Konfigurieren von GETVPN mit COOP-Schlüsselservern und Zertifikatauthentifizierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Group Encrypted Transport VPN (GETVPN) für die Verwendung digitaler Zertifikate für die Authentifizierung und für COOP-Schlüsselserver konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- GETVPN (Group Encrypted Transport VPN)

-Public Key Infrastructure (PKI)

- Zertifizierungsstelle (CA)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- CSR1000V - Cisco IOS® XE, Version 16.12.03 - als Cisco IOS® XE Key Server, Group Member und CA Server.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

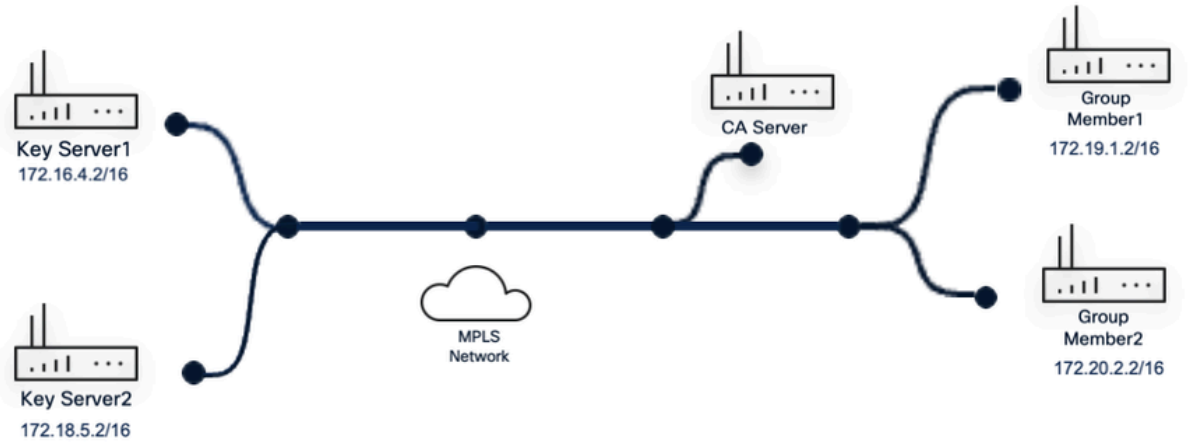
Hintergrundinformationen

In einer GETVPN-Bereitstellung ist der Schlüsselserver die wichtigste Einheit, da der KS die Kontrollebene beibehält. Mit einem einzigen Gerät zur Verwaltung einer kompletten GETVPN-Gruppe entsteht ein Single Point of Failure.

Um dieses Szenario abzumildern, unterstützt GETVPN mehrere Key-Server, die als kooperatives (COOP) KSs bezeichnet werden und Redundanz und Recovery bieten, wenn ein Key-Server nicht erreichbar ist.

Konfigurieren

Netzwerkdiagramm



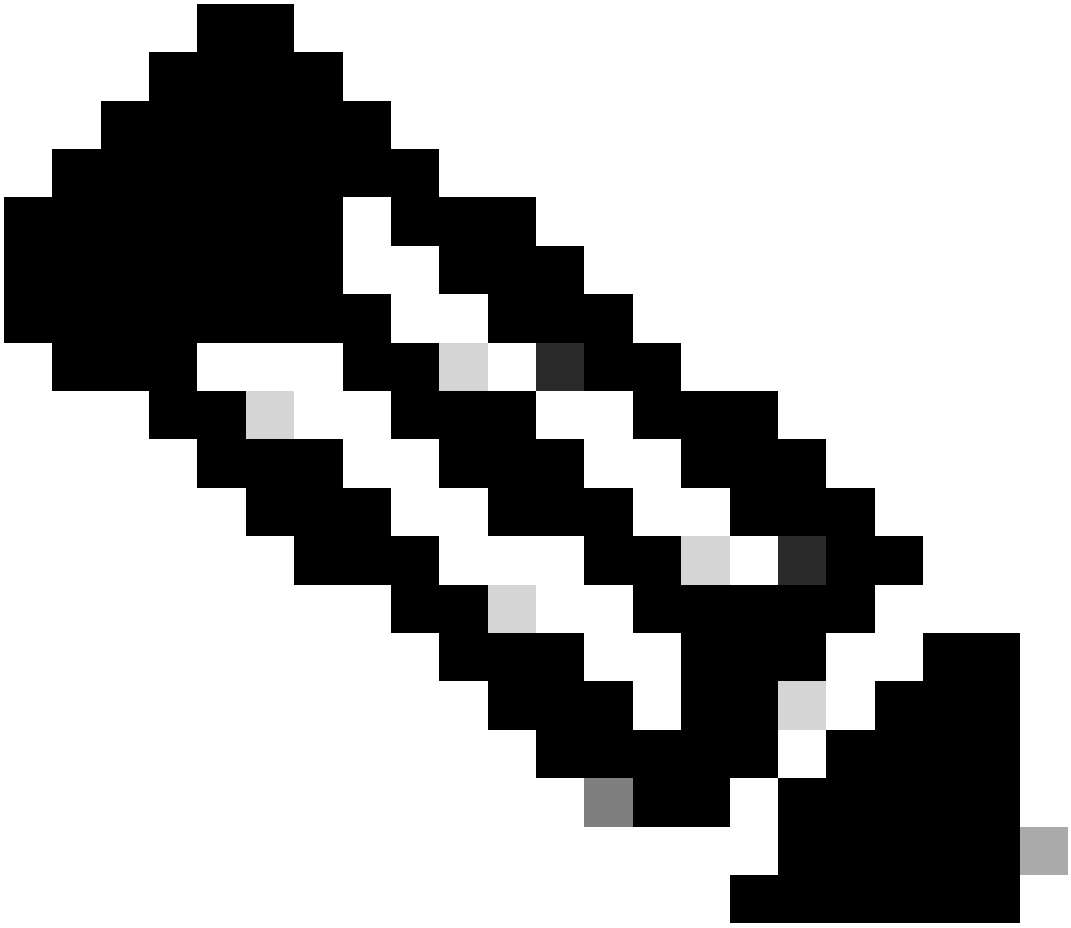
GETVPN-Topologie

Konfigurationen

PKI für die Authentifizierung

PKI nutzt seine Infrastruktur, um die beim Einsatz von PSKs auftretenden Hauptverwaltungsprobleme zu überwinden. Die PKI-Infrastruktur fungiert als Zertifizierungsstelle (Certificate Authority, CA), die Identitätszertifikate ausstellt (und dann verwaltet).

Jeder Router eines Gruppenmitglieds, dessen Zertifikatsinformationen mit der ISAKMP-Identität übereinstimmen, ist autorisiert und kann sich beim KS registrieren.



Anmerkung: Zertifikate können von jeder Zertifizierungsstelle ausgestellt werden. Für dieses Handbuch wird ein CSR1000V als CA konfiguriert, um allen Geräten in der Bereitstellung Zertifikate zur Authentifizierung ihrer Identität auszustellen.

CA# Krypto-PKI-Server anzeigen

crypto pki server ca-server

Datenbankebene vollständig

Datenbankarchiv pkcs12 Kennwort 7 1511021F07257A767B73

Name des Ausstellers CN=Root-CA.cisco.com OU=LAB

gewähren auto hash sha255

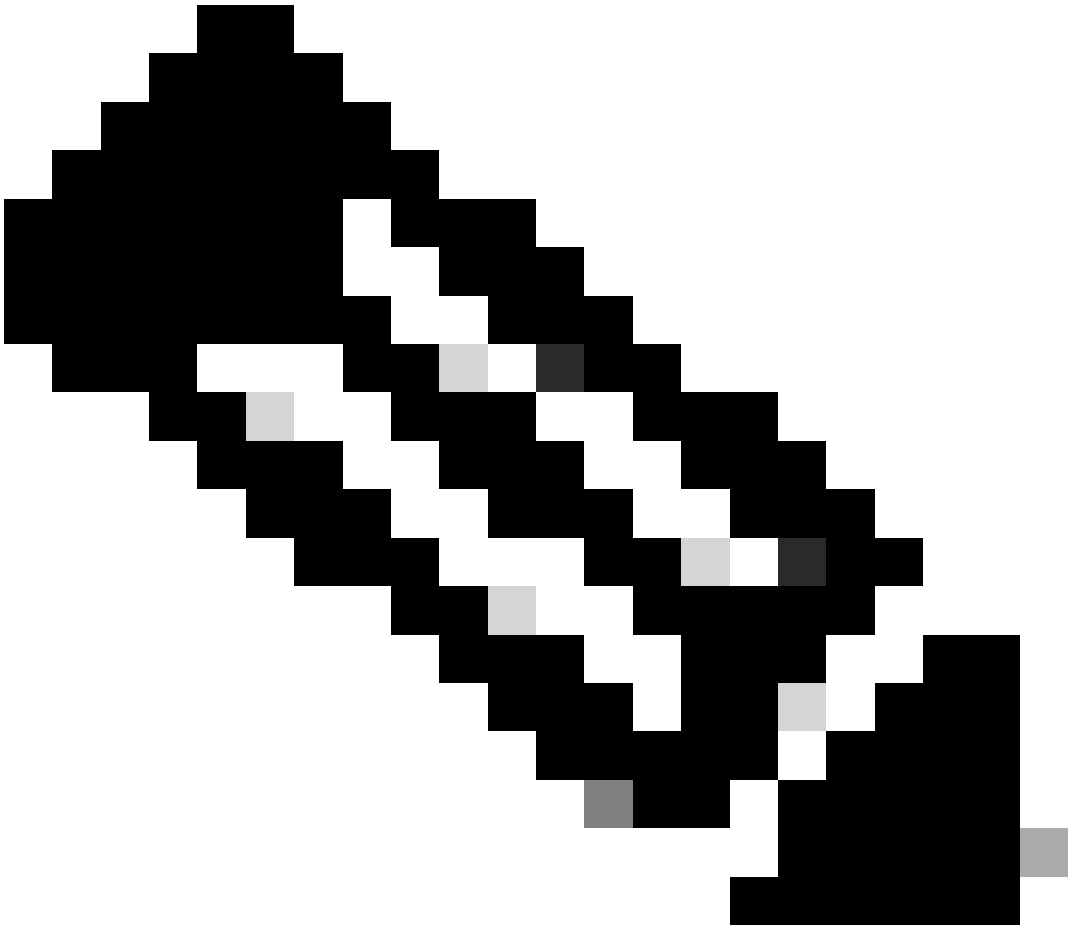
Lebenszeitzertifikat 5000

Lebenszeitzertifikat 7300

eku server-auth client-auth

Datenbank-URL nvram

1.- Bei PKI-basierten Bereitstellungen muss das Identitätszertifikat einer Zertifizierungsstelle (Certificate Authority, CA) für jedes Gerät abgerufen werden. Erstellen Sie auf den Key-Server- und Group-Member-Routern eine RSA-Tastatur, die in ihrer Vertrauenspunktkonfiguration verwendet wird.



> Anmerkung: Zur Demonstration dieses Leitfadens verwenden alle Schlüsselserver und Router der Gruppenmitglieder in dieser Topologie dieselbe Konfiguration.

Schlüsselserver

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**

Gruppenmitglied

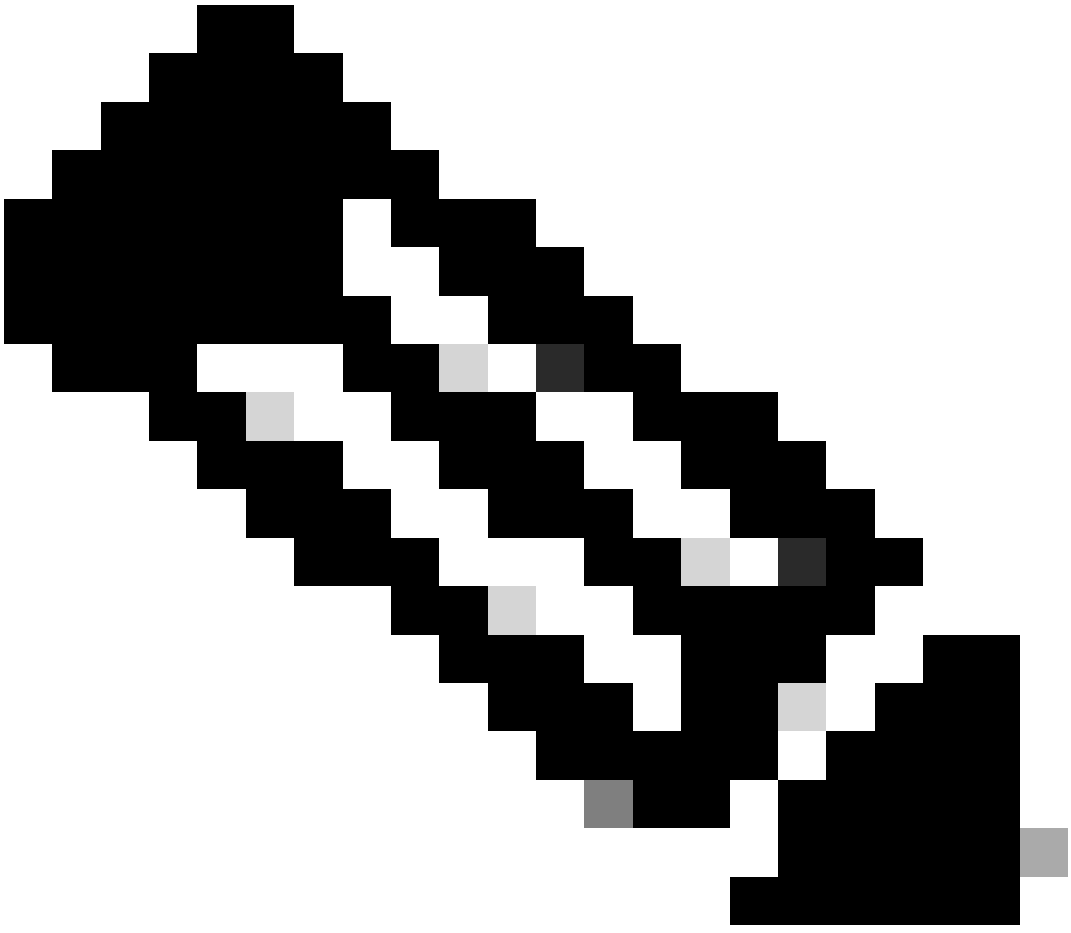
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)#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



Anmerkung: Der Name des RSA-Schlüssels wird auf allen Geräten wiederverwendet, um die Konsistenz zu erhalten, und er hat keine Auswirkungen auf andere Einstellungen, da

---

jeder RSA-Schlüssel in seinem Rechenwert eindeutig ist.

2.- Das Zertifikat der Zertifizierungsstelle muss zuerst im Vertrauenspunkt installiert werden. Dies kann entweder durch die Authentifizierung des Vertrauenspunkts oder durch eine direkte Registrierung erfolgen. Da zuvor kein Zertifizierungsstellenzertifikat installiert wurde, wird zuerst die Trustpoint-Authentifizierungsprozedur ausgelöst.

Schlüsselserver

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.

Gruppenmitglied

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-Überprüfen Sie auf beiden Geräten, dass die neu ausgestellten Zertifikate in ihre jeweiligen authentifizierten Trustpoints importiert werden (das CA-Zertifikat muss ebenfalls importiert werden). Verwenden Sie dazu den Befehl 'show crypto pki Certificates verbose'.

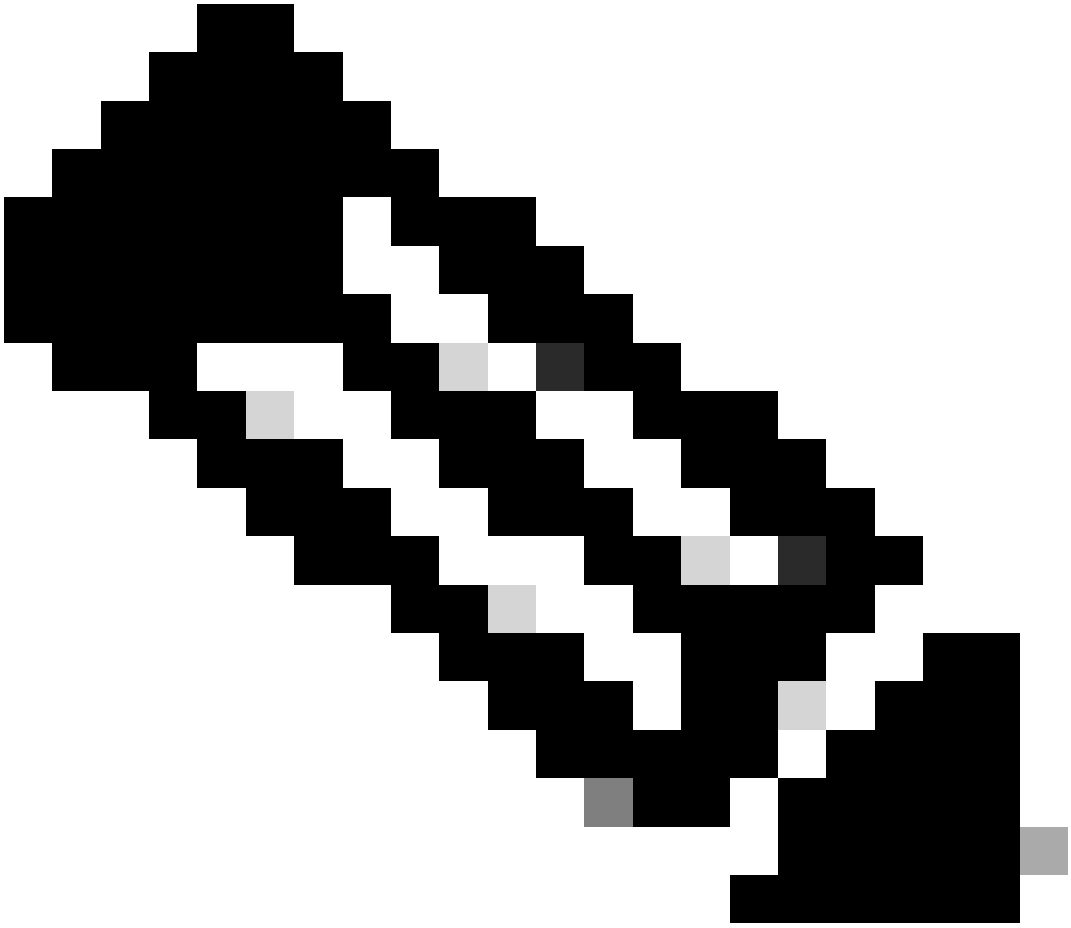
Schlüsselserver

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

Gruppenmitglied

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



Anmerkung: Stellen Sie bei der Zertifikatsauthentifizierung sicher, dass das bereitgestellte Zertifikat über die richtigen Parameter verfügt, um die Identität des Geräts zu validieren, z. B. Common Name (CN), Extended Key Usage (EKU), Validity Date.

GETVPN konfigurieren

Wichtige Funktionen von GETVPN basieren auf der vorherigen Konfiguration, die vor ISAKMP- und GDOI-Funktionen konfiguriert werden sollte.

4.- Generieren Sie auf dem primären Schlüsselserver einen exportierbaren RSA-Schlüssel mit der Bezeichnung "getKey". Dieser Schlüssel muss auf allen Schlüsselservern identisch sein. Daher ist die Exportfunktion für die folgenden Schritte von entscheidender Bedeutung:

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.- Definieren Sie eine erweiterte Zugriffsliste mit dem interessanten Datenverkehr, den die Router

der Gruppenmitglieder beim Weiterleiten verschlüsseln müssen. Definieren Sie auf dem sekundären Schlüsselserver dieselbe Zugriffsliste mit demselben Namen.

Primärer Schlüsselserver

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

Sekundärer Schlüsselserver

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- Konfigurieren Sie die ISAKMP-Richtlinie, den IPsec-Transformationssatz und das IPsec-Profil, die zum Herstellen der sicheren Verbindung mit den GMs verwendet werden, um mit dem GDOI-Gruppennachrichtenaustausch zu beginnen.

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**

Konfigurieren von COOP

7.- In einer kooperativen Implementierung müssen die beteiligten Schlüsselserver identisch konfiguriert sein. Exportieren Sie den zuvor erstellten, exportierbaren RSA-Schlüssel vom primären Schlüsselserver, und importieren Sie sowohl private als auch öffentliche Schlüssel in den sekundären Schlüsselserver (KS2). In einem Szenario, in dem der primäre Schlüsselserver nicht mehr reagiert, steuert der sekundäre Schlüsselserver weiterhin den Schlüssel für alle GM-Geräte in der Gruppe.

Primärer Schlüsselserver

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-----

Sekundärer Schlüsselserver

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- Periodisches ISAKMP muss für die COOP KSs konfiguriert werden. Auf diese Weise kann das primäre KS die sekundären Schlüsselserver überwachen

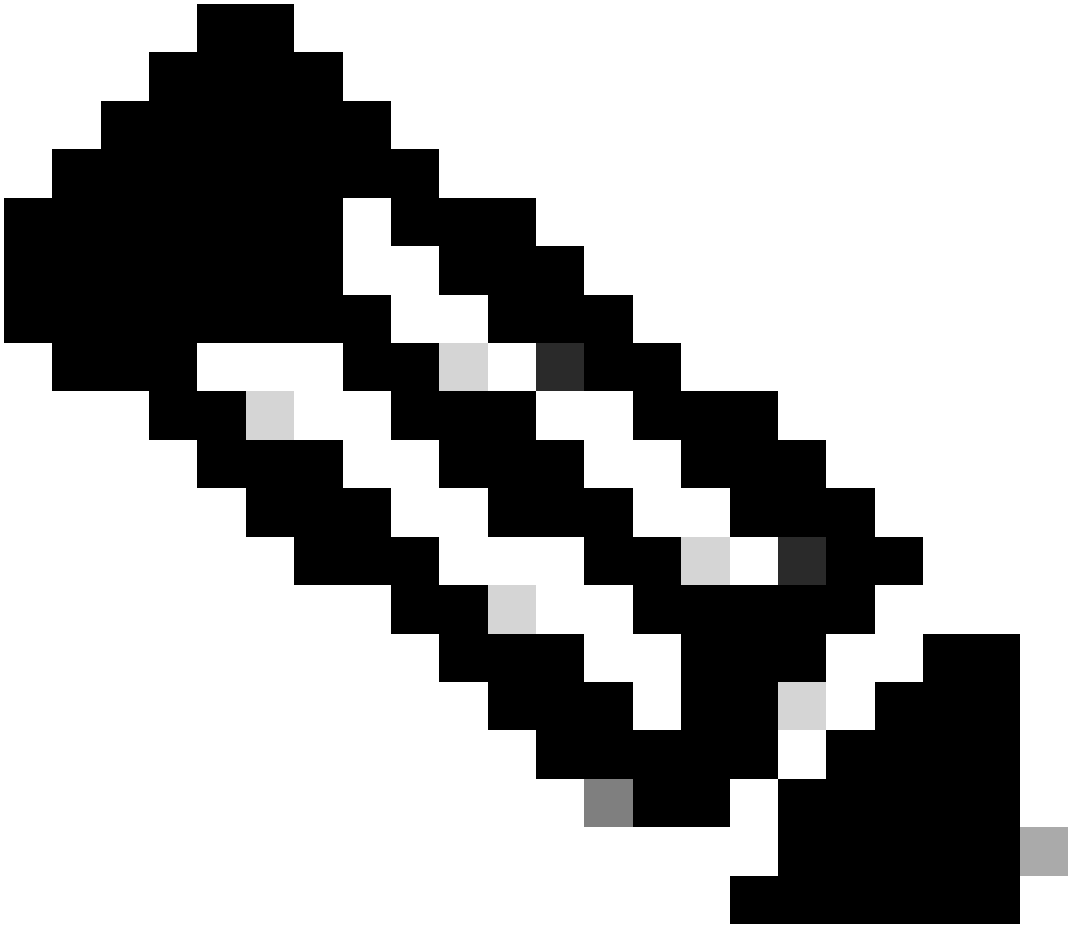
Primärer Schlüsselserver

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

Sekundäre Schlüsselserver

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

COOP-Schlüsselserver tauschen unidirektionale Kommunikation von primär zu sekundär aus. Wenn ein sekundäres KS innerhalb von 30 Sekunden nicht vom primären KS hört, versucht das sekundäre KS, das primäre KS zu kontaktieren und fordert aktualisierte Informationen an. Hört das sekundäre KS über einen Zeitraum von 60 Sekunden nicht vom primären KS, wird ein COOP-Wiederwahlvorgang ausgelöst und ein neues primäres KS gewählt.



Anmerkung: Ein periodisches DPD zwischen GM und KS ist nicht erforderlich.

Die Auswahl zwischen den Schlüsselservern basiert auf dem konfigurierten Wert mit der höchsten Priorität. Wenn sie identisch sind, basiert sie auf der höchsten IP-Adresse. Konfigurieren Sie auf jedem Schlüsselserver dieselbe GDOI-Gruppe mit denselben Krypto-Richtlinien und erweiterten Zugriffslisten.

Primärer Schlüsselserver

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)#r**ekey authentication mypubkey rsa getKey** KS(gkm-local-server)# **rekey transport unicast**

9.- Aktivieren Sie innerhalb derselben lokalen Servereinstellungen die Krypto-Richtlinien für den Datenverkehr auf Datenebene und die Zugriffsliste, die zuvor konfiguriert wurden.

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

Über die lokalen Servereinstellungen wird die Konfigurationsebene festgelegt, auf der die COOP-Schlüsselserverfunktion aktiviert ist. Die definierte Priorität bestimmt die Rolle für diesen Schlüsselserver. Die sekundären Schlüsselserver müssen explizit konfiguriert werden, damit sich alle KS gegenseitig kennen.

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**

Der letzte Teil der COOP-Schlüsselserver-Konfiguration ist die Definition der Quell-IP-Adresse des Schlüsselpakets. Dabei handelt es sich um eine IP-Adresse, die in einer der Schnittstellen des Schlüsselserver-Routers konfiguriert ist.

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

Replikation derselben Konfigurationsschritte auf dem sekundären Schlüsselserver, Konfiguration einer niedrigeren Priorität, um den Router als sekundären Server zu identifizieren und die primäre KS-Adresse zu registrieren.

Sekundärer Schlüsselserver

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.- Bei einem Gruppenmitglied-Router sind die GDOI-Gruppeneinstellungen im Vergleich zu den Schlüsselservern weniger konfiguriert. Ein Gruppenmitglied muss lediglich die ISAKMP-Richtlinie

konfigurieren, die gleiche Authentifizierungsmethode und die GDOI-Gruppe verwenden und über die IP-Adressen der Schlüsselserver verfügen, bei denen sich der GM-Router registrieren kann.

Gruppenmitglied

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**

Gruppenmitglied 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**

Überprüfung

Überprüfen Sie in jeder Phase der Konfiguration die Einstellungen wie folgt:

ACLs für Datenverkehr auf Datenebene auf wichtigen Servern

Dieser Befehl show wird verwendet, um zu bestätigen, dass keine Fehler mit dem interessanten Datenverkehr definiert sind.

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-Registrierungsstatus:

Mit dem Befehl 'show crypto gkm ks coop' wird der aktuelle COOP-Status zwischen den Schlüsselservern angezeigt. Er gibt an, wer der primäre Schlüsselserver ist, zu welcher GDOI-Gruppe sie gehören, ihre individuelle und Peer-Priorität sowie Timer für die nächsten Nachrichten, die von primären zu sekundären Servern gesendet werden.

Primärer Schlüsselserver

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

Sekundärer Schlüsselserver

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

Zeigt Informationen zur Gruppe GETVPN und Versionsinformationen zum kooperativen Schlüsselserver an.

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

Gruppenmitgliedschaft

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

Fehlerbehebung

COOP-Schlüsselserver-Wahl

Die Syslog-Meldungen können beim Nachverfolgen und Identifizieren von Problemen mit dem COOP-Prozess helfen. Aktivieren Sie das GDOI-Debugging auf den COOP-Schlüsselservern, um

nur Informationen zu diesem Prozess anzuzeigen.

KS# **debug crypto gdoi ks coop**

Wenn die COOP-Auswahl beginnt, wird die nächste Syslog-Meldung auf allen Schlüsselservern angezeigt.

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

Nach Abschluss des Auswahlprozesses zeigt die Meldung "COOP_KS_TRANS_TO_PRI" Informationen über den neuen primären Schlüsselserver an. Die Meldung wird auf dem primären und sekundären Schlüsselserver angezeigt. Das Vorgängerprimär wird beim ersten Wahlvorgang voraussichtlich "KEINE" anzeigen.

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

Bei einer erneuten Auswahl des Schlüsselservers enthält die Nachricht die IP-Adresse des vorherigen primären Servers.

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

Wenn die Verbindung zu sekundären COOP-Schlüsselservern unterbrochen wird, wird die Meldung "COOP_KS_UNREACH" angezeigt. Primäres KS verfolgt den Zustand aller sekundären KSs und verwendet diese Meldung, um den Verlust der Verbindung zu einem sekundären KS anzuzeigen. Ein sekundäres KS verfolgt nur den Zustand des primären KS. Diese Meldung auf dem sekundären KS weist auf einen Verbindungsverlust mit dem primären KS hin.

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

Wenn die Verbindung zwischen den COOP KSs wiederhergestellt ist, wird eine "COOP_KS_REACH" Meldung angezeigt.

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

PKI-Registrierungsprobleme

Beim Debuggen von Problemen mit der Vertrauenspunktregistrierung oder der Authentifizierung verwenden Sie PKI-Debugging.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.