Configurazione del tunnel FlexVPN da sito a sito con un peer con indirizzo IP dinamico

Sommario

Introduzione

Questo documento descrive come configurare un tunnel VPN da sito a sito FlexVPN tra 2 router Cisco quando il peer remoto ha un indirizzo IP dinamico.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FlexVPN
- Protocollo IKEv2

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Esempio di rete

Topologia per Dynamic Peer

La topologia di questo esempio mostra un router Cisco e un altro router Cisco che ha un indirizzo IP dinamico sulla sua interfaccia pubblica.

Configurazioni

In questa sezione viene descritto come configurare il tunnel FlexVPN da sito a sito su un router Cisco quando il peer remoto utilizza un indirizzo IP dinamico.

In questo esempio di configurazione il metodo di autenticazione utilizzato è PSK (Pre-Shared-Key). È tuttavia possibile utilizzare anche PKI (Public Key Infrastructure).

Configurazione sul router della sede centrale

Nell'esempio, è stato usato il protocollo IKEv2 Smart Defaults del router. La funzione IKEv2 Smart Defaults riduce al minimo la configurazione di FlexVPN coprendo la maggior parte degli scenari di utilizzo. I valori predefiniti per le smart card IKEv2 possono essere personalizzati per scenari di utilizzo specifici, sebbene questa operazione non sia consigliata. Le impostazioni predefinite intelligenti includono i criteri di autorizzazione IKEv2, la proposta IKEv2, i criteri IKEv2, il profilo IPsec (Internet Protocol Security) e il set di trasformazioni IPsec.

Per rivedere i valori predefiniti del dispositivo, è possibile eseguire i comandi elencati di seguito.

- mostra le impostazioni predefinite dei criteri di autorizzazione crypto ikev2
- mostra valore predefinito proposta crypto ikev2
- visualizzare le impostazioni predefinite del criterio crypto ikev2
- mostra profilo ipsec di crittografia predefinito

- show crypto ipsec transform-set predefinito

1. Configurare il keyring IKEv2.

- In questo caso, poiché il router della sede centrale non conosce l'ip del peer perché è dinamico, l'identità corrisponde a qualsiasi indirizzo ip.
- Vengono configurate anche le chiavi remote e locali.
- Si consiglia di avere chiavi forti per evitare qualsiasi vulnerabilità.

```
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
```

2. Configurare il modello di autenticazione, autorizzazione e accounting (AAA).

- In questo modo viene creata la struttura di gestione per gli utenti che possono connettersi per questa istanza.
- Poiché la negoziazione della connessione viene avviata da questo dispositivo, il modello fa riferimento al proprio database locale per determinare gli utenti autorizzati.

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

3. Configurare il profilo IKEv2.

- Poiché l'indirizzo IP del peer remoto è dinamico, non è possibile utilizzare un indirizzo IP specifico per identificare il peer.
- È tuttavia possibile identificare il peer remoto per dominio, FQDN o ID chiave definito nel dispositivo peer.

- È necessario aggiungere il gruppo Autenticazione, autorizzazione e accounting (AAA) per il metodo di autorizzazione del profilo. Il metodo utilizzato è PSK.
- Se il metodo di autenticazione è PKI, viene specificato cert anziché PKI.
- Poiché l'obiettivo è creare un'interfaccia a tunnel virtuale dinamico (dVTI), questo profilo è collegato a un modello virtuale

```
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
```

4. Configurare il profilo IPsec.

- Se non si utilizza il profilo predefinito, è possibile configurare un profilo IPSec personalizzato.
- Il profilo IKEv2 creato nel passaggio 3 è mappato a questo profilo IPSec.

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

5. Configurare l'interfaccia di loopback e l'interfaccia del modello virtuale.

- Poiché il dispositivo remoto dispone di un indirizzo IP dinamico, è necessario creare un dVTI da un modello.
- L'interfaccia del modello virtuale è un modello di configurazione da cui vengono create le interfacce di accesso virtuale dinamiche.

```
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
```

Configurazione router per filiali

Per il router di diramazione, configurare il Keyring IKEv2, il modello AAA, il profilo IPsec e il profilo IKEv2 come indicato nei passaggi precedenti con le modifiche di configurazione necessarie e quelle descritte di seguito:

1. Configurare l'identità locale inviata al router della sede centrale come identificatore.

```
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
```

5. Configurare l'interfaccia statica del tunnel virtuale.

- Poiché l'indirizzo IP del router della sede centrale è noto e non cambia, viene configurata un'interfaccia VTI statica.

```
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
```

Configurazione del routing

Nell'esempio, il routing viene definito durante la creazione dell'associazione di sicurezza (SA) IKEv2 con la configurazione di un elenco di controllo di accesso. Definisce il traffico da inviare sulla VPN. È possibile anche configurare protocolli di routing dinamico, ma non rientra nell'ambito di questo documento.

Passaggio 5. Definire l'ACL.

Router della sede centrale:

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

Router per filiali:

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

Passaggio 6. Modificare i profili di autorizzazione IKEv2 su ciascun router per impostare l'ACL.

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

Configurazione completa router sede centrale

```
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
```

Configurazione completa router filiale

```
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
```

Verifica

Per verificare il tunnel, è necessario verificare che le fasi 1 e 2 siano attive e funzionino correttamente.

```
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:
```

È inoltre necessario verificare che l'interfaccia di accesso virtuale sia nello stato ATTIVO.

```
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
```

Risoluzione dei problemi

In questa sezione viene descritto come risolvere i problemi relativi alla definizione del tunnel

Se la negoziazione IKE ha esito negativo, completare i seguenti passaggi:

1. Verificare lo stato corrente con questi comandi:

- show crypto ikev2 sa
- show crypto ipsec sa
- mostra sessione crittografica

2. Utilizzare questi comandi per eseguire il debug del processo di negoziazione del tunnel:

- debug crypto ikev2
- debug crypto ipsec

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).