

Configurar o GETVPN com servidores de chaves COOP e autenticação de certificado

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[PKI para autenticação](#)

[Configurar GETVPN](#)

[Configurando o COOP](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o Group Encrypted Transport VPN (GETVPN) para usar certificados digitais para autenticação e servidores de chave COOP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN de transporte criptografado de grupo (GETVPN)
- Public Key Infrastructure (PKI)
- autoridade de certificado (CA)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- CSR1000V - Cisco IOS® XE, Versão 16.12.03 - como servidor de chave Cisco IOS® XE, membro do grupo e servidor CA.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

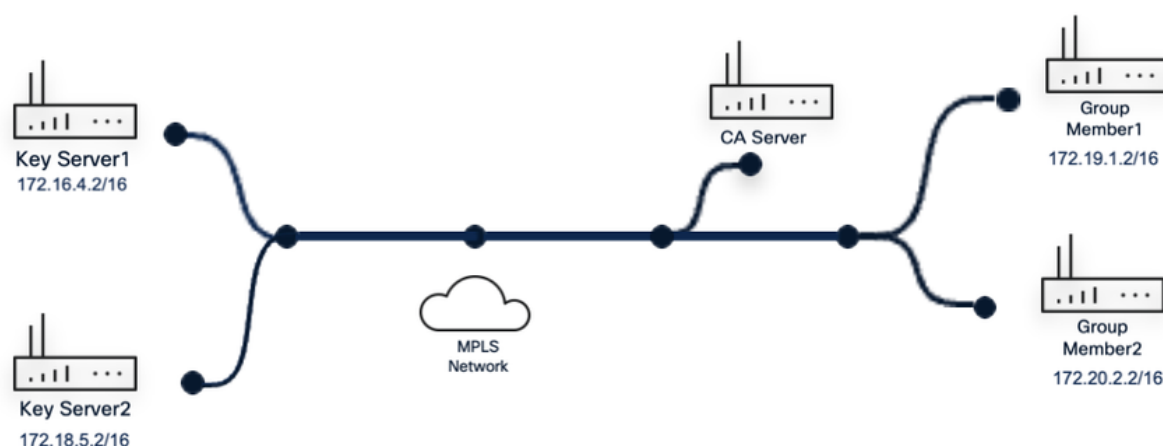
Informações de Apoio

Em uma implantação de GETVPN, o servidor de chaves é a entidade mais importante porque o KS mantém o plano de controle. Com um único dispositivo para gerenciar um grupo GETVPN completo, ele cria um único ponto de falha.

Para mitigar este cenário, o GETVPN suporta vários Servidores de Chaves chamados KSs cooperativos (COOP) que fornecem redundância e recuperação se um Servidor de Chaves se tornar inalcançável.

Configurar

Diagrama de Rede



Topologia GETVPN

Configurações

PKI para autenticação

A PKI usa sua infraestrutura para superar as principais dificuldades de gerenciamento encontradas ao usar PSKs. A infraestrutura da PKI atua como uma autoridade de certificação (CA) que emite (e depois mantém) certificados de identidade.

Qualquer roteador membro do grupo cujas informações de certificado correspondam à identidade de ISAKMP é autorizado e pode se registrar no KS.



Note: Os certificados podem ser emitidos por qualquer CA. Para este guia, um CSR1000V é configurado como uma CA para emitir certificados para todos os dispositivos na implantação para autenticar sua identidade.

CA# show crypto pki server

crypto pki server ca-server

nível de banco de dados concluído

database archive pkcs12 password 7 1511021F07257A767B73

nome do emissor CN=Root-CA.cisco.com OU=LAB

grant auto hash sha255

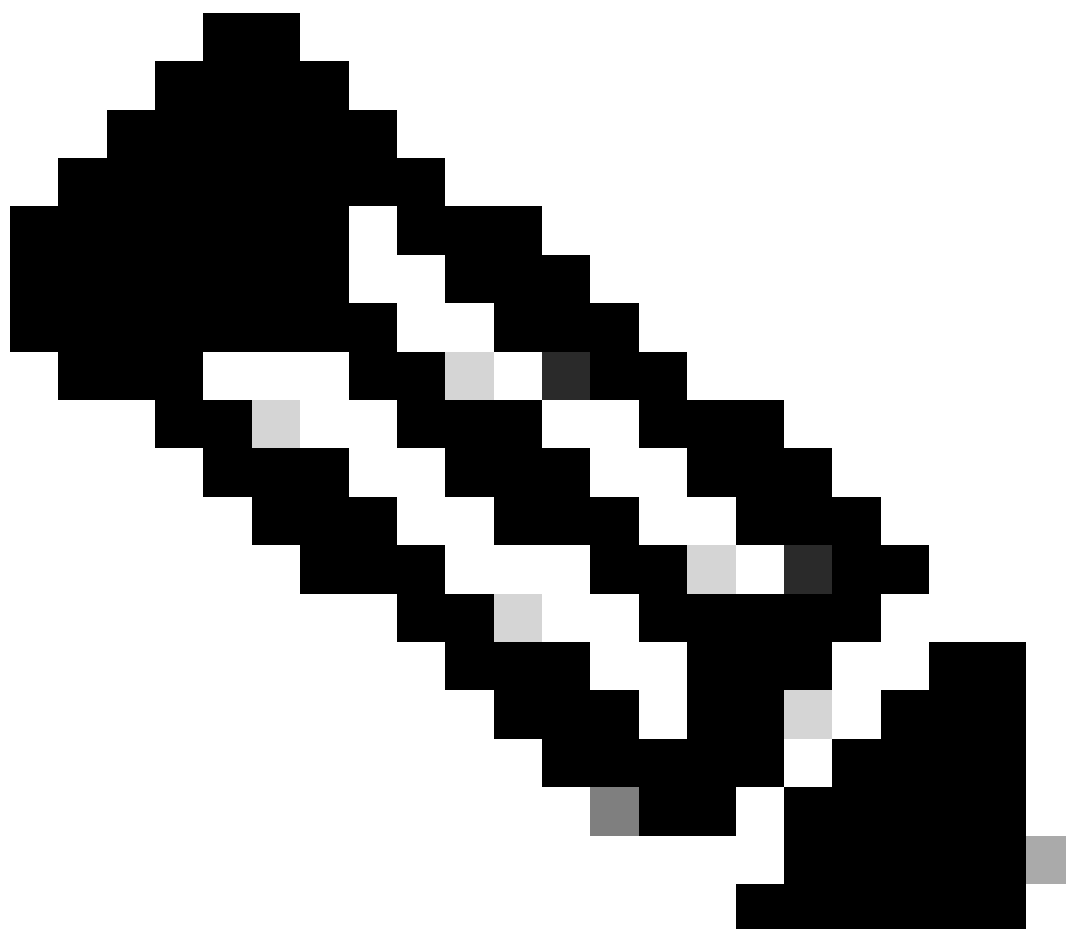
lifetime certificate 5000

lifetime ca-certificate 7300

eku server-auth client-auth

nvram de url de banco de dados

1.- Em implantações baseadas em PKI, o certificado de identidade de uma autoridade de certificação (CA) para cada dispositivo deve ser obtido. Nos roteadores do servidor de chaves e do membro do grupo, crie um par de chaves RSA usado na configuração do ponto confiável.



Note: Para fins de demonstração deste guia, todos os servidores de chave e roteadores membros do grupo nesta topologia compartilham a mesma configuração.

Servidor de chaves

```
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**

Membro do grupo

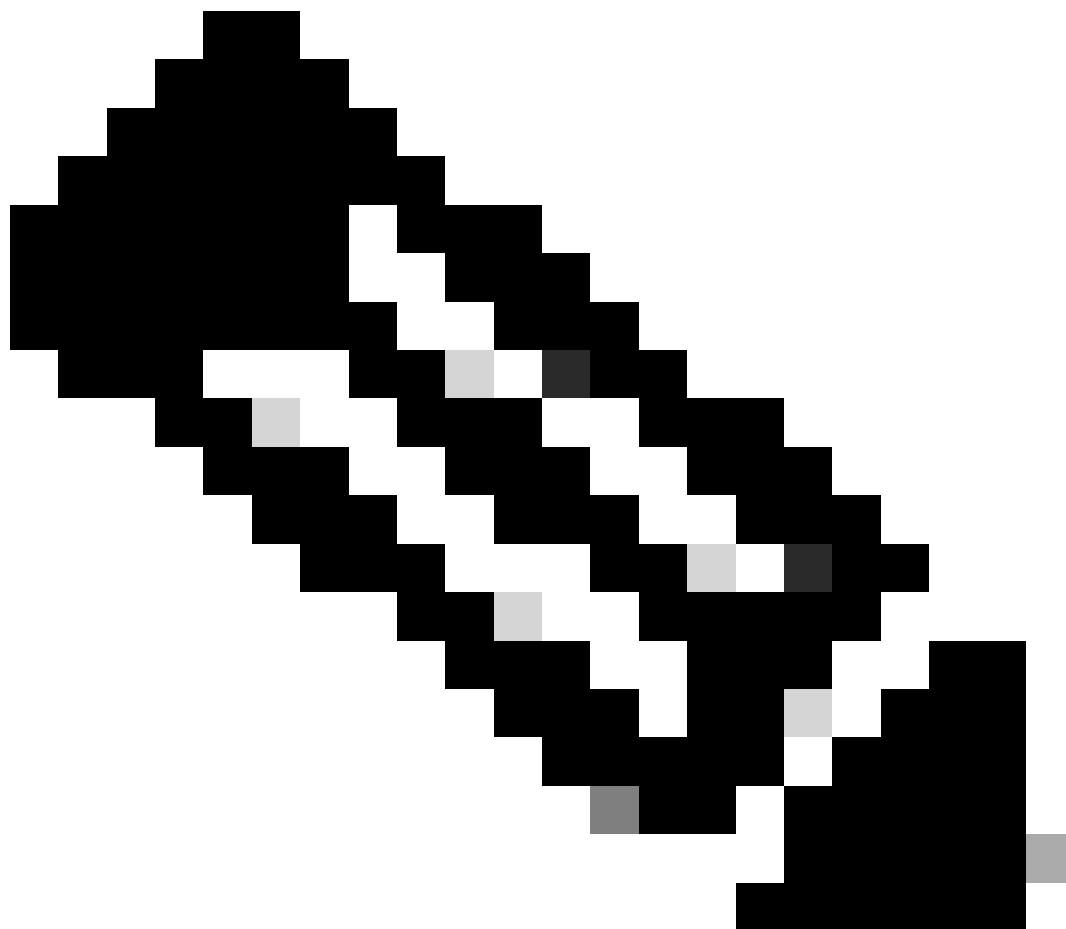
GM(config)# **crypto key generate rsa modulus 2049 general-keys label pkikey** The name for the keys will be: **pkikey** % The key modulus size is 2049 bits % Generating 2049 bit RSA keys, keys are non-exportable... [OK] (elapsed time was 0 seconds) GM(config)# **crypto pki trustpoint GETVPN** GM(ca-trustpoint)#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



Note: O nome da chave RSA é reutilizado em todos os dispositivos para manter a consistência e não afeta outras configurações porque cada chave RSA é exclusiva em seu valor computacional.

2.- O certificado da CA deve ser instalado primeiro no ponto confiável. Isso pode ser feito autenticando o ponto confiável ou se inscrevendo diretamente. Como não há nenhum certificado CA instalado anteriormente, o procedimento de autenticação de ponto confiável é disparado primeiro.

Servidor de chaves

```
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.

Membro do 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' command will show the fingerprint.

3-Verifique se em ambos os dispositivos os certificados emitidos recentemente são importados

em seus respectivos pontos de confiança autenticados (o certificado CA também deve ser importado) usando o comando 'show crypto pki certificates verbose'.

Servidor de chaves

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

Membro do 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



Note: Para autenticação de certificado, certifique-se de que o certificado fornecido tenha os parâmetros corretos para validar a identidade do dispositivo, como Nome comum (CN), Uso estendido de chave (EKU), Data de validade.

Configurar GETVPN

Recursos importantes do GETVPN dependem da configuração anterior, que é recomendável ter configurado antes dos recursos ISAKMP e GDOI.

4.- No servidor de chave primário, gere uma chave RSA exportável com o rótulo 'getKey'. Esta chave deve ser idêntica em todos os servidores de chaves. Portanto, o recurso exportável é essencial para as próximas etapas:

```
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.- Defina uma lista de acesso estendida com o tráfego interessante que os roteadores do

membro do grupo devem criptografar ao passar. No servidor de chaves secundário, defina a mesma lista de acesso usando o mesmo nome.

Servidor de Chave Primária

```
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 chave secundária

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

6- Configure a política ISAKMP , o conjunto de transformação IPsec e o perfil IPsec usados para estabelecer a conectividade segura com os GMs para começar com a troca de mensagens do 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
```

Configurando o COOP

7.- Em uma implementação cooperativa, os servidores de chave envolvidos devem ter uma configuração idêntica. Exporte a chave RSA exportável criada anteriormente do servidor de chaves primário e importe as chaves privadas e públicas para o servidor de chaves secundário (KS2). Em um cenário em que o servidor de chave primário não responde, o servidor de chave secundário continua com o controle da chave para todos os dispositivos do GM no grupo.

Servidor de Chave Primária

```
KS(config)# crypto key export rsa getKey pem terminal 3des cisco123 % Key name: getKey Usage: General Purpose Key Key data: -----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBA dGV3ZPaGQcsAqO1H9gmJWJNEeQvTND/oSrhN+jSSm+8f27RvDnIMYLDl9MndZ+rPqCPM/3NxE075bOsrT7B2uOpCBmAJK9iiTsr01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGS zbaErQCH7evvjutYHE6DhOTTLubxQIDAQAB -----END PUBLIC KEY----- -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,AA98923B28E00DCCto1Wym6cRvqEXBl97UZdGyusf3cW/iumb7oD9/09q5if4ouoE
```

```
brPykL3No0WMI7h56WQPiAHZLu5IZ+CTQHwwgYvXwHNpOHjmTMOgf9FG856GosM3kjP58QDupSc1W70+C9
```

```
zsCM3QmwbRs6JGBP5Rb36f+895xoyqzWA8G5sQlize1oP4lM3Zx5DukgTXLzIDL7w0dPEYBd1aDhAJQf8dB/Zu
```

```
GvQWxad4gL6SssEyzigbzdSdRwBS+0DLOm05hOUU8rNiWit1TCsTPflwuTjlyxgRbyKvtXdoURvuTP3M6/Doppe2
```

```
n26bXC2DcURk8nMtIrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb
```

```
AI286GHqCOW2AxDcoMzcanQYw1VNngHG7SUsbaday7enuJtwbf2Pjkf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C
```

2PkLiQvQwuYi8J9SgM+391aFr0NRXFHrM7T9MQcBBIcbo0BtfG4ICBulltpG+BpCty/XW99dvuhqh9hqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

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

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

Servidor de chave secundária

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-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFtHBAAdGV3ZPaGQcsAqO

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

5bOsrT7B2uOpCBmAJK9iiTsf01Qc4Izu5fwWcK2CN5OvLhyR2pKPviqwkSmGSz 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

n26bXC2DcURk8nMtlrIHAPvvh5KbxdyHtBrvgmlZH/ryKfx33fPoVu/TaYggMoWFTizfBgr643UoFOIcFgdhasQsn8Lb

AI286GHqCOw2AxDcoMzcanQYw1VNngHG7SUsbaday7enuJtwbf2PjKf9u0vo7bw2y8OiIXgrhQ9FOugNVqL+Ik7C

2PkLiQvQwuYi8J9SgM+391aFr0NRXFHrM7T9MQcBBIcbo0BtfG4ICBulltpG+BpCty/XW99dvuhqh9hqfy2sKqF4H

K3EGAmhHSTV2wqxTvK/UQbNt7zbXwLGy326tDdYg6BSQYNjcaTADwPzd1PBa5JJJ1v9ZIRJSy42l7wWcuYAZpJ

9CRnKpLvW1CGhNqk5kmJzypqmurWtuzxJQiJhysp5halOicdjEKVVr1SHLOxxmCJ09rJe27degR2iwwvWQjewrA0K

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

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

quit

% Key pair import succeeded.

8- O ISAKMP periódico deve ser configurado para os KSs COOP. Desta forma, o KS primário pode monitorar os Servidores de Chaves secundários

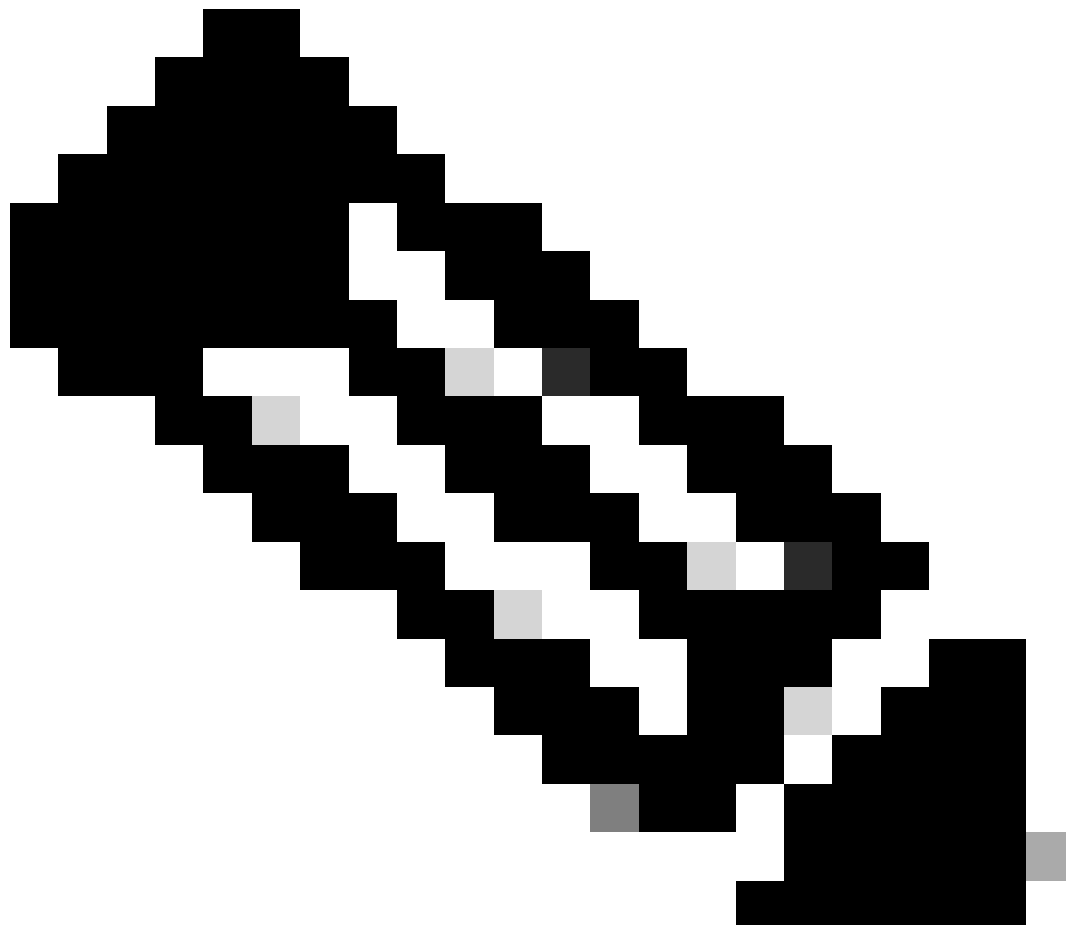
Servidor de Chave Primária

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

Servidores de chave secundária

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

Os Servidores de Chaves COOP trocam a comunicação unidirecional do primário para o secundário. Se um KS secundário não ouvir do KS primário durante um intervalo de 30 segundos, o KS secundário tenta contatar o KS primário e solicita informações atualizadas. Se o KS secundário não ouvir do KS primário durante um intervalo de 60 segundos, um processo de reeleição COOP é acionado e um novo KS primário é eleito.



Note: A DPD periódica entre GM e KS não é necessária.

A escolha entre os servidores de chaves é baseada no valor de prioridade mais alta configurado. Se forem iguais, será baseado no endereço IP mais alto. Configure em cada servidor de chaves o mesmo grupo GDOI usando as mesmas políticas de criptografia, listas de acesso estendidas.

Servidor de Chave Primária

```
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 das mesmas configurações de servidor local, ative as políticas de criptografia destinadas ao tráfego do plano de dados e à lista de acesso que foram configuradas anteriormente.

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

Nas configurações do servidor local está o nível de configuração em que a função de servidor de chave COOP está habilitada, a prioridade definida decide a função para esse Servidor de Chave. Os Servidores de Chaves secundários devem ser configurados explicitamente para que todos os KS estejam cientes um do outro.

```
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
```

A parte final da configuração do servidor de chaves COOP é a definição do endereço IP de origem do pacote de chaves, que é um endereço IP configurado em uma das interfaces do roteador do servidor de chaves.

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

Replique as mesmas etapas de configuração no servidor de chave secundário, configurando uma prioridade mais baixa para identificar o roteador como um servidor secundário e registrar o endereço primário KS.

Servidor de chave secundária

```
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.- Em um roteador Membro do Grupo, as configurações do grupo GDOI consistem em menos configuração em comparação com os Servidores de Chaves. Um membro do grupo só precisa ter

a política ISAKMP configurada , usar o mesmo método de autenticação, grupo GDOI e ter os endereços IP dos servidores de chaves nos quais o roteador GM pode se registrar.

Membro do 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
```

Membro do 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
```

Verificar

Verifique as configurações de cada estágio da configuração da seguinte maneira:

ACLs para tráfego de plano de dados em servidores de chave

Esse comando show é usado para confirmar que não há erros com o tráfego interessante 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
```

Status de registro COOP:

O comando 'show crypto gkm ks coop' exibe o status COOP atual entre os Servidores de Chave, indicando a quem o Servidor de Chave primário pertence, o grupo GDOI ao qual pertencem, sua prioridade individual e de peer e os temporizadores relativos às próximas mensagens a serem enviadas dos servidores primários para os secundários.

Servidor de Chave Primária

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

Servidor de chave secundária

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 rcvd: 0 New GM Temporary Blocking Enforced?: No Per-user timer remaining time: 0 Antireplay Sequence Number: 4 Peer Sessions: Session 1: Server handle: 1073741828 Peer Address: 10.191.61.114 Peer Version: 1.0.27 Peer Priority: 100 Peer KS Role: Primary , Peer KS Status: Alive Antireplay Sequence Number: 30 IKE status: Established Counters: Ann msgs sent: 2 Ann msgs sent with reply request: 1 Ann msgs rcv: 28 Ann msgs rcv with reply request: 1 Packet sent drops: 1 Packet Recv drops: 0 Total bytes sent: 468 Total bytes rcv: 16913

Exibe informações sobre o grupo GETVPN e informações de versão sobre o servidor de chave cooperativa.

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 membro do 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 sent : 0 ACL Downloaded From KS 10.191.61.115: access-list permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.255.255 access-list permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.0.0.255 KEK POLICY: Rekey Transport Type : Unicast Lifetime (secs) : 85185 Encrypt Algorithm : 3DES Key Size : 192 Sig Hash Algorithm : HMAC_AUTH_SHA Sig Key Length (bits) : 1296 TEK POLICY for the current KS-Policy ACEs Downloaded: GigabitEthernet1: IPsec SA: spi: 0x535F673B(1398761275) transform: esp-aes esp-sha-hmac sa timing:remaining key lifetime (sec): (5988) Anti-Replay(Counter Based) : 64 tag method : disabled alg key size: 16 (bytes) sig key size: 20 (bytes) encaps: ENCAPS_TUNNEL KGS POLICY: REG_GM: local_addr 10.191.61.116 overall check P2P POLICY: REG_GM: local_addr 10.191.61.116

Troubleshooting

Escolha do Servidor de Chaves COOP

As mensagens de syslog podem ajudar a rastrear e identificar problemas com o processo COOP. Ative a depuração GDOI nos servidores de chaves COOP para exibir somente informações

relacionadas a este processo.

KS# `debug crypto gdoi ks coop`

Quando o processo de eleição COOP começa, a próxima mensagem de syslog é vista em todos os servidores de chave.

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

Após a conclusão do processo de eleição, a mensagem "COOP_KS_TRANS_TO_PRI" exibe informações sobre o novo Servidor de Chave primário, a mensagem é vista nos Servidores de Chave primários e secundários. Espera-se que a primária anterior mostre "NONE" na primeira vez do processo de eleição.

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

Se houver reeleição do Servidor de Chaves, a mensagem incluirá o endereço IP do servidor primário anterior.

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

Quando a conectividade é perdida para os servidores de chave secundária COOP, a mensagem "COOP_KS_UNREACH" é exibida. O KS primário rastreia o estado de todos os KSs secundários e usa esta mensagem para indicar perda de conectividade para um KS secundário. Um KS secundário só rastreia o estado do KS primário. Essa mensagem no KS secundário indica perda de conectividade com o KS primário.

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

Quando a conectividade é restaurada entre os COOP KSs, uma mensagem "COOP_KS_REACH" é exibida.

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

Problemas de inscrição de PKI

Ao depurar problemas de inscrição ou autenticação de pontos confiáveis, use depurações de PKI.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.