 위해 이 토폴로지의 모든 키 서버 및 그룹 구성원 라우터는 동일한 컨피그레이션을 공유합니다.

키 서버

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**

그룹 구성원

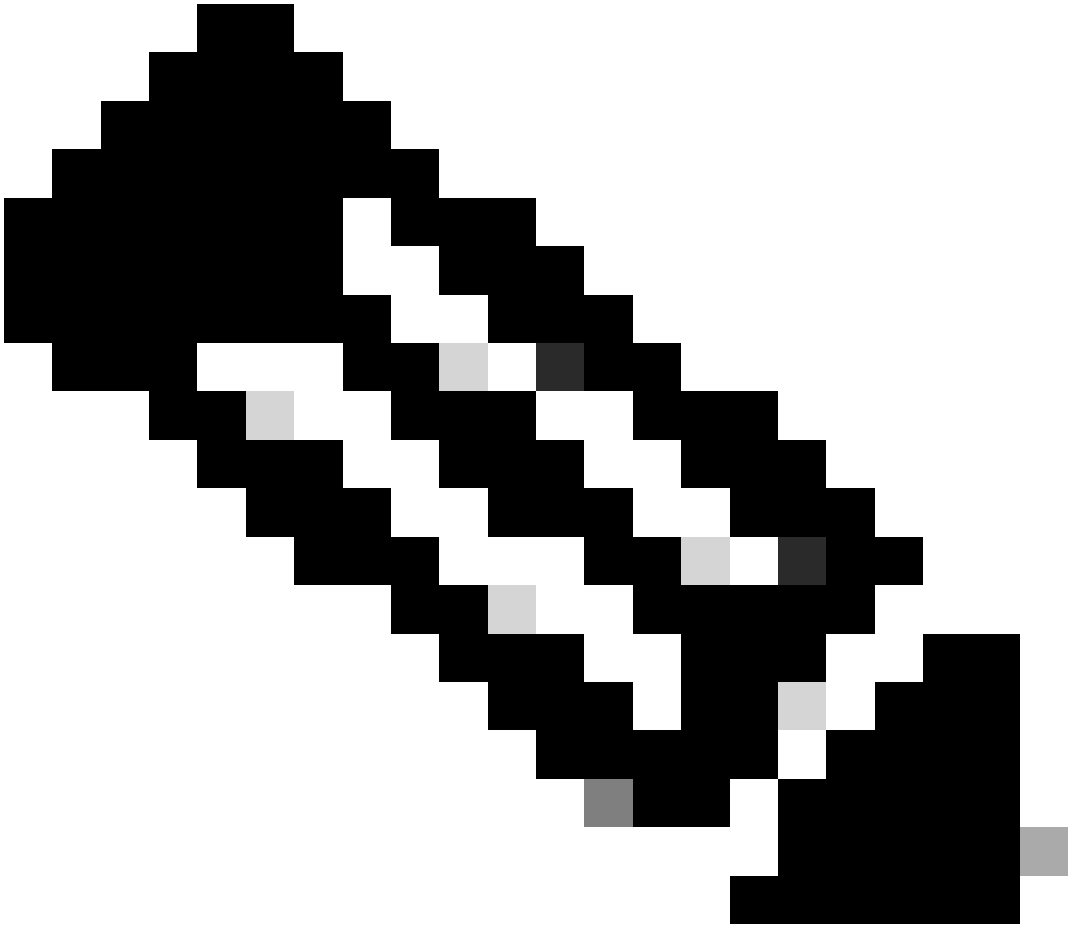
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)#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



참고: RSA 키 이름은 일관성을 유지하기 위해 모든 디바이스에서 재사용되며, 각 RSA 키가 계산 값에서 고유하기 때문에 다른 설정에는 영향을 주지 않습니다.

2.- CA의 인증서를 먼저 신뢰 지점에 설치해야 합니다. 이 작업은 신뢰 지점을 인증하거나 직접 등

록하여 수행할 수 있습니다. 이전에 설치된 CA 인증서가 없으므로 신뢰 지점 인증 절차가 먼저 트리거됩니다.

키 서버

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.

그룹 구성원

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' commandwill show the fingerprint.

3-두 디바이스에서 'show crypto pki certificates verbose' 명령을 사용하여 새로 발급된 인증서가 각각의 인증된 신뢰 지점에서 가져오기되는지 확인합니다(CA 인증서도 가져와야 함).

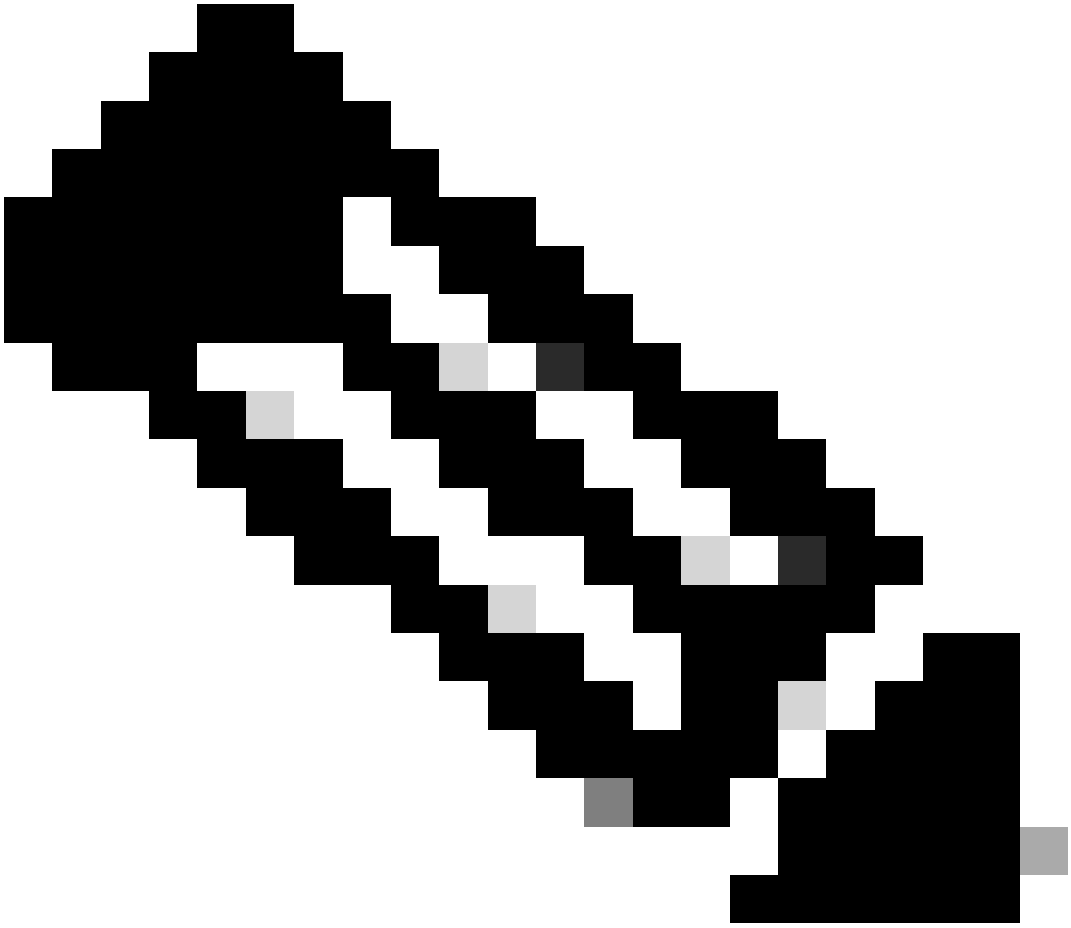
키 서버

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

그룹 구성원

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



참고: 인증서 인증의 경우 제공된 인증서에 CN(Common Name), EKU(Extended Key Usage), Validation Date(유효 날짜) 등과 같은 디바이스 ID를 검증할 수 있는 올바른 매개변수가 있는지 확인합니다.

GETVPN 구성

GETVPN의 중요한 기능은 ISAKMP 및 GDOI 기능 전에 구성하는 것이 권장되는 이전 컨피그레이션을 사용합니다.

4.- 기본 키 서버에서 레이블이 'getKey'인 내보내기 가능한 RSA 키를 생성합니다. 이 키는 모든 키 서버에서 동일해야 합니다. 따라서 내보낼 수 있는 기능은 다음 단계에 필수적입니다.

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)

5.- 그룹 구성원 라우터가 통과할 때 암호화해야 하는 관심 있는 트래픽을 사용하여 확장 액세스 목록을 정의합니다. 보조 키 서버에서 동일한 이름을 사용하여 동일한 access-list를 정의합니다.

기본 키 서버

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

보조 키 서버

KS2(config)# **ip access-list extended data_plane** KS2(config-ext-nacl)# 10 permit ip 10.0.0 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

6- GDOI 그룹 메시지 교환으로 시작하기 위해 GM과의 보안 연결을 설정하는 데 사용되는 ISAKMP 정책, IPsec 변환 세트 및 IPsec 프로필을 구성합니다.

KS(config)# **crypto isakmp policy 10** KS(config-isakmp)# **encryption aes 256** KS(config-iskamp)# **hash sha256** KS(config-iskamp)# **group 14** KS(config-iskamp)# **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**

COOP 구성

7.- 공동 구현 시 관련된 주요 서버의 구성이 동일해야 합니다. 기본 키 서버에서 이전에 생성한 내보내기 가능한 RSA 키를 내보내고 개인 키와 공개 키를 모두 보조 키 서버(KS2)로 가져옵니다. 기본 키 서버가 응답하지 않는 시나리오에서 보조 키 서버는 그룹 내의 모든 GM 디바이스에 대한 키 재설정 제어를 계속 수행합니다.

기본 키 서버

KS(config)# **crypto key export rsa getKey pem terminal 3des cisco123** % Key name: getKey Usage: General Purpose Key Key data: -----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAdGV3ZPaGQcsAqO
1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NXE07
5bOsrT7B2uOpCBmAJK9iiTsfr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,AA98923B28E00DCCto1Wym6cRvqEXBlt97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

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

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

보조 키 서버

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,AA98923B28E00DCCto1Wym6cRvqEXBlt97UZdGyusf3cW/iumb7oD9/09q5if4ouoE

brPykL3No0WMI7h56WQPiAHzLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9

zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlizE1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu

GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/DOppe2

n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNgHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFrf0NRXFHrM7T9MQcBBIcbo0BtfG4ICBuIltpG+BpCty/XW99dvuhqh9hjqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwvvWQjewrA0K

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

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

quit

% Key pair import succeeded.

8- COOP KS에 대해 주기적인 ISAKMP를 구성해야 합니다. 이렇게 하면 기본 KS가 보조 키 서버를 모니터링할 수 있습니다

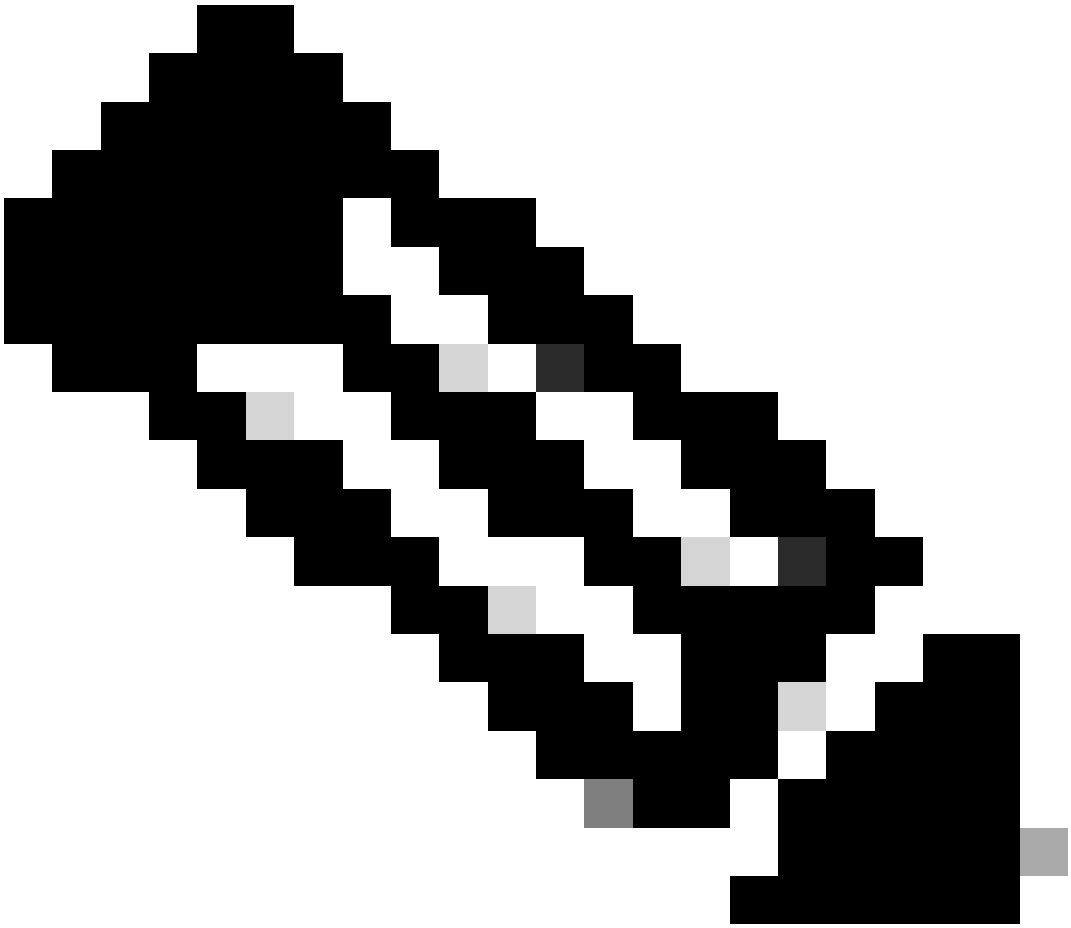
기본 키 서버

KS(config)# **crypto isakmp keepalive 15 periodic**

보조 키 서버

KS2(config)# **crypto isakmp keepalive 15 periodic**

COOP 키 서버는 기본 서버에서 보조 서버로 단방향 통신을 교환합니다. 만약 2차 KS가 30초 간격으로 1차 KS로부터 아무런 연락을 받지 못하면, 2차 KS는 1차 KS에 연락을 시도하고, 업데이트된 정보를 요청한다. 제2 KS가 60초 간격으로 제1 KS로부터 청취를 받지 못하면, COOP 재선택 프로세스가 트리거되고, 새로운 제1 KS가 선택된다.



참고: GM과 KS 간의 주기적인 DPD는 요구되지 않는다.

키 서버 간의 선택은 구성된 가장 높은 우선순위 값을 기준으로 합니다. 동일한 경우 가장 높은 IP 주소를 기반으로 합니다. 동일한 암호화 정책, 확장 액세스 목록을 사용하여 각 키 서버에서 동일한 GDOI 그룹을 구성합니다.

기본 키 서버

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**

9.- 동일한 로컬 서버 설정에서 이전에 구성된 데이터 플레인 트래픽 및 액세스 목록에 대해 의도된 암호화 정책을 활성화합니다.

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

로컬 서버 설정은 COOP 키 서버 기능이 활성화된 컨피그레이션 수준이며, 정의된 우선순위에 따라 이 키 서버의 역할이 결정됩니다. 보조 키 서버는 모든 KS가 서로를 인식할 수 있도록 명시적으로 구성해야 합니다.

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**

COOP 키 서버 컨피그레이션의 마지막 부분은 키 패킷의 소스 IP 주소 정의이며, 이는 키 서버 라우터의 인터페이스 중 하나에 구성된 IP 주소입니다.

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

보조 키 서버에서 동일한 컨피그레이션 단계를 복제하여 낮은 우선순위를 구성하여 라우터를 보조 서버로 식별하고 기본 KS 주소를 등록합니다.

보조 키 서버

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**

10.- 그룹 구성원 라우터에서 GDOI 그룹 설정은 Keys Server에 비해 컨피그레이션이 적습니다. 그룹 멤버는 ISAKMP 정책을 구성하고 동일한 인증 방법인 GDOI 그룹을 사용하며 GM 라우터가 등록할 수 있는 키 서버의 IP 주소만 있으면 됩니다.

그룹 구성원

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**

그룹 구성원 2

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**

다음을 확인합니다.

다음과 같이 컨피그레이션의 모든 단계에서 설정을 확인합니다.

키 서버의 데이터 플레인 트래픽에 대한 ACL

이 show 명령은 정의된 흥미로운 트래픽에 대한 실수가 없음을 확증하는 데 사용됩니다.

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

COOP 등록 상태:

'show crypto gkm ks coop' 명령은 기본 키 서버가 누구인지, 기본 키 서버가 속한 GDOI 그룹, 개별 및 피어 우선 순위, 기본 서버에서 보조 서버로 전송할 다음 메시지에 대한 타이머를 나타내는 키 서버 간의 현재 COOP 상태를 표시합니다.

기본 키 서버

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 recv: 32 Ann msgs recv with reply request: 4 Packet sent drops: 3 Packet Recv drops: 0 Total bytes sent: 42550002 Total bytes recv: 22677

보조 키 서버

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 recv: 28 Ann msgs recv with reply request: 1 Packet sent drops: 1 Packet Recv drops: 0 Total bytes sent: 468 Total bytes recv: 16913

그룹 GETVPN에 대한 정보 및 협력 키 서버에 대한 버전 정보를 표시합니다.

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

그룹 구성원 등록

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 sents : 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 chech P2P POLICY: REG_GM: local_addr 10.191.61.116

문제 해결

COOP 키 서버 선택

syslog 메시지는 COOP 프로세스의 문제를 추적하고 식별하는 데 도움이 될 수 있습니다. COOP 키 서버에서 GDOI 디버깅을 활성화하여 이 프로세스와 관련된 정보만 표시합니다.

KS# **debug crypto gdoi ks coop**

COOP 선택 프로세스가 시작되면 모든 키 서버에서 다음 syslog 메시지가 표시됩니다.

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

선택 프로세스를 완료한 후 "COOP_KS_TRANS_TO_PRI" 메시지에 새 기본 키 서버에 대한 정보가 표시됩니다. 이 메시지는 기본 및 보조 키 서버에 표시됩니다. 이전 예비선거에서는 선거 과정의 첫 번째에 '없음'이 나타날 것으로 예상된다.

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

Key Server 재선택이 있는 경우 메시지에 이전 기본 서버의 IP 주소가 포함됩니다.

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

COOP 보조 키 서버에 대한 연결이 끊기면 "COOP_KS_UNREACH" 메시지가 표시됩니다. 기본 KS는 모든 보조 KS의 상태를 추적하며 이 메시지를 사용하여 보조 KS에 대한 연결이 끊겼음을 나타냅니다. 보조 KS는 기본 KS의 상태만 추적합니다. 보조 KS에 대한 이 메시지는 기본 KS와의 연결이 끊겼음을 나타냅니다.

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

COOP KS 간에 연결이 복원되면 "COOP_KS_REACH" 메시지가 표시됩니다.

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

PKI 등록 문제

신뢰 지점 등록 또는 인증 문제를 디버깅할 때 PKI 디버그를 사용합니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.