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

Índice

Introdução

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 o Internet como a interconexão entre o hub e o spokes, o spokes igualmente tem de acesso direto entre si sem o custo adicional, mas foi muito difícil, se não impossível, estabelecer e/ou controlar uma rede de malha (parcial) completa. 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 os recursos do hub dos usos do hub e pode incorrer atrasos do acréscimo, especialmente ao usar a criptografia IPSec, desde que o hub precisará de decifrar os pacotes recebidos do spokes de emissão e recriptografar o tráfego dos enviar então 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.

Enquanto as redes de hub-and-spoke do IPsec foram distribuídas e cresceram em tamanho, tornou-se mais desejável mandá-las distribuir tão dinamicamente pacotes IP como possível. Nas redes de hub-and-spoke mais velhas do Frame Relay isto foi realizado executando um protocolo de roteamento dinâmico como o OSPF ou o EIGRP sobre os Link 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 de IPsec e protocolos de roteamento dinâmico. Os protocolos de roteamento dinâmico confiam em usar o Protocolo IP multicast ou os pacotes de transmissão, mas o IPsec não apoia o Multicast de criptografia ou os pacotes de transmissão. O método atual de solução desse problema é utilizar Generic Routing Encapsulation (GRE) Tunnels em combinação com criptografia de IPSec.

Os túneis GRE apoiam o transporte do Protocolo IP multicast e dos pacotes de transmissão à 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 forem configurados, os endereços IP de Um ou Mais Servidores Cisco ICM NT para os valores-limite do túnel (**origem de túnel…**, o **destino de túnel…**) deve ser sabido pelo outro valor-limite e deve ser o roteável sobre o Internet. Isto significa que o hub e todo o Roteadores do spoke nesta rede devem ter endereços IP de Um ou Mais Servidores Cisco ICM NT NON-privados estáticos.

Para conexões pequenas do local ao Internet, é típico para que o endereço IP externo de um raio mude cada vez que conecta ao Internet porque seu provedor de serviço do Internet (ISP) fornece dinamicamente o endereço de interface externa (através do protocolo de configuração dinâmica host (DHCP)) cada vez que o spoke vem na linha (Asymmetric Digital Subscriber Line (ADSL) 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 limitações acima e algumas outro são resumidas nos seguintes quatro pontos:

- O IPsec usa um Access Control List (ACL) para definir que dados devem ser cifrada. 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 grandes redes de hub-and-spoke, o tamanho da configuração no roteador de hub pode tornar-se muito grande, até ao ponto em que é inusável. 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 a necessidade do spokes de falar diretamente um com o otro sobre o IPSec VPN, então a rede de hub-and-spoke deve se transformar uma malha cheia. Desde que já não se sabe que spokes precisará de falar diretamente um com o otro, uma malha cheia é exigida, mesmo que cada spoke não possa precisar de falar diretamente com cada outro spoke. Também, não é praticável configurar o IPsec em um roteador pequeno do spoke de modo que tenha a conectividade direta com todo Roteadores restante do spoke na rede; falou assim o Roteadores pode precisar de ser mais roteadores 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

Ao não usar a solução de DMVPN, o túnel de criptografia IPSec não é iniciado até que haja o tráfego de dados que exige o uso deste túnel de IPsec. Pode tomar 1 aos segundos 10 para terminar a iniciação do túnel de IPsec e o tráfego de dados é deixado cair durante este tempo. Ao usar o GRE com IPsec, a configuração do túnel GRE já inclui o par do túnel GRE (o **destino de túnel…**) endereço, que igualmente é o endereço do ipsec peer. Esses dois endereços são pré-configurados.

Se você usa o Tunnel Endpoint Discovery (TED) e os mapas cripto dinâmico no roteador de hub, a seguir você pode evitar ter que preconfigure os endereços do ipsec peer no hub, mas uma ponta de prova e a resposta TED precisam de ser enviadas e recebido antes que a negociação de ISAKMP possa começar. 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 de DMVPN, o IPsec é provocado imediatamente para túneis GRE pontos a ponto e multipontos. 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 necessidade dos comandos set peer ... ou match address ... porque essas informações derivam diretamente do túnel GRE associado ou dos mapeamentos de NHRP.

```
crypto ipsec profile <profile-name> set transform-set <transform-name>
```

O comando seguinte associa uma interface de túnel com o perfil IPSec.

```
interface tunnel<number> ... tunnel protection ipsec profile <profile-name>
```

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

Nenhuma GRE ou informação IPSec sobre um spoke são configurados no roteador de hub na rede de DMVPN. O túnel GRE do roteador do spoke é configurado (através dos comandos NHRP) com informação 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. Toda esta informação é aprendida dinamicamente através do 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 roteador novo do spoke é configurado com a informação do hub, e quando começa acima, registra-se dinamicamente com o roteador de hub. O protocolo de roteamento dinâmico propaga a informação de roteamento para o este falou ao hub. O hub propaga essas novas informações de roteamento para os demais spokes. Igualmente propaga a informação de roteamento do

outro spokes a 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 de DMVPN, um roteador é o hub, e todo o Roteadores restante (spokes) é configurado com túneis ao hub. Os túneis spoke-hub estão continuamente ativos, e não é necessário configurar um túnel direto de um spoke para outro. Em lugar de, quando um spoke quer transmitir um pacote a um outro spoke (tal como a sub-rede atrás de um outro spoke), usa o NHRP para determinar dinamicamente o endereço de destino obrigatório do spoke do alvo. 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-soke será automaticamente desfeito após um período (configurável) de inatividade.

Suportando Dynamic Routing Protocols

A solução de DMVPN é baseada nos túneis GRE que apoiam pacotes do Multicast/IP de broadcast do Tunelamento, assim que a solução de DMVPN igualmente apoia os protocolos de roteamento dinâmico que são executado sobre os 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 a linha de configuração do **<spoke-n-addr> do Multicast do mapa do nhrp IP** para cada spoke. Com a solução DMVPN, os endereços do spoke não são conhecidos com antecedência, por isso essa configuração não é possível. Em lugar de, o NHRP pode ser configurado para adicionar automaticamente o cada falou à lista do destino multicast no hub com o **comando ip nhrp map multicast dynamic**. Com este comando, quando o Roteadores do spoke registra seu mapeamento NHRP do unicast com o servidor de NHRP (hub), o NHRP igualmente criará uma transmissão/mapeamento de multicast para este 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 pala ativar esse recurso. Se o Cisco Express Forwarding Switching é permitido na interface do túnel GRE e interfaces física que parte/entrantes, a seguir os pacotes de túnel GRE multipontos serão comutados por 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 executado nos roteadores Cisco através de um conjunto de comandos que definem a criptografia e então um **comando crypto map <map-name>** aplicados na interface externa do roteador. Devido a este projeto e ao fato de que não há atualmente um padrão para usar o IPsec para cifrar o Protocolo IP multicast/pacotes de transmissão, os pacotes do protocolo de IP Routing não podem “ser enviados” através do túnel de IPsec e nenhuma mudanças de roteamento não podem

dinamicamente ser propagadas ao outro lado do túnel de IPsec.

Nota: Todos os protocolos de roteamento dinâmico exceto pacotes da transmissão ou do IP de transmissão múltipla do uso BGP. Túneis GRE são utilizados em combinação com o IPsec para solucionar esse problema.

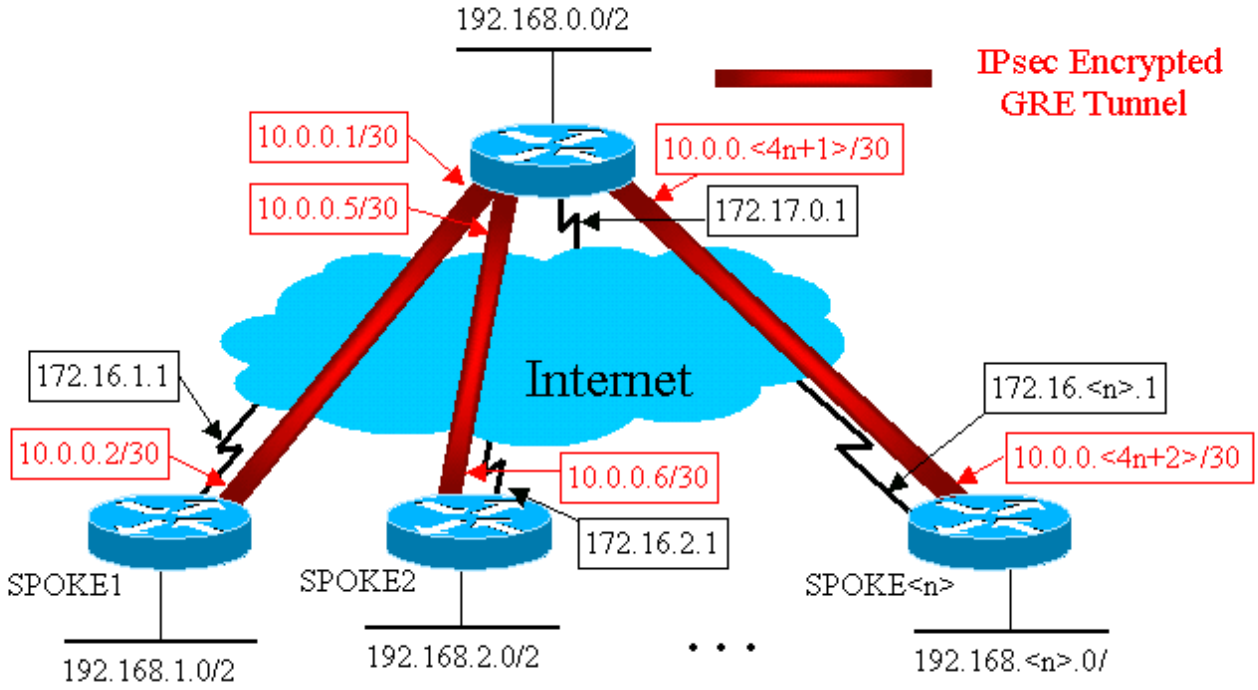
Os túneis GRE são executados em roteadores Cisco usando uma interface de túnel virtual (**tunnel<#> da relação**). O protocolo do tunelamento GRE é projetado segurar o Protocolo IP multicast/pacotes de transmissão assim que um protocolo de roteamento dinâmico pode “ser executado sobre” um túnel GRE. Os pacotes de túnel GRE são pacotes IP de unicast que encapsulam o pacote IP de 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 a criptografia IPSec, você pode usar um protocolo do Dynamic IP Routing para atualizar as tabelas de roteamento no ambas as extremidades do túnel criptografado. As entradas de tabela de IP Routing para as redes que eram instruídas através do túnel criptografado terão a outra extremidade do túnel (endereço IP de Um ou Mais Servidores Cisco ICM NT da interface do túnel GRE) como o salto seguinte IP. Assim, se as redes mudam em ambos os lados do túnel, a seguir o outro lado aprenderá dinamicamente da mudança e a Conectividade continuará sem nenhumas alterações de configuração no 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 parar “a migração” em qualquer momento se esse exemplo da configuração específica combina seus requisitos de design de rede.

Hub and spoke do 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.<n>.1 set
transform-set trans2 match address <n+100> ! 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<n> bandwidth 1000 ip address
10.0.0.<4n-3> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! 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 <n+100>
permit gre host 172.17.0.1 host 172.16.<n>.1
```

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 do 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.<n>.0 0.0.0.255 no
auto-summary ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1
```

Na configuração acima, os ACL são usados para definir que tráfego será cifrado. 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 uma ou outra extremidade, os pacotes do túnel IP GRE não mudarão, assim que este ACL não precisa de mudar.

Nota: Ao usar versões de Cisco IOS Software antes de 12.2(13)T, você deve aplicar o comando configuration do **vpnmap1 do crypto map** às interfaces do 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 do 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 mudança 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 original de linhas de configuração no roteador de hub para definir as características do crypto map para cada roteador do spoke. Este trecho da configuração define o cripto ACL e a interface do túnel de GRE para tal roteador de raio. Estas características são na maior parte as mesmas para todo o spokes, à exceção dos endereços IP de Um ou Mais Servidores Cisco ICM NT (**ajuste o par…**, o **destino de túnel…**).

Olhando a configuração acima no roteador de hub, você vê que há pelo menos 13 linhas de configuração pelo roteador do spoke; quatro para o crypto map, um para o ACL cripto, e oito para a interface do túnel GRE. O número total de linhas de configuração, se havia 300 roteadores spoke, é 3.900. Você igualmente precisa 300 (/30) de sub-rede para endereçar cada link do túnel. Uma configuração deste tamanho é muito dura de controlar e ainda mais difícil ao pesquisar defeitos a 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.

Nota: Durante o uso de mapas de criptografia dinâmicos, o túnel de criptografia IPsec deve ser iniciado pelo roteador do concentrador. Você pode igualmente usar o **<interface> unnumbered IP** para reduzir o número de sub-redes necessárias para os túneis GRE, mas este pode fazer a pesquisa de defeitos de um mais atrasado mais difícil.

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 de DMVPN introduz os seguintes comandos new:

```
crypto ipsec profile <name> <ipsec parameters> tunnel protection ipsec profile <name> ip nhrp map multicast dynamic
```

O comando crypto ipsec profile <name> é usado como um mapa cripto 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 que é exigido sob o perfil é o grupo da transformação. O endereço do ipsec peer e a cláusula do endereço do fósforo… para o proxy IPSec são derivados automaticamente dos mapeamentos NHRP para o túnel GRE.

O comando tunnel protection ipsec profile <name> é configurado sob a interface do túnel GRE e usado para associar a interface do túnel GRE com o perfil IPSec. Além, o comando tunnel protection ipsec profile <name> pode igualmente ser usado com um túnel GRE ponto a ponto. Neste caso, ele irá obter as informações de peer e proxy do IPsec a partir da configuração da origem e do destino do túnel. Dessa forma, a configuração é simplificada pois o peer de IPsec e os crypto ACLs não são mais necessários.

Nota: O comando tunnel protection… especifica que a criptografia IPSec estará feita depois que o encapsulamento de GRE foi adicionado ao pacote.

Estes primeiros dois comandos new são similares a configurar um crypto map e a atribuir o crypto map a uma relação 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.

Nota: Ao usar o comando tunnel protection… na interface de túnel, um comando crypto map… não é configurado na interface enviada física.

O último comando new, Multicast do mapa do nhrp IP dinâmico, permite que o NHRP adicione automaticamente o Roteadores do spoke aos mapeamentos NHRP do Multicast quando este Roteadores do spoke inicia o túnel do mGRE+IPsec e registra seus mapeamentos NHRP do unicast. Isto é precisado de permitir protocolos de roteamento dinâmico de trabalhar sobre os túneis do mGRE+IPsec entre o hub e o spokes. Se este comando não estava disponível, a seguir o roteador de hub precisaria de ter uma linha de configuração separada para um mapeamento de multicast a cada spoke.

Nota: Com essa configuração, os roteadores de spoke devem iniciar a conexão do 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.

Nota: O exemplo a seguir mostra interfaces de túnel GRE ponto a ponto nos roteadores de spoke e linhas de configuração do NHRP adicionadas nos roteadores de hub e de spoke para dar suporte ao 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.<n>.1 set
transform-set trans2 match address <n+100> ! 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<n> bandwidth 1000 ip address
10.0.0.<4n-1> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! 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 <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

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
```

Roteador do Spoke<n> (idoso)

```
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 !
```

Roteador do Spoke<n> (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.<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 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 !
```

No Roteadores do spoke, a máscara de sub-rede mudou, e os comandos NHRP foram adicionados sob a interface de túnel. Os comandos NHRP são necessários desde que o roteador de hub está usando agora o NHRP para traçar o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de túnel do spoke ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface física do spoke.

```
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 ...
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. **Os comandos ip nhrp authentication…, ip nhrp network-id… e tunnel key…** estão usados traçar os pacotes de túnel e os pacotes NHRP à interface do túnel GRE e à rede NHRP multipontos corretas quando são recebidos no hub. **O mapa do nhrp IP…** e os comandos dos **nhs do nhrp IP**… são usados pelo NHRP no falaram para anunciar o mapeamento NHRP do spokes (10.0.0.<n+1> --> 172.16.<n>.1) ao hub. O endereço 10.0.0.<n+1> é recuperado do **comando ip address… na** interface de túnel e o endereço 172.16.<n>.1 é recuperado do **comando tunnel destination… na** interface de túnel.

Em um caso onde houvesse 300 Roteadores do spoke, esta mudança reduziria o número de linhas de configuração no hub de 3900 linhas a 16 linhas (uma redução de 3884 linhas). A configuração em cada roteador do spoke aumentaria pelas linhas 6.

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. Este pacote será pegarado pelo ipsec peer da outra extremidade, que responderá ao primeiro par. 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. Isto foi testado e trabalhos, embora havia um erro nas versões anterior do Cisco IOS Software onde o TED forçou todo o tráfego IP entre os dois ipsec peer a ser cifrado, 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.

```
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
```

 Roteador do Spoke<n> (idoso) 

```
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.<n>.1 host
172.17.0.1
```

 Roteador do Spoke<n> (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
```

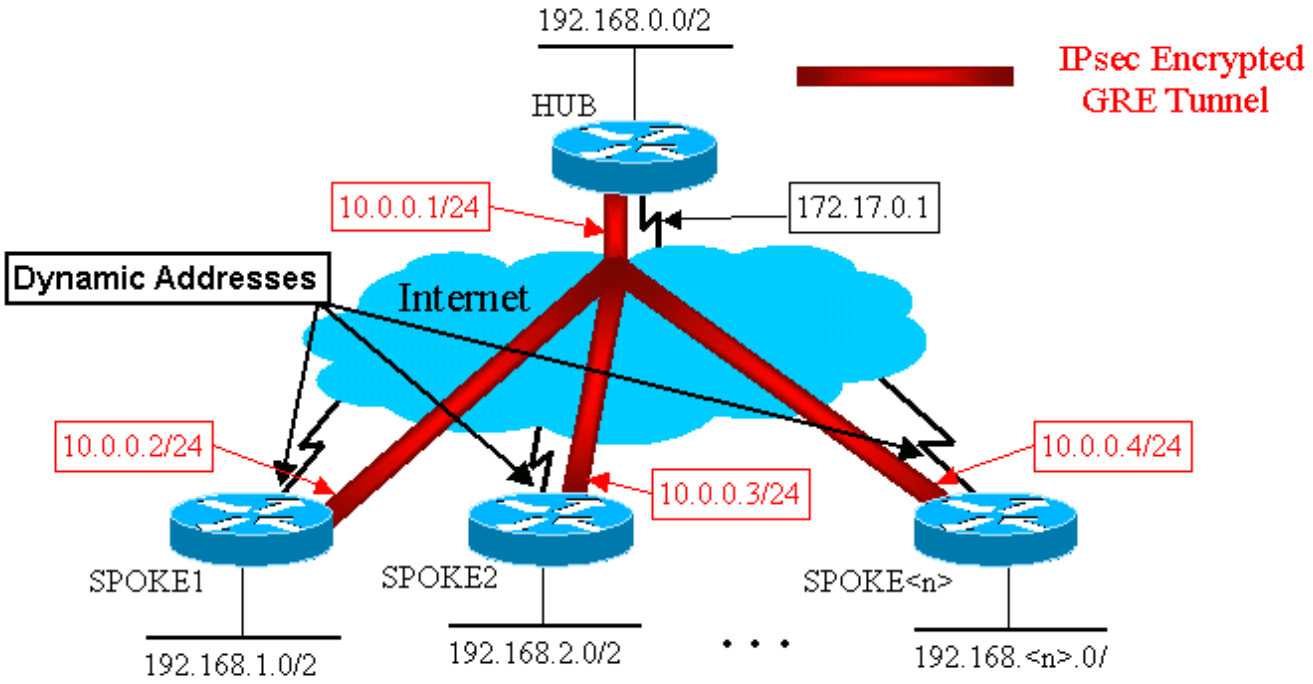
A funcionalidade usada na configuração do spoke é a seguinte.

- Quando a interface de túnel GRE for ativada, começará a enviar pacotes de registro do NHRP para o roteador de hub. Estes pacotes de registro NHRP provocarão o IPsec a ser iniciado. No roteador do spoke, o <peer-address> e os **comandos match ip access-list <ACL> do** par do grupo são configurados. O ACL especifica o GRE como o protocolo, algum para a fonte, e o endereço IP de Um ou Mais Servidores Cisco ICM NT do hub para o destino.**Nota:** É importante notar que algum está sendo usado como a fonte no ACL, e este deve ser o caso desde que o endereço IP de Um ou Mais Servidores Cisco ICM NT do roteador do spoke é dinâmico e, consequentemente, não conhecido antes que a interface física esteja 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 de modo que o origem de IP no proxy IPSec do spokes seja apenas o endereço atual da interface física do spokes (/32), um pouco do que o “alguns” do ACL. Se o “alguns” do ACL foram usados como a fonte no proxy IPSec, impossibilitariam todo o outro roteador do spoke igualmente de estabelecer um túnel

do IPsec+GRE com este 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. Também, o hub adiciona o roteador do spoke a sua lista do mapeamento de multicast NHRP. O hub começará a enviar Dynamic IP Routing Multicast Packets para o spoke (se um Dynamic Routing Protocol estiver configurado). O spoke assentará bem então em um vizinho de protocolo de roteamento do hub, e trocarão 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's e o mapeamento para os endereços IP da interface do túnel do spoke's são obtidos dinamicamente pelo hub por meio do NHRP. Permite que o endereço IP da interface física externa do spoke' seja atribuído de forma dinâmica.

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**
- O ACL cripto (101) especifica uma sub-rede como a fonte 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 que é usado host-será baseado sub-rede-baseou um pouco então.

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. São não somente estes dois similares, mas todo o spoke configurações de roteador será similar. Na maioria dos casos, todos os do spokes endereços IP exclusivos da necessidade simplesmente em suas relações, e o resto de suas configurações serão os mesmos. 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 portando, ele deve executar o Cisco IOS versão 12.2(13)T ou posterior. Isto permite-lhe alguma flexibilidade em decidir quando você precisa de promover seu Roteadores do spoke que está distribuído já. 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 do Spoke<n> (antes do 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 do Spoke<n> (após o 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. Removeu o **comando crypto map vpnmap1 das** relações do ethernet0 e puseram o **comando tunnel protection ipsec profile vpnprof** sobre a relação do tunnel0.
3. Removido a ACL de criptografia, access-list 101 permit gre any host 172.17.0.1.

Nesse caso, os endereços de peer do IPsec e os proxies são automaticamente desviados da configuração da origem e do destino do túnel. Os pares e os proxys são como segue (como 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 fornece a capacidade para que o Roteadores do spoke aprenda dinamicamente o endereço exterior da interface física do outro Roteadores do 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. O Roteadores do spoke aprende estas redes (secundárias) através do protocolo do Dynamic IP Routing que é executado sobre o 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.

Nota: O Dynamic Routing Protocol é executado apenas em enlaces de hub e spoke, e não em enlaces 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 de girar o horizonte fora rachado na interface de túnel mgre no hub, se não o RASGO não anunciará as rotas aprendidas através da parte traseira da relação mGRE para fora que a mesma relação.

`no ip split-horizon`
Nenhuma outra alteração é necessária. O RASGO usará automaticamente o salto seguinte original IP nas rotas que anuncia para trás para fora a mesma relação onde aprendeu estas 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 <as>`
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 anuncioando 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 <as>`
Nota: O comando no ip next-hop-self eigrp <as> será começar disponível no Cisco IOS Release 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 são queridos, a seguir você deve usar o processo que liga a interface de túnel no Roteadores do spoke.
- Do contrário, você precisará usar um Routing Protocol diferente sobre o DMVPN.

OSPF

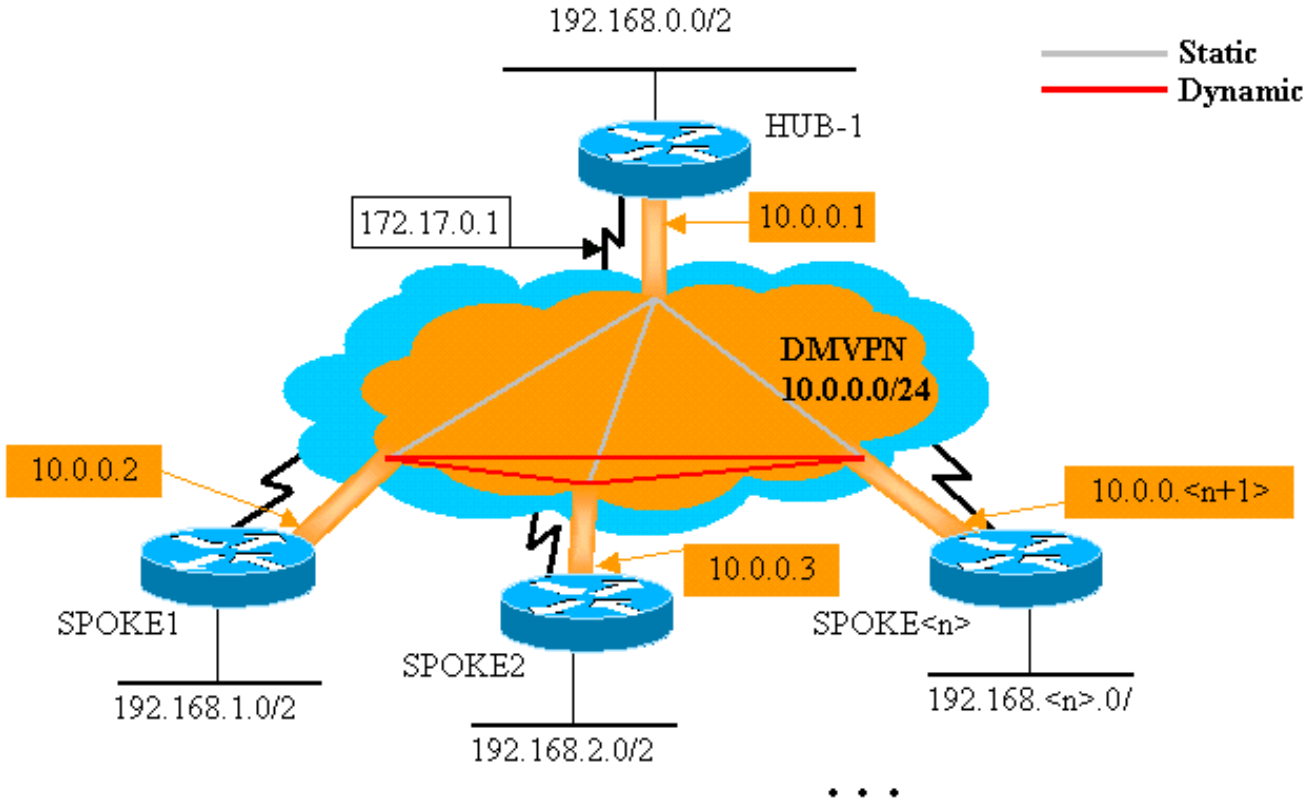
Como o OSPF é um Routing Protocol de estado de link, não há problemas de horizonte de divisão. Normalmente, para interfaces multiponto, você configura o tipo de rede OSPF para ser ponto para multiponto, mas isso faria com o OSPF adicionasse rotas de host à tabela de roteamento nos roteadores de spoke. 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 igualmente precisa de certificar-se de que o roteador de hub será o Designated Router (DR) 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: **prioridade 2 OSPF IP**
- Spoke: **prioridade 0 OSPF IP**

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 ajustado para transmitir e a prioridade é ajustado a 2. que ajustam o tipo de rede OSPF para transmitir fará com que o OSPF instale rotas para redes atrás do Roteadores do spokes com um endereço de próximo salto IP como o endereço do túnel GRE para esse roteador do 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 como segue:

- 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 o 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 comando ip nhrp map multicast ... não foi necessário porque o túnel de GRE era ponto a ponto. Nesse caso, os pacotes de transmissão múltipla serão encapsulados automaticamente através do túnel ao único possível destino. Este comando é precisado agora porque o túnel GRE do spokes mudou a multiponto e há mais então um possível destino.
- 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+Ipsec, 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 do 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.<n>.0 0.0.0.255 area 0 !
```

Observe que as configurações de todos os roteadores spoke são muito semelhantes. As únicas diferenças são os endereços IP de Um ou Mais Servidores Cisco ICM NT nas interfaces local. Isto ajuda ao distribuir um grande número Roteadores do spoke. Todos os roteadores spoke podem ser configurados igualmente, e somente os endereços de interface de IP local precisam ser adicionados.

Neste momento, olhe as tabelas de roteamento e as tabelas do mapeamento NHRP no hub, Spoke1, e Roteadores de Spoke2 para ver as condições inicial (imediatamente depois que Spoke1 e Roteadores de Spoke2 vem acima) e as circunstâncias depois que Spoke1 e Spoke2 criaram um link dinâmico entre elas.

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 0 205
```

```
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 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 seguinte sequência de evento ocorre para construir o túnel spoke-to-spoke direto do mGRE+IPsec.

1. O roteador Spoke1 recebe o pacote de ping com o destino 192.168.2.3. Olha acima este destino na tabela de roteamento e encontra que precisa de enviar para fora a este pacote a relação do tunnel0 ao nexthop IP, 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 de Spoke1 cria um pacote de requisição da resolução de NHRP e envia-o a seu NHS (o roteador de 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 de Spoke1 recebe a resposta da resolução de NHRP, e entra em 10.0.0.3 — o mapeamento >172.16.2.75 em sua tabela do 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 de Spoke1 inicia o ISAKMP com 172.16.2.75 e negocia o ISAKMP e o sas de IPSec. O proxy IPSec é derivado do **comando tunnel source <address> do** 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. Uma vez que o túnel de IPsec terminou a construção, todos os pacotes de dados mais adicionais à sub-rede 192.168.2.0/24 estão enviados diretamente a Spoke2.
7. Depois que um pacote destinado a 192.168.2.3 foi enviado ao host, este host enviará um pacote de informação de retorno a 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 de Spoke2 cria um pacote de requisição da resolução de NHRP e envia-o a seu NHS (o roteador de hub).
9. O roteador de hub verifica sua tabela do mapeamento NHRP para ver se há o destino 10.0.0.2 e encontra que traça ao 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 de Spoke2 recebe a resposta da resolução de NHRP, e entra em 10.0.0.2 — > 172.16.1.24 que traça em sua tabela do 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. Spoke1 e Spoke2 podem agora enviar pacotes diretamente entre si. 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 exluir 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 NHRP são usados dentro do último minuto antes de expirar, a seguir um pedido e uma resposta da resolução de NHRP estarão enviados para refrescar a entrada antes que esteja suprimida. Do contrato, o mapeamento NHRP será excluído e isso acionara o IPsec para limpar os SAs do IPsec.

IPSec VPN de multiponto dinâmico com hubs dual

Com algumas linhas de configuração adicionais ao Roteadores do spoke você pode estabelecer roteadores de hub duplos (ou múltiplo), para a Redundância. Há duas maneiras de configurar o hub dual DMVPN.

- Uma única rede de DMVPN com cada spoke usando uma única interface do túnel GRE multiponto e apontando a dois Hubs diferentes como seu servidor de próximo salto (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.Além disso, os roteadores de hub terão somente uma única interface do túnel GRE multiponto.

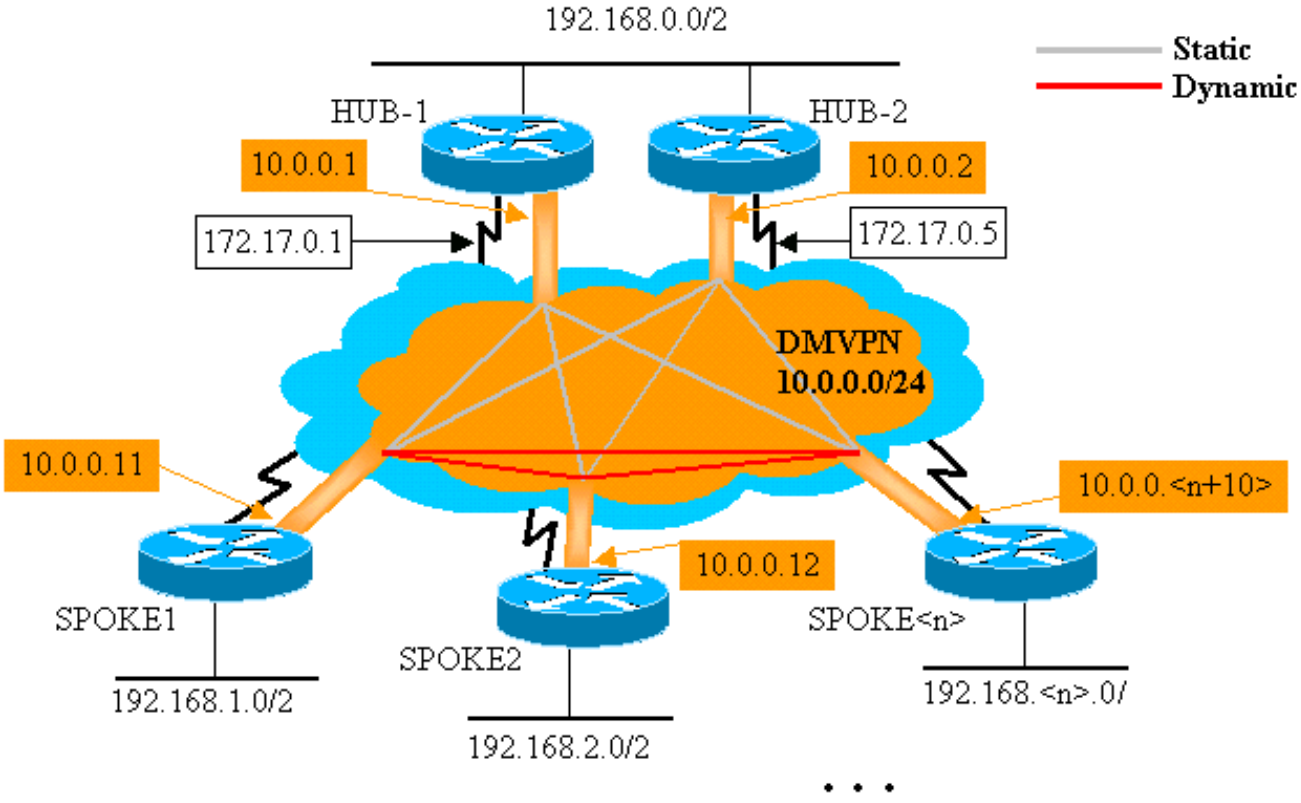
Os exemplos seguintes olharão configurando estas duas encenações diferentes para o hub dual DMVPN. Na maioria dos casos, as diferenças realçadas são relativas à configuração do único concentrador de DMVPN.

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 é neste caso ter um único DMVPN “nuvem” com todo o Hubs (dois neste caso) e todo o spokes conectado a esta sub-rede única (“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. Desde que o Roteadores do spoke é vizinhos de roteamento com os roteadores de hub sobre a mesma interface de túnel mgre, você não pode usar o link nem conecta diferenças (como a métrica, custe, atrase, ou largura de banda) para alterar o medidor do protocolo de roteamento dinâmico para preferir um hub sobre o outro hub quando são ambas acima. 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.

Nota: Normalmente, o problema acima é realmente considerado quando os roteadores de hub são co-localizados. Quando eles não são co-alocados, 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 mudança na configuração de Hub1 é mudar 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. O um principal diferença é que Hub2 é igualmente um spoke (ou cliente) de Hub1, fazendo a Hub1 o hub preliminar e de Hub2 o hub secundário. Isto é feito de modo que Hub2 seja um vizinho de 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 Hub1 e Hub2, Hub2 não participaria no roteamento OSPF quando Hub1 é igualmente acima. Quando o Hub1 estiver inativo, o Hub2 será o OSPF DR para o DMVPN (rede NBMA). Quando Hub1 vem apoio, tomará acabar-se o OSPF DR 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.


```
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 do 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.<n>.0 0.0.0.255 area 0 !
```

Neste momento, você pode olhar as tabelas de roteamento, as tabelas do mapeamento NHRP, e as conexões IPSec no Roteadores de Hub1, de Hub2, de Spoke1, e de Spoke2 para ver as condições inicial (imediatamente depois do Roteadores de Spoke1 e de Spoke2 venha acima).

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 0 5
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 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 conectado 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, Ethernet1/0/3O
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. Isto significa que Hub1 estará preferido para o tráfego de encaminhamento ao Roteadores do spoke, como pode ser visto no roteador R2. Isto tomará do problema do roteamento assimétrico descrito na primeira bala acima.

O roteamento assimétrico na outra direção, conforme descrito no segundo item com marcador acima, ainda está lá. Ao utilizar OSPF como o Dynamic Routing Protocol, você poderá corrigir isso com uma solução que use o comando distance ... sob o roteador ospf 1, nos spokes, para que as rotas obtidas via Hub 1 tenham preferência sobre as rotas obtidas 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

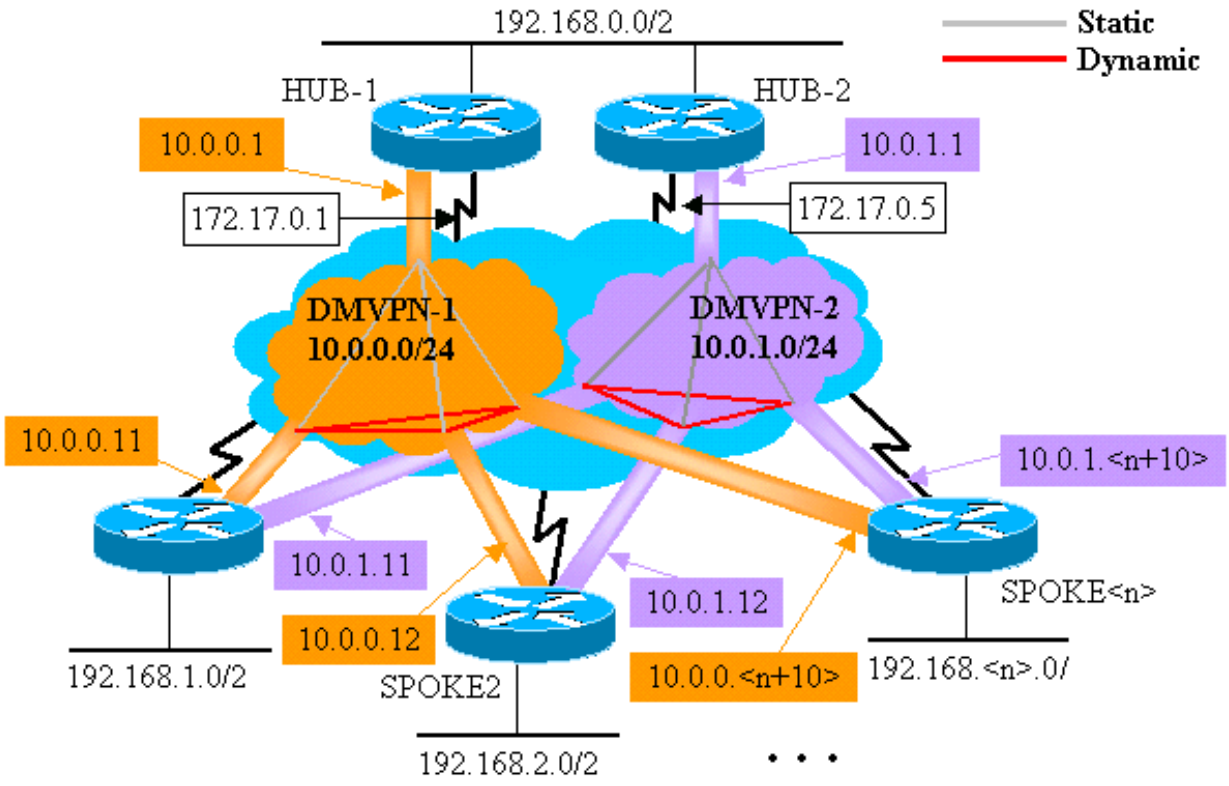
O hub duplo, com layout duplo de DMVPN, é ligeiramente mais difícil de configurar, mas proporciona um controle melhor do roteamento através do DMVPN. A ideia é ter um dois DMVPN separado “nuvens”. Cada hub (dois nesse caso) está conectado a uma sub-rede DMVPN ("rede") e os spokes estão conectados nas 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.

Nota: O problema acima em geral só é importante quando os roteadores de hub são co-alocados. Quando eles não são co-alocados, 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. As relações múltiplas do p-pGRE em um roteador do spoke podem usar o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT do **origem de túnel…**, mas as relações múltiplas mGRE em um roteador do spoke devem ter um endereço IP de Um ou Mais Servidores Cisco ICM NT da **fonte do** túnel exclusivo**…**. 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. Esse endereço é comparado com o endereço de origem do túnel, mas como ambos os túneis têm o mesmo endereço de origem, 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 pacotes GRE não têm esse problema, uma vez que possuem um valor de chave de túnel para diferenciar as duas interfaces mGRE. Começando nos Cisco IOS Software Releases 12.3(5) e 12.3(7)T, um parâmetro adicional foi introduzido para superar esta limitação: **proteção do túnel….compartilhado**. A palavra-chave **compartilhada** indica que as relações do mutiple mGRE usarão a criptografia IPSec com o mesmo endereço IP de origem. Se você tem uma versão anterior você pode usar túneis do p-pGRE neste hub dual com layout duplo DMVPN. No caso do túnel p-pGRE, os endereços IP de origem e de destino podem ser usados para correspondência. Para túneis do p-pGRE deste exemplo será usado neste hub dual com layout duplo DMVPN e para não usar 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 !
```

Neste caso, as configurações de Hub1 e de Hub2 são similares. O 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. Os valores de ip address ..., ip nhrp network-id ..., tunnel key ... e tunnel destination ... 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 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 ! 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 do 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 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.<n+10> 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 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 momento, deixe-nos olhar as tabelas de roteamento, as tabelas do mapeamento NHRP, e conexões IPSec no Roteadores de Hub1, de Hub2, de Spoke1 e de Spoke2 para ver as condições inicial (imediatamente depois do Roteadores de Spoke1 e de Spoke2 venha acima).

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 HMAC_MD5+DES_56_CB 36 0
```

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 o Roteadores do spoke está fazendo o balanceamento de carga por pacote, a seguir você poderia obter pacotes estragados.

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 quer Hub1 ser o preliminar e Hub2 a ser o backup, a seguir você pode ajustar o atraso nas interfaces de túnel do hub para ser diferente.

Hub1:

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

Hub2:

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

Nota: Neste exemplo, 50 foi adicionado ao retardo na interface do túnel no Hub2 porque ele é menor que o retardo 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 foi aumentado por mais de 100, a seguir Hub2 enviaria pacotes para o Roteadores do spoke com Hub1 através da relação de Ethernet1, embora o Roteadores atrás de Hub1 e de Hub2 ainda assim preferiria corretamente Hub-1 para enviar pacotes ao Roteadores do 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. Isto toma da edição descrito na primeira bala acima.

O problema descrito no segundo item acima ainda está lá, mas visto haver duas interfaces de túnel p-pGRE, será possível configurar o retardo ... nas interfaces de túnel separadamente para alterar a métrica do EIGRP para as rotas aprendidas da relação entre o Hubs 1 e 2.

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 quer usar ambo o Hubs equilibrando o spokes através do Hubs, com proteção de failover e nenhum roteamento assimétrico, a seguir a configuração de roteamento é mais complexa, mas você pode fazê-la ao usar o EIGRP. Para realizar isto, ajuste o **atraso… nas** interfaces de túnel dos roteadores de hub de volta a ser igual e use então o **comando offset-list <acl> out <offset> <interface> no** Roteadores do spoke aumentar a métrica EIGRP para rotas anunciou para fora as interfaces do túnel GRE ao hub alternativo. O retardo desigual ... entre as interfaces Tunnel0 e Tunnel1 no spoke ainda é usado; portanto, o roteador spoke preferirá seu roteador de hub principal. 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 !
```

Nota: O valor de deslocamento de 12800 (50*256) foi adicionado à métrica EIGRP porque é menor de 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 alternativo enviará pacotes diretamente ao Roteadores do spoke, um pouco do que enviando estes pacotes através dos Ethernet para atravessar o roteador de hub preliminar para aquele 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.

Nota: Se o valor do deslocamento de tempo foi aumentado em mais de 25600 (100*256), então os hubs encaminharão os pacotes pela metade dos roteadores de spoke por outro hub via interface de Ethernet mesmo se os roteadores atrás dos hubs preferirem o hub correto para enviar os pacotes aos roteadores de spoke.

Nota: O comando saída de lista de distribuição 1 também foi adicionado, pois é possível que as

rotas conhecidas de um roteador de hub via uma interface de túnel em um raio possa ser anunciado de volta para o outro hub pelo outro túnel. O comando distribute-list ... assegura que o roteador de concentrador somente possa anunciar suas próprias rotas.

Nota: Se você prefere controlar as propagandas do roteamento nos roteadores de hub um pouco do que no Roteadores do spoke, a seguir os **comandos offset-list <acl1> in <value> <interface> e distribute-list <acl2> in** podem ser configurados nos roteadores de hub em vez no spokes. A lista de acesso <acl2> alistaria as rotas de trás todo o spokes e a lista de acesso <acl1> alistaria somente as rotas do spokes de trás onde um outro roteador de hub é ser o hub preliminar.

Com estas mudanças as rotas olham como o seguinte:

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 de DMVPN fornece a seguinte funcionalidade para escalar melhor grandes e redes pequenas do IPSec VPN.

- O DMVPN permite a melhor escamação na malha cheia ou no IPsec VPN da malha parcial.Éespecialmente útil quando o tráfego spoke-to-spoke é esporádico (por exemplo, cada spoke não está enviando constantemente dados a cada outro spoke). Permite o algum falou para enviar dados diretamente a todo o outro spoke, como por muito tempo há uma conectividade IP direta entre o spokes.
- DMVPN suporta nós IPsec com endereços dinamicamente atribuídos (tais como o cabo, o ISDN, e o DSL).Isto se aplica a hub-e-spoke e também a redes em malha. É possível que o DMVPN requisite 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 spoke novo e o protocolo de roteamento dinâmico propagará o roteamento ao hub e a todo spokes restante.
- O DMVPN reduz o tamanho da configuração necessária em todo o Roteadores no 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.Isto significa que um protocolo de roteamento dinâmico pode ser usado, e o “Hubs redundante” pode ser apoiado 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