Sitio dinámico para localizar el túnel IKEv2 VPN entre el ejemplo de configuración dos ASA

Contenido

Introducción

Este documento describe cómo configurar un túnel del intercambio de claves de Internet versión 2 (IKEv2) VPN del sitio a localizar entre dos dispositivos de seguridad adaptantes (ASA) donde un ASA tiene un IP Address dinámico y el otro tiene un IP Address estático.

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.

- Versión de ASA 5505
- Versión de ASA 9.1(5)

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

Hay dos maneras que esta configuración puede ser configurada:

- Con el grupo de túnel DefaultL2LGroup
- Con un grupo de túnel Nombrado

La diferencia en la configuración más grande entre los dos escenarios es el Internet Security Association and Key Management Protocol (ISAKMP) ID usado por el telecontrol ASA. Cuando el DefaultL2LGroup se utiliza en el ASA estático, el ISAKMP ID del par tiene que ser el direccionamiento. Sin embargo si utilizan a un grupo de túnel Nombrado, el ISAKMP ID del par tiene que ser lo mismo el nombre de grupo de túnel usando este comando:

```
crypto isakmp identity key-id <tunnel-group_name>
```

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 dinámicos remotos, que incluye las claves previamente compartidas, tiene que ser idéntica y no permite mucho granularity con la configuración de las directivas.

Diagrama de la red

Configurar

Esta sección describe la configuración en cada ASA dependiendo de qué solución usted decide utilizar.

Solución 1 - Uso del DefaultL2LGroup

Ésta es la manera más simple de configurar un túnel del LAN a LAN (L2L) entre dos ASA cuando un ASA consigue su direccionamiento dinámicamente. El grupo DefaultL2L es un grupo de túnel preconfigurado en el ASA y todas las conexiones que no hacen juego explícitamente ninguna caída del grupo del túnel particular en esta conexión. Puesto que el ASA dinámico no tiene un constante predeterminó la dirección IP, él significa que el admin no puede configurar el Statis ASA para permitir la conexión en un grupo de túnel específico. En esta situación, el grupo DefaultL2L puede ser utilizado para permitir las conexiones dinámicas.

> Consejo: Con este método, la desventaja es que todos los pares tendrán la misma clave previamente compartida puesto que solamente una clave previamente compartida se puede definir por el grupo de túnel y todos los pares conectarán con el mismo grupo de túnel

DefaultL2LGroup.

Configuración estática ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

En el Administrador de dispositivos de seguridad adaptante (ASDM), usted puede configurar el DefaultL2LGroup como se muestra aquí:

ASA dinámico

```
crypto isakmp identity key-id <tunnel-group_name>
```

En el ASDM, usted puede utilizar al Asisitente estándar para configurar el perfil de la conexión apropiado o usted puede agregar simplemente una nueva conexión y seguir el procedimiento estándar.

Solución 2 - Cree a un grupo de túnel definido por el usario

Este método requiere slighly más configuración, pero permite más granularity. Cada par puede tener su propia política diferenciados y clave previamente compartida. Al menos aquí es importante cambiar el ISAKMP ID en el par dinámico de modo que utilice un nombre en vez de una dirección IP. Esto permite que el ASA estático haga juego la petición entrante de la inicialización ISAKMP al grupo de túnel adecuado y utilice las directivas correctas.

Configuración estática ASA

```
crypto isakmp identity key-id <tunnel-group_name>
```

En el ASDM, el nombre del perfil de la conexión es una dirección IP por abandono. Tan cuando usted lo crea, usted debe cambiarlo para darle un nombre tal y como se muestra en del tiro de pantalla aquí:

Configuración dinámica ASA

El ASA dinámico se configura casi la misma manera en ambas soluciones con la adición de un comando como se muestra aquí:

```
crypto isakmp identity key-id DynamicSite2Site1
```

Según lo descrito previamente, por abandono el ASA utiliza la dirección IP de la interfaz que el túnel VPN está asociado como al ISAKMP CLAVE-ID. Al menos en este caso, el clave-ID en el ASA dinámico es lo mismo que el nombre del grupo de túnel en el ASA estático. Tan en cada par dinámico, la clave-identificación será diferente y un grupo de túnel correspondiente debe ser creado en el ASA estático con el nombre correcto.

En el ASDM, esto se puede configurar tal y como se muestra en de este tiro de pantalla:

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

En el ASA estático

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

```
crypto isakmp identity key-id DynamicSite2Site1
```

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

```
crypto isakmp identity key-id DynamicSite2Site1
```

En el ASA dinámico

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

```
crypto isakmp identity key-id DynamicSite2Site1
```

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

```
crypto isakmp identity key-id DynamicSite2Site1
```

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.

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.

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

- **paquete crypto IKEv2 DEB**
- **DEB IKEv2 crypto interno**