Ejemplo de Configuración de Túnel VPN Sitio-a-Sitio Dinámico IKEv2 entre un ASA y un enrutador con Software IOS

Contenido

Introducción

En este documento se describe cómo configurar un túnel sitio-a-sitio de intercambio de claves de Internet versión 2 (IKEv2) entre un dispositivo de seguridad adaptante (ASA) y un enrutador Cisco si el enrutador tiene una dirección IP dinámica y el ASA tiene una dirección IP estática en las interfaces públicas correspondientes.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS® versión 15.1(1)T o posterior
- ASA Cisco, versión 8.4(1) en adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico.Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada).Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

En este documento se discuten los siguientes escenarios:

- Escenario 1:Un ASA se configura con una dirección IP estática que utiliza un grupo de túnel determinado y el enrutador se configura con una dirección IP dinámica.
- Escenario 2:Un ASA y el enrutador se configuran con una dirección IP dinámica.
- Escenario 3:Este escenario no se discute aquí.En este escenario, el ASA se configura con una dirección IP estática pero utiliza el grupo de túnel DefaultL2LGroup.La configuración para esto es similar a la qué se describe en el artículo Ejemplo de Configuración de Túnel Sitio-a-Sitio Dinámico v2 entre Dos ASA.

La diferencia más importante en la configuración entre los escenarios 1 y 3 es el ID de Protocolo de asociación de seguridad de Internet y administración de claves (ISAKMP)que utiliza el enrutador remoto.Cuando el enrutador estático utiliza el DefaultL2LGroup, el ID de ISAKMP del par del enrutador debe corresponderse con la dirección del ASA.Sin embargo, si se utiliza un grupo de túnel determinado, el ID de ISAKMP del par del enrutador debe ser el mismo que el nombre del grupo de túnel configurado en el ASA.Esto se logra con este comando en el enrutador:

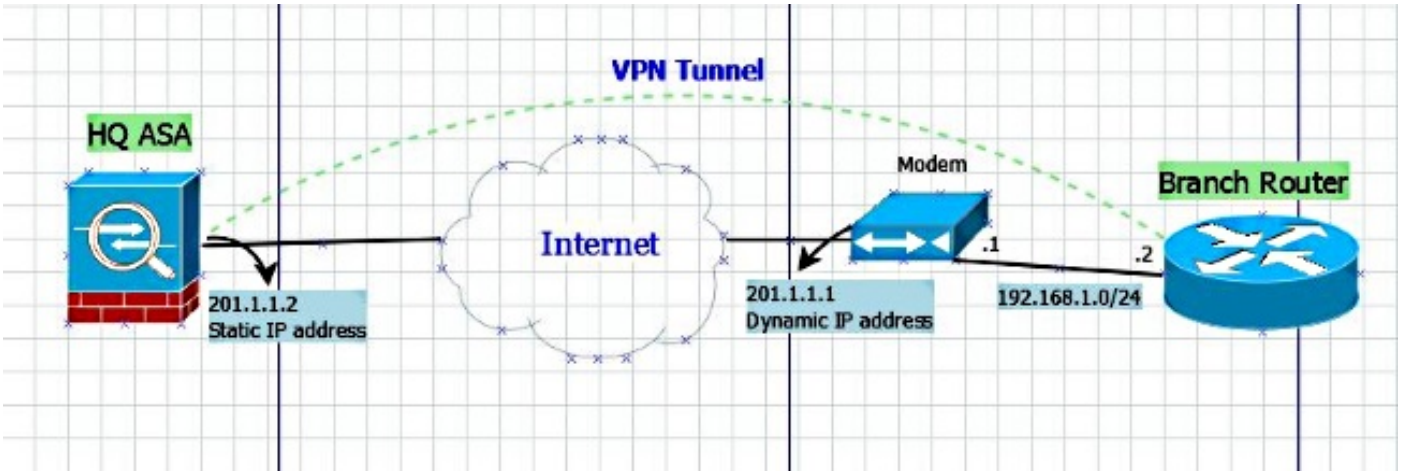
```
identity local key-id
```

La ventaja de usar grupos de túnel determinados en el ASA estático es que, cuando se utiliza el DefaultL2LGroup, la configuración de los enrutadores/ASA dinámicos remotos, que incluye las claves previamente compartidas, debe ser idéntica y no permite que haya demasiada granularidad en las directivas de configuración.

Configurar

Escenario 1

Diagrama de la red



Configuración

En esta sección se describe la configuración del ASA y el enrutador sobre la base de la configuración de un grupo de túnel determinado.

Configuración de ASA Estático

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Configuración del Enrutador Dinámico

Se configura el enrutador dinámico casi de la misma manera que se configuraría en casos donde el enrutador actúa como sitio dinámico del túnel IKEv2 L2L, con la adición de un comando como se muestra a continuación:

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Por lo tanto, para cada par dinámico, la id de clave es diferente y debe crearse un grupo de túnel correspondiente en el ASA estático con el nombre correcto, lo que aumenta la granularidad de las directivas que se implementan en un ASA.

Escenario 2

> **Nota**: Esta configuración sólo es posible cuando al menos un lado es un router.Si ambos lados fueran ASA, esta configuración no funcionará.En la versión 8.4, el ASA no puede utilizar el nombre de dominio completo (FQDN) con el comando set peer, pero se ha solicitado una mejora de CSCus37350 en las próximas versiones.

Si la dirección IP del ASA remoto es dinámica y tiene un FQDN de interfaz de VPN, deberá definir el FQDN del ASA remoto en lugar de la dirección IP del ASA remoto, con el siguiente comando:

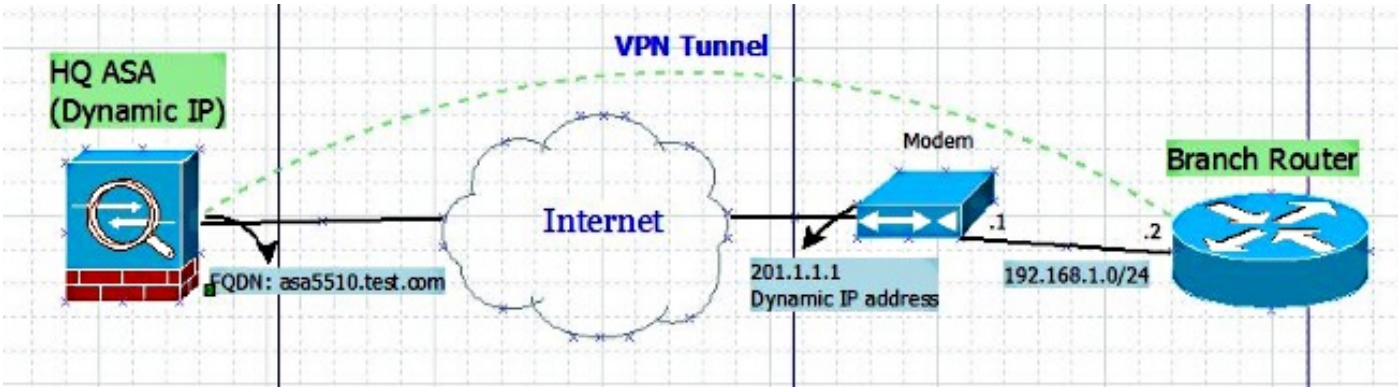
```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

Consejo:La palabra clave dinámica es opcional.Cuando especifica el nombre de servidor de un par IPSec remoto con el comando set peer, también puede establecer la palabra clave dinámica, que aplaza la resolución del nombre de domino del servidor (DNS) hasta el momento antes de establecer el túnel IPSec.

Aplazar dicha resolución permite que el Software Cisco IOS detecte cambios en la dirección IP del par IPSec remoto.Así, el software puede comunicarse con el par mediante la nueva dirección IP.Si la palabra clave dinámica no se establece, se resuelve el nombre de servidor inmediatamente después de que se especifique.Así pues, el Software Cisco IOS no podrá detectar un cambio y, por lo tanto, intentará comunicarse mediante la dirección IP previamente determinada.

Diagrama de la red



Configuración

Configuración de ASA Dinámico

La configuración del ASA se realiza de la misma manera que en la Configuración de ASA Estático, con la única excepción de que la dirección IP no se define como estática en la interfaz física.

Configuración del router

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
```

```
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel

crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

ASA Estático

- Aquí está el resultado del comando show crypto IKEv2 sa det:

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                Remote     Status         Role
120434199        201.1.1.2/4500        201.1.1.1/4500      READY    RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
      Remote id: S2S-IKEv2
     Local req mess id: 43             Remote req mess id: 2
     Local next mess id: 43            Remote next mess id: 2
     Local req queued: 43              Remote req queued: 2
     Local window: 1                   Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected  outside
Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- Aquí está el resultado del comando show crypto ipsec sa:

```
interface: outside
   Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2
```

```
     local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
     current_peer: 201.1.1.1


     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
     path mtu 1500, ipsec overhead 82(52), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 41AA84F4
     current inbound spi : 00853C02

   inbound esp sas:
     spi: 0x00853C02 (8731650)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4101119/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x41AA84F4 (1101694196)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4055039/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Enrutador Dinámico

- Aquí está el resultado del comando show crypto IKEv2 sa detail:

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
      Local id: S2S-IKEv2
     Remote id: 201.1.1.2
     Local req msg id:  2              Remote req msg id:  48
     Local next msg id: 2              Remote next msg id: 48
     Local req queued:  2              Remote req queued:  48
```

```
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

  IPv6 Crypto IKEv2  SA
```

- Aquí está el resultado del comando show crypto ipsec sa:

```
interface: GigabitEthernet0/0
   Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
   #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.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
    plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x853C02(8731650)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x41AA84F4(1101694196)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x853C02(8731650)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

Enrutador Dinámico (con ASA Di´namico Remoto)

- Aquí está el resultado del comando show crypto IKEv2 sa detail:

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1516 sec
     CE id: 1034, Session-id: 24
     Status Description: Negotiation done
     Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
      Local id: S2S-IKEv2
      Remote id: asa5510.test.com
     Local req msg id:  2              Remote req msg id:  73
     Local next msg id: 2              Remote next msg id: 73
     Local req queued:  2              Remote req queued:  73
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

Nota:El ID remoto y local en esta salida es el grupo de túnel determinado que definió en el ASA para verificar si cae en el grupo de túnel adecuado.Esto puede comprobarse además mediante una depuración de IKEv2 en cualquier extremo.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show.Utilice la herramienta para ver una análisis de información de salida del comando show.

Nota:Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

En el enrutador Cisco IOS, utilice:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

En el ASA, utilice:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```