Configurar o túnel FlexVPN site a site com um peer com endereço IP dinâmico

Contents

Introdução

Este documento descreve como configurar um túnel VPN site a site FlexVPN entre 2 Cisco Routers quando o peer remoto tem um endereço IP dinâmico.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Protocolo IKEv2

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo CSR1000V
- Software Cisco IOS® XE, versão 17.3.4

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

Informações de Apoio

Diagrama de Rede

Topologia para Par Dinâmico

A topologia neste exemplo mostra um roteador Cisco e outro roteador Cisco que tem um endereço IP dinâmico em sua interface pública.

Configurações

Esta seção descreve como configurar o túnel FlexVPN site a site em um roteador Cisco quando o peer remoto usa um endereço IP dinâmico.

Neste exemplo de configuração, o método de autenticação usado é a Chave pré-compartilhada (PSK); no entanto, a infraestrutura de chave pública (PKI) também pode ser usada.

Configuração no roteador da matriz

Neste exemplo, foram usados os padrões inteligentes IKEv2 do roteador. O recurso IKEv2 Smart Defaults minimiza a configuração do FlexVPN, cobrindo a maioria dos casos de uso. Os padrões inteligentes IKEv2 podem ser personalizados para casos de uso específicos, embora isso não seja recomendado. Os padrões inteligentes incluem a política de Autorização IKEv2, a proposta IKEv2, a política IKEv2, o Perfil de Segurança de Protocolo de Internet (IPsec) e o conjunto de transformação IPsec.

Para revisar os valores padrão em seu dispositivo, você pode executar os comandos listados abaixo.

- show crypto ikev2 authorization policy default
- show crypto ikev2 proposal default
- show crypto ikev2 policy default

- show crypto ipsec profile default
- show crypto ipsec transform-set default

Etapa 1 Configurar o chaveiro IKEv2.

- Nesse caso, como o roteador da matriz não conhece o ip do peer devido à sua identidade dinâmica, ele corresponde a qualquer endereço ip.
- As chaves local e remota também são configuradas.
- Recomenda-se ter chaves fortes para evitar qualquer vulnerabilidade.

```
crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123
```

Etapa 2 Configurar o modelo de Autenticação, Autorização e Contabilização (AAA).

- Isso cria a estrutura de gerenciamento para os usuários que podem se conectar a esta instância.
- Como a negociação da conexão é iniciada a partir desse dispositivo, o modelo faz referência ao seu banco de dados local para determinar os usuários autorizados.

```
aaa new-model
aaa authorization network FLEXVPN local
```

Etapa 3 Configurar o perfil IKEv2.

- Como o endereço IP do peer remoto é dinâmico, você não pode usar um endereço IP específico para identificar o peer.
- No entanto, você pode identificar o peer remoto por domínio, FQDN ou ID de chave definido no dispositivo peer.

- O grupo AAA (Authentication, Authorization and Accounting) precisa ser adicionado ao método de autorização do perfil, especificando que PSK é o método usado.
- Se o método de autenticação for PKI aqui, ele será especificado como cert em vez de PKI .
- Como o objetivo é criar uma Dynamic Virtual Tunnel Interface (dVTI), esse perfil está vinculado a um modelo virtual

```
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
```

```
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1
```

Etapa 4 Configurar o perfil IPsec.

- Um perfil IPsec personalizado pode ser configurado se você não usar o perfil padrão.
- O perfil IKEv2 criado na Etapa 3 é mapeado para esse perfil IPsec.

```
crypto ipsec profile defualt
 set ikev2-profile FLEXVPN_PROFILE
```

Etapa 5 Configurar a interface de Loopback e a Virtual Template Interface.

- Como o dispositivo remoto tem um endereço IP dinâmico, um dVTI precisa ser criado a partir de um modelo.
- Essa interface de modelo virtual é um modelo de configuração a partir do qual as interfaces de acesso virtual dinâmicas são criadas.

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
```

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default
```

Configuração do roteador da filial

Para o roteador da filial, configure o Keyring IKEv2, o modelo AAA, o perfil IPsec e o perfil IKEv2, conforme indicado nas etapas anteriores, com as alterações de configuração necessárias e as descritas a seguir:

1. Configure a identidade local que é enviada ao roteador da matriz como identificador.

```
crypto ikev2 profile FLEXVPN_PROFILE
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
```

Etapa 5 Configurar A Interface Do Túnel Virtual Estático.

- Como o endereço IP do roteador da matriz é conhecido e não muda, uma interface VTI estática é configurada.

```
interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default
```

Configuração de roteamento

Neste exemplo, o roteamento é definido durante o estabelecimento da Associação de Segurança (SA) IKEv2 com a configuração de uma Lista de Controle de Acesso. Isso define o tráfego a ser enviado pela VPN. Você também pode configurar protocolos de roteamento dinâmico, mas ele não está no escopo deste documento.

Etapa 5. Defina a ACL.

Roteador da matriz:

```
ip access-list standard Flex-ACL
 permit 10.10.10.0 255.255.255.0
```

Roteador da filial:

```
ip access-list standard Flex-ACL
 permit 10.20.20.0 255.255.255.0
```

Etapa 6. Modifique os perfis de autorização IKEv2 em cada roteador para definir a ACL.

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL
```

Configuração completa do roteador da matriz

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback1
 ip address 192.168.1.1 255.255.255.0

interface Loopback10
 ip address 10.10.10.10 255.255.255.255

interface GigabitEthernet0
 ip address 172.16.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default

ip access-list standard Flex-ACL
 5 permit 10.10.10.0 255.255.255.0
```

Configuração completa do roteador da filial

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer HUB
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
```

```
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback20
 ip address 10.20.20.20 255.255.255.255

interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface GigabitEthernet0
 ip address dhcp
 negotiation auto

ip access-list standard Flex-ACL
 10 permit 10.20.20.0 255.255.255.0
```

Verificar

Para verificar o túnel, você deve verificar se a Fase 1 e a Fase 2 estão ativas e funcionando corretamente.

```
Headquarter#show crypto ikev2 sa detail
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.1.1/500        172.16.2.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/74645 sec
      CE id: 61256, Session-id: 1
      Status Description: Negotiation done
      Local spi: D5129F36B1180175       Remote spi: F9298874F90BFEC7
      Local id: 172.16.1.1
      Remote id: 172.16.2.1
      Local req msg id:  16             Remote req msg id:  31
      Local next msg id: 16             Remote next msg id: 31
      Local req queued:  16             Remote req queued:  31
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
      Remote subnets:                  -------------> This section shows the traffic to be routed acros
      192.168.1.10 255.255.255.255
```

```
      10.20.20.20 255.255.255.255

 IPv6 Crypto IKEv2  SA
```

Fase 2, Ipsec

```
Headquarter#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
   current_peer 172.16.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 225, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 225, #pkts decrypt: 225, #pkts verify: 225
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
     current outbound spi: 0xC124D7C1(3240417217)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xC2AADCAB(3265977515)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2912, flow_id: CSR:912, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4607993/628)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC124D7C1(3240417217)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2911, flow_id: CSR:911, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4608000/628)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Você também precisa verificar se a interface de Acesso Virtual está no estado UP.

```
show interface Virtual-Access1
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (192.168.1.1)
  MTU 9934 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.16.1.1, destination 172.16.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
  Last input 20:53:34, output 20:53:34, output hang never
  Last clearing of "show interface" counters 20:55:43
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     586 packets input, 149182 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1860 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Troubleshooting

Esta seção descreve como solucionar problemas de estabelecimento de túnel

Conclua estas etapas se a negociação de IKE falhar:

1. Verifique o estado atual com estes comandos:

- show crypto ikev2 sa
- show crypto ipsec sa
- show crypto session

2. Use estes comandos para depurar o processo de negociação do túnel:

- debug crypto ikev2
- debug crypto ipsec

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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

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

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