Configurer un tunnel FlexVPN site à site avec un homologue avec une adresse IP dynamique

Table des matières

Introduction

Ce document décrit comment configurer un tunnel VPN de site à site FlexVPN entre 2 routeurs Cisco lorsque l'homologue distant a une adresse IP dynamique.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Protocole IKEv2

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphérique CSR1000V
- Logiciel Cisco IOS® XE, version 17.3.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Diagramme du réseau

Topologie de l'homologue dynamique

Dans cet exemple, la topologie présente un routeur Cisco et un autre routeur Cisco dont l'interface publique comporte une adresse IP dynamique.

Configurations

Cette section décrit comment configurer le tunnel FlexVPN site à site sur un routeur Cisco lorsque l'homologue distant utilise une adresse IP dynamique.

Dans cet exemple de configuration, la méthode d'authentification utilisée est Pre-Shared-Key (PSK). Cependant, l'infrastructure à clé publique (PKI) peut également être utilisée.

Configuration sur le routeur du siège

Dans cet exemple, les valeurs Smart Defaults IKEv2 du routeur ont été utilisées. La fonctionnalité Smart Defaults d'IKEv2 réduit la configuration FlexVPN en couvrant la plupart des cas d'utilisation. Les paramètres par défaut intelligents IKEv2 peuvent être personnalisés pour des cas d'utilisation spécifiques, bien que cela ne soit pas recommandé. Les valeurs par défaut intelligentes incluent la stratégie d'autorisation IKEv2, la proposition IKEv2, la stratégie IKEv2, le profil IPsec (Internet Protocol Security) et l'ensemble de transformation IPsec.

Pour vérifier les valeurs par défaut de votre périphérique, vous pouvez exécuter les commandes répertoriées ci-dessous.

- show crypto ikev2 authorization policy default
- show crypto ikev2 proposition default
- show crypto ikev2 policy default
- show crypto ipsec profile default

- show crypto ipsec transform-set default

Étape 1 - Configurez le porte-clés IKEv2.

- Dans ce cas, comme le routeur du siège social ne connaît pas l'adresse IP de l'homologue en raison de sa dynamique, l'identité qu'il recherche correspond à une adresse IP.
- Les clés distantes et locales sont également configurées.
- Il est recommandé d'avoir des clés fortes pour éviter toute vulnérabilité.

```
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
```

Étape 2 - Configurez le modèle AAA (Authentication, Authorization and Accounting).

- Ceci crée l'infrastructure de gestion pour les utilisateurs qui peuvent se connecter pour cette instance.
- Comme la négociation de connexion est lancée à partir de ce périphérique, le modèle référence sa base de données locale pour déterminer les utilisateurs autorisés.

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

Étape 3 - Configurez le profil IKEv2.

- Étant donné que l'adresse IP de l'homologue distant est dynamique, vous ne pouvez pas utiliser une adresse IP spécifique pour identifier l'homologue.
- Vous pouvez cependant identifier l'homologue distant par domaine, nom de domaine complet ou ID de clé défini sur l'appareil homologue.

- Le groupe AAA (Authentication, Authorization and Accounting) doit être ajouté pour la méthode d'autorisation du profil spécifiant que PSK est la méthode utilisée.
- Si la méthode d'authentification est ICP ici, elle est spécifiée comme cert au lieu de ICP .
- L'objectif étant de créer une interface de tunnel virtuel dynamique (dVTI), ce profil est lié à un modèle virtuel

```
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
```

Étape 4 - Configurez le profil IPsec.

- Un profil IPsec personnalisé peut être configuré si vous n'utilisez pas le profil par défaut.
- Le profil IKEv2 créé à l'étape 3 est mappé à ce profil IPsec.

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

Étape 5 - Configurez l’interface de bouclage et l’interface de modèle virtuel.

- Étant donné que le périphérique distant possède une adresse IP dynamique, une dVTI doit être créée à partir d'un modèle.
- Cette interface de modèle virtuel est un modèle de configuration à partir duquel des interfaces d'accès virtuel dynamiques sont créées.

```
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
```

Configuration du routeur Branch

Pour le routeur de filiale, configurez le porte-clés IKEv2, le modèle AAA, le profil IPsec et le profil IKEv2 comme indiqué dans les étapes précédentes avec les modifications de configuration nécessaires et celles décrites ci-dessous :

1. Configurez l’identité locale envoyée au routeur du siège social en tant qu’identificateur.

```
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
```

Étape 5 - Configurez l’interface de tunnel virtuel statique.

- Étant donné que l’adresse IP du routeur du siège social est connue et ne change pas, une interface VTI statique est configurée.

```
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
```

Configuration du routage

Dans cet exemple, le routage est défini lors de l'établissement de l'association de sécurité IKEv2 avec la configuration d'une liste de contrôle d'accès. Définit le trafic à envoyer sur le VPN. Vous pouvez également configurer des protocoles de routage dynamique, mais cela ne fait pas partie de la portée de ce document.

Étape 5. Définissez l'ACL.

Routeur du siège :

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

Routeur de filiale :

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

Étape 6. Modifiez les profils d'autorisation IKEv2 sur chaque routeur pour définir la liste de contrôle d'accès.

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

Configuration complète du routeur du siège

```
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
```

Configuration complète du routeur de 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
```

Vérifier

Pour vérifier le tunnel, vous devez vérifier que les phases 1 et 2 fonctionnent correctement.

```
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
```

Phase 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:
```

Vous devez également vérifier que l'interface d'accès virtuel est à l'état 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
```

Dépannage

Cette section décrit comment dépanner l'établissement du tunnel

Effectuez ces étapes si la négociation IKE échoue :

1. Vérifiez l'état actuel à l'aide des commandes suivantes :

- show crypto ikev2 sa
- show crypto ipsec sa
- show crypto session [afficher la session avec chiffrement]

2. Utilisez ces commandes afin de déboguer le processus de négociation de tunnel :

- debug crypto ikev2
- debug crypto ipsec

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.