Configure GETVPN with COOP Key Servers and Certificate Authentication

Contents

Introduction

This document describes how to configure Group Encrypted Transport VPN (GETVPN) to use digital certificates for authentication and COOP Key Servers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Group Encrypted Transport VPN (GETVPN)

- Public Key Infrastructure (PKI)

- Certificate Authority (CA)

Components Used

The information in this document is based on these software versions:

- CSR1000V - Cisco IOS® XE, Version 16.12.03 - as Cisco IOS® XE Key Server, Group Member and CA Server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

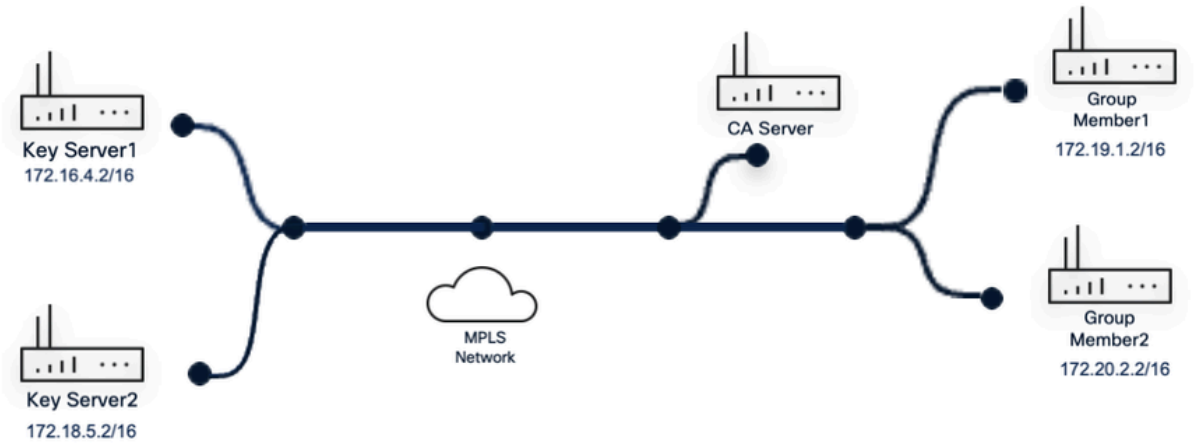
Background Information

In a GETVPN deployment, the Key Server is the most important entity because the KS maintains the control plane. With a single device to manage a complete GETVPN group, it creates a single point of failure.

To mitigate this scenario, GETVPN supports multiple Key Servers called cooperative (COOP) KSs which provide redundancy and recovery if a Key Server becomes unreachable.

Configure

Network Diagram



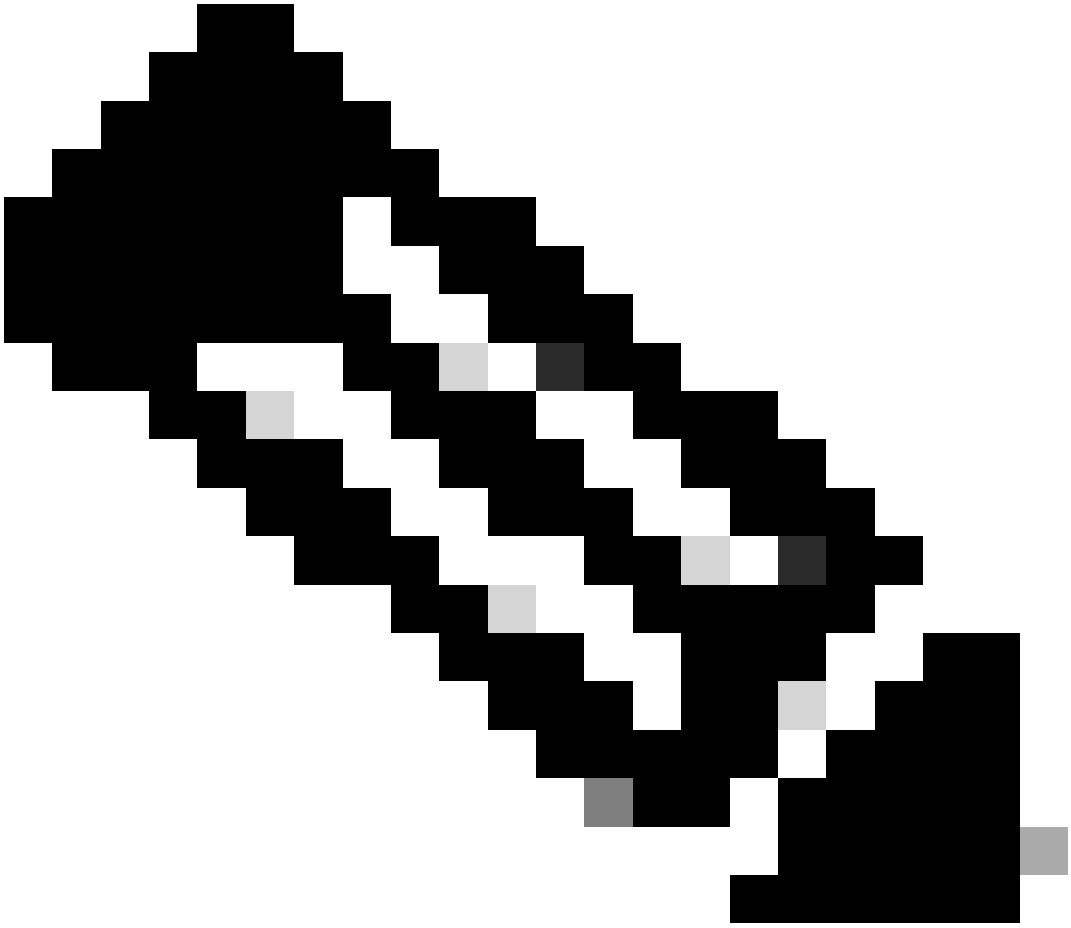
GETVPN Topology

Configurations

PKI for authentication

PKI uses its infrastructure to overcome the key management difficulties encountered when using PSKs. The PKI infrastructure acts as a certificate authority (CA) which issues (and then maintains) identity certificates.

Any Group Member router whose certificate information matches the ISAKMP identity is authorized and can register to the KS.



Note: Certificates can be issued by any CA. For this guide, a CSR1000V is configured as a CA to issue certificates to all devices in the deployment to authenticate their identity.

CA# **show crypto pki server**

crypto pki server ca-server

database level complete

database archive pkcs12 password 7 1511021F07257A767B73

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

grant auto hash sha255

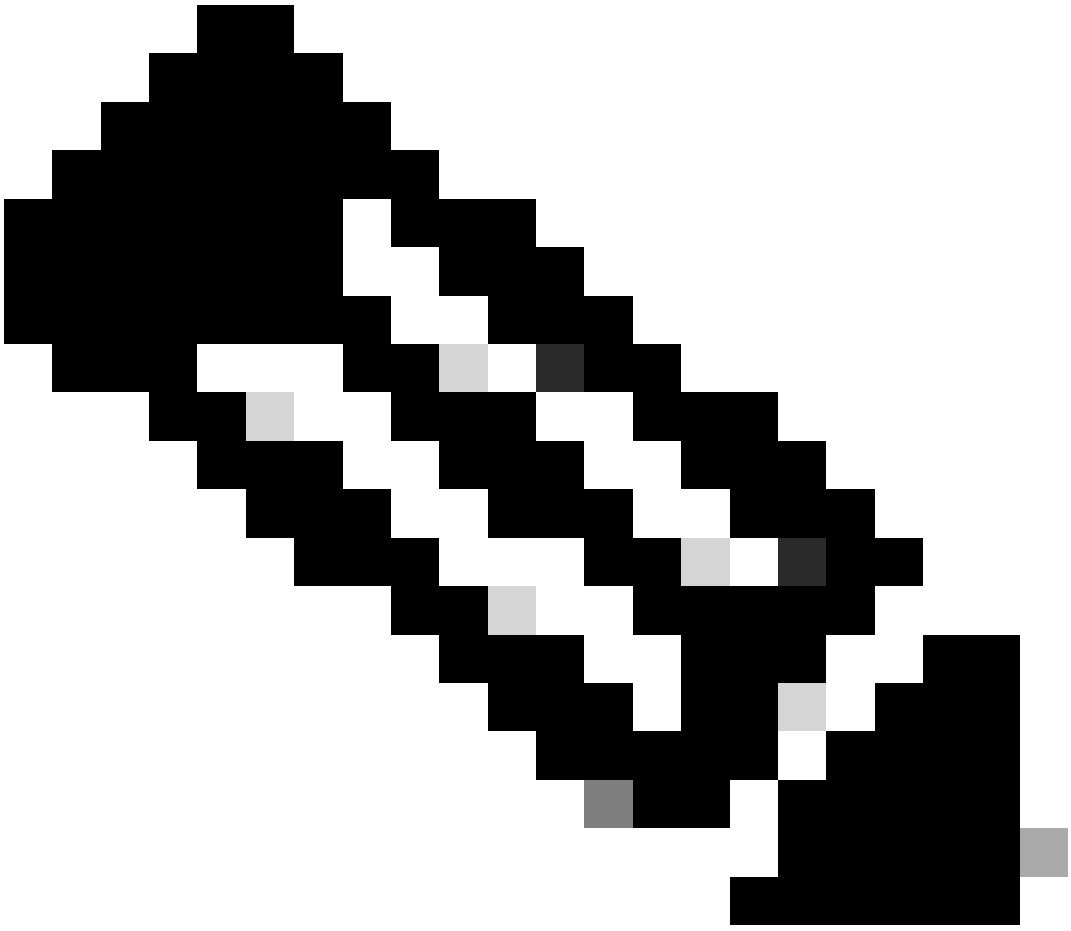
lifetime certificate 5000

lifetime ca-certificate 7300

eku server-auth client-auth

database url nvram

1.- In PKI-based deployments, the identity certificate from a certificate authority (CA) for each device must be obtained. In the Key Server and Group Member routers, create a RSA keypair used in their trustpoint configuration.



> **Note**: For the purpose of the demonstration of this guide, all Key Servers and Group Members routers in this topology share the same configuration.

Key Server

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**

Group Member

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**

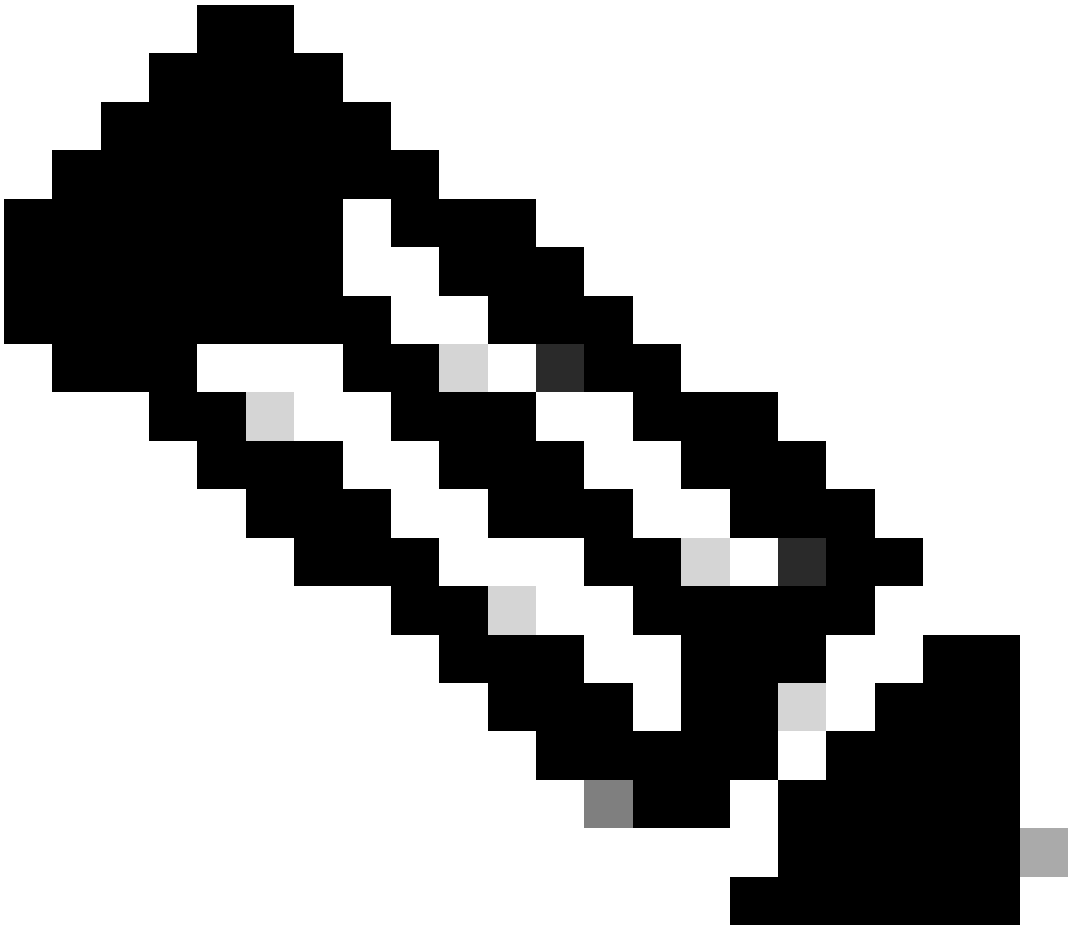
trustpoint GETVPN GM(ca-trustpoint)# **enrollment url http://10.191.61.120:80**

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**



Note: The RSA key name is reused on all devices to keep consistency and it does not affect other settings because each RSA key is unique in its computational value.

2.- The certificate from the CA must be installed first in the trustpoint. This can be done either by authenticating the trustpoint or enrolling directly. Because there is no CA certificate previously installed, the trustpoint authentication procedure is triggered first.

Key Server

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.

Group Member

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-Verify on both devices the newly issued certificates are imported in their respective authenticated trustpoints (the CA certificate must be imported as well) using the command 'show crypto pki certificates verbose'.

Key Server

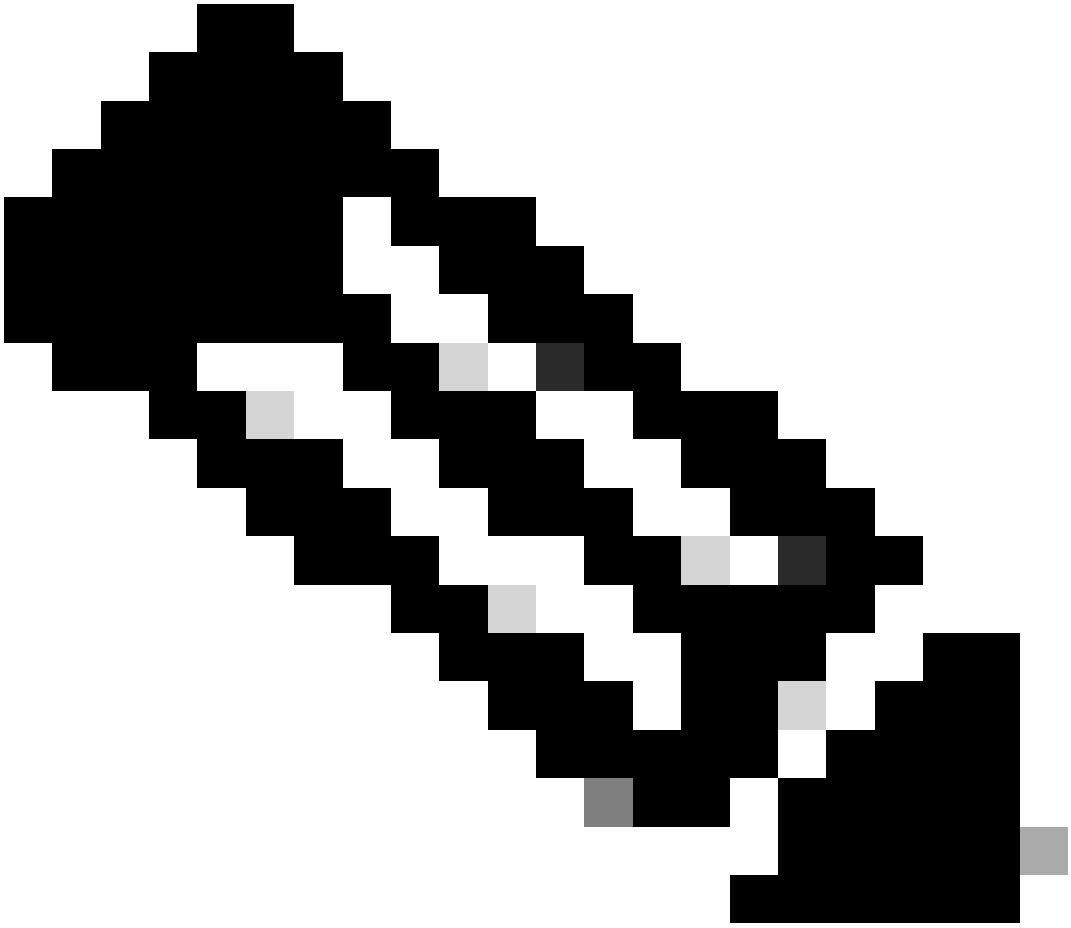
KS# **show crypto pki certificates verbose GETVPN**

. **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

Group Member

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



Note: For certificate authentication, make sure the provided certificate has the correct parameters to validate the identity of the device such as the Common Name (CN), Extended Key Usage (EKU), Validity Date.

Configure GETVPN

Important features of GETVPN rely on the previous configuration which is recommended to have configured before ISAKMP and GDOI features.

4.- On the primary Key Server, generate an exportable RSA key with the label 'getKey'. This key must be identical on all Key Server. Therefore, the exportable feature is essential for the next steps:

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.- Define an extended access-list with the interesting traffic that the Group Member routers must encrypt when passing through. On the secondary Key Server, define the same access-list using the same name.

Primary Key Server

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

Secondary Key Server

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 the ISAKMP policy , IPsec trasnform-set, and IPsec profile used to establish the secure connectivity with the GMs to begin with the GDOI group message exchange.

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**

Configuring COOP

7.- In a Cooperative implementation, the Key Servers involved must have an identical configuration. Export the previously created exportable RSA key from the primary Key Server and import both private and public keys into the secondary Key Server (KS2). In a scenario where the primary Key Server becomes unresponsive, the secondary Key Server continues with the control of the rekey to all GM devices within the group.

Primary Key Server

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-----

Secondary Key Server

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- Periodic ISAKMP must be configured for the COOP KSs. This way, the primary KS can monitor the secondary Key Servers

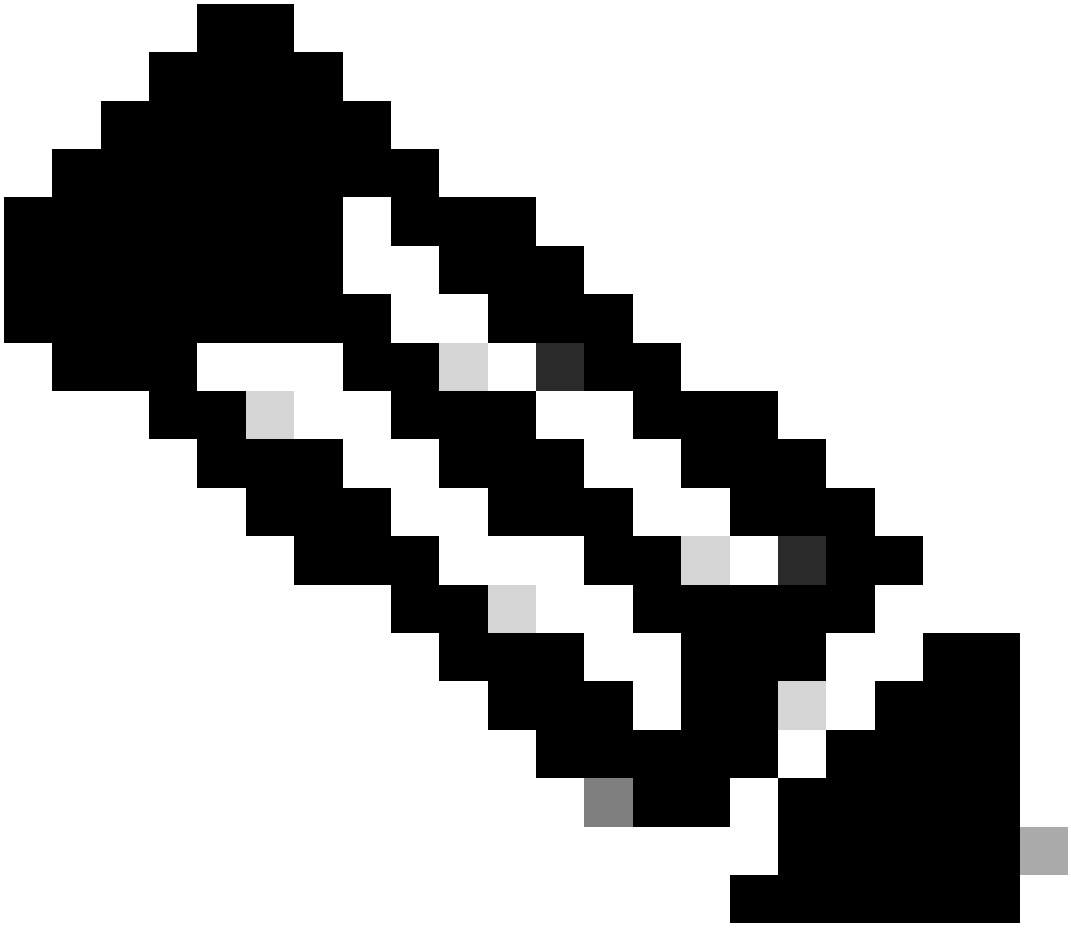
Primary Key Server

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

Secondary Key Servers

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

COOP Key Servers exchange one-way communication from primary to secondary. If a secondary KS does not hear from the primary KS over a 30 second interval, the secondary KS tries to contact the primary KS and requests updated information. If the secondary KS does not hear from the primary KS over a 60 second interval, a COOP reelection process is triggered and a new primary KS is elected.



Note: Periodic DPD between GM and KS is not required.

Election between the Key Servers is based on the highest-priority value configured. If they are same, it is based on highest IP address. Configure on each Key Server the same GDOI group using the same crypto policies, extended access-lists.

Primary Key Server

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.- Within the same local server settings, enable the crypto policies intended for the data-plane traffic and the access-list that were previously configured.

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

Over the local server settings is the configuration level where the COOP key server function is enabled, the priority defined decides the role for this Key Server. The secondary Key Servers must be configured

explicitly so all KS are aware of each other.

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**

The final part of the COOP Key Server configuration is the definition of the source IP address of the key packet, which is an IP address configured in one of the interfaces of the Key Server router.

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

Replicate the same configuration steps on the Secondary Key Server, configuring a lower priority to identify the router as a secondary server and register the primary KS address.

Secondary Key Server

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.- Over a Group Member router, the GDOI group settings consists of less configuration in comparison with the Keys Servers. A group member is only required to have the ISAKMP policy configured , use the same authentication method, GDOI group, and have the IP addresses of the Key Servers the GM router is able to register to.

Group Member

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**

Group Member 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**

Verify

Verify the settings from every stage of the configuration as follows:

ACLs for data-plane traffic on Key Servers

This show command is used to corroborate the are no mistakes with the interesting traffic defined.

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 registration status:

The command '**show crypto gkm ks coop**' displays the current COOP status between the Key Servers, indicating who the primary Key Server is, the GDOI group they belong to, their individual and peer priority and timers regarding the next messages to send from primary to secondary servers.

Primary Key Server

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

Secondary Key Server

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

Displays information for the group GETVPN and version information about the cooperative key server.

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

Group Member registration

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

COOP Key Server election

The syslog messages can help in track and identify issues with the COOP process. Enable GDOI debugging on the COOP Key Servers to display information related on this process only.

KS# **debug crypto gdoi ks coop**

When the COOP election process begins, the next syslog message is seen on all Key Servers.

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

After completing the election process, the message "**COOP_KS_TRANS_TO_PRI"** displays information about the new primary Key Server, the message is seen on primary and secondary Key Servers. The Previous Primary is expected to show "**NONE**" at the first time of the election process.

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

If there is Key Server reelection the message includes the IP address of the previous primary server.

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

When connectivity gets lost to COOP Secondary Key Servers, the "**COOP_KS_UNREACH"** message is displayed. Primary KS tracks the state of all secondary KSs and uses this message to indicate loss of connectivity to a secondary KS. A secondary KS only tracks the state of the primary KS. This message on the secondary KS indicates loss of connectivity with the primary KS.

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

When the connectivity is restored among the COOP KSs, a "**COOP_KS_REACH**" message is displayed.

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

PKI enrollment issues

When debugging trustpoint enrolling or authenticating issues, use PKI debugs.

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