Troubleshooting Zona-basado del Firewall

Contenido

Introducción

Este documento contiene la información de Troubleshooting para el Firewall zona-basado.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Usando el VPN con el Firewall Zona-basado de la directiva
- Diseño del Firewall de la directiva y guía Zona-basados de la aplicación

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Convenciones

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

Incapaz de pasar el tráfico VPN

Problema

El problema es que el tráfico VPN no puede pasar a través del Firewall zona-basado.

Solución

Permita que el tráfico del cliente VPN sea examinado por el Firewall zona-basado del ® del Cisco IOS.

Por ejemplo, aquí están las líneas a agregar en la configuración del router:

```
access-list 103 permit ip 172.16.1.0 0.0.0.255 172.22.10.0 0.0.0.255 class-map type inspect
match-all sdm-cls-VPNOutsideToInside-1  match access-group 103 policy-map type inspect sdm-
inspect-all  class type inspect sdm-cls-VPNOutsideToInside-1   inspect zone-pair security sdm-
zp-out-in source out-zone destination in-zone  service-policy type inspect sdm-inspect-all
```

Incapaz de pasar GRE/PPTP

Problema

El problema es que el tráfico GRE/PPTP no puede pasar con el Firewall zona-basado.

Solución

Permita que el tráfico del cliente VPN sea examinado por el Firewall Cisco IOS zona-basado.

Por ejemplo, aquí están las líneas a agregar en la configuración del router:

```
agw-7206>enablegw-7206#conf tgw-7206(config)#policy-map type inspect outside-to-insidegw-
7206(config-pmap)#no class type inspect outside-to-insidegw-7206(config-pmap)#no class class-
defaultgw-7206(config-pmap)#class type inspect outside-to-insidegw-7206(config-pmap-
c)#inspect%No specific protocol configured in class outside-to-inside for inspection.All
protocols will be inspectedgw-7206(config-pmap-c)#class class-defaultgw-7206(config-pmap-
c)#dropgw-7206(config-pmap-c)#exitgw-7206(config-pmap)#exit
```

Verifique la configuración

```
gw-7206#show run policy-map outside-to-insidepolicy-map type inspect outside-to-inside class
type inspect PPTP-Pass-Through-Traffic  pass class type inspect outside-to-inside  inspect class
```

```
class-default  drop
```

Alcance de la red

Problema

Después de que la directiva para el Firewall zona-basado se aplique en el router del Cisco IOS, las redes no son accesibles.

Solución

Este problema pudo ser el Asymmetric Routing. El Firewall Cisco IOS no trabaja en los entornos con el Asymmetric Routing. Los paquetes no se garantizan para volver a través del mismo router.

El Firewall Cisco IOS sigue el estado de las sesiones TCP/UDP. Un paquete debe salir y volver del mismo router para el mantenimiento exacto de la información del estado.

Incapaz de pasar el tráfico del DHCP con un Firewall Zona-basado

Problema

Usted no puede pasar el tráfico del DHCP con un Firewall zona-basado.

Solución

Inhabilite el examen del tráfico de la uno mismo-zona para resolver este problema.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- AnyConnect en el IOS con el Firewall Zona-basado (ZBFW)