Sitio dinámico para localizar el túnel IKEv2 VPN entre un ASA y un ejemplo de configuración del router IOS

Contenido

Introducción

Este documento describe cómo configurar un túnel del intercambio de claves de Internet versión 2 (IKEv2) VPN del sitio a localizar entre un dispositivo de seguridad adaptante (ASA) y un router Cisco donde el router tiene un IP Address dinámico y el ASA tiene un IP Address estático en las interfaces del público-revestimiento.

Prerequisites

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.

- Versión del ® del Cisco IOS 15.1(1)T o más adelante
- Versión de ASA de Cisco 8.4(1) o más 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

Este documento discute estos escenarios:

- Escenario 1: Un ASA se configura con un IP Address estático que utilice a un grupo de túnel Nombrado y configuran al router con un IP Address dinámico.

- Escenario 2: Un ASA se configura con un IP Address dinámico y configuran al router con un IP Address dinámico.

- Escenario 3: Este escenario no se discute aquí. En este escenario, el ASA se configura con un IP Address estático pero utiliza al grupo de túnel DefaultL2LGroup. La configuración para esto es similar a qué se describe en el sitio dinámico para localizar el túnel IKEv2 VPN entre el artículo del ejemplo de configuración dos ASA.

La diferencia en la configuración más grande entre los escenarios 1 y 3 es el Internet Security Association and Key Management Protocol (ISAKMP) ID usado por el router remoto. Cuando el DefaultL2LGroup se utiliza en el ASA estático, el ISAKMP ID del par en el router debe ser el direccionamiento del ASA. Sin embargo, si utilizan a un grupo de túnel Nombrado, el ISAKMP ID del par en el router debe ser lo mismo que el nombre de grupo de túnel configurado en el ASA. Esto se logra con este comando en el router:

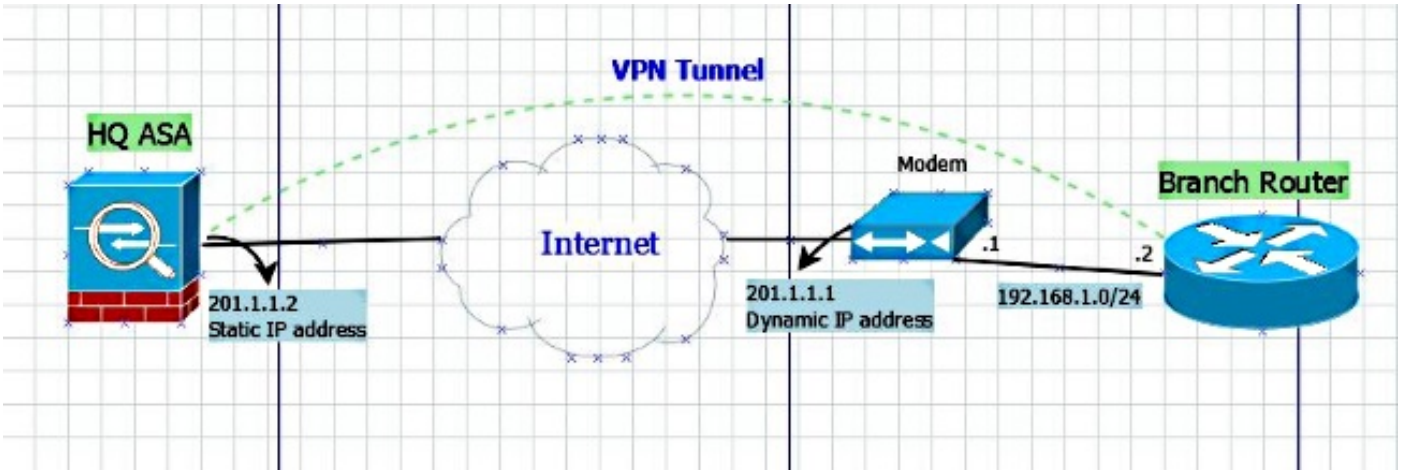
```
identity local key-id <name of the tunnel-group on the static ASA>
```

La ventaja de usar a los grupos de túnel Nombrados en el ASA estático es que cuando se utiliza el DefaultL2LGroup, la configuración en los ASA/el Routers dinámicos remotos, que incluye las claves previamente compartidas, debe ser idéntica y no permite mucho granularity con la configuración de las directivas.

Configurar

Escenario 1

Diagrama de la red



Configuración

Esta sección describe la configuración en el ASA y el router basados en la configuración Nombrada del grupo de túnel.

Configuración estática ASA

```
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 router dinámica

Configuran al router dinámico casi la misma manera que usted configura normalmente en caso de

que el router sea un sitio dinámico para el túnel IKEv2 L2L con la adición de un comando como se muestra aquí:

```
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
```

Tan en cada par dinámico, la clave-identificación es diferente y un grupo de túnel correspondiente debe ser creado en el ASA estático con el nombre correcto, que también aumenta el granularity de los polocies que se implementan en un ASA.

Escenario 2

> **Note**: Esta configuración es solamente posible cuando por lo menos un lado es un router. Si los ambos lados son ASA, esta configuración no trabaja ahora. En la versión 8.4, el ASA no puede utilizar el nombre de dominio completo (FQDN) con el **comando set peer**, pero la mejora CSCus37350 se ha pedido para las futuras versiones.

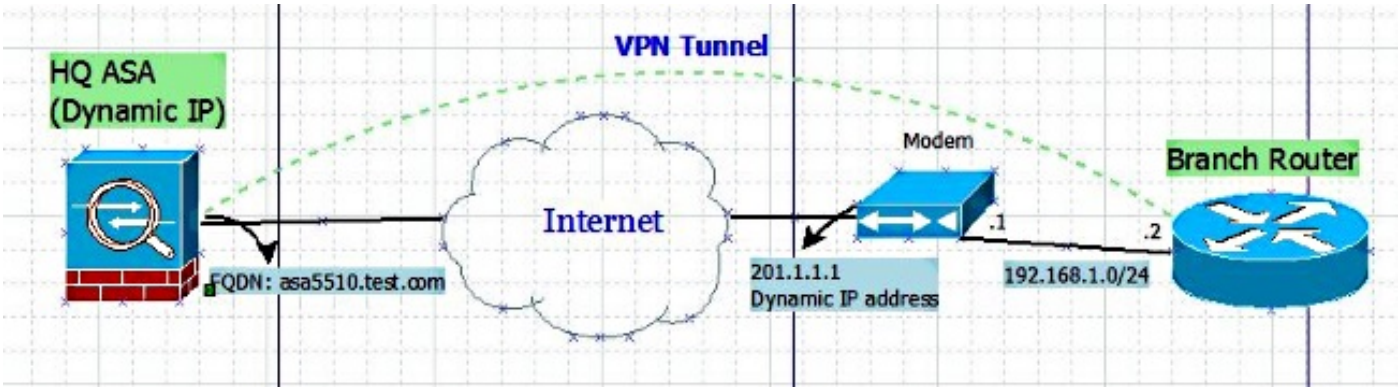
Si la dirección IP del telecontrol el ASA es dinámica también sin embargo tiene un Nombre de dominio totalmente calificado (FQDN) asignado para su interfaz VPN, después bastante que la dirección IP del telecontrol ASA, usted ahora definen el FQDN del telecontrol ASA con este comando en el router:

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

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

> **Tip**: **La palabra clave dinámica** es opcional. Cuando usted especifica el nombre de host de un peer IPSec remoto vía el **comando set peer**, usted puede también publicar la palabra clave dinámica, se ha establecido que difiere la resolución del Domain Name Server (DNS) del nombre de host hasta que justo antes del túnel IPsec.
>
> La resolución que difiere permite al Cisco IOS Software para detectar si la dirección IP del peer IPSec remoto ha cambiado. Así, el software puede entrar en contacto al par en la nueva dirección IP. Si la palabra clave dinámica no se publica, se resuelve el nombre de host inmediatamente después que se especifica. Así pues, el Cisco IOS Software no puede detectar un cambio y, por lo tanto, las tentativas de la dirección IP de conectar con la dirección IP que resolvió previamente.

Diagrama de la red



Configuración

Configuración dinámica ASA

La configuración en el ASA es lo mismo que la [configuración estática ASA] con solamente una excepción, que es que la dirección IP en la interfaz física no está definida estáticamente.

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 **crypto del det IKEv2 sa de la demostración**:

```
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**:

```
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
```

Router dinámico

- Aquí está el resultado del **comando detail crypto IKEv2 sa de la demostración**:

```
 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**:

```
 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
```

Router dinámico (con el ASA dinámico remoto)

- Aquí está el resultado del **comando detail crypto IKEv2 sa de la demostración**:

```
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
```

Note: El ID remoto y local en esta salida es el **grupo de túnel Nombrado que** usted definió en el ASA para verificar si usted se cae en el grupo de túnel adecuado. Esto puede también ser verificada si usted hace el debug de IKEv2 en cualquier extremo.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su

configuración.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

> **Note**: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

En el router del 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
```