

# Configurar DMVPN Fase 3 Usando IKEv2 com Autenticação de Certificado

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Preparar a infraestrutura do certificado](#)

[Configuração de criptografia IKEv2 e IPSec](#)

[Configuração do túnel](#)

[Verificar](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve informações sobre como configurar a Dynamic Multipoint VPN (DMVPN) fase 3 com autenticação de certificado usando IKEv2.

## Pré-requisitos

### Requisitos

A Cisco recomenda ter conhecimento dos seguintes tópicos:

- Conhecimento básico de DMVPN.
- Conhecimento básico do EIGRP.
- Conhecimento Básico de Infraestrutura de Chave Pública (PKI).

### Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Cisco C8000v (VXE) executando o Cisco IOS® versão 17.3.8a.

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.

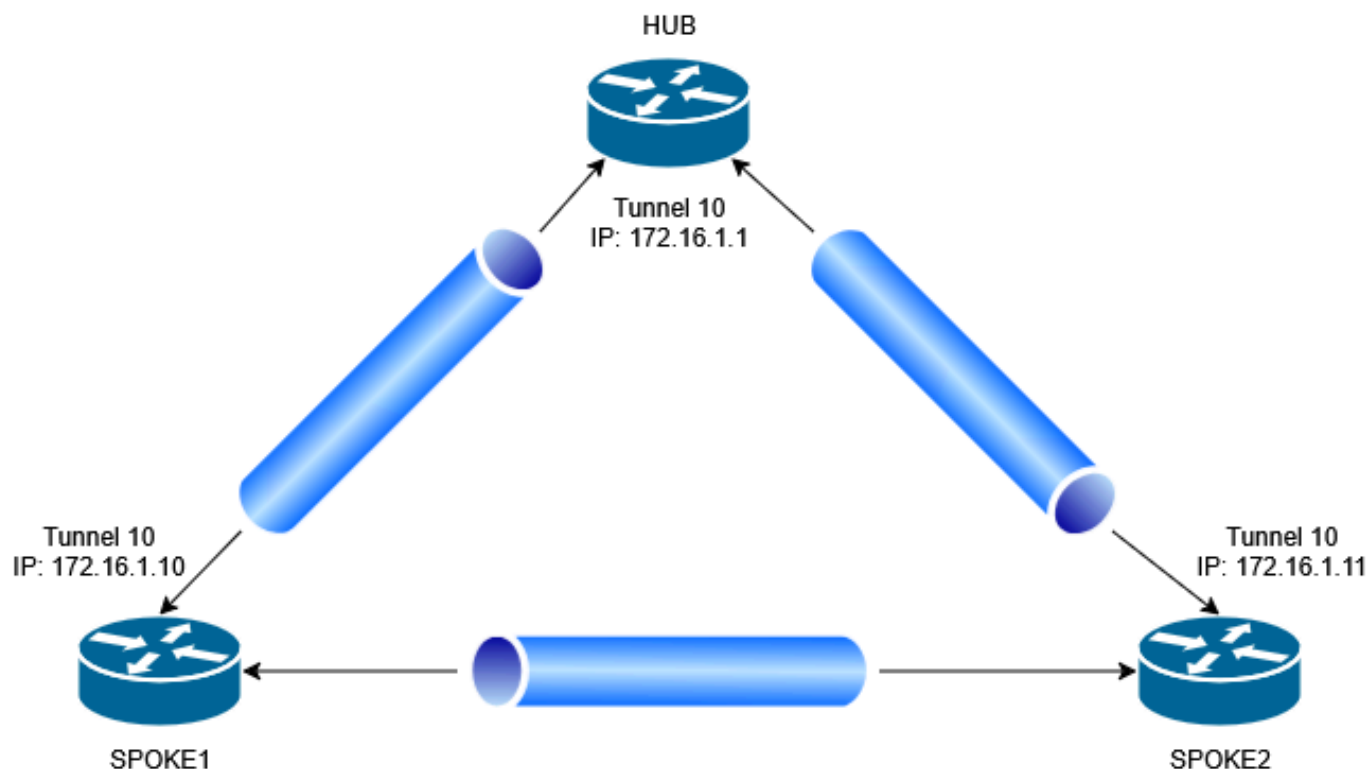
## Informações de Apoio

A Dynamic Multipoint VPN (DMVPN) Fase 3 introduz a conectividade direta spoke-to-spoke, permitindo que as redes VPN operem de forma mais eficiente ao ignorar o hub para a maioria dos caminhos de tráfego. Este design minimiza a latência e otimiza a utilização de recursos. O uso do Next Hop Resolution Protocol (NHRP) permite que os spokes identifiquem uns aos outros dinamicamente e criem túneis diretos, suportando topologias de rede grandes e complexas. O Internet Key Exchange versão 2 (IKEv2) fornece o mecanismo subjacente para estabelecer túneis seguros nesse ambiente. Comparado aos protocolos anteriores, o IKEv2 oferece medidas de segurança avançadas, processos de rechaveamento mais rápidos e suporte avançado para mobilidade e várias conexões. Sua integração com a Fase 3 do DMVPN garante que a configuração do túnel e o gerenciamento de chaves sejam tratados de forma segura e eficaz. Para fortalecer ainda mais a segurança da rede, o IKEv2 suporta autenticação de certificação digital. Essa abordagem permite que os dispositivos verifiquem identidades entre si usando certificados, o que simplifica o gerenciamento e reduz os riscos associados a segredos compartilhados. A confiança baseada em certificado é especialmente benéfica em implantações expansivas, nas quais o gerenciamento de chaves individuais seria desafiador. Juntos, a Fase 3 do DMVPN, o IKEv2 e a autenticação de certificado fornecem uma estrutura de VPN robusta. Essa solução atende aos requisitos de empresas modernas, garantindo conectividade flexível, proteção sólida de dados e operações simplificadas.

## Configurar

Esta seção fornece instruções passo a passo para configurar a Fase 3 do DMVPN com IKEv2 usando autenticação baseada em certificado. Conclua estas etapas para ativar a conectividade VPN segura e escalável entre os roteadores Hub e Spoke.

## Diagrama de Rede



## Configurações

Preparar a infraestrutura do certificado

Certifique-se de que todos os dispositivos (hubs e spokes) tenham os certificados digitais necessários instalados. Esses certificados devem ser emitidos por uma CA confiável e registrados corretamente em cada dispositivo para habilitar a autenticação de certificado IKEv2 segura. Para registrar um certificado em roteadores Hub e Spoke, siga estas etapas:

1. Configure um ponto confiável com as informações necessárias usando o comando `crypto pki trustpoint <Nome do Ponto Confiável>`.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki trustpoint myCertificate
```

```
Hub(ca-trustpoint)# enrollment terminal
```

```
Hub(ca-trustpoint)# ip-address 10.10.1.2
```

```
Hub(ca-trustpoint)# subject-name cn=Hub, o=cisco
```

```
Hub(ca-trustpoint)# revocation-check none
```

2. Autentique o ponto confiável usando o comando `crypto pki authenticate <Nome do ponto confiável>`.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki authenticate myCertificate
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

---

 **Observação:** depois de emitir o comando `crypto pki authenticate`, você deve colar o certificado da Autoridade de Certificação (CA) que é usada para assinar os certificados do dispositivo. Esta etapa é essencial para estabelecer a confiança entre o dispositivo e a CA antes de continuar com o registro de certificado nos roteadores Hub e Spoke.

---

3. Gere a chave privada e a CSR (Certificate Signing Request) usando o comando `crypto pki enroll <Trustpoint Name>`.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki enroll myCertificate
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will include: cn=Hub, o=cisco
```

```
% The subject name in the certificate will include: Hub
```

```
% Include the router serial number in the subject name? [yes/no]: n
```

```
% The IP address in the certificate is 10.10.1.2
```

```
Display Certificate Request to terminal? [yes/no]: yes
```

```
Certificate Request follows:
```

```
MIICsDCCAQgCAQAwSjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAMTA0hVQjEjEqMBAG
CSqGSIb3DQEJAhYDSFVCMByGCSqGSIb3DQEJCBMjMTAuMTAuMS4yMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAO/M40+ivsQJhpF0PRUxdCGSUVgLQUhzQ
cwnuMtSbfn5fMKIj7w06Qa7Gvx2rjrdoyxH9JgXjTEMzMv6HP9/EuN2o+qKzR/+
CNzMUDJobb01BNbe0WKL4IAQjbvNT0yA5iuUzHZCgMrCFG3oU7v+a2tMiSZihvdu
+m2JSDNXn5cXyewQbQsEaELA00yos12t6BQyzM3FRU23dCwnFVwY1VAADC7CrNh3
o44SiFYW5HtWq1tU1cLTY4sjNf6XJQxjmHPudbUp164RdfUSo37Zjvjt7S800oLU
+XUBrE3aRDlwJ+Ug2D031Zwzfc+rBZ1BsKWlYFB1Lk3mL9RA1nf3eQIDAQABoCEw
HwYJKoZIhvcNAQKOMRIwEDA0BgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
ggEBAEKUQRWZ+YeCx9T7kuzIaDwJ53vMqq6rITDJcNF9FJ4IgJ7PsxF0cWxm7MM
030i1yq1K/4X7Mb5Iz6CjtdyXVqakgcEPY7W9No03Xo8Nxb4pFfe19E02Xuj8fxm
GTqi7UAw8Zs1zJ2jrS7bXasVMb5jjr39cqQkrXfNIaWf1Sw6IA3oKfTelq8/iCJu
TEjF0D8Si2PWziuxJVS4Adjg5GxbJpd/tDKrKUuvqD2z4HD3M40oGVvoBWQ0tjhB
4gx1q2D209K0nMCvVZr0fp/PFd6+cYc57E73ZPVSGQpHIiWcYtuRKdKArN6vRcP
iiugceU2F3L14CI7wXMYqCxQOGU=
```

```
---End - This line not part of the certificate request---
```

```
Redisplay enrollment request? [yes/no]:
```

---

 **Note:** A chave privada usada durante esse processo é a chave privada padrão gerada pelo roteador. No entanto, o uso de chaves privadas personalizadas também é suportado, se necessário.

---

4. Depois de gerar o CSR, envie-o à Autoridade de Certificação (CA) para ser assinado.

5. Depois que o certificado for assinado, use o comando `crypto pki import <Nome do ponto de confiança> certificate` para importar o certificado assinado associado ao ponto de confiança criado.

```
<#root>
```

```
Hub(config)#
```

```
crypto pki import myCertificate certificate
```

```
% You must authenticate the Certificate Authority before  
you can import the router's certificate.
```

6. Cole o certificado assinado pela CA no formato PEM.

### Configuração de criptografia IKEv2 e IPSec

A configuração para Crypto IKEv2 e IPSec pode ser a mesma nos spokes e no hub. Isso ocorre porque elementos como as propostas e as cifras usadas devem sempre corresponder em todos os dispositivos para garantir que o túnel possa ser estabelecido com sucesso. Essa consistência garante a interoperabilidade e a comunicação segura no ambiente da fase 3 do DMVPN.

1. Configure uma proposta IKEv2.

```
crypto ikev2 proposal ikev2  
encryption aes-cbc-256  
integrity sha256  
group 14
```

2. Configure um perfil IKEv2.

```
<#root>
```

```
crypto ikev2 profile ikev2Profile  
match identity remote address 0.0.0.0  
identity local address 10.10.1.2  
  
authentication remote rsa-sig
```

```
authentication local rsa-sig
```

```
pki trustpoint
```

```
myCertificate
```



Note: Aqui é onde a autenticação do certificado PKI é definida e o ponto confiável usado para a autenticação.

---

### 3. Configure um perfil IPsec e um conjunto de transformação.

```
crypto ipsec transform-set ipsec esp-aes 256 esp-sha256-hmac
mode tunnel
crypto ipsec profile ipsec
set transform-set ipsec
set ikev2-profile ikev2Profile
```

## Configuração do túnel

Esta seção aborda a configuração de túneis para o Hub e os Spokes, focalizando especificamente a Fase 3 da configuração DMVPN.

### 1. Configuração de túnel de hub.

```
interface Tunnel10
ip address 172.16.1.1 255.255.255.0
no ip redirects
no ip split-horizon eigrp 10
ip nhrp authentication cisco123
ip nhrp network-id 10
ip nhrp redirect
tunnel source GigabitEthernet1
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

### 2. Configuração de túnel Spoke1.

```
interface Tunnel10
ip address 172.16.1.10 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
```

```
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet2
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

### 3. Configuração de túnel Spoke2.

```
interface Tunnel10
ip address 172.16.1.11 255.255.255.0
no ip redirects
ip nhrp authentication cisco123
ip nhrp map 172.16.1.1 10.10.1.2
ip nhrp map multicast 10.10.1.2
ip nhrp network-id 10
ip nhrp nhs 172.16.1.1
tunnel source GigabitEthernet3
tunnel mode gre multipoint
tunnel protection ipsec profile ipsec
end
```

## Verificar

Para confirmar se a rede DMVPN Fase 3 está funcionando corretamente, use estes comandos:

- show dmvpn interface <Tunnel Name>
- show crypto ikev2 sa
- show crypto ipsec sa peer <peer IP>

Com o comando show dmvpn interface <Tunnel Name>, você pode ver as sessões ativas entre o hub e os spokes. Da perspectiva de Spoke1, a saída pode refletir essas conexões estabelecidas.

<#root>

SPOKE1#

**show dmvpn interface tunnel10**

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete

N - NATed, L - Local, X - No Socket

T1 - Route Installed, T2 - Nexthop-override, B - BGP

C - CTS Capable, I2 - Temporary

# Ent --> Number of NHRP entries with same NBMA peer

NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting

UpDn Time --> Up or Down Time for a Tunnel

=====

Interface: Tunnel10, IPv4 NHRP Details

Type:Spoke, NHRP Peers:2,

```
# Ent Peer NBMA Addr Peer Tunnel Add
```

#### State

```
UpDn Tm Attrb
-----
 1 10.10.1.2          172.16.1.1
```

#### UP

```
1w6d S
 1 10.10.3.2          172.16.1.11
```

#### UP

```
00:00:04 D
```

O comando `show crypto ikev2 sa` sa exibe os túneis IKEv2 formados entre os spokes e o hub, confirmando negociações bem-sucedidas da Fase 1.

```
<#root>
```

```
SPOKE1#
```

```
show crypto ikev2 sa
```

```
IPv4 Crypto IKEv2 SA
```

```
Tunnel-id Local Remote fvrf/ivrf
```

#### Status

```
1 10.10.2.2/500 10.10.3.2/500 none/none
```

#### READY

```
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
```

#### RSA

```
Life/Active Time: 86400/184 sec
```

```
Tunnel-id Local Remote fvrf/ivrf
```

#### Status

```
2 10.10.2.2/500 10.10.1.2/500 none/none
```

#### READY

```
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
```

#### RSA



Life/Active Time: 86400/37495 sec

IPv6 Crypto IKEv2 SA

Usando o comando `show crypto ipsec sa peer <peer IP>`, você pode verificar os túneis IPSec estabelecidos entre os spokes e o hub, garantindo o transporte seguro de dados dentro da rede DMVPN.

<#root>

SPOKE1#show

**crypto ipsec sa peer 10.10.3.2**

interface: Tunnel10

Crypto map tag: Tunnel10-head-0, local addr 10.10.2.2

protected vrf: (none)

local ident (addr/mask/prot/port): (10.10.2.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (10.10.3.2/255.255.255.255/47/0)

current\_peer 10.10.3.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.10.2.2, remote crypto endpt.: 10.10.3.2

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2

current outbound spi: 0xF341E02E(4081180718)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x8ED55E26(2396347942)

transform: esp-256-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2701, flow\_id: CSR:701, sibling\_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0

sa timing: remaining key lifetime (k/sec): (4607999/3188)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0xF341E02E(4081180718)

transform: esp-256-aes esp-sha256-hmac ,

in use settings ={Tunnel, }

conn id: 2702, flow\_id: CSR:702, sibling\_flags FFFFFFFF80000048, crypto map: Tunnel10-head-0

sa timing: remaining key lifetime (k/sec): (4607999/3188)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

## Troubleshooting

Para solucionar problemas, você pode usar estes comandos:

- `debug dmvpn condition peer [nbma/tunnellIP]`, permite a depuração condicional para sessões DMVPN específicas a um endereço IP de túnel ou NBMA de um peer, ajudando a isolar problemas relacionados a esse peer.
- `debug dmvpn all all`, permite a depuração abrangente de todos os aspectos do DMVPN, incluindo NHRP, crypto IKE, IPsec, proteção de túnel e soquetes de criptografia. É recomendável usar esse comando com um filtro condicional para evitar sobrecarregar o roteador com informações excessivas de depuração.
- `show dmvpn`, Exibe o status DMVPN atual, incluindo interfaces de túnel, mapeamentos NHRP e informações de peer.
- `show crypto ikev2 sa`, Mostra o status das Associações de Segurança IKEv2, útil para verificar negociações de VPN da Fase 1.
- `show crypto ipsec sa`, Exibe Associações de Segurança IPsec, mostrando o status do túnel da Fase 2 e estatísticas de tráfego.

### 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.