Configuración de GETVPN con servidores de claves COOP y autenticación de certificados

Contenido

Introducción

Este documento describe cómo configurar Group Encrypted Transport VPN (GETVPN) para utilizar certificados digitales para la autenticación y servidores de claves COOP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de transporte cifrado de grupo (GETVPN)

-Public Key Infrastructure (PKI)

-Autoridad de certificación (CA)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CSR1000V - Cisco IOS® XE, versión 16.12.03 - como servidor de claves, miembro de grupo y servidor de CA de Cisco IOS® XE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

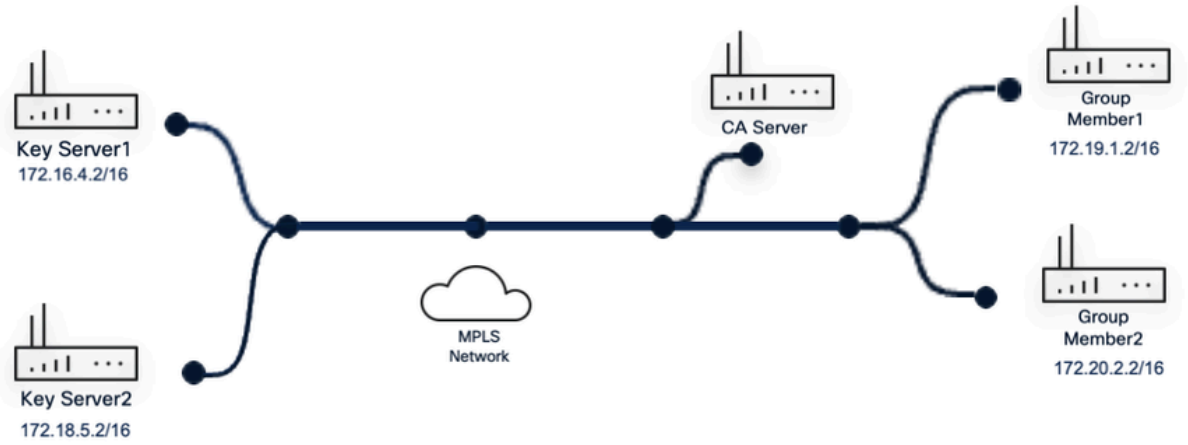
Antecedentes

En una implementación de GETVPN, el servidor de claves es la entidad más importante porque el KS mantiene el plano de control. Con un solo dispositivo para administrar un grupo GETVPN completo, se crea un único punto de falla.

Para mitigar este escenario, GETVPN admite varios servidores de claves denominados KS cooperativos (COOP) que proporcionan redundancia y recuperación si un servidor de claves se vuelve inalcanzable.

Configurar

Diagrama de la red



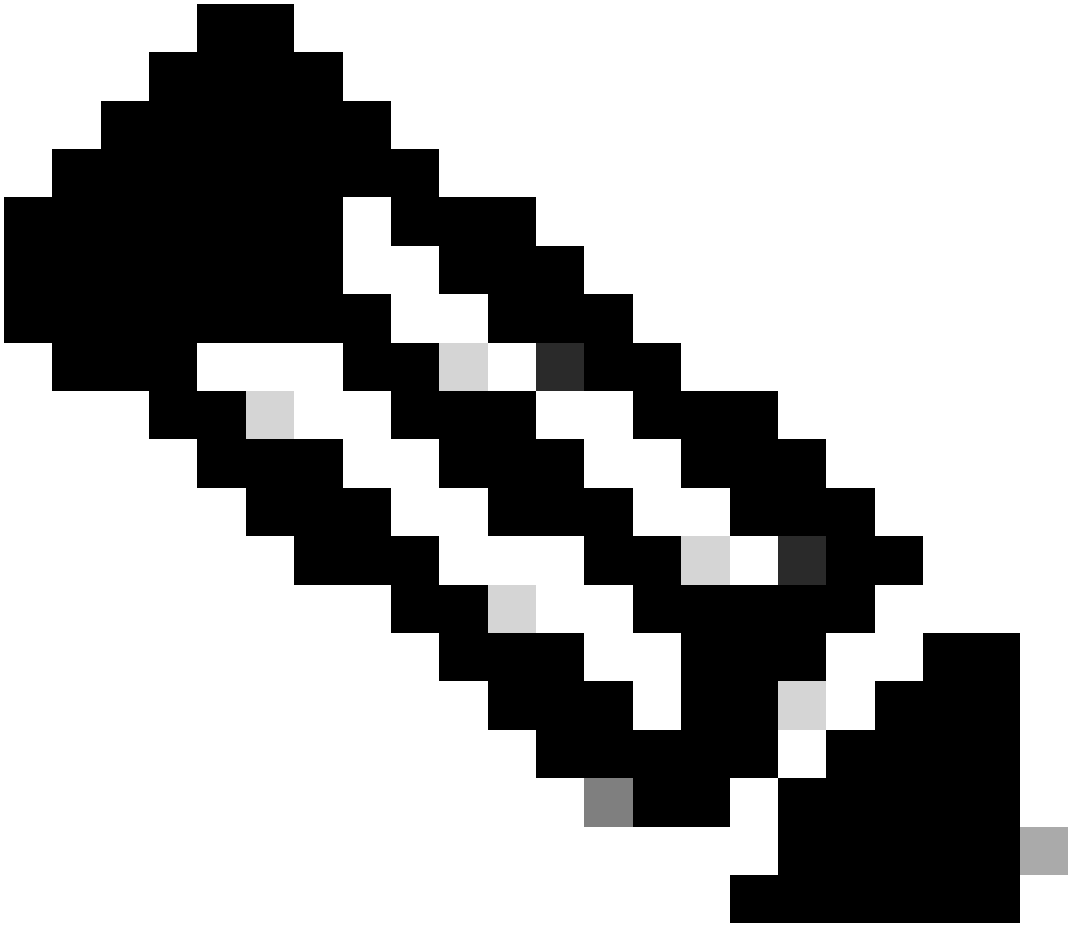
Topología GETVPN

Configuraciones

PKI para autenticación

PKI utiliza su infraestructura para superar las dificultades de gestión clave que surgen al utilizar PSK. La infraestructura PKI actúa como una autoridad de certificación (CA) que emite (y mantiene) certificados de identidad.

Cualquier router miembro del grupo cuya información de certificado coincida con la identidad ISAKMP está autorizado y puede registrarse en el KS.



Nota: Los certificados pueden ser emitidos por cualquier CA. En esta guía, se configura un CSR1000V como CA para emitir certificados a todos los dispositivos de la implementación con el fin de autenticar su identidad.

CA# show crypto pki server

crypto pki server ca-server

nivel de base de datos completo

database archive pkcs12 password 7 1511021F07257A767B73

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

grant auto hash sha255

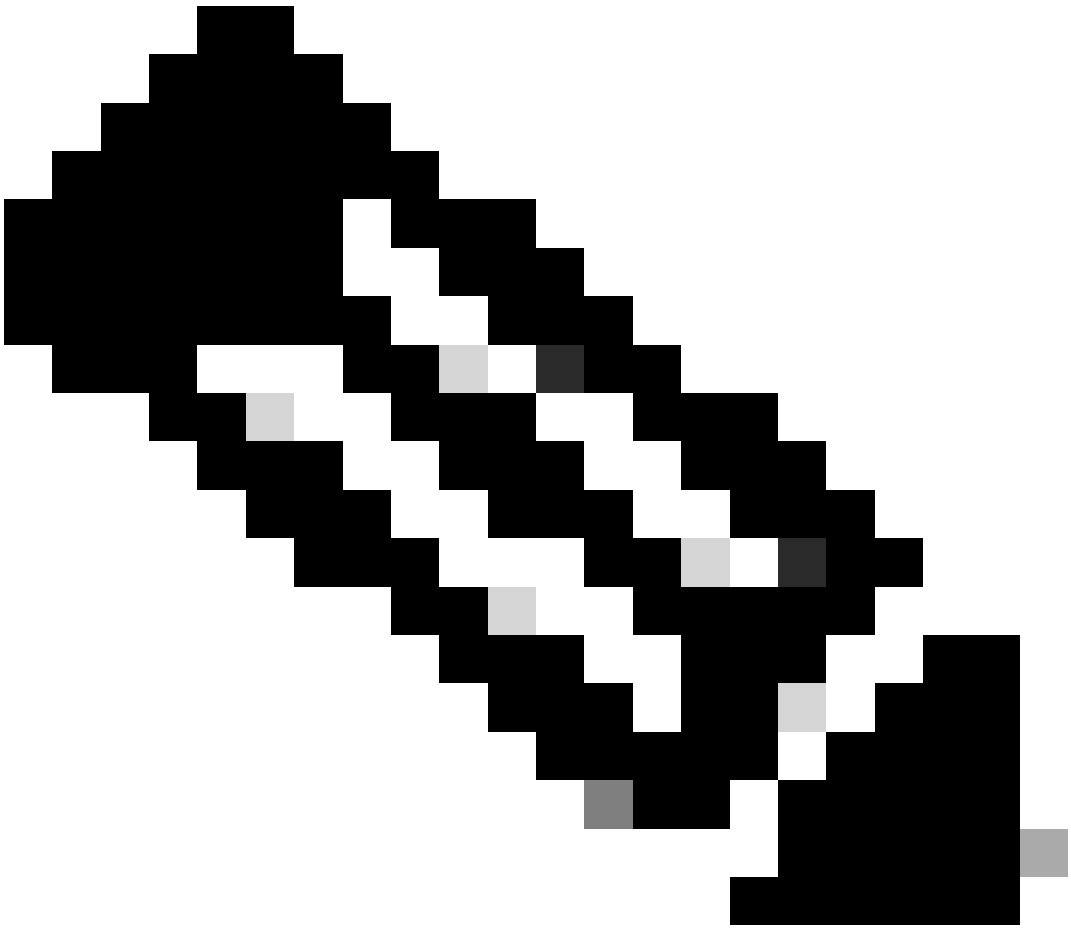
lifetime certificate 5000

lifetime ca-certificate 7300

eku server-auth client-auth

database url nvram

1.- En las implementaciones basadas en PKI, se debe obtener el certificado de identidad de una autoridad de certificación (CA) para cada dispositivo. En los routers Servidor de claves y Miembro de grupo, cree un par de claves RSA utilizado en su configuración de punto de confianza.



> Nota: Para la demostración de esta guía, todos los servidores de claves y los routers de miembros de grupo de esta topología comparten la misma configuración.

Servidor de claves

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**

Miembro del grupo

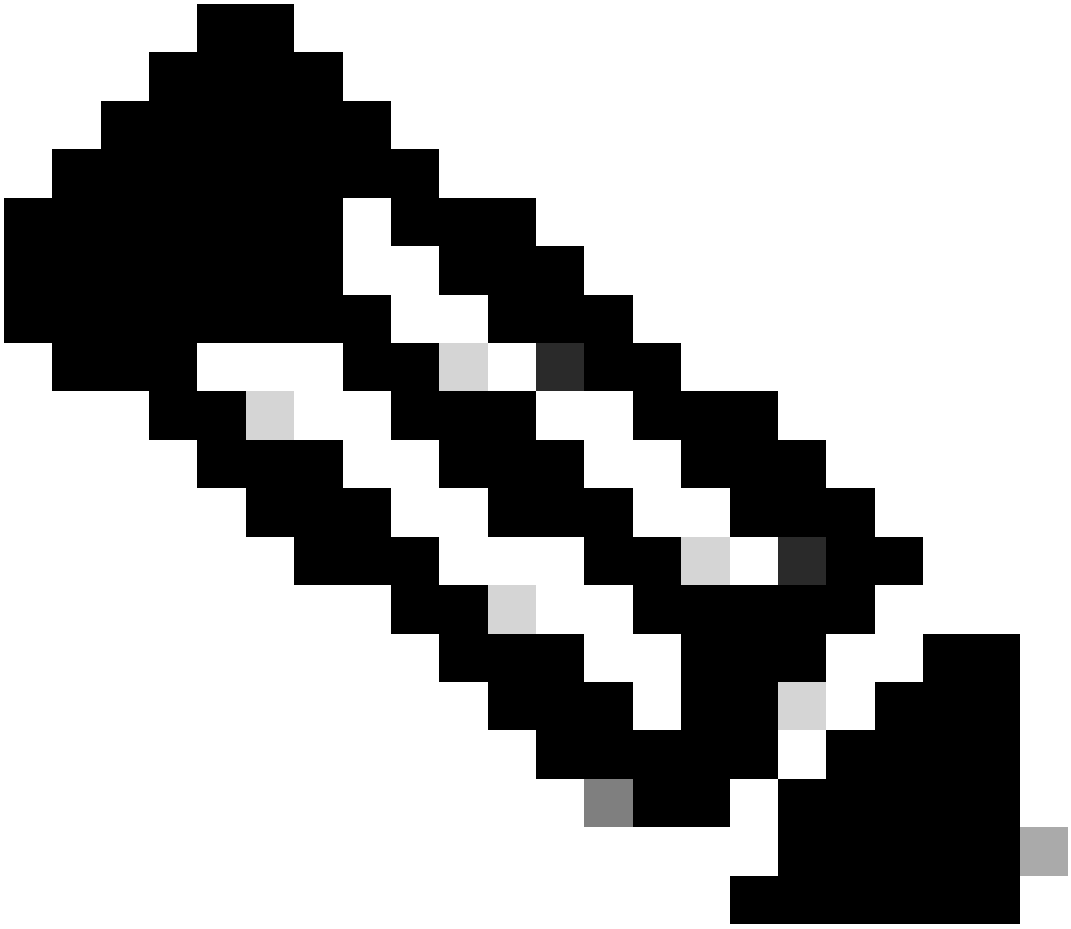
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)#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



Nota: El nombre de la clave RSA se reutiliza en todos los dispositivos para mantener la coherencia y no afecta a otros ajustes, ya que cada clave RSA es única en su valor computacional.

2.- El certificado de la CA se debe instalar primero en el punto de confianza. Esto se puede hacer autenticando el punto de confianza o inscribiéndose directamente. Dado que no hay ningún certificado de CA instalado anteriormente, se activa primero el procedimiento de autenticación de punto de confianza.

Servidor de claves

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.

Miembro del grupo

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-Verifique en ambos dispositivos que los certificados recién emitidos se importen en sus

respectivos puntos de confianza autenticados (el certificado de CA también debe importarse) mediante el comando 'show crypto pki certificates verbose'.

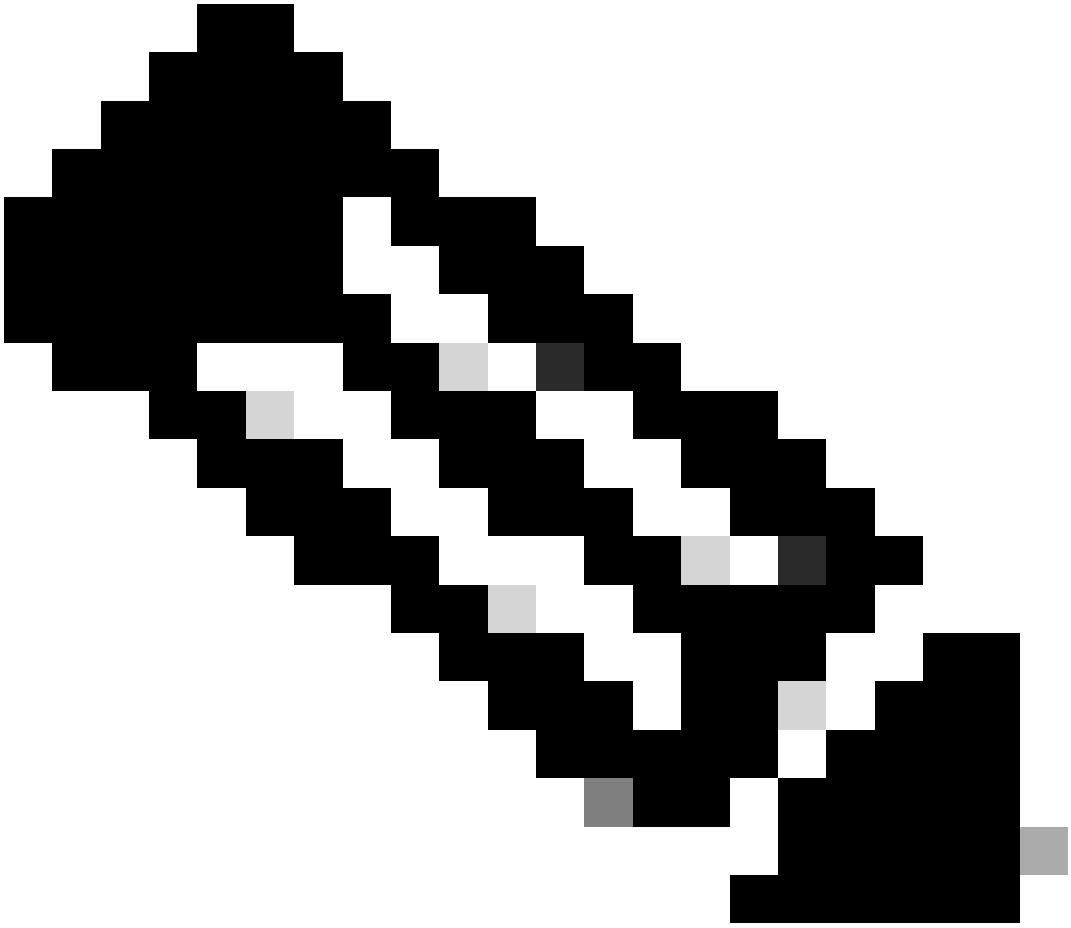
Servidor de claves

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

Miembro del grupo

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



Nota: Para la autenticación de certificados, asegúrese de que el certificado proporcionado tiene los parámetros correctos para validar la identidad del dispositivo, como el nombre común (CN), el uso extendido de claves (EKU) y la fecha de validez.

Configuración de GETVPN

Las características importantes de GETVPN se basan en la configuración anterior, que se recomienda haber configurado antes que las características ISAKMP y GDOI.

4.- En el servidor de claves principal, generar una clave RSA exportable con la etiqueta 'getKey'. Esta clave debe ser idéntica en todos los servidores de claves. Por lo tanto, la característica exportable es esencial para los siguientes pasos:

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.- Definir una lista de acceso extendida con el tráfico interesante que los routers del Grupo

Miembro deben cifrar al pasar a través. En el servidor de claves secundario, defina la misma lista de acceso con el mismo nombre.

Servidor de clave principal

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

Servidor de claves secundarias

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- Configure la política ISAKMP , el conjunto de transformación IPsec y el perfil IPsec utilizados para establecer la conectividad segura con los GM para comenzar con el intercambio de mensajes de grupo GDOI.

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**

Configuración de COOP

7.- En una implementación Cooperativa, los Servidores Clave involucrados deben tener una configuración idéntica. Exporte la clave RSA exportable creada anteriormente desde el servidor de claves principal e importe las claves pública y privada en el servidor de claves secundario (KS2). En un escenario en el que el servidor de claves principal deja de responder, el servidor de claves secundario continúa con el control de la regeneración de claves para todos los dispositivos GM dentro del grupo.

Servidor de clave principal

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-----

Servidor de claves secundarias

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- Se debe configurar el ISAKMP periódico para los COOP KS. De esta manera, el KS primario puede monitorear los servidores de claves secundarios

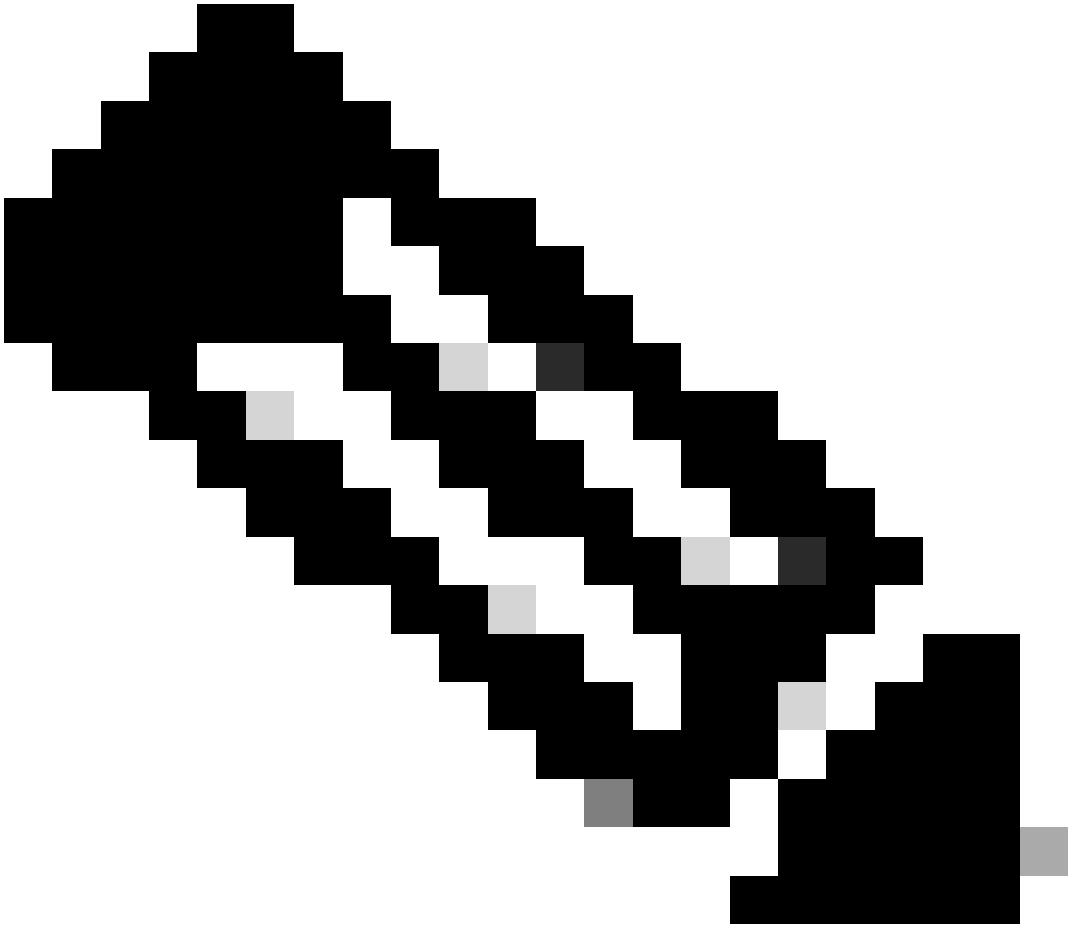
Servidor de clave principal

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

Servidores de claves secundarias

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

Los servidores de claves COOP intercambian comunicación unidireccional de principal a secundario. Si un KS secundario no oye del KS primario durante un intervalo de 30 segundos, el KS secundario intenta ponerse en contacto con el KS primario y solicita información actualizada. Si el KS secundario no recibe información del KS primario durante un intervalo de 60 segundos, se activa un proceso de reelección de COOP y se elige un nuevo KS primario.



Nota: No se requiere DPD periódica entre GM y KS.

La elección entre los servidores de claves se basa en el valor de prioridad más alta configurado. Si son iguales, se basa en la dirección IP más alta. Configure en cada servidor de claves el mismo grupo GDOI utilizando las mismas políticas de cifrado, listas de acceso ampliadas.

Servidor de clave principal

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.- Dentro de la misma configuración del servidor local, habilite las políticas criptográficas destinadas al tráfico del plano de datos y la lista de acceso que se configuraron previamente.

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

En la configuración del servidor local está el nivel de configuración en el que se habilita la función de servidor de claves COOP, la prioridad definida decide la función para este servidor de claves. Los servidores de claves secundarios deben configurarse explícitamente para que todos los KS se conozcan entre sí.

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**

La parte final de la configuración del servidor de claves COOP es la definición de la dirección IP de origen del paquete de claves, que es una dirección IP configurada en una de las interfaces del router del servidor de claves.

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

Replique los mismos pasos de configuración en el Servidor de claves secundarias, configurando una prioridad inferior para identificar el router como servidor secundario y registrar la dirección KS principal.

Servidor de claves secundarias

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.- En un router de miembro de grupo, la configuración del grupo GDOI consiste en menos configuración en comparación con los servidores de claves. Un miembro del grupo sólo necesita tener la política ISAKMP configurada , utilizar el mismo método de autenticación, el grupo GDOI, y

tener las direcciones IP de los servidores de claves con los que el router GM puede registrarse.

Miembro del grupo

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**

Miembro del grupo 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**

Verificación

Verifique las configuraciones de cada etapa de la configuración de la siguiente manera:

ACL para tráfico de plano de datos en servidores de claves

Este comando show se utiliza para corroborar que no hay errores con el tráfico interesante definido.

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

Estado de registro de COOP:

El comando 'show crypto gkm ks coop' muestra el estado COOP actual entre los servidores de claves, indicando quién es el servidor de claves principal, el grupo GDOI al que pertenecen, su prioridad individual y de peer y los temporizadores con respecto a los siguientes mensajes a enviar de los servidores primarios a los secundarios.

Servidor de clave principal

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

Servidor de claves secundarias

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

Muestra información del grupo GETVPN e información de versión sobre el servidor de claves cooperativo.

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

Registro de miembros de grupo

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

Troubleshoot

elección del servidor de claves COOP

Los mensajes de syslog pueden ayudar en el seguimiento e identificación de problemas con el proceso COOP. Habilite la depuración GDOI en los servidores de claves COOP para mostrar información relacionada solamente con este proceso.

KS# **debug crypto gdoi ks coop**

Cuando comienza el proceso de elección de COOP, el siguiente mensaje de syslog se ve en todos los servidores de claves.

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

Después de completar el proceso de elección, el mensaje "COOP_KS_TRANS_TO_PRI" muestra información sobre el nuevo servidor de claves principal, el mensaje se ve en los servidores de claves principal y secundaria. Se espera que la Primaria anterior muestre "NONE" en la primera vez del proceso electoral.

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

Si hay una reelección del servidor de claves, el mensaje incluye la dirección IP del servidor principal anterior.

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

Cuando se pierde la conectividad con los servidores de claves secundarias COOP, se muestra el mensaje "COOP_KS_UNREACH". El KS primario rastrea el estado de todos los KS secundarios y utiliza este mensaje para indicar la pérdida de conectividad a un KS secundario. Un KS secundario sólo rastrea el estado del KS primario. Este mensaje en el KS secundario indica pérdida de conectividad con el KS primario.

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

Cuando se restaura la conectividad entre los COOP KS, se muestra un mensaje "COOP_KS_REACH".

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

Problemas de inscripción PKI

Cuando depure problemas de inscripción o autenticación de trustpoint, utilice depuraciones PKI.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).