Site-to-site FlexVPN-tunnel configureren met peer met dynamisch IP-adres

Inhoud

Inleiding

Dit document beschrijft hoe u een FlexVPN site-to-site VPN-tunnel kunt configureren tussen twee Cisco-routers wanneer de externe peer een dynamisch IP-adres heeft.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN
- IKEv2-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CSR1000V-apparaat
- Cisco IOS® XE-software, versie 17.3.4

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Netwerkdiagram

Topologie voor Dynamic Peer

De topologie in dit voorbeeld toont een Cisco-router en een andere Cisco-router met een dynamisch IP-adres op zijn openbare interface.

Configuraties

In deze sectie wordt beschreven hoe u de Site-to-Site FlexVPN-tunnel op een Cisco-router kunt configureren wanneer de externe peer een dynamisch IP-adres gebruikt.

In dit configuratievoorbeeld is de gebruikte verificatiemethode Pre-Shared-Key (PSK), maar kan ook Public Key Infrastructure (PKI) worden gebruikt.

Configuratie op hoofdkwartierrouter

In dit voorbeeld zijn de IKEv2 Smart Defaults van de router gebruikt. De functie IKEv2 slimme standaardwaarden minimaliseert de FlexVPN-configuratie door de meeste gebruikscases te dekken. De slimme gebreken IKEv2 kunnen voor specifieke gebruiksgevallen worden aangepast, hoewel dit niet wordt geadviseerd. De slimme standaardwaarden zijn onder meer het IKEv2-autorisatiebeleid, het IKEv2-voorstel, het IKEv2-beleid, het IPsec-profiel (Internet Protocol Security) en de IPsec-transformatieset.

Om de standaardwaarden op uw apparaat te bekijken, kunt u de onderstaande opdrachten uitvoeren.

- toon crypto ikev2 autorisatiebeleid standaard
- standaard crypto ikev2 voorstel tonen
- standaard crypto ikev2-beleid tonen

- standaard crypto ipsec-profiel tonen
- standaard crypto ipsec transformatie-set tonen

Stap 1 Configuratie van IKEv2-sleutelring.

- In dit geval, aangezien de hoofdkwartierrouter niet de peer ip kent toe te schrijven aan het dynamisch zijn de identiteit het aan om het even welk ip adres aanpast.
- Remote en lokale toetsen worden ook geconfigureerd.
- Aanbevolen wordt om sterke toetsen te hebben om elke kwetsbaarheid te vermijden.

```
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
```

Stap 2 Het configureren van het verificatie-, autorisatie- en accounting (AAA) model.

- Hierdoor ontstaat een beheerskader voor de gebruikers die bij deze instantie verbinding kunnen maken.
- Aangezien de verbindingsonderhandeling vanaf dit apparaat wordt geïnitieerd, verwijst het model naar zijn lokale database om te bepalen welke gebruikers geautoriseerd zijn.

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

Stap 3 Configureer het IKEv2-profiel.

- Gezien het feit dat het externe peer IP-adres dynamisch is, kunt u geen specifiek IP-adres gebruiken om de peer te identificeren.
- U kunt echter de externe peer per domein, FQDN of Key-id op het peer-apparaat identificeren.

- De groep voor verificatie, autorisatie en accounting (AAA) moet worden toegevoegd voor de autorisatiemethode van het profiel waarin PSK wordt gespecificeerd.
- Indien de authenticatiemethode hier PKI is, wordt deze als zekerheid gespecificeerd in plaats van PKI .
- Aangezien het doel is om een Dynamic Virtual Tunnel Interface (dVTI) te maken, is dit profiel gekoppeld aan een virtuele sjabloon

```
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
```

Stap 4 Configuratie van het IPsec-profiel.

- Er kan een aangepast IPsec-profiel worden geconfigureerd als u het standaardprofiel niet gebruikt.
- Het IKEv2-profiel dat in Stap 3 is gemaakt, wordt aan dit IPsec-profiel toegewezen.

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

Stap 5 Configureer de Loopback-interface en de virtuele Sjablooninterface.

- Aangezien het externe apparaat een dynamisch IP-adres heeft, moet een dVTI worden gemaakt op basis van een sjabloon.
- Deze virtuele sjablooninterface is een configuratiesjabloon waaruit dynamische Virtual-Access interfaces worden gemaakt.

```
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
```

Configuratie van vestigingsrouter

Voor de vertakkingsrouter moet u het IKEv2-sleutelprofiel, het AAA-model, het IPsec-profiel en het IKEv2-profiel configureren zoals aangegeven in de vorige stappen met de benodigde configuratiewijzigingen en de volgende stappen:

1. Configureer de lokale identiteit die als identificatie naar de hoofdkwartierrouter wordt verzonden.

```
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
```

Stap 5 Configureer de statische virtuele tunnelinterface.

- Gezien het feit dat het IP-adres voor de router voor het hoofdkantoor bekend is en niet verandert, wordt er een statische VTI-interface geconfigureerd.

```
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
```

Routingconfiguratie

In dit voorbeeld is routing gedefinieerd tijdens de oprichting van de IKEv2 Security Association (SA) met de configuratie van een toegangscontrolelijst. Dit definieert het verkeer dat via VPN moet worden verzonden. U kunt ook dynamische routeringsprotocollen configureren, maar dit valt niet onder het bereik van dit document.

Stap 5. Definieer de ACL.

Hoofdkwartier router:

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

Vestigingsrouter:

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

Stap 6. Wijzig de IKEv2-autorisatieprofielen op elke router om de ACL in te stellen.

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

Hoofdkwartier router volledige configuratie

```
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
```

Vestigingsrouter volledige configuratie

```
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
```

Verifiëren

Om de tunnel te verifiëren, moet u fase 1 en fase 2 controleren zijn omhoog en het werken behoorlijk.

```
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:
```

U moet ook controleren of de interface voor virtuele toegang zich in de UP-staat bevindt.

```
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
```

Problemen oplossen

In deze sectie wordt beschreven hoe u problemen kunt oplossen in de tunnelinrichting

Voltooi deze stappen als de IKE-onderhandeling mislukt:

1. Controleer de huidige status met deze opdrachten:

- show crypto ikev2 sa

- crypto ipsec tonen
- cryptosessie tonen

2. Gebruik deze opdrachten om het tunnelonderhandelingsproces te debuggen:

- debug crypto ikev2
- debug crypto ipsec

Gerelateerde informatie

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.