

Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)

Contents

[Introduction](#)

[Informações de Apoio](#)

[A solução DMVPN](#)

[Início automático da criptografia IPsec](#)

[Criação de túnel dinâmico para links “spoke-to-hub”](#)

[Criação de túnel dinâmico para tráfego “spoke-to-spoke”](#)

[Suportando Dynamic Routing Protocols](#)

[Cisco Express Forwarding Fast Switching para mGRE](#)

[Utilizando o Dynamic Routing Over IPsec Protected VPNs](#)

[Configuração de base](#)

[Exemplos das Tabelas de Roteamento nos Roteadores de Hub e Spoke](#)

[Reduzindo o tamanho da configuração do roteador do hub](#)

[Suportando endereços dinâmicos nos spokes](#)

[Concentrador e pontos remotos multipontos dinâmicos](#)

[VPN IPsec multiponto dinâmico](#)

[RIP](#)

[EIGRP](#)

[OSPF](#)

[Condições iniciais](#)

[Condições depois que um link dinâmico é criado entre Spoke1 e Spoke2](#)

[IPSec VPN de multiponto dinâmico com hubs dual](#)

[Hub dual - Disposição de DMVPN única](#)

[Condições e alterações iniciais](#)

[Hub duplo - Disposição de DMVPN dupla](#)

[Condições e alterações iniciais](#)

[Conclusão](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento discute os VPN IPSEC multiponto dinâmicos (DMVPN) e por que uma empresa pôde querer projetar ou migrar sua rede para utilizar esta nova solução do IPsec VPN no Cisco IOS® Software.

[Informações de Apoio](#)

As empresas podem precisar fazer interconexão de muitos locais em um local principal e talvez também de um local com o outro na Internet durante a criptografia do tráfego para protegê-lo. Por exemplo, uma rede de lojas varejistas, que precisa se conectar à matriz da empresa para fins de inventário ou pedidos, também pode necessitar de conexão com outras lojas da empresa para verificar a disponibilidade de produtos. No passado, a única maneira de fazer a conexão era usar uma rede de Camada 2, como ISDN ou Frame Relay, para interconectar tudo. A configuração e o pagamento desses links fisicamente conectados do tráfego IP interno podem ser demorados e caros. Se todos os locais (incluindo o principal) já tiverem acesso relativamente barato à Internet, este acesso à Internet também poderá ser usado para comunicação IP interna entre os armazenamentos e as matrizes usando túneis de IPsec para garantir a privacidade e a integridade dos dados.

Para que as empresas construam grandes redes IPsec que interconectem todos os seus sites na Internet, você precisa ser capaz de escalonar essa rede. O IPsec criptografa o tráfego entre dois pontos finais (peers) e a criptografia é realizada pelos dois pontos finais que estiverem utilizando um segredo compartilhado. Como esse segredo é compartilhado somente entre esses dois pontos finais, as redes criptografadas são inerentemente uma coleção de links ponto a ponto. Por causa disso, o IPsec é, intrinsecamente, uma rede de túnel de ponto a ponto. O método mais viável para escala de uma rede grande ponto a ponto é organizá-la em uma rede hub-and-spoke ou uma rede em malha completa (parcial). Na maioria das redes, a maior parte do tráfego IP ocorre entre os spokes e o hub e uma parte muito pequena ocorre entre os spokes; portanto, o design "hub-and-spoke" é, em muitos casos, a melhor opção. Este projeto também é compatível com redes Frame Relay mais antigas, pois era proibitivo pagar por enlaces entre todos as estações em tais redes.

Ao usar a Internet como a interconexão entre hub e spokes, os spokes também têm acesso direto entre si sem nenhum custo adicional, mas tem sido muito difícil, se não impossível, configurar e/ou gerenciar uma rede de malha completa (parcial). Geralmente, redes em malha completas ou parciais são recomendáveis porque podem reduzir custos no caso de o tráfego spoke-to-spoke conseguir ser feito diretamente em vez do uso de um hub. O tráfego spoke-to-spoke que atravessa o hub usa recursos de hub e pode sofrer atrasos extras, especialmente ao usar criptografia IPsec, já que o hub precisará descriptografar os pacotes recebidos dos spokes de envio e, em seguida, criptografar novamente o tráfego para enviá-lo ao spoke de recepção. Outro exemplo onde o tráfego direto de spoke a spoke seria útil é o caso em que dois spokes estão na mesma cidade, e o hub está do outro lado do país.

À medida que as redes hub-and-spoke IPsec eram implantadas e cresciam em tamanho, tornou-se mais desejável que elas roteiem pacotes IP da forma mais dinâmica possível. Nas redes hub-and-spoke mais antigas do Frame Relay, isso foi realizado com a execução de um protocolo de roteamento dinâmico como OSPF ou EIGRP nos links do Frame Relay. Isso foi útil para anunciar dinamicamente o alcance de redes spoke e também para suportar a redundância na rede de IP Routing. Se a rede perdeu um roteador de hub, um roteador de hub de reserva pode assumir automaticamente para manter a conectividade das redes spoke.

Há um problema fundamental com túneis IPsec e protocolos de roteamento dinâmico. Os protocolos de roteamento dinâmico dependem do uso de pacotes IP multicast ou broadcast, mas o IPsec não suporta pacotes de multicast ou broadcast de criptografia. O método atual de solução desse problema é utilizar Generic Routing Encapsulation (GRE) Tunnels em combinação com criptografia de IPsec.

Os túneis GRE suportam o transporte de pacotes IP multicast e broadcast para a outra extremidade do túnel GRE. O pacote de túnel GRE é um pacote IP de unicast; portanto o pacote GRE pode ser criptografado utilizando IPsec. Neste cenário, a GRE faz o trabalho de

encapsulamento e o IPsec realiza a parte de criptografia do suporte à rede VPN. Quando os túneis GRE são configurados, os endereços IP para os pontos finais do túnel (**origem do túnel ...**, **destino do túnel ...**) devem ser conhecidos pelo outro ponto final e devem ser roteáveis pela Internet. Isso significa que o hub e todos os roteadores spoke nessa rede devem ter endereços IP estáticos não privados.

Para pequenas conexões de site com a Internet, é típico que um endereço IP externo de um spoke mude cada vez que ele se conecta à Internet porque seu ISP (Internet Service Provider, Provedor de Internet) fornece dinamicamente o endereço da interface externa (via Dynamic Host Configuration Protocol (DHCP)) cada vez que o spoke se conecta on-line (ADSL, Asymmetric digital subscriber line, linha digital de assinante assimétrico) e serviços de cabo). Essa locação dinâmica do "endereço externo" do roteador permite que o ISP esgote o uso do espaço de endereço de Internet, uma vez que os usuários não estarão todos on-line ao mesmo tempo. Talvez seja consideravelmente mais caro pagar o provedor para alocar um endereço estático para o roteador do spoke. A execução de um Dynamic Routing Protocol sobre um IPsec VPN exige o uso de túneis GRE, mas você perderá a opção de ter raios com IP Addresses alocados dinamicamente em suas interfaces físicas exteriores.

As restrições acima referidas e outras são resumidas nos quatro pontos seguintes:

- O IPsec usa uma lista de controle de acesso (ACL) para definir quais dados devem ser criptografados. Assim sendo, a cada vez em que uma nova (sub)rede for adicionada atrás de um spoke ou do hub, o cliente deve alterar o ACL em ambos os roteadores, do hub e do spoke. Se o SP gerencia o roteador, o cliente deve notificar o SP para que a ACL do IPsec seja alterada e permita que o novo tráfego seja criptografado.
- Com redes hub-and-spoke grandes, o tamanho da configuração no roteador Hub pode se tornar muito grande, na medida em que não seja utilizável. Por exemplo, um roteador precisa de até 3900 linhas de configuração para suportar 300 roteadores citados. Isto é grande o suficiente que seria difícil exibir a configuração e encontrar a seção da configuração que é relevante para um problema atual que está sendo depurado. Além disso, a configuração desse tamanho pode ser grande demais para se ajudar em NVRAM e precisaria ser armazenada na memória Flash.
- O GRE + IPsec deve conhecer o endereço do peer do ponto final. Os endereços IP dos spokes são conectados diretamente à Internet por meio de seu próprio ISP e normalmente são configurados de modo que os endereços de suas interfaces externas não sejam fixos. Os endereços IP podem mudar a cada vez que o site ficar on-line (por meio do DHCP).
- Se os spokes precisam se comunicar diretamente entre si através do IPsec VPN, então a rede hub-and-spoke deve se tornar uma malha completa. Como ainda não se sabe quais raios terão que se comunicar diretamente entre si, é necessária uma malha completa, mesmo que cada fala não precise falar diretamente com cada outro. Além disso, não é viável configurar o IPsec em um roteador spoke pequeno para que ele tenha conectividade direta com todos os outros roteadores spoke na rede; portanto, os roteadores spoke podem precisar ser roteadores mais potentes.

[A solução DMVPN](#)

A solução DMVPN utiliza GRE multiponto (mGRE) e protocolo de resolução de salto seguinte (NHRP), com IPsec e alguns novos aprimoramentos, para solucionar os problemas descritos acima de maneira escalável.

Início automático da criptografia IPsec

Quando não estiver usando a solução DMVPN, o túnel de criptografia IPsec não será iniciado até que haja tráfego de dados que exija o uso desse túnel IPsec. Pode levar de 1 a 10 segundos para concluir o início do túnel IPsec e o tráfego de dados é descartado durante esse período. Ao usar o GRE com IPsec, a configuração do túnel GRE já inclui o endereço do peer de túnel GRE (**tunnel destination ...**), que também é o endereço do peer IPsec. Esses dois endereços são pré-configurados.

Se você usar o Tunnel Endpoint Discovery (TED) e mapas de criptografia dinâmicos no roteador de hub, poderá evitar ter que pré-configurar os endereços de peer IPsec no hub, mas uma prova e resposta TED precisarão ser enviadas e recebidas antes que a negociação ISAKMP possa iniciar. Isso não deve ser necessário desde que, ao usar o GRE, os endereços de origem e destino do peer já sejam conhecidos. Eles estão na configuração ou resolvidos com o NHRP (para túneis GRE multiponto).

Com a solução DMVPN, o IPsec é disparado imediatamente para túneis GRE ponto a ponto e multiponto. Não é necessário configurar as ACLs de criptografia, pois elas serão derivadas automaticamente dos endereços de origem e de destino do túnel de GRE. Os seguintes comandos são usados para definir os parâmetros de criptografia do IPsec. Observe que não há nenhum **peer definido ...** ou **correspondência de endereço...** comandos necessários porque essas informações são derivadas diretamente do túnel GRE associado ou mapeamentos NHRP.

```
crypto ipsec profile
```

```
set transform-set
```

O comando a seguir associa uma interface de túnel ao perfil IPsec.

```
interface tunnel
```

```
...
```

```
tunnel protection ipsec profile
```

Criação de túnel dinâmico para links “spoke-to-hub”

Nenhuma informação de GRE ou IPsec sobre um spoke está configurada no roteador de hub na rede DMVPN . O túnel GRE do roteador spoke é configurado (através de comandos NHRP) com informações sobre o roteador de hub. Quando o roteador spoke é iniciado, ele inicia automaticamente o túnel IPsec com o roteador de hub conforme descrito acima. Ele usa o NHRP para notificar o roteador do hub quanto ao seu endereço IP na interface física atual. Isso é útil por três motivos:

- Se o roteador spoke possui seu endereço IP de interface física, atribuído dinamicamente (tal como com ADLS ou CableModem), então o roteador de hub não pode ser configurado com esta informação, já que todas as vezes que o roteador spoke recarregar, ele obterá um novo endereço IP de interface física.
- A configuração do roteador hub é abreviada e simplificada, pois não é necessário ter nenhuma informação de GRE ou IPsec sobre os roteadores de peer. Todas essas informações são aprendidas dinamicamente via NHRP.
- Ao adicionar um novo roteador spoke a uma rede DMVPN, não é necessário alterar a configuração no hub ou em qualquer um dos roteadores spoke atuais. O novo roteador spoke é configurado com as informações do hub e, quando é iniciado, é registrado dinamicamente com o roteador hub. O protocolo de roteamento dinâmico propaga as informações de roteamento para esse spoke para o hub. O hub propaga essas novas informações de roteamento para os demais spokes. Ele também propaga as informações de roteamento dos outros spokes para este spoke.

Criação de túnel dinâmico para tráfego “spoke-to-spoke”

Conforme afirmado, atualmente, em uma rede em malha, todos os túneis IPsec ponto a ponto IPsec (ou IPsec+GRE) devem ser configurados em todos os roteadores, mesmo que alguns ou todos os túneis não estejam em execução ou sejam necessários em todas as ocasiões. Com a solução DMVPN, um roteador é o hub e todos os outros roteadores (spokes) são configurados com túneis para o hub. Os túneis spoke-hub estão continuamente ativos, e não é necessário configurar um túnel direto de um spoke para outro. Em vez disso, quando um spoke deseja transmitir um pacote a outro spoke (como a sub-rede atrás de outro spoke), ele usa o NHRP para determinar dinamicamente o endereço de destino necessário do spoke de destino. O roteador de hubs age como o servidor NHRP e processa essa solicitação para o spoke de origem. Os dois pontos remotos podem então criar um túnel IPsec dinamicamente entre si (através da interface mGRE única) e os dados podem ser transferidos diretamente. Esse túnel dinâmico tipo spoke-to-spoke será automaticamente desfeito após um período (configurável) de inatividade.

Suportando Dynamic Routing Protocols

A solução DMVPN é baseada em túneis GRE que suportam pacotes IP multicast/broadcast de encapsulamento, portanto, a solução DMVPN também suporta protocolos de roteamento dinâmico executados nos túneis IPsec+mGRE. Anteriormente, o NHRP exigia a configuração explícita do mapeamento de difusão/multicast para os endereços IP de destino do túnel para suportar pacotes IP de multicast e difusão em túneis GRE. Por exemplo, no hub, você precisaria da linha de configuração `ip nhrp map multicast <spoke-n-addr>` para cada spoke. Com a solução DMVPN, os endereços do spoke não são conhecidos com antecedência, por isso essa configuração não é possível. Em vez disso, o NHRP pode ser configurado para adicionar automaticamente cada spoke à lista de destino multicast no hub com o comando `ip nhrp map`

multicast dynamic. Com esse comando, quando os roteadores spoke registram seu mapeamento unicast NHRP com o servidor NHRP (hub), o NHRP também criará um mapeamento de broadcast/multicast para esse spoke. Isto elimina a necessidade de conhecimento antecipado de endereços de spoke.

Cisco Express Forwarding Fast Switching para mGRE

No momento, o tráfego em uma interface mGRE é comutado pelo processo, resultando em um desempenho fraco. A solução DMVPN adiciona a switching do Cisco Express Forwarding para o tráfego mGRE, resultando em um desempenho muito melhor. Não existe nenhum comando de configuração necessário para ativar esse recurso. Se a comutação Cisco Express Forwarding for permitida na interface do túnel GRE e nas interfaces físicas de saída/entrada, os pacotes de túnel GRE multiponto serão comutados pelo Cisco Express Forwarding.

Utilizando o Dynamic Routing Over IPsec Protected VPNs

Esta seção descreve o estado atual de ocorrências (solução pré-DMVPN). O IPsec é implementado em roteadores Cisco por meio de um conjunto de comandos que definem a criptografia e, em seguida, um comando **crypto map <map-name>** aplicado na interface externa do roteador. Devido a esse design e ao fato de não haver atualmente um padrão para usar o IPsec para criptografar pacotes de multicast/broadcast IP, os pacotes do protocolo de roteamento IP não podem ser "encaminhados" através do túnel IPsec e quaisquer alterações de roteamento não podem ser propagadas dinamicamente para o outro lado do túnel IPsec.

Observação: todos os protocolos de roteamento dinâmico, exceto o BGP, usam pacotes IP de broadcast ou multicast. Túneis GRE são utilizados em combinação com o IPsec para solucionar esse problema.

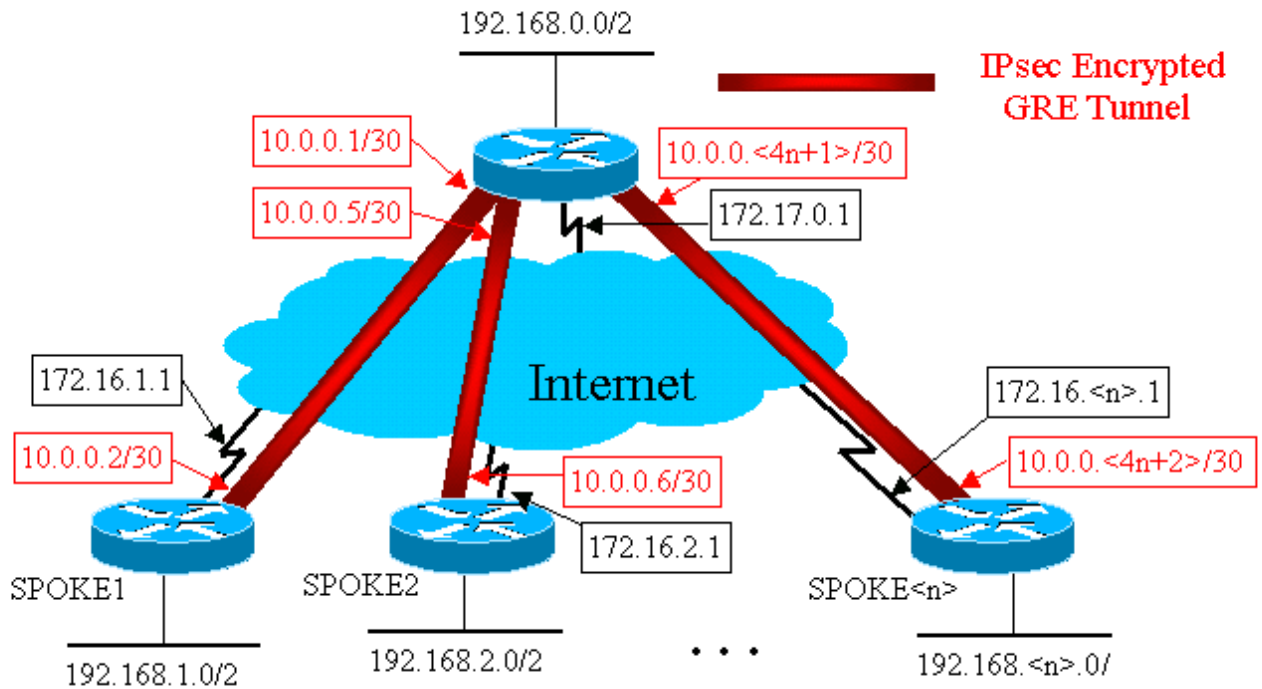
Os túneis GRE são implementados nos roteadores Cisco usando uma interface de túnel virtual (**interface tunnel<#>**). O protocolo de tunelamento GRE foi projetado para tratar pacotes de multicast/broadcast IP para que um protocolo de roteamento dinâmico possa ser "executado" em um túnel GRE. Os pacotes de túnel GRE são pacotes IP unicast que encapsulam o pacote IP multicast/unicast original. Depois, você pode usar IPsec para criptografar o pacote de túnel GRE. Você também pode executar IPsec no modo de transporte e economizar 20 bytes, pois GRE já encapsulou o pacote de dados original; portanto, ele não precisa encapsular o pacote IP de GRE em outro cabeçalho de IP.

Quando estiver executando o IPsec em modo de transporte, existe uma limitação de que os endereços de origem e destino do pacote a ser criptografado devem ser compatíveis com os endereços de peer de IPsec (o próprio roteador). Neste caso, isto simplesmente significa que o ponto final do túnel de GRE e os endereços de peer IPsec devem ser os mesmos. Não é um problema, pois os mesmos roteadores são os pontos finais de túnel IPsec e GRE. Combinando túneis GRE com criptografia IPsec, você pode usar um protocolo de roteamento IP dinâmico para atualizar as tabelas de roteamento em ambas as extremidades do túnel criptografado. As entradas da tabela de roteamento IP para as redes que foram aprendidas através do túnel criptografado terão a outra extremidade do túnel (endereço IP da interface do túnel GRE) como o salto seguinte IP. Assim, se as redes mudarem em ambos os lados do túnel, o outro lado aprenderá dinamicamente a mudança e a conectividade continuará sem nenhuma alteração na configuração dos roteadores.

Configuração de base

Esta é uma configuração padrão IPsec+GRE ponto a ponto. Depois disso, há uma série de exemplos de configuração em que recursos específicos da solução DMVPN são adicionados em passos para mostrar as diferentes potencialidades de DMVPN. Cada exemplo amplia os exemplos anteriores para mostrar como usar a solução DMVPN em projetos de rede de maior complexidade. Esta sucessão de exemplos pode ser utilizada como modelo para migrar um IPsec+GRE VPN atual para um DMVPN. Você pode interromper a "migração" em qualquer ponto se esse exemplo de configuração específico corresponder aos requisitos do projeto de rede.

Hub e spoke IPsec + GRE (n = 1,2,3,...)



```

Roteador de Hub

version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set trans2
 match address 101
crypto map vpnmap1 20 ipsec-isakmp
 set peer 172.16.2.1
 set transform-set trans2
 match address 102
. . .
crypto map vpnmap1 <10*n> ipsec-isakmp
 set peer 172.16.

```

```
interface Tunnel1
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.1.1
!
interface Tunnel2
  bandwidth 1000
  ip address 10.0.0.5 255.255.255.252
  ip mtu 1400
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.16.2.1
!
. . .
!
interface Tunnel

!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
  crypto map vpnmap1
!
interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
!
access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
...
access-list
```

 roteador spoke1 

```
version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
```



```

!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.1.1 255.255.255.252
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre host 172.16.1.1 host
172.17.0.1

```

 roteador spoke2 

```

version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
set peer 172.17.0.1
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.6 255.255.255.252
ip mtu 1400
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
ip address 172.16.2.1 255.255.255.252
crypto map vpnmap1

```

```

!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre host 172.16.2.1 host
172.17.0.1

```

Roteador Spoke<n>

```

version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 ipsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<4n-2> 255.255.255.252
 ip mtu 1400
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.<n>.1 255.255.255.252
 crypto map vpnmap1
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.

```

Na configuração acima, as ACLs são usadas para definir qual tráfego será criptografado. Nos roteadores de hub e de spoke, essa ACL precisa apenas corresponder aos pacotes IP do túnel GRE. Não importa como as redes mudam em ambas as extremidades, os pacotes de túnel IP do GRE não serão alterados, portanto, essa ACL não precisa ser alterada.

Observação: ao usar as versões do software Cisco IOS anteriores à 12.2(13)T, você deve aplicar

o comando de configuração **crypto map vpnmap1** às interfaces de túnel GRE (Tunnel<x>) e à interface física (Ethernet0). Com o Cisco IOS versão 12.2(13)T e posterior, você apenas aplica o comando **crypto map vpnmap1 configuration** à interface física (Ethernet0).

[Exemplos das Tabelas de Roteamento nos Roteadores de Hub e Spoke](#)

Tabela de Roteamento no Roteador de Hub

```
172.17.0.0/24 is subnetted, 1 subnets
C      172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
C      10.0.0.0 is directly connected, Tunnel1
C      10.0.0.4 is directly connected, Tunnel2
...
C      10.0.0.<4n-4> is directly connected, Tunnel<n>
C      192.168.0.0/24 is directly connected, Ethernet1
D      192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
D      192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
...
D      192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Tabela de Roteamento no Roteador Spoke1

```
172.16.0.0/24 is subnetted, 1 subnets
C      172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
C      10.0.0.0 is directly connected, Tunnel1
D      10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
...
D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
D      192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
C      192.168.1.0/24 is directly connected, Loopback0
D      192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
...
D      192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Tabela de Roteamento no Roteador Spoke<n>

```
172.16.0.0/24 is subnetted, 1 subnets
C      172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
D      10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
D      10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
...
C      10.0.0.<4n-4> is directly connected, Tunnel0
D      192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
D      192.168.1.0/24 [90/3097600] via 10.0.0.1,
```

```
22:01:21, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
...
C    192.168.<n>.0/24 is directly connected, Ethernet0
```

Essa é uma configuração de trabalho básica, utilizada como um ponto de partida para a comparação com configurações mais complexas possível com a utilização da solução DMVPN. A primeira alteração reduzirá o tamanho da configuração no roteador de hub. Isso não faz diferença com poucos roteadores spoke, mas pode ser grave se houver mais de 50 a 100 roteadores spoke.

Reduzindo o tamanho da configuração do roteador do hub

No exemplo a seguir, a configuração é minimamente alterada no roteador de hub das interfaces múltiplas do túnel GRE ponto a ponto até uma interface única de túnel multiponto GRE. Essa é a primeira etapa na solução do DMVPN.

Há um bloco exclusivo de linhas de configuração no roteador de hub para definir as características do mapa de criptografia para cada roteador de spoke. Este trecho da configuração define o cripto ACL e a interface do túnel de GRE para tal roteador de raio. Essas características são em grande parte as mesmas para todos os spokes, exceto para endereços IP (**set peer ...**, **tunnel destination ...**).

Olhando para a configuração acima no roteador de hub, você vê que há pelo menos 13 linhas de configuração por roteador spoke; quatro para o mapa de criptografia, um para a ACL de criptografia e oito para a interface de túnel GRE. O número total de linhas de configuração, se havia 300 roteadores spoke, é 3.900. Você também precisa de 300 (/30) sub-redes para endereçar cada link de túnel. Uma configuração desse tamanho é muito difícil de gerenciar e ainda mais difícil ao solucionar problemas da rede VPN. Para reduzir esse valor, você pode usar mapas de criptografia dinâmica, o que reduz o valor acima em 1200 linhas, deixando 2700 linhas em uma rede de 300 spokes.

Observação: ao usar mapas de criptografia dinâmicos, o túnel de criptografia IPsec deve ser iniciado pelo roteador spoke. Você também pode usar **ip unnumbered <interface>** para reduzir o número de sub-redes necessárias para os túneis GRE, mas isso pode dificultar a solução de problemas mais tarde.

Com a solução DMVPN, você pode configurar uma única interface de túnel GRE multiponto e um único perfil IPsec no roteador de hub para lidar com todos os roteadores de spoke. Isso permite que o tamanho da configuração no roteador de hub permaneça constante, não importa quantos roteadores de spoke sejam adicionados à rede de VPN.

A solução DMVPN apresenta os seguintes novos comandos:

```
crypto ipsec profile
```

O comando **crypto ipsec profile <name>** é usado como um mapa de criptografia dinâmico e é projetado especificamente para interfaces de túnel. Esse comando é usado para definir os parâmetros para criptografia IPsec no spoke-to-hub e nos túneis de VPN do spoke-to-hub. O único parâmetro necessário sob o perfil é o conjunto de transformação. O endereço de peer IPsec e o **endereço de correspondência...** para o proxy IPsec são derivadas automaticamente dos mapeamentos NHRP para o túnel GRE.

O comando **tunnel protection ipsec profile <name>** é configurado na interface do túnel GRE e é usado para associar a interface do túnel GRE ao perfil IPsec. Além disso, o comando **tunnel protection ipsec profile <name>** também pode ser usado com um túnel GRE ponto a ponto. Nesse caso, ele derivará as informações de peer e proxy do IPsec da **origem do túnel ...** e **destino do túnel ...** configuração. Dessa forma, a configuração é simplificada pois o peer de IPsec e os crypto ACLs não são mais necessários.

Observação: o comando **tunnel protection ...** especifica que a criptografia IPsec será feita depois que o encapsulamento GRE tiver sido adicionado ao pacote.

Esses dois primeiros comandos novos são semelhantes a configurar um mapa de criptografia e atribuir o mapa de criptografia a uma interface usando o comando **crypto map <name>**. A grande diferença é que, com os novos comandos, você não precisa especificar o endereço de peer de IPsec ou um ACL para combinar os pacotes a ser criptografados. Esses parâmetros são automaticamente definidos a partir dos mapeamentos NHRP para a interface de túnel mGRE.

Observação: ao usar o comando **tunnel protection ...** na interface do túnel, um **mapa de criptografia ...** não está configurado na interface de saída física.

O último novo comando, **ip nhrp map multicast dynamic**, permite que o NHRP adicione automaticamente roteadores spoke aos mapeamentos NHRP multicast quando esses roteadores spoke iniciam o túnel mGRE+IPsec e registram seus mapeamentos unicast NHRP. Isso é necessário para permitir que os protocolos de roteamento dinâmico funcionem nos túneis mGRE+IPsec entre o hub e os spokes. Se esse comando não estivesse disponível, o roteador do hub precisaria ter uma linha de configuração separada para um mapeamento multicast para cada spoke.

Observação: com essa configuração, os roteadores spoke devem iniciar a conexão de túnel mGRE+IPsec, já que o roteador de hub não está configurado com nenhuma informação sobre os spokes. Mas isso não é um problema, porque com o DMVPN, o túnel mGRE+IPsec é iniciado automaticamente quando o roteador de raio é iniciado e permanece sempre ativado.

Observação: o exemplo a seguir mostra interfaces de túnel GRE ponto a ponto nos roteadores spoke e linhas de configuração NHRP adicionadas nos roteadores hub e spoke para suportar o túnel mGRE no roteador de hub. A configuração é alterada da seguinte forma:

```
Roteador de hub (antigo)

crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.16.1.1
  set transform-set trans2
  match address 101
crypto map vpnmap1 20 IPsec-isakmp
  set peer 172.16.2.1
  set transform-set trans2
```

```

match address 102
. . .
crypto map vpnmap1 <10n> IPsec-isakmp
  set peer 172.16.

!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
  crypto map vpnmap1
!
access-list 101 permit gre host 172.17.0.1 host
172.16.1.1
access-list 102 permit gre host 172.17.0.1 host
172.16.2.1
. . .
access-list

```

Roteador de hub (novo)

```

crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0

```

Spoke<n> Router (antigo)

```

crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252
  ip mtu 1400

```

```

delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
!
interface Ethernet0
 ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
. . .
!
access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
!

```

Spoke<n> Router (novo)

```

crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.

delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
 ip address 172.16.<n>.1 255.255.255.252
  crypto map vpnmap1
!
. . .
!
access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
!

```

Nos roteadores spoke, a máscara de sub-rede foi alterada e os comandos NHRP foram adicionados na interface de túnel. Os comandos NHRP são necessários, pois o roteador de hub agora está usando o NHRP para mapear o endereço IP da interface de túnel de spoke para o endereço IP da interface física do spoke.

```
ip address 10.0.0.
```

```

ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000

```

```
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
...
tunnel key 100000
```

A sub-rede está agora /24, em vez de /30, portanto todos os nós estão na mesma sub-rede, em vez de sub-redes diferentes. Os raios continuam a enviar tráfego raio a raio através do concentrador, uma vez que estão usando uma interface de túnel GRE. A **autenticação ip nhrp ...**, **ip nhrp network-id ...** e **chave de túnel ...** comandos são usados para mapear os pacotes de túnel e os pacotes NHRP para a interface de túnel GRE multiponto correta e a rede NHRP quando eles são recebidos no hub. O **mapa ip nhrp ...** e **ip nhrp nhs ...** comandos são usados pelo NHRP no spoke para anunciar o mapeamento NHRP de spokes (10.0.0.<n+1> —> 172.16.<n>.1) para o hub. O endereço 10.0.0.<n+1> é recuperado do **endereço ip ...** na interface do túnel e o endereço 172.16.<n>.1 é recuperado do **destino do túnel ...** na interface túnel.

Em um caso em que há 300 roteadores spoke, essa alteração reduziria o número de linhas de configuração no hub de 3.900 linhas para 16 linhas (uma redução de 3.884 linhas). A configuração em cada roteador spoke aumentaria em 6 linhas.

[Suportando endereços dinâmicos nos spokes](#)

Em um roteador Cisco, cada peer IPsec precisa estar configurado com o endereço IP de outro peer IPsec antes que o túnel IPsec possa ser ativado. Isso pode ser um problema se um roteador spoke tiver um endereço dinâmico em sua interface física, o que é comum para roteadores que estão conectados via enlaces por DSL ou cabo.

O TED permite que um correspondente IPsec encontre outro correspondente IPsec através do envio de um pacote especial de Internet Security Association and Key Management Protocol (ISAKMP) ao endereço IP de destino do pacote de dados original que necessitava ser criptografado. A suposição de que esse pacote atravessará a rede interveniente no mesmo caminho usada pelo pacote do túnel IPsec. Esse pacote será coletado pelo peer IPsec de outra extremidade, que responderá ao primeiro peer. Os dois roteadores negociarão as Associações de Segurança (SAs) ISAKMP e IPsec e ativarão o túnel IPsec. Isso só funcionará se os pacotes de dados a serem criptografados tiverem endereços IP roteáveis.

O TED pode ser utilizado em combinação com os túneis GRE conforme a configuração na seção anterior. Isso foi testado e funciona, embora houvesse um bug em versões anteriores do software Cisco IOS em que o TED forçou todo o tráfego IP entre os dois pares IPsec a ser criptografado, não apenas os pacotes de túnel GRE. A solução DMVPN oferece este recurso e recursos adicionais sem que os hosts precisem utilizar endereços de IP de Internet roteáveis e sem precisar enviar pacotes de prova e resposta Com uma pequena modificação, a configuração da última seção pode ser usada para suportar roteadores do tipo spoke com endereços IP dinâmicos em suas interfaces físicas externas.

Roteador de hub (sem alteração)

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
```



```

ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0

```

Spoke<n> Router (antigo)

```

crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 match address 101
!
...
!
access-list 101 permit gre host 172.16.

```

Spoke<n> Router (novo)

```

crypto map vpnmap1 10 IPsec-isakmp
 set peer 172.17.0.1
 set transform-set trans2
 set security-association level per-host
 match address 101
!
...
!
access-list 101 permit gre any host 172.17.0.1

```

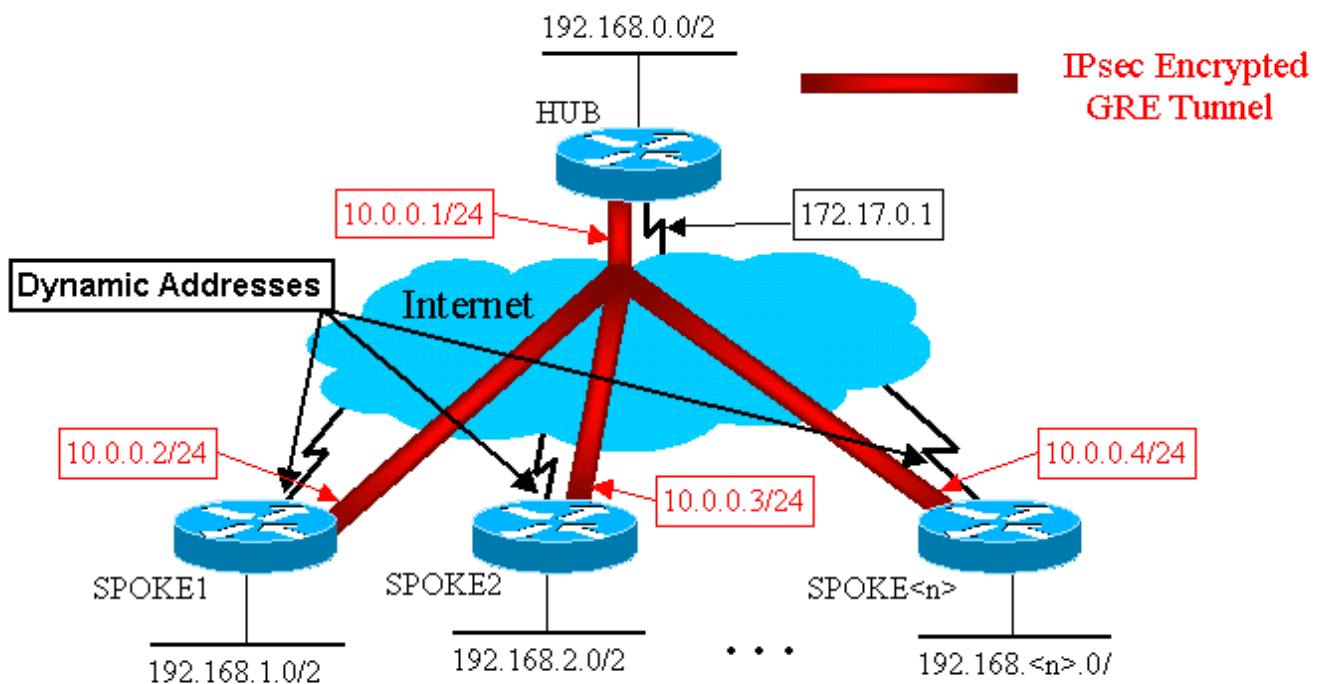
A funcionalidade usada na configuração do spoke é a seguinte.

- Quando a interface de túnel GRE for ativada, começará a enviar pacotes de registro do NHRP para o roteador de hub. Esses pacotes de registro de NHRP dispararão o IPsec a ser iniciado. No roteador spoke, os comandos `set peer <peer-address>` e **match ip access-list <ACL>** são configurados. A ACL especifica o GRE como o protocolo, qualquer para a origem e o endereço IP do hub para o destino. **Observação:** é importante observar que qualquer um está sendo usado como origem na ACL, e esse deve ser o caso, pois o endereço IP do roteador spoke é dinâmico e, portanto, desconhecido antes da interface física estar ativa. Uma sub-rede IP pode ser usada para a origem na ACL se a interface de spoke dinâmica for ser restrita a um endereço dentro dessa sub-rede.
- O comando **set security-association level per-host** é usado para que a origem IP no proxy IPsec de spokes seja apenas o endereço de interface física (/32) atual, em vez de "any" da ACL. Se "any" da ACL fosse usado como origem no proxy IPsec, isso impediria qualquer

outro roteador spoke de também configurar um túnel IPsec+GRE com esse hub. Isso ocorre porque o proxy de IPsec resultante no hub seria equivalente a permit gre host 172.17.0.1 any. Isso significaria que todos os pacotes do túnel GRE destinados a qualquer spoke seriam criptografados e enviados ao primeiro spoke que estabelecesse um túnel com o hub, pois seu proxy IPsec corresponde pacotes GRE para cada spoke.

- Uma vez que o túnel do IPsec é configurado, um pacote de registros NHRP passa do roteador de spoke para o NHS (Próximo servidor de saltos) configurado. O NHS é o roteador de hub desta rede de hub e raios. O pacote de registro NHRP fornece as informações para o roteador do hub para criar um mapeamento de NHRP para esse roteador de ponto de spoke. Com esse mapeamento, o roteador de hub pode encaminhar pacotes de dados IP unicast para o roteador de spoke pelo túnel mGRE+Ipsec. Além disso, o hub adiciona o roteador spoke à sua lista de mapeamento multicast NHRP. O hub começará a enviar Dynamic IP Routing Multicast Packets para o spoke (se um Dynamic Routing Protocol estiver configurado). O spoke se tornará um vizinho do protocolo de roteamento do hub e trocará atualizações de roteamento.

Hub e Spoke IPsec + mGRE



```

Roteador de Hub

version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
  
```

```

!
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
!

```

Observe, na configuração de concentrador acima, que os endereços IP dos roteadores de raio não estão configurados. A interface física externa do spoke e o mapeamento para os endereços IP da interface do túnel do spoke são aprendidos dinamicamente pelo hub via NHRP. Isso permite que o endereço IP da interface física externa do spoke seja atribuído dinamicamente.

roteador spoke1

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400

```

```
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
ip address dhcp hostname Spoke1
crypto map vpnmap1
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
access-list 101 permit gre 172.16.1.0 0.0.0.255 host
172.17.0.1
```

roteador spoke2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto map vpnmap1 local-address Ethernet0
crypto map vpnmap1 10 IPsec-isakmp
set peer 172.17.0.1
set security-association level per-host
set transform-set trans2
match address 101
!
interface Tunnel0
bandwidth 1000
ip address 10.0.0.3 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
!
interface Ethernet0
ip address dhcp hostname Spoke2
crypto map vpnmap1
```

```

!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
access-list 101 permit gre 172.16.2.0 0.0.0.255 host
172.17.0.1

```



As primeiras observações a serem feitas sobre as configurações do spoke são:

- O endereço IP da interface física externa (ethernet0) é dinâmico via DHCP.**ip address dhcp hostname Spoke2**
- A ACL de criptografia (101) especifica uma sub-rede como origem para o proxy IPsec.**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- O comando a seguir no mapa de criptografia de IPSec especifica que a associação de segurança será por host.**definir o nível de associação de segurança por host**
- Todos os túneis fazem parte da mesma sub-rede, pois todos eles se conectam por meio da mesma interface de GRE multiponto no roteador de hubs.**endereço ip 10.0.0.2 255.255.255.0**

A combinação desses três comandos torna desnecessária a configuração do endereço IP da interface física externa do spoke'. O proxy IPsec usado será baseado em host e não em sub-rede.

A configuração nos roteadores spoke não tem o endereço IP do roteador de hub configurado, uma vez que precisa iniciar o túnel IPsec+GRE. Observe a semelhança entre as configurações de Spoke1 e Spoke2. Essas duas configurações de roteador spoke não são apenas semelhantes, mas todas serão semelhantes. Na maioria dos casos, todos os spokes simplesmente precisam de endereços IP exclusivos em suas interfaces, e o restante de suas configurações será o mesmo. Isso o torna possível para configurar e implementar muitos roteadores spoke rapidamente.



Os dados NHRP se parecem com os seguintes no concentrador e pontos remotos.


Roteador de Hub


```

Hub#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 01:25:18,
expire 00:03:51
   Type: dynamic, Flags: authoritative unique
registered
   NBMA address: 172.16.1.4
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03
   Type: dynamic, Flags: authoritative unique
registered
   NBMA address: 172.16.2.10
...
 10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created
00:06:00, expire 00:04:25
   Type: dynamic, Flags: authoritative unique
registered
   NBMA address: 172.16.<n>.41

```


roteador spoke1


```
Spoke1#sho ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 4d08h,
never expire
  Type: static, Flags: authoritative
  NBMA address: 172.17.0.1
```

Concentrador e pontos remotos multipontos dinâmicos

A configuração dos roteadores spoke acima não depende dos recursos da solução DMVPN, por isso os roteadores spoke podem executar as versões do Cisco IOS Software anteriores a 12.2(13)T. A configuração no roteador do hub depende dos recursos DMVPN e portanto, ele deve executar o Cisco IOS versão 12.2(13)T ou posterior. Isso permite alguma flexibilidade na decisão de quando você precisa atualizar seus roteadores spoke que já estão implantados. Se os roteadores do seu ponto remoto também estiverem executando o Cisco IOS versão 12.2(13)T ou posterior, você poderá simplificar a configuração de raio da seguinte maneira.

Roteador spoke<n> (anterior ao Cisco IOS 12.2(13)T)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host
  set transform-set trans2
  match address 101
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000
  tunnel source Ethernet0
  tunnel destination 172.17.0.1
  tunnel key 100000
!
interface Ethernet0
  ip address dhcp hostname Spoke<n>
  crypto map vpnmap1
!
. . .
!
access-list 101 permit gre any host 172.17.0.1
```

Roteador spoke<n> (após Cisco IOS 12.2(13)T)

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
```

```

bandwidth 1000
ip address 10.0.0.<n+1> 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
delay 1000
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address dhcp hostname Spoke<n>
!

```

Observe que fizemos o seguinte:

1. Removemos o comando `crypto map vpnmap1 10 ipsec-isakmp` e o substituímos por `crypto ipsec profile vpnprof`.
2. Removido o comando **`crypto map vpnmap1`** das interfaces Ethernet0 e colocado o comando **`tunnel protection ipsec profile vpnprof`** na interface Tunnel0.
3. Removido a ACL de criptografia, `access-list 101 permit gre any host 172.17.0.1`.

Nesse caso, os endereços de peer IPsec e os proxies são automaticamente derivados da **origem do túnel ...** e **destino do túnel ...** configuração. Os peers e proxies são os seguintes (conforme visto na saída do comando **`show crypto ipsec sa`**):

```

...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):    (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...

```

Em resumo, as configurações completas a seguir incluem todas as alterações formadas até este momento a partir da [Configuração básica](#) (“hub and spoke” IPsec+GRE).

Roteador de Hub

```

version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000

```

```

ip address 10.0.0.1 255.255.255.0
ip mtu 1400
ip nhrp authentication test
ip nhrp map multicast dynamic
ip nhrp network-id 100000
ip nhrp holdtime 600
no ip split-horizon eigrp 1
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!

```

Não há nenhuma alteração na configuração do hub.

roteador spoke1

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!

```



```
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
 no auto-summary
!
```

roteador spoke2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
!
interface Ethernet1
 ip address 192.168.2.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
 no auto-summary
!
```

VPN IPsec multiponto dinâmico

Os conceitos e a configuração nesta seção mostram os recursos completos de DMVPN. O NHRP oferece a capacidade dos roteadores spoke de aprender dinamicamente o endereço da interface física externa dos outros roteadores spoke na rede VPN. Isso significa que um roteador spoke terá informação suficiente para criar de forma dinâmica um túnel IPsec+mGRE diretamente para outros roteadores spoke. Isso é vantajoso, já que, se esse tráfego de dados spoke-to-spoke fosse

enviado via roteador de hub, deveria ser codificado/decodificado, aumentando duas vezes o retardo e a carga no roteador de hub. Para usar esse recurso, os roteadores citados precisam ser comutados de p-pGRE (GRE de ponto a ponto) para interfaces de túnel de mGRE (GRE de multipontos). Eles também precisam saber as (sub-)redes que estão disponíveis atrás dos outros spokes com um salto seguinte de IP do endereço IP do túnel do outro roteador spoke. Os roteadores spoke aprendem essas (sub)redes através do protocolo de roteamento IP dinâmico em execução no túnel IPsec+mGRE com o hub.

O Dynamic IP Routing Protocol em execução no roteador de hub pode ser configurado de forma a refletir as rotas aprendidas de um spoke de volta à mesma interface a todos os outros spokes, mas a nó IP seguinte nessas rotas geralmente será o roteador do hub e não o roteador do spoke a partir do qual o hub aprendeu essa rota.

Observação: o protocolo de roteamento dinâmico é executado somente nos links hub e spoke, mas não nos links spoke-to-spoke dinâmicos.

Os Dynamic Routing Protocols (RIP, OSPF e EIGRP) precisam ser configurados no roteador de hub para anunciar as rotas de volta à interface de túnel de mGRE e para definir o salto seguinte de IP para o roteador de spoke de origem das rotas aprendidas em um spoke quando a rota é anunciada novamente fora dos demais spokes.

A seguir encontram-se requisitos para as configurações do Routing Protocol.

RIP

Você precisa desativar o split horizon na interface do túnel mGRE no hub, caso contrário, o RIP não anunciará rotas aprendidas pela interface mGRE de volta nessa mesma interface.

```
no ip split-horizon
```

Nenhuma outra alteração é necessária. O RIP usará automaticamente o próximo salto IP original em rotas que ele anunciará novamente na mesma interface onde aprendeu essas rotas.

EIGRP

Será necessário desligar o horizonte dividido na interface do túnel mGRE no hub, caso contrário o EIGRP não anunciará as rotas aprendidas por meio da interface mGRE que voltaram para a mesma interface.

```
no ip split-horizon eigrp
```

O EIGRP, por padrão, configurará o próximo salto de IP para ser o roteador de hub para rotas que ele está anunciando, mesmo quando estiver anunciando as rotas de volta para a mesma interface em que as aprendeu. Por isso, nesse caso, você precisa do seguinte comando de

configuração para instruir o EIGRP a usar o próximo salto do IP original ao anunciar essas rotas.

```
no ip next-hop-self eigrp
```

Observação: o comando `no ip next-hop-self eigrp <as>` estará disponível a partir do Cisco IOS versão 12.3(2). Para versões do Cisco IOS entre 12.2(13)T e 12.3(2), é necessário fazer o seguinte:

- Se túneis dinâmicos de spoke para spoke não forem desejados, então o comando acima não será necessário.
- Se os túneis dinâmicos spoke-to-spoke forem desejados, você deverá usar a comutação de processo na interface de túnel nos roteadores spoke.
- Do contrário, você precisará usar um Routing Protocol diferente sobre o DMVPN.

OSPF

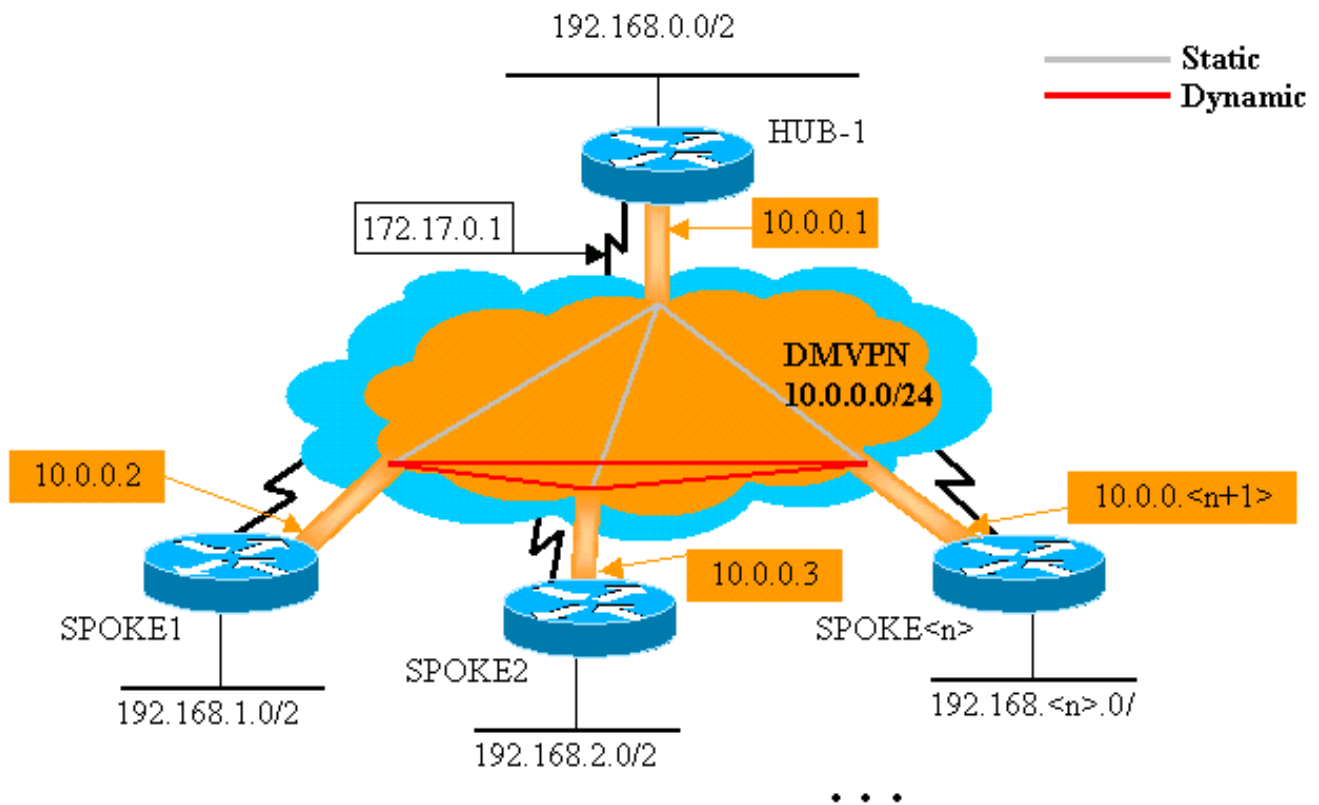
Como o OSPF é um Routing Protocol de estado de link, não há problemas de horizonte de divisão. Normalmente, para interfaces multiponto, você configura o tipo de rede OSPF para ser ponto para multiponto, mas isso faria com o OSPF adicionasse rotas de host à tabela de roteamento nos roteadores de spoke. Essas rotas de host podem causar pacotes destinados às redes por trás de outros roteadores spoke, a serem encaminhados diretamente via hub e não para outro spoke. Para contornar o problema, configure o tipo de rede OSPF para ser transmitido com o comando.

```
ip ospf network broadcast
```

Você também precisa verificar se o roteador do hub será o DR (Designated Router, roteador designado) para a rede IPsec+mGRE. Isto é feito via configuração da prioridade de OSPF como sendo maior que 1 no hub e 0 nos spokes.

- Hub: `ip ospf priority 2`
- Falado: `ip ospf priority 0`

Hub único de DMVPN



Roteador de Hub

```

version 12.3
!
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0

```

```

ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!

```

A única alteração na configuração do hub é que o OSPF é o Routing Protocol em vez do EIGRP. Observe que o tipo de rede OSPF está definido como broadcast e a prioridade está definida como 2. Definir o tipo de rede OSPF para broadcast fará com que o OSPF instale rotas para redes através dos roteadores spokes com um endereço IP do próximo salto como o endereço de túnel GRE para esse roteador spoke.

roteador spoke1

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!

```

A configuração nos roteadores spoke agora é muito semelhante à configuração no hub. As diferenças são as seguintes:

- A prioridade de OSPF é definida como 0. Os roteadores de raio não podem se transformar em DR para a rede de multiacesso sem broadcast mGRE (NBMA). Somente o roteador de hubs possui conexões estáticas diretas com todos os roteadores de spoke. O DR deve ter acesso a todos os membros da rede NBMA.
- Há mapeamentos unicast e multicast de NHRP configurados para o roteador de hub.

```
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
```

Na configuração anterior, o **ip nhrp map multicast ...** não era necessário um comando, pois o túnel GRE era ponto a ponto. Nesse caso, os pacotes multicast serão automaticamente encapsulados através do túnel para o único destino possível. Esse comando agora é necessário porque o túnel GRE de spokes mudou para multipoint e há mais de um destino possível.

- Quando o roteador spoke surge, ele deve iniciar a conexão de túnel com o hub, desde que o roteador de hub não esteja configurado com nenhuma informação sobre os roteadores spoke e os roteadores spoke possam ter endereços IP atribuídos dinamicamente. Os roteadores de raio também são configurados com o concentrador, como seus NHRP NHS.

```
ip nhrp nhs 10.0.0.1
```

Com o comando acima, o roteador spoke enviará pacotes NHRP Registration (Registro de NHRP), por meio do túnel mGRE+Ipssec, ao roteador hub, em intervalos regulares. Esses pacotes de registro fornecem as informações de mapeamento do NHRP de raio necessárias pelo roteador de hub para pacotes de túnel de volta para os roteadores de raio.

```
roteador spoke2

version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.3 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
ip ospf network broadcast
ip ospf priority 0
 delay 1000
```

```

tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.3.1 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0
!

```

Roteador Spoke<n>

```

version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.<n+1> 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<n>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.

```

!

Observe que as configurações de todos os roteadores spoke são muito semelhantes. As únicas diferenças são os endereços IP nas interfaces locais. Isso ajuda a implantar um grande número de roteadores spoke. Todos os roteadores spoke podem ser configurados igualmente, e somente os endereços de interface de IP local precisam ser adicionados.

Neste ponto, examine as tabelas de roteamento e as tabelas de mapeamento NHRP nos roteadores Hub, Spoke1 e Spoke2 para ver as condições iniciais (logo após os roteadores Spoke1 e Spoke2 aparecerem) e as condições depois que Spoke1 e Spoke2 criaram um link dinâmico entre eles.

Condições iniciais

Informações sobre o roteador de hub

```
Hub#show ip route
    172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Ethernet0
    10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C       192.168.0.0/24 is directly connected, Ethernet1
O       192.168.1.0/24 [110/2] via 10.0.0.2, 00:19:53,
Tunnel0
O       192.168.2.0/24 [110/2] via 10.0.0.3, 00:19:53,
Tunnel0
Hub#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:57:27,
expire    00:04:13
    Type: dynamic, Flags: authoritative unique registered
    NBMA address: 172.16.1.24
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 07:11:25,
expire    00:04:33
    Type: dynamic, Flags: authoritative unique registered
    NBMA address: 172.16.2.75
Hub#show crypto engine connection active
  ID  Interface  IP-Address  State Algorithm
Encrypt Decrypt
 204 Ethernet0  172.17.0.1   set  HMAC_SHA+DES_56_CB
0
 205 Ethernet0  172.17.0.1   set  HMAC_SHA+DES_56_CB
0
 2628 Tunnel0     10.0.0.1     set  HMAC_MD5
0  402
 2629 Tunnel0     10.0.0.1     set  HMAC_MD5
357  0
 2630 Tunnel0     10.0.0.1     set  HMAC_MD5
0  427
 2631 Tunnel0     10.0.0.1     set  HMAC_MD5
308  0
```

Informações do Spoke1 Router

```
Spoke1#show ip route
    172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.24 is directly connected, Ethernet0
```



```

10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:31:46,
Tunnel0
C    192.168.1.0/24 is directly connected, Ethernet1
O    192.168.2.0/24 [110/2] via 10.0.0.3, 00:31:46,
Tunnel0
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
never expire
Type: static, Flags: authoritative used
NBMA address: 172.17.0.1
Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm
Encrypt Decrypt
  2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB
0      0
2064 Tunnel0 10.0.0.2 set HMAC_MD5
0      244
2065 Tunnel0 10.0.0.2 set HMAC_MD5
276      0

```

Informação do roteador Spoke2

```

Spoke2#show ip route
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Tunnel0
O    192.168.0.0/24 [110/2] via 10.0.0.1, 00:38:52,
Tunnel0
O    192.168.1.0/24 [110/2] via 10.0.0.2, 00:38:52,
Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet1
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:32:10,
never expire
Type: static, Flags: authoritative used
NBMA address: 172.17.0.1
Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm
Encrypt Decrypt
 17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB
0      0
2070 Tunnel0 10.0.0.3 set HMAC_MD5
0      279
2071 Tunnel0 10.0.0.3 set HMAC_MD5
316      0

```

Nesse ponto, emitimos o comando "ping" de 192.168.1.2 para 192.168.2.3. Estes endereços são para os hosts por trás dos roteadores Spoke1 e Spoke2, respectivamente. A sequência de eventos a seguir ocorre para criar o túnel spoke-to-spoke mGRE+IPsec.

1. O roteador Spoke1 recebe o pacote de ping com o destino 192.168.2.3. Ele procura esse destino na tabela de roteamento e descobre que precisa encaminhar esse pacote pela interface Tunnel0 para o IP Nexthop, 10.0.0.3.
2. O roteador Spoke1 verifica a tabela de mapeamento de NHRP para o destino 10.0.0.3 e descobre que não há entrada. O roteador Spoke1 cria um pacote de solicitação de resolução NHRP e o envia ao NHS (o roteador Hub).

3. O roteador do hub verifica o destino 10.0.0.3 em sua tabela de mapeamento NHRP e descobre que ele está mapeado para o endereço 172.16.2.75. O roteador Hub cria um pacote de resposta de resolução NHRP e o envia para o roteador Spoke1.
4. O roteador Spoke1 recebe a resposta de resolução NHRP e insere o mapeamento 10.0.0.3 → 172.16.2.75 na sua tabela de mapeamento NHRP. A adição do mapeamento de NHRP aciona o IPsec para iniciar um túnel IPsec com o peer 172.16.2.75.
5. O roteador Spoke1 inicia o ISAKMP com 172.16.2.75 e negocia as SAs ISAKMP e IPsec. O proxy IPsec é derivado do **comando tunnel source <address> Tunnel0** e do mapeamento NHRP.

```
local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
```

6. Quando o túnel IPsec terminar de ser criado, todos os pacotes de dados adicionais para a sub-rede 192.168.2.0/24 serão enviados diretamente para o Spoke2.
7. Depois que um pacote destinado a 192.168.2.3 for encaminhado ao host, esse host enviará um pacote de retorno para 192.168.1.2. Quando o roteador Spoke2 recebe este pacote destinado para o 192.168.1.2, ele verifica o destino na tabela de roteamento e identifica que ele deve encaminhá-lo para fora da interface Tunnel0 e para o próximo salto IP 10.0.0.2.
8. O roteador Spoke2 verifica o destino 10.0.0.2 na tabela de mapeamento NHRP e descobre que não há uma entrada. O roteador Spoke2 cria um pacote de solicitação de resolução de NHRP e o envia ao NHS (o roteador Hub).
9. O roteador do hub verifica o destino 10.0.0.2 em sua tabela de mapeamento NHRP e descobre que ele está mapeado para o endereço 172.16.1.24. O roteador de hub cria um pacote de resposta de resolução NHRP e o envia para o roteador Spoke2.
10. O roteador Spoke2 recebe a resposta de resolução NHRP e insere o mapeamento 10.0.0.2 → 172.16.1.24 em sua tabela de mapeamento NHRP. A inclusão do mapeamento de NHRP aciona IPsec para iniciar um túnel de IPsec com o peer 172.16.1.24, mas já existe um túnel de IPsec com esse peer; portanto, não é preciso fazer mais nada.
11. O Spoke1 e o Spoke2 agora podem encaminhar pacotes diretamente um para o outro. Se o mapeamento de NHRP não for utilizado para encaminhamento de pacotes do tempo de espera, esse mapeamento de NHRP será excluído. A exclusão da entrada de mapeamento NHRP acionará o IPsec para excluir os IPsec SAs desse link direto.

Condições depois que um link dinâmico é criado entre Spoke1 e Spoke2

Informações do Spoke1 Router

```
Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:34:16,
never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
 10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:05,
expire 00:03:35
  Type: dynamic, Flags: router unique used
  NBMA address: 172.16.2.75
Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm
Encrypt Decrypt
 2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB
```

```

0          0
   3 Ethernet0  172.16.1.24   set  HMAC_SHA+DES_56_CB
0          0
2064 Tunnel0   10.0.0.2           set  HMAC_MD5
0          375
2065 Tunnel0   10.0.0.2           set  HMAC_MD5
426        0
2066 Tunnel0   10.0.0.2           set  HMAC_MD5
0          20
2067 Tunnel0   10.0.0.2           set  HMAC_MD5
19         0

```

Informação do roteador Spoke2

```

Spoke2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 02:18:25,
never expire
   Type: static, Flags: authoritative used
   NBMA address: 172.17.0.1
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:00:24,
expire 00:04:35
   Type: dynamic, Flags: router unique used
   NBMA address: 172.16.1.24
Spoke2#show crypto engine connection active
  ID Interface  IP-Address  State Algorithm
Encrypt Decrypt
  17 Ethernet0  172.16.2.75   set  HMAC_SHA+DES_56_CB
0          0
  18 Ethernet0  172.16.2.75   set  HMAC_SHA+DES_56_CB
0          0
2070 Tunnel0   10.0.0.3       set  HMAC_MD5
0          407
2071 Tunnel0   10.0.0.3       set  HMAC_MD5
460        0
2072 Tunnel0   10.0.0.3       set  HMAC_MD5
0          19
2073 Tunnel0   10.0.0.3       set  HMAC_MD5
20         0

```

Na saída acima, você pode ver que Spoke1 e Spoke2 têm mapeamentos NHRP para cada um dos roteadores de hub, e construíram e usaram um túnel mGRE+IPsec. Os mapeamentos de NHRP irão expirar depois de cinco minutos (valor atual do tempo de espera de NHRP = 300 segundos). Se os mapeamentos de NHRP forem usados no último minuto antes de expirar, uma solicitação de resolução e resposta de NHRP serão enviadas para atualizar a entrada antes de ela ser excluída. Do contrato, o mapeamento NHRP será excluído e isso acionará o IPsec para limpar os SAs do IPsec.

IPSec VPN de multiponto dinâmico com hubs dual

Com algumas linhas de configuração adicionais para os roteadores spoke, você pode configurar roteadores hub duplos (ou múltiplos), para redundância. Há duas maneiras de configurar DMVPNs de hub duplo.

- Uma única rede DMVPN com cada spoke usando uma única interface de túnel GRE multiponto e apontando para dois hubs diferentes como o Next-Hop-Server (NHS). Os roteadores de hub só terão uma única interface de túnel GRE.
- Redes de DMVPN duplas com cada spoke tendo duas interfaces de túnel GRE (sejam elas

ponto a ponto ou multiponto) e cada túnel GRE conectado a um roteador de hub diferente. Novamente, os roteadores de hub terão apenas uma única interface de túnel GRE multiponto.

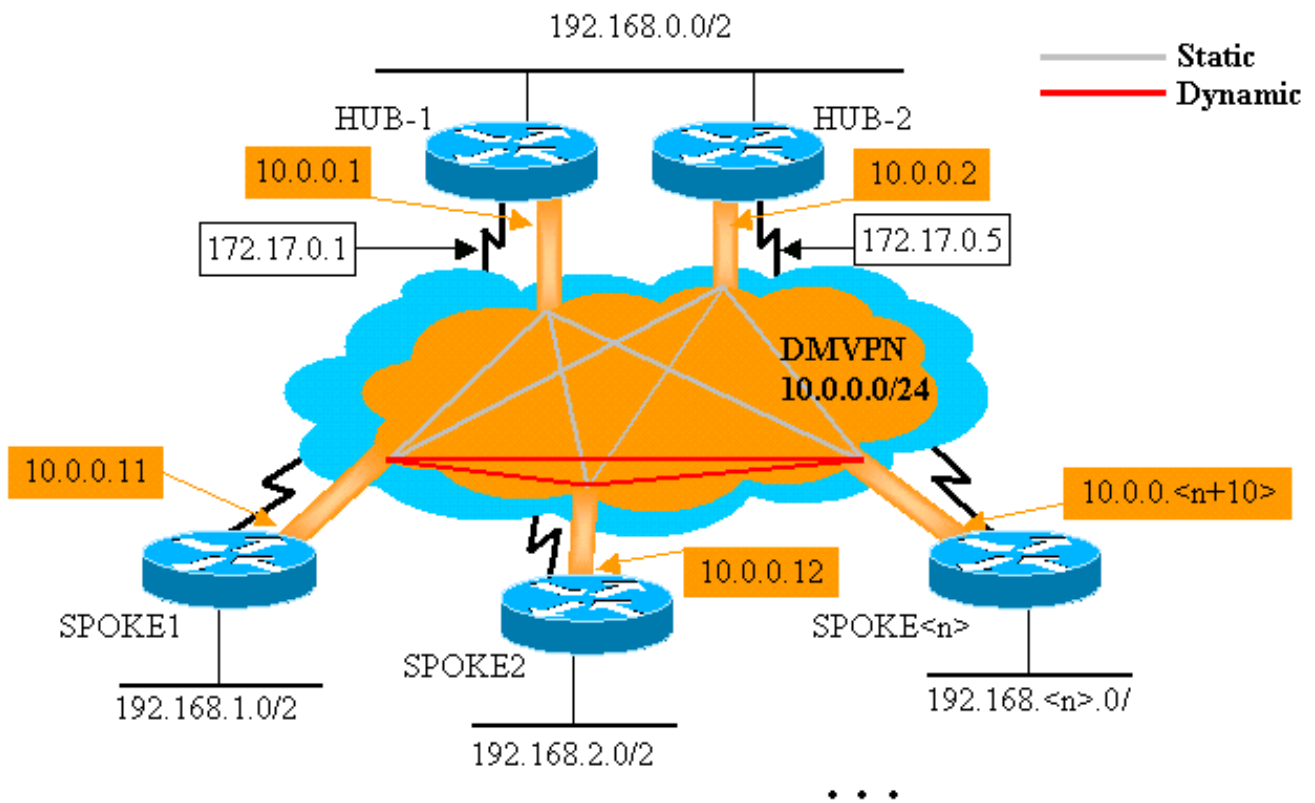
Os exemplos a seguir vão analisar a configuração desses dois cenários diferentes para DMVPNs de hub duplo. Na maioria dos casos, as diferenças realçadas são relativas à configuração do único concentrador de DMVPN.

Hub dual - Disposição de DMVPN única

O hub dual com a disposição de DMVPN único é bastante fácil de configurar, mas não permite tanto controle sobre o roteamento através do DMVPN como o hub dual com a disposição de DMVPN dual. A ideia nesse caso é ter uma única "nuvem" DMVPN com todos os hubs (dois nesse caso) e todos os spokes conectados a essa única sub-rede ("nuvem"). Os mapeamentos estáticos de NHRP dos spokes para os hubs definem os enlaces IPsec+mGRE estáticos nos quais o Dynamic Routing Protocol será executado. O Dynamic Routing Protocol não será executado nos links IPsec+mGRE entre os spokes. Como os roteadores spoke são vizinhos de roteamento com os roteadores de hub sobre a mesma interface de túnel mGRE, você não pode usar diferenças de link ou de interface (como métrica, custo, atraso ou largura de banda) para modificar as métricas do protocolo de roteamento dinâmico para preferir um hub ao outro quando ambos estiverem ativos. Se essa preferência for necessária, deve-se usar as técnicas internas da configuração do Routing Protocol. Por essa razão, pode ser melhor utilizar o EIGRP ou o RIP em vez de OSPF para o Dynamic Routing Protocol.

Observação: o problema acima é geralmente apenas um problema se os roteadores de hub estiverem co-localizados. Quando eles não são co-aloçados, o roteamento dinâmico normal provavelmente prefere o roteador de hub correto, mesmo quando a rede de destino pode ser alcançada por meio de qualquer um dos roteadores de hub.

Hub dual - Disposição de DMVPN única



Roteador de Hub

```

version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof

```

```

!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
!

```

Roteador do hub 2

```

version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
  bandwidth 900
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.1
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast
  ip ospf priority 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.5 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.2 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 1
  network 192.168.0.0 0.0.0.255 area 0
!

```

A única alteração na configuração do Hub1 é alterar o OSPF para usar duas áreas. A área 0 é usada para a rede subordinada aos dois hubs e a área 1 é usada para a rede DMVPN e redes subordinadas aos roteadores de raio. O OSPF poderia usar uma única área, mas duas áreas

foram usadas aqui para demonstrar a configuração de várias áreas de OSPF.

A configuração para o Hub2 é basicamente a mesma do Hub1, com as devidas alterações de endereço IP. A diferença principal é que o Hub2 também é um spoke (ou cliente) do Hub1, tornando o Hub1 o hub primário e o Hub2 o hub secundário. Isso é feito para que o Hub2 seja um vizinho OSPF com Hub1 sobre o túnel mGRE. Como o Hub1 é o DR da OSPF, ele deve possuir uma conexão direta com todos os outros roteadores da OSPF na interface mGRE (rede NBMA). Sem o link direto entre o Hub1 e o Hub2, o Hub2 não participaria do roteamento OSPF quando o Hub1 também está ativo. Quando o Hub1 estiver inativo, o Hub2 será o OSPF DR para o DMVPN (rede NBMA). Quando o Hub1 voltar a funcionar, ele assumirá a função de DR do OSPF para o DMVPN.

Os roteadores apoiados pelo Hub1 e pelo Hub2 utilizarão o Hub1 para enviar pacotes às redes spoke porque a largura de banda da interface de túnel GRE está definida como 1000 Kb/s versus 900 Kb/s no Hub2. Em comparação, os roteadores spoke enviam pacotes das redes atrás dos roteadores de hub para Hub 1 e Hub2, pois há apenas uma interface de túnel de mGRE em cada roteador spoke e haverá duas rotas de custo igual. Se o equilíbrio de carga por pacote estiver sendo usado, isso poderá causar pacotes estragados.

```
roteador spoke1

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.5
 ip nhrp map 10.0.0.2 172.17.0.5
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 ip nhrp nhs 10.0.0.2
 ip ospf network broadcast
 ip ospf priority 0
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
```

```

!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 1
 network 192.168.1.0 0.0.0.255 area 1
!

```

As diferenças na configuração dos roteadores de raio são as seguintes:

- Na nova configuração, o spoke é configurado com mapeamentos NHRP estáticos para o Hub2 e este é incluído como um próximo servidor de saltos. Original:

```

ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp nhs 10.0.0.1

```

Novo:

```

ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2

```

- As áreas de OSPF nos roteadores spoke foram alteradas para área 1.

Lembre-se de que, definindo o mapeamento estático NHRP e o NHS em um roteador de spoke para um hub, você irá executar o Dynamic Routing Protocol por esse túnel. Isso define o roteamento hub-and-spoke ou a rede vizinha. Observe que o Hub2 é um hub para todos os concentradores e também é um concentrador para Hub1. Facilita o design, a configuração e a modificação de redes multicamada hub-and-spoke quando você estiver usando a solução DMVPN.

 roteador spoke2 

```

version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast 172.17.0.1

```



```

ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2
ip ospf network broadcast
ip ospf priority 0
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
  ip address dhcp hostname Spoke1
!
interface Ethernet1
  ip address 192.168.2.1 255.255.255.0
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0
!

```

Roteador Spoke<n>

```

version 12.3
!
hostname Spoke<n>
!
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
!
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+10> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
ip nhrp map multicast 172.17.0.1
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp map multicast 172.17.0.5
ip nhrp map 10.0.0.2 172.17.0.5
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip nhrp nhs 10.0.0.2
ip ospf network broadcast
ip ospf priority 0
delay 1000
tunnel source Ethernet0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof

```

```

!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 network 192.168.
!

```

Neste ponto, você pode observar as tabelas de roteamento, as tabelas de mapeamento NHRP e as conexões IPsec nos roteadores Hub1, Hub2, Spoke1 e Spoke2 para ver as condições iniciais (logo após os roteadores Spoke1 e Spoke2 aparecerem).

Condições e alterações iniciais

Informação do Hub1 Router

```

Hub1#show ip route
 172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 C       192.168.0.0/24 is directly connected, Ethernet1
 O       192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17,
Tunnel0
 O       192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17,
Tunnel0
Hub1#show ip nhrp
 10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.17.0.5
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:49
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 1w3d,
expire 00:04:06
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
Hub1#show crypto engine connection active
 ID Interface IP-Address State Algorithm
Encrypt Decrypt
  4 Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB
0
  5 Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB
0
  6 Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB
0
3532 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB
0 232
3533 Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB

```

```

212      0
 3534 Tunnel0      10.0.0.1      set  HMAC_MD5+DES_56_CB
0        18
 3535 Tunnel0      10.0.0.1      set  HMAC_MD5+DES_56_CB
17       0
 3536 Tunnel0      10.0.0.1      set  HMAC_MD5+DES_56_CB
0        7
 3537 Tunnel0      10.0.0.1      set  HMAC_MD5+DES_56_CB
7        0

```

Informação do Hub2 Router

```

Hub2#show ip route
      172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C      192.168.0.0/24 is directly connected, Ethernet1
O      192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15,
Tunnel0
O      192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15,
Tunnel0
Hub2#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 1w3d,
expire 00:03:15
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.24
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 00:46:17,
expire 00:03:51
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.75
Hub2#show crypto engine connection active
  ID Interface  IP-Address  State Algorithm
Encrypt Decrypt
  4 Ethernet0   171.17.0.5   set  HMAC_SHA+DES_56_CB
0        0
  5 Ethernet0   171.17.0.5   set  HMAC_SHA+DES_56_CB
0        0
  6 Ethernet0   171.17.0.5   set  HMAC_SHA+DES_56_CB
0        0
 3520 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
0        351
 3521 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
326      0
 3522 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
0        311
 3523 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
339      0
 3524 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
0        25
 3525 Tunnel0     10.0.0.2     set  HMAC_MD5+DES_56_CB
22       0

```

Informações do Spoke1 Router

```

Spoke1#show ip route
      172.16.0.0/24 is subnetted, 1 subnets

```

```

C      172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
C      10.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31,
Tunnel0
      [110/11] via 10.0.0.2, 00:39:31,
Tunnel0
C      192.168.1.0/24 is directly connected, Ethernet1
O      192.168.2.0/24 [110/2] via 10.0.0.12, 00:37:58,
Tunnel0
Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:56:40,
never expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active
  ID Interface  IP-Address  State Algorithm
Encrypt Decrypt
   1 Ethernet0  172.16.1.24  set  HMAC_SHA+DES_56_CB
0      0
   2 Ethernet0  172.16.1.24  set  HMAC_SHA+DES_56_CB
0      0
 2010 Tunnel0   10.0.0.11   set  HMAC_MD5+DES_56_CB
0      171
 2011 Tunnel0   10.0.0.11   set  HMAC_MD5+DES_56_CB
185    0
 2012 Tunnel0   10.0.0.11   set  HMAC_MD5+DES_56_CB
0      12
 2013 Tunnel0   10.0.0.11   set  HMAC_MD5+DES_56_CB
13     0

```

Informação do roteador Spoke2

```

Spoke2#show ip route
      172.16.0.0/24 is subnetted, 1 subnets
C      172.16.2.0 is directly connected, Ethernet0
      10.0.0.0/24 is subnetted, 1 subnets
C      10.0.0.0 is directly connected, Tunnel0
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56,
Tunnel0
      [110/11] via 10.0.0.2, 00:57:56,
Tunnel0
O      192.168.1.0/24 [110/2] via 10.0.0.11, 00:56:14,
Tunnel0
C      192.168.2.0/24 is directly connected, Ethernet1
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.1
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 6w6d, never
expire
  Type: static, Flags: authoritative used
  NBMA address: 172.17.0.5
Spoke2#show crypto engine connection active
  ID Interface  IP-Address  State Algorithm
Encrypt Decrypt
   2 Ethernet0  172.16.2.75  set  HMAC_SHA+DES_56_CB

```

0	0				
	3	Ethernet0	172.16.2.75	set	HMAC_SHA+DES_56_CB
0	0				
	3712	Tunnel0	10.0.0.12	set	HMAC_MD5+DES_56_CB
0	302				
	3713	Tunnel0	10.0.0.12	set	HMAC_MD5+DES_56_CB
331	0				
	3716	Tunnel0	10.0.0.12	set	HMAC_MD5+DES_56_CB
0	216				
	3717	Tunnel0	10.0.0.12	set	HMAC_MD5+DES_56_CB
236	0				

Há um alguns problemas interessantes a serem destacados a respeito das tabelas de roteamento no Hub1, Hub2, Spoke1 e Spoke2:

- Os dois roteadores do concentrador possuem rotas de custos iguais para as redes por trás dos roteadores de raio.Hub1:

```
O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0
O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0
```

Hub2:

```
O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0
O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0
```

Isso significa que Hub1 e Hub 2 anunciarão o mesmo custo das redes atrás dos roteadores de spoke para os roteadores na rede atrás dos roteadores de hub. Por exemplo, a tabela de roteamento em um roteador, R2, que esteja conectada diretamente à LAN 192.168.0.0/24 seria assim:R2:

```
O IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/30
O IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3
```

- Os roteadores spoke possuem rotas de custo equivalentes por meio dos roteadores de hub para a rede por trás dos roteadores de hub.Spoke1:

```
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
[110/11] via 10.0.0.2, 00:39:31, Tunnel0
```

Spoke2:

```
O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
[110/11] via 10.0.0.2, 00:57:56, Tunnel0
```

Se os roteadores de spoke estiverem fazendo balanceamento de carga por pacote, você poderá obter pacotes fora de ordem.

Para evitar o roteamento assimétrico ou o balanceamento de carga por pacote nos enlaces para os dois concentradores, você precisa configurar o Routing Protocol para preferir um caminho do tipo “spoke-to-hub” em ambas as direções. Se você desejar que o Hub1 seja o principal e o Hub2 o backup, você pode configurar para que o custo de OSPF nas interfaces de túnel de hub seja diferente.

Hub1:

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2:

```
interface tunnel0
```

```
...
ip ospf cost 20
```

Agora as rotas são apresentadas da seguinte forma:

Hub1:

```
O    192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O    192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Hub2:

```
O    192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O    192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O    IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O    IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Os dois roteadores hub agora têm custos diferentes nas rotas das redes por trás dos roteadores spoke. Isso significa que o Hub1 será preferido para encaminhar o tráfego aos roteadores spoke, como pode ser visto no roteador R2. Isso cuidará do problema de roteamento assimétrico descrito no primeiro marcador acima.

O roteamento assimétrico na outra direção, conforme descrito no segundo item com marcador acima, ainda está lá. Ao usar o OSPF como o protocolo de roteamento dinâmico, você pode corrigir isso com uma solução alternativa usando a **distância ...** sob **router ospf 1** nos spokes para preferir rotas aprendidas via Hub1 sobre rotas aprendidas via Hub2.

Spoke1:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
 access-list 1 permit any
```

Spoke2:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
 access-list 1 permit any
```

Agora as rotas são apresentadas da seguinte forma:

Spoke1:

```
O    192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Spoke2:

```
O    192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

A configuração de roteamento acima protegerá contra roteamento assimétrico, enquanto permite o failover para o hub2 caso o hub1 fique inativo. Significa que quando os dois hubs estão ativados, apenas o Hub 1 é usado. É possível que a configuração de roteamento se torne

complexa, especialmente se estiver usando o OSPF, caso deseje usar os dois hubs, balanceando os spokes nos hubs, com proteção contra failover e roteamento não assimétrico. Por esta razão, o concentrador dual com disposição DMVPN dual pode ser a melhor opção.

Hub duplo - Disposição de DMVPN dupla

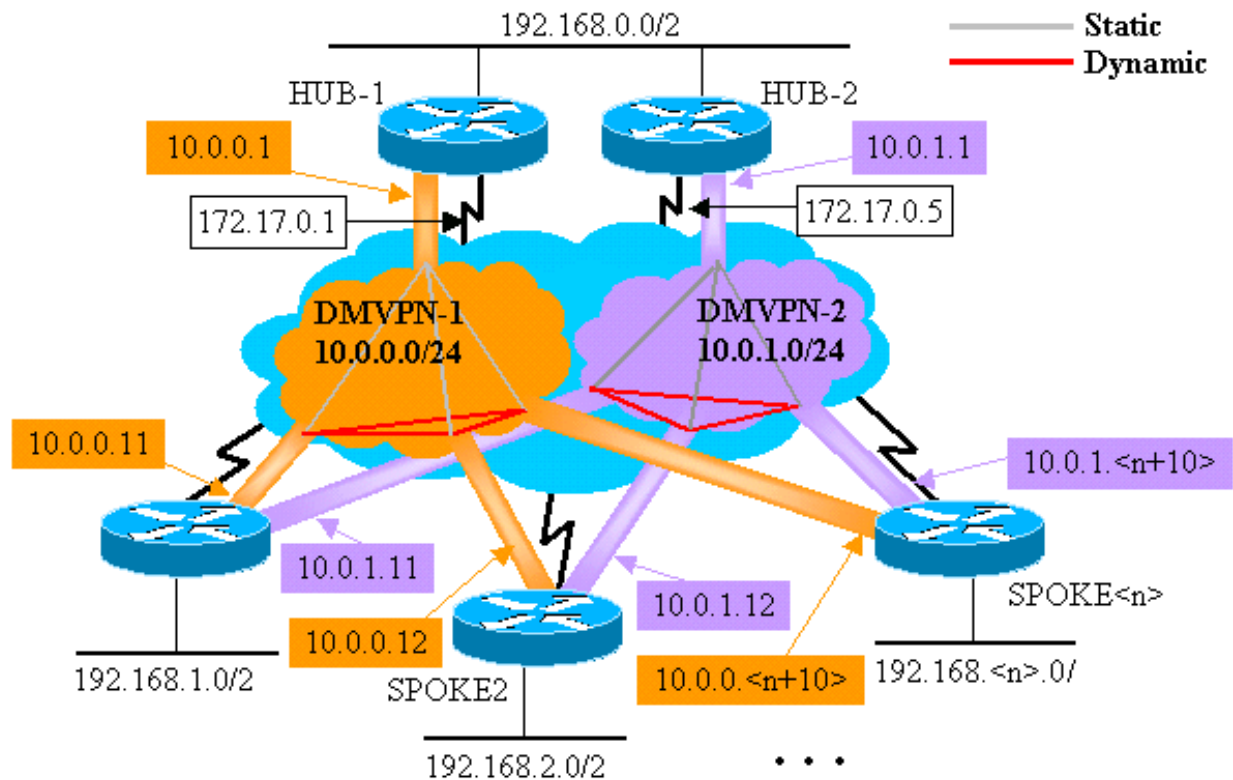
O hub duplo, com layout duplo de DMVPN, é ligeiramente mais difícil de configurar, mas proporciona um controle melhor do roteamento através do DMVPN. A ideia é ter duas "nuvens" DMVPN separadas. Cada hub (dois nesse caso) está conectado a uma sub-rede DMVPN ("rede") e os spokes estão conectados nas duas sub-redes DMVPN ("redes"). Como os roteadores spoke estão fazendo o roteamento dos vizinhos com os dois roteadores hub nas duas interfaces de túnel GRE, você pode usar as diferenças de configuração de interface (por exemplo, largura de banda, custo e retardo) para modificar a métrica do Dynamic Routing Protocol e escolher um dos dois hubs quando ambos estiverem conectados.

Observação: o problema acima geralmente só é relevante se os roteadores de hub estiverem co-localizados. Quando eles não são co-aloçados, o roteamento dinâmico normal provavelmente prefere o roteador de hub correto, mesmo quando a rede de destino pode ser alcançada por meio de qualquer um dos roteadores de hub.

Você pode usar interfaces de túnel p-pGRE ou mGRE nos roteadores spoke. Várias interfaces p-pGRE em um roteador spoke podem usar a mesma **origem de túnel ...** Endereço IP, mas várias interfaces mGRE em um roteador spoke devem ter uma **origem de túnel** exclusiva ... Endereço IP. Isso acontece porque, quando o IPsec está iniciando, o primeiro pacote é um pacote ISAKMP que precisa ser associado a um dos túneis mGRE. O pacote ISAKMP apresenta apenas o endereço IP de destino (endereço do peer IPsec remoto) com o qual a associação deve ser estabelecida. Este endereço é comparado com a **origem do túnel ...** endereço, mas como ambos os túneis têm a mesma **origem de túnel ...** endereço, a primeira interface de túnel mGRE é sempre comparada. Isso significa que os pacotes de dados de multicast recebidos podem estar associados à interface mGRE errada, quebrando qualquer Dynamic Routing Protocol.

Os próprios pacotes GRE não têm esse problema, pois têm a **chave do túnel ...** para diferenciar as duas interfaces mGRE. Começando nas versões 12.3(5) e 12.3(7)T do software Cisco IOS, um parâmetro adicional foi introduzido para superar essa limitação: **proteção de túnel...compartilhado**. A palavra-chave **compartilhada** indica que várias interfaces mGRE usarão a criptografia IPsec com o mesmo endereço IP de origem. Se você tiver uma versão anterior, poderá usar túneis p-pGRE neste hub duplo com layout DMVPN duplo. No caso do túnel p-pGRE, a **origem do túnel ...** e o **destino do túnel ...** Os endereços IP podem ser usados para correspondência. Para este exemplo, os túneis p-pGRE serão usados neste hub duplo com layout DMVPN duplo e não usarão o qualificador **compartilhado**.

Hub duplo - Disposição de DMVPN dupla



As seguintes alterações destacadas são relativas às configurações dinâmicas de concentrador e ponto remoto multiponto ilustradas anteriormente nesse documento.

Roteador do hub 1

```

version 12.3
!
hostname Hub1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint

```



```
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

Roteador do hub 2

```
version 12.3
!
hostname Hub2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.1.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100001
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.5 255.255.255.252
!
interface Ethernet1
 ip address 192.168.0.2 255.255.255.0
!
router eigrp 1
 network 10.0.1.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

Nesse caso, as configurações de Hub1 e Hub2 são semelhantes. A principal diferença é que cada um é o hub de um DMVPN diferente. Cada DMVPN usa um diferente:

- Sub-rede de IP (10.0.0.0/24, 10.0.0.1/24)
- Identificação de rede NHRP (100000, 100001)
- Chave de túnel (100000, 100001)

O Dynamic Routing Protocol foi comutado de OSPF para EIGRP, uma vez que é mais fácil configurar e gerenciar uma rede de NBMA usando EIGRP, conforme descrito mais adiante neste documento.

roteador spoke1

```

version 12.3
!
hostname Spoke1
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
router eigrp 1

```

```
network 10.0.0.0 0.0.0.255
network 10.0.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
no auto-summary
!
```

Cada roteador de spoke é configurado com duas interfaces de túnel p-pGRE, uma em cada DMVPN. O endereço ip ..., ip nhrp network-id ..., tunnel key ... e destino do túnel ... são usados para diferenciar entre os dois túneis. O Dynamic Routing Protocol, EIGRP, é executado em ambas as sub-redes de túnel p-pGRE e é usado para selecionar uma interface p-pGRE (DMVPN) em vez da outra.

roteador spoke2

```
version 12.3
!
hostname Spoke2
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnell
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke2
```

```
!  
interface Ethernet1  
 ip address 192.168.2.1 255.255.255.0  
!  
router eigrp 1  
 network 10.0.0.0 0.0.0.255  
 network 10.0.1.0 0.0.0.255  
 network 192.168.2.0 0.0.0.255  
 no auto-summary  
!
```

Roteador Spoke<n>

```
version 12.3  
!  
hostname Spoke<n>  
!  
crypto isakmp policy 1  
 authentication pre-share  
crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0  
!  
crypto ipsec transform-set trans2 esp-des esp-md5-hmac  
 mode transport  
!  
crypto ipsec profile vpnprof  
 set transform-set trans2  
!  
interface Tunnel0  
 bandwidth 1000  
 ip address 10.0.0.  
  
 ip mtu 1400  
 ip nhrp authentication test  
 ip nhrp map 10.0.0.1 172.17.0.1  
 ip nhrp network-id 100000  
 ip nhrp holdtime 300  
 ip nhrp nhs 10.0.0.1  
 delay 1000  
 tunnel source Ethernet0  
 tunnel destination 172.17.0.1  
 tunnel key 100000  
 tunnel protection ipsec profile vpnprof  
!  
interface Tunnel1  
 bandwidth 1000  
 ip address 10.0.1.  
  
 ip mtu 1400  
 ip nhrp authentication test  
 ip nhrp map 10.0.1.1 172.17.0.5  
 ip nhrp network-id 100001  
 ip nhrp holdtime 300  
 ip nhrp nhs 10.0.1.1  
 delay 1000  
 tunnel source Ethernet0
```

```

tunnel destination 172.17.0.5
tunnel key 100001
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address dhcp hostname Spoke<x>
!
interface Ethernet1
 ip address 192.168.<n>.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.<n>.0 0.0.0.255
 no auto-summary
!

```

Neste ponto, vamos observar as tabelas de roteamento, as tabelas de mapeamento NHRP e as conexões IPsec nos roteadores Hub1, Hub2, Spoke1 e Spoke2 para ver as condições iniciais (logo após os roteadores Spoke1 e Spoke2 aparecerem).

Condições e alterações iniciais

Informação do Hub1 Router

```

Hub1#show ip route
 172.17.0.0/30 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 2 subnets
 C       10.0.0.0 is directly connected, Tunnel0
 D       10.0.1.0 [90/2611200] via 192.168.0.2,
00:00:46, Ethernet1
 C       192.168.0.0/24 is directly connected, Ethernet1
 D       192.168.1.0/24 [90/2841600] via 10.0.0.11,
00:00:59, Tunnel0
 D       192.168.2.0/24 [90/2841600] via 10.0.0.12,
00:00:34, Tunnel0
Hub1#show ip nhrp
 10.0.0.12/32 via 10.0.0.12, Tunnel0 created 23:48:32,
expire 00:03:50
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.2.75
 10.0.0.11/32 via 10.0.0.11, Tunnel0 created 23:16:46,
expire 00:04:45
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 172.16.1.24
Hub1#show crypto engine connection active
 ID Interface  IP-Address  State  Algorithm
Encrypt Decrypt
 15 Ethernet0  172.17.63.18  set
HMAC_SHA+DES_56_CB      0      0
 16 Ethernet0  10.0.0.1      set
HMAC_SHA+DES_56_CB      0      0
 2038 Tunnel0   10.0.0.1      set
HMAC_MD5+DES_56_CB     0      759
 2039 Tunnel0   10.0.0.1      set
HMAC_MD5+DES_56_CB     726     0
 2040 Tunnel0   10.0.0.1      set
HMAC_MD5+DES_56_CB     0      37
 2041 Tunnel0   10.0.0.1      set

```

Informação do Hub2 Router

```
Hub2#show ip route
 172.17.0.0/30 is subnetted, 1 subnets
 C    172.17.0.4 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 2 subnets
 D    10.0.0.0 [90/2611200] via 192.168.0.1,
00:12:22, Ethernet1
 C    10.0.1.0 is directly connected, Tunnel0
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.1.11,
00:13:24, Tunnel0
 D    192.168.2.0/24 [90/2841600] via 10.0.1.12,
00:12:11, Tunnel0
Hub2#show ip nhrp
 10.0.1.12/32 via 10.0.1.12, Tunnel3 created 06:03:24,
expire 00:04:39
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.2.75
 10.0.1.11/32 via 10.0.1.11, Tunnel3 created 23:06:47,
expire 00:04:54
   Type: dynamic, Flags: authoritative unique registered
   NBMA address: 172.16.1.24
Hub2#show crypto engine connection active
  ID Interface  IP-Address  State  Algorithm
Encrypt Decrypt
  4 Ethernet0  171.17.0.5   set
HMAC_SHA+DES_56_CB      0      0
  6 Ethernet0  171.17.0.5   set
HMAC_SHA+DES_56_CB      0      0
 2098 Tunnel0   10.0.1.1     set
HMAC_MD5+DES_56_CB      0     722
 2099 Tunnel0   10.0.1.1     set
HMAC_MD5+DES_56_CB     690      0
 2100 Tunnel0   10.0.1.1     set
HMAC_MD5+DES_56_CB      0     268
 2101 Tunnel0   10.0.1.1     set
HMAC_MD5+DES_56_CB     254      0
```

Informações do Spoke1 Router

```
Spoke1#show ip route
 172.16.0.0/24 is subnetted, 1 subnets
 C    172.16.1.0 is directly connected, Ethernet0
 10.0.0.0/24 is subnetted, 1 subnets
 C    10.0.0.0 is directly connected, Tunnel0
 C    10.0.1.0 is directly connected, Tunnel1
 D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:26:30, Tunnel1
                                [90/2841600] via 10.0.0.1,
00:26:30, Tunnel0
 C    192.168.1.0/24 is directly connected, Ethernet1
 D    192.168.2.0/24 [90/3097600] via 10.0.1.1,
00:26:29, Tunnel1
                                [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0
Spoke1#show ip nhrp
 10.0.0.1/32 via 10.0.0.1, Tunnel0 created 23:25:46,
never expire
   Type: static, Flags: authoritative
```

```

NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire
Type: static, Flags: authoritative
NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm
Encrypt Decrypt
16 Ethernet0 172.16.1.24 set
HMAC_SHA+DES_56_CB 0 0
18 Ethernet0 172.16.1.24 set
HMAC_SHA+DES_56_CB 0 0
2118 Tunnel0 10.0.0.11 set
HMAC_MD5+DES_56_CB 0 181
2119 Tunnel0 10.0.0.11 set
HMAC_MD5+DES_56_CB 186 0
2120 Tunnel1 10.0.1.11 set
HMAC_MD5+DES_56_CB 0 105
2121 Tunnel1 10.0.1.11 set
HMAC_MD5+DES_56_CB 110 0

```

Informação do roteador Spoke2

```

Spoke2#show ip route
172.16.0.0/24 is subnetted, 1 subnets
C    172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
C    10.0.0.0 is directly connected, Tunnel0
C    10.0.1.0 is directly connected, Tunnel1
D    192.168.0.0/24 [90/2841600] via 10.0.1.1,
00:38:04, Tunnel1
                                [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.1.1,
00:38:02, Tunnel1
                                [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0
C    192.168.2.0/24 is directly connected, Ethernet1
Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1d02h, never
expire
Type: static, Flags: authoritative used
NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 1d02h, never
expire
Type: static, Flags: authoritative used
NBMA address: 172.17.0.5
Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm
Encrypt Decrypt
8 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0
9 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0
2036 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 585
2037 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 614 0
2038 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 0 408
2039 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 424 0

```

Novamente, existem alguns fatores interessantes a serem observados sobre tabelas de roteamento em Hub1, Hub2, Spoke1 e Spoke2:

- Os dois roteadores do concentrador possuem rotas de custos iguais para as redes por trás dos roteadores de raio. Hub1:

```
D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0
```

Hub2:

```
D 192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0
```

Isso significa que Hub1 e Hub 2 anunciarão o mesmo custo das redes atrás dos roteadores de spoke para os roteadores na rede atrás dos roteadores de hub. Por exemplo, a tabela de roteamento em um roteador, R2, que esteja conectado diretamente à LAN 192.168.0.0/24 seria assim:R2:

```
D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                               [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D 192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                               [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
```

- Os roteadores spoke possuem rotas de custo equivalentes por meio dos roteadores de hub para a rede por trás dos roteadores de hub. Spoke1:

```
D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1
                               [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0
```

Spoke2:

```
D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                               [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0
```

Se os roteadores spoke estiverem fazendo balanceamento de carga por pacote, você poderá obter pacotes fora de ordem.

Para evitar o roteamento assimétrico ou o balanceamento de carga por pacote nos enlaces para os dois concentradores, você precisa configurar o Routing Protocol para preferir um caminho do tipo “spoke-to-hub” em ambas as direções. Se você deseja que o Hub1 seja o principal e o Hub2 seja o backup, você pode definir o atraso nas interfaces do túnel de hub como diferente.

Hub1:

```
interface tunnel0
...
delay 1000
...
```

Hub2:

```
interface tunnel0
...
delay 1050
...
```

Observação: neste exemplo, 50 foi adicionado ao atraso na interface do túnel no Hub2 porque é menor que o atraso na interface Ethernet1 entre os dois hubs (100). Fazendo isso, o Hub2 continuará a encaminhar pacotes diretamente para os roteadores spoke, mas anunciará uma rota menos desejável que o Hub1 para roteadores atrás de Hub1 e Hub2. Se o atraso fosse aumentado em mais de 100, o Hub2 encaminharia pacotes para os roteadores spoke através do Hub1 através da interface Ethernet1, embora os roteadores atrás do Hub1 e do Hub2 ainda preferissem corretamente o Hub-1 para enviar pacotes aos roteadores spoke.

Agora as rotas são apresentadas da seguinte forma:

Hub1:

```
D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2:

```
D 192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D 192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D 192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Os dois roteadores de hub têm diferentes custos para as rotas da rede para os roteadores de spoke, portanto, nesse caso, o Hub1 será preferido para encaminhar tráfego para os roteadores de spoke, como se vê em R2. Isso resolve o problema descrito no primeiro marcador acima.

O problema descrito no segundo marcador acima ainda existe, mas como você tem duas interfaces de túnel p-pGRE, você pode definir o **atraso** ... nas interfaces de túnel separadamente para alterar a métrica do EIGRP para as rotas aprendidas de Hub1 versus Hub2.

Spoke1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Agora as rotas são apresentadas da seguinte forma:

Spoke1:

```
D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D 192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2:

```
D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D 192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

A configuração de roteamento acima protegerá contra roteamento assimétrico, enquanto permite o failover para o hub2 caso o hub1 fique inativo. Significa que quando os dois hubs estão ativados, apenas o Hub 1 é usado.

Se você quiser usar ambos os hubs balanceando os spokes nos hubs, com proteção contra failover e sem roteamento assimétrico, a configuração de roteamento é mais complexa, mas você

pode fazer isso ao usar o EIGRP. Para fazer isso, defina o **atraso...** nas interfaces de túnel dos roteadores de hub, retorne a ser igual e use o comando **offset-list <acl> out <offset> <interface>** nos roteadores de spoke para aumentar a métrica EIGRP para rotas anunciadas nas interfaces de túnel GRE para o hub de backup. O **atraso desigual...** entre as interfaces Tunnel0 e Tunnel1 no spoke ainda é usado, de modo que o roteador spoke preferirá seu roteador hub primário. As alterações nos roteadores de raio são as seguintes:

roteador spoke1

```
version 12.3
!
hostname Spoke1
!
...
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.11 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1500
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
 offset-list 1 out 12800 Tunnel1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.1.0
 distribute-list 1 out
 no auto-summary
!
access-list 1 permit 192.168.1.0
!
```

roteador spoke2

```

version 12.3
!
hostname Spoke2
!
...
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp network-id 100000
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.0.1
 delay 1500
 tunnel source Ethernet0
 tunnel destination 172.17.0.1
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Tunnel1
 bandwidth 1000
 ip address 10.0.1.12 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map 10.0.1.1 172.17.0.5
 ip nhrp network-id 100001
 ip nhrp holdtime 300
 ip nhrp nhs 10.0.1.1
 delay 1000
 tunnel source Ethernet0
 tunnel destination 172.17.0.5
 tunnel key 100001
 tunnel protection ipsec profile vpnprof
!
...
!
router eigrp 1
 offset-list 1 out 12800 Tunnel1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 network 192.168.2.0
 distribute-list 1 out
 no auto-summary
!
 access-list 1 permit 192.168.2.0
!

```

Observação: o valor de deslocamento de 12800 (50×256) foi adicionado à métrica do EIGRP porque é menor que 25600 (100×256). É este valor (25600) que é adicionado à métrica do EIGRP para as rotas aprendidas entre os roteadores do hub. Usando 12800 no comando **offset-list**, o roteador de hub de backup encaminhará pacotes diretamente para os roteadores spoke, em vez de encaminhar esses pacotes via Ethernet para passar pelo roteador de hub primário para esses spokes. A métrica nas rotas anunciadas pelos roteadores hub ainda será aquela em que o roteador hub principal correto será o preferido. Lembre-se de que metade dos spokes possuem o hub1 como seu roteador primário e a outra metade o hub 2.

Observação: se o valor de deslocamento fosse aumentado em mais de 25600 (100×256), os hubs encaminhariam pacotes para metade dos roteadores spoke através do outro hub através da

interface Ethernet1, mesmo que os roteadores atrás dos hubs ainda preferissem o hub correto para enviar pacotes aos roteadores spoke.

Observação: o comando **distribute-list 1 out** também foi adicionado, pois é possível que as rotas aprendidas de um roteador de hub através de uma interface de túnel em um spoke possam ser anunciadas de volta ao outro hub através do outro túnel. A **lista de distribuição ...** garante que o roteador spoke só possa anunciar suas próprias rotas.

Observação: se você preferir controlar os anúncios de roteamento nos roteadores de hub em vez de nos roteadores de spoke, os **offset-list <acl1> em <value> <interface>** e **distribute-list <acl2> nos** comandos podem ser configurados nos roteadores de hub em vez de nos spokes. A lista de acesso <acl2> listaria as rotas por trás de todos os spokes e a lista de acesso <acl1> listaria apenas as rotas por trás dos spokes, onde outro roteador de hub será o hub principal.

Com essas alterações, as rotas se parecem com as seguintes:

Hub1:

```
D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D 192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2:

```
D 192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D 192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D 192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1:

```
D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2:

```
D 192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

Conclusão

A solução DMVPN fornece a seguinte funcionalidade para dimensionar melhor redes VPN IPsec grandes e pequenas.

- O DMVPN permite melhor dimensionamento em VPNs IPsec de malha completa ou em malha parcial. Ele é especialmente útil quando o tráfego spoke-to-spoke é esporádico (por exemplo, cada spoke não está enviando dados constantemente para cada outro spoke). Ele permite que qualquer spoke envie dados diretamente a qualquer outro spoke, desde que haja conectividade IP direta entre os spokes.
- O DMVPN suporta nós IPsec com endereços atribuídos dinamicamente (como cabo, ISDN e DSL). Isto se aplica a hub-e-spoke e também a redes em malha. É possível que o DMVPN requirite que o link hub-spoke esteja constantemente ativo.

- O DMVPN simplifica a adição de nós de VPN. Para adicionar um novo roteador de spoke, basta configurá-lo e conectá-lo à rede (embora talvez seja necessário adicionar informações de autorização do ISAKMP para o novo spoke no hub). O hub aprenderá dinamicamente sobre o novo spoke e o protocolo de roteamento dinâmico propagará o roteamento para o hub e todos os outros spokes.
- O DMVPN reduz o tamanho da configuração necessária em todos os roteadores na VPN. Esse também é o caso das redes VPN somente hub-and-spoke de GRE+IPsec.
- O DMVPN usa o GRE e, portanto, suporta o tráfego de roteamento dinâmico e multicast de IP no VPN. Isso significa que um protocolo de roteamento dinâmico pode ser usado, e "hubs" redundantes podem ser suportados pelo protocolo. São suportados aplicativos multicast também.
- O DMVPN oferece suporte ao tunelamento dividido nos spokes.

[Informações Relacionadas](#)

- [Dynamic Multipoint VPN \(DMVPN\)](#)
- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)