Resolución de Problemas de Inspección de Firewall de Política Basada en Zona IOS para el protocolo PPTP con GRE

Contenido

Introducción

Este documento describe un problema encontrado con el firewall basado en zonas (ZBF), desde el que ZBF no inspecciona correctamente el protocolo de túnel punto a punto (PPTP) con encapsulación de routing genérico (GRE) .

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la configuración de Cisco ZBF en los routers IOS.

Componentes Utilizados

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

- Routers de servicios integrados (ISR G1)
- IOS 15M&T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

PPTP es un método de implementación de redes privadas virtuales. PPTP utiliza un canal de

control sobre TCP y un túnel GRE que funciona para encapsular paquetes PPP.

Se inicia un túnel PPTP al par en el puerto TCP 1723. Esta conexión TCP se utiliza luego para iniciar y administrar un segundo túnel GRE al mismo par.

El túnel GRE se utiliza para transportar paquetes PPP encapsulados, lo que permite el túnel de cualquier protocolo que se pueda transportar dentro de PPP. Si se incluyen NetBEUI e IPX.

Problema: Resolución de Problemas de Inspección de Firewall de Política Basada en Zona IOS para el protocolo PPTP con GRE

Se confirma que el ZBF no inspecciona el PPTP con el tráfico GRE y esto se debe a que no abre los orificios de anclaje necesarios para permitir el paso del tráfico de retorno, aquí un ejemplo de una configuración ZBF típica para la inspección del protocolo PPTP con el tráfico GRE:

```
ip access-list extended 160
permit gre any any

class-map type inspect match-all PPTP-GRE
match access-group 160

policy-map type inspect WAN-LAN-pmap
 class class-default
  drop

policy-map type inspect LAN-WAN-pmap
class type inspect PPTP-GRE
  inspect
 class class-default
  drop

zone security LAN
zone security WAN

zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-pmap
zone-pair security WAN-LAN source WAN destination LAN
 service-policy type inspect WAN-LAN-pmap
```

> **Nota:** Tenga en cuenta que en el ejemplo de configuración la conexión PPTP se inicia desde la LAN a la zona WAN.

> **Nota:** Aunque la conexión TCP del PPTP se muestra como establecida en el resultado **show policy-firewall sessions** del ZBF, la conexión PPTP no funciona a través del router.

Solución

Para permitir las conexiones VPN PPTP con GRE a través de ZBF, debe cambiar la acción de **inspección** de las reglas ZBF para una **acción de paso** en ambas direcciones del flujo de tráfico en los pares de zonas involucrados, de la siguiente manera:

```
ip access-list extended 160
permit gre any any

class-map type inspect match-all PPTP-GRE
match access-group 160

policy-map type inspect WAN-LAN-pmap
class type inspect PPTP-GRE
  pass
 class class-default
 drop

policy-map type inspect LAN-WAN-pmap
class type inspect PPTP-GRE
  pass
 class class-default
 drop

zone security LAN
zone security WAN

zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-pmap
zone-pair security WAN-LAN source WAN destination LAN
 service-policy type inspect WAN-LAN-pmap
```

Después de aplicar este cambio de configuración de ZBF, la conexión VPN PPTP con GRE funcionará bien a través del ZBF.

Información Relacionada

Para permitir el tráfico del protocolo GRE y Encapsulating Security Payload (ESP) a través de un firewall de políticas basado en zonas, utilice la acción **pass**. El GRE y los protocolos ESP no soportan la inspección stateful y si utiliza la acción **inspect** en el ZBF, el tráfico para estos protocolos se descarta.

Guía de configuración de seguridad: Firewall de políticas basado en zonas, Cisco IOS Release 15M&T

Error relacionado

CSCtn52424 ZBF ENH: Implementar la inspección de PPTP con transferencia dinámica de GRE