Contenido

Introducción

Este documento proporciona la información sobre cómo configurar un dispositivo del gateway de VPN para actuar siempre como respondedor en una negociación IKE. El dispositivo responderá a cualquier negociación crypto que hayan iniciado sus peers.

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.

- Router Cisco con el Software Release 12.4(24)T y Posterior de Cisco IOS®
- Dispositivo de seguridad adaptante de Cisco (ASA) con la versión 7.0 y posterior

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- Cisco PIX Firewall con la versión de software 7.0 y posterior

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Cualquier negociación crypto tiene dos partidos para desempeñar los papeles del iniciador y del respondedor. El iniciador envía las ofertas crypto al respondedor que contiene diversos parámetros sobre el cifrado, los algoritmos de autenticación, reintroduciendo las opciones y los valores del curso de la vida y así sucesivamente. El respondedor elige la oferta correcta y una sesión de criptografía establece. El papel desempeñado por un dispositivo final se puede ver por esta salida de comando:

```
Router#show crypto isakmp sa1   IKE Peer: XX.XX.XX.XX    Type    : L2L             Role    :
initiator    Rekey   : no              State   : MM_ACTIVEASA(config)#show crypto isakmp sa
detailIKE Peer    Type  Dir   Rky    State      Encrypt    Hash  Auth       Lifetime1
209.165.200.225 User  Resp  No   AM_Active    3des      SHA   preshrd     86400
```

Ventajas de la característica del modo del respondedor-Solamente IKE

Puesto que han ocurrido el advenimiento de las características del Red privada virtual (VPN) que permiten las negociaciones IKE bidireccionales simultáneas (con o sin el tráfico interesante), los problemas con la dirección y la recuperación de datos del duplicado IKE SA. El IKE como protocolo no tiene ninguna capacidad de comparar las negociaciones IKE para determinar si hay ya una negociación de la existencia o del en-proceso entre dos pares que ocurren. Estas negociaciones duplicados pueden ser costosas en términos de recursos y confusión a los administradores de router. Cuando un dispositivo se configura como dispositivo del respondedor-solamente, no iniciará los modos principales, agresivos, o rápidos IKE (para el establecimiento IKE y IPSec SA), ni reintroducirá el IKE y el SA de IPSec. Por lo tanto, la probabilidad del duplicado SA se reduce.

La otra ventaja de esta característica es permitir el soporte controlado para las conexiones de negociación en una dirección solamente en un escenario del balanceo de carga. No se recomienda que los servidores o el Hubs inician las conexiones VPN hacia los clientes o el spokes porque estos dispositivos son todos que son accedidos por una dirección IP del solo-revestimiento según lo hecho publicidad vía el balanceador de la carga. Si el Hubs fuera iniciar la conexión, él estaría haciendo tan usando una dirección IP individual, así evitando las ventajas del balanceador de la carga. Lo mismo es verdad de reintroducir las peticiones que son originadas del Hubs o de los servidores detrás del balanceador de la carga.

Un router que se configurará como dispositivo del respondedor-Solamente en una negociación crypto

El Cisco IOS Software Release 12.4(24)T introduce las funciones del router para responder siempre a las negociaciones IKE iniciadas por sus pares. La limitación principal es que esta característica es configurable solamente bajo perfil de ipsec y es relevante solamente a un escenario de la interfaz virtual. Ningún soporte para los escenarios de los parásitos atmosféricos o de la correspondencia cifrada dinámica.

Para configurar a su router como respondedor-solamente, realice estos pasos:

```
enable configure terminal crypto ipsec profile <name>   responder-only
```

Un ASA que se configurará como dispositivo del respondedor-Solamente en una negociación crypto

En las conexiones de LAN a LAN generales del IPSec, el ASA puede funcionar como el iniciador o el respondedor. En las conexiones del IPSec cliente-a-LAN, el ASA funciona solamente como el respondedor. Un ASA se puede configurar como responde-solamente dispositivo en las conexiones VPN del LAN a LAN. Sin embargo, la restricción es que el dispositivo en el otro extremo del túnel VPN debe ser uno de éstos:

- Dispositivo de las 5500 Series de Cisco ASA
- Concentrador del Cisco VPN de la serie 3000
- Firewall de la serie del Cisco PIX 500 que funciona con el software 7.0 y posterior

Para configurar su ASA como dispositivo del respondedor-solamente, publique este comando:

respuesta-solamente determinada del Tipo de conexión del mymap 10 de la correspondencia de criptografía del hostname(config)#

Nota: Se sugiere para configurar un dispositivo del gateway de VPN como respondedor-solamente donde los pares múltiples VPN terminan.

Información Relacionada

- Configurando a túnel de LAN a LAN y de router a router con un router que inicia al modo agresivo IKE
- Ejemplos y notas técnicas de la configuración de ASA de Cisco
- Soporte Técnico y Documentación - Cisco Systems