Identificar e Solucionar Problemas de Inspeção de Firewall de Política Baseada em Zona IOS para o protocolo PPTP com GRE

Contents

Introduction

Este documento descreve um problema encontrado com o Zone-Based Firewall (ZBF), de onde o ZBF não inspeciona corretamente o Point-to-Point Tunneling Protocol (PPTP) com Generic Routing Encapsulation (GRE) .

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da configuração do Cisco ZBF em roteadores IOS.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteadores de serviços 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O PPTP é um método de implementação de redes virtuais privadas. O PPTP usa um canal de

controle sobre o TCP e um túnel GRE que opera para encapsular pacotes PPP.

Um túnel PPTP é iniciado para o peer na porta TCP 1723. Essa conexão TCP é então usada para iniciar e gerenciar um segundo túnel GRE para o mesmo peer.

O túnel GRE é usado para transportar pacotes PPP encapsulados, o que permite o túnel de qualquer protocolo que possa ser transportado dentro do PPP. Se, NetBEUI e IPX estão incluídos.

Problema: Identificar e Solucionar Problemas de Inspeção de Firewall de Política Baseada em Zona IOS para o protocolo PPTP com GRE

Confirmado que o ZBF não inspeciona o PPTP com tráfego GRE e isso ocorre porque ele não abre os orifícios de pinos necessários para permitir a passagem do tráfego de retorno, aqui está um exemplo de uma configuração ZBF típica para a inspeção do protocolo PPTP com tráfego 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
```

> **Note**: Considere que no exemplo de configuração a conexão PPTP é iniciada da LAN para a zona WAN.

> **Note**: Embora a conexão TCP do PPTP seja mostrada como estabelecida na saída **show policy-firewall sessions** do ZBF, a conexão PPTP não funciona através do roteador.

Solução

Para permitir as conexões VPN PPTP com GRE através do ZBF, você precisa alterar a **ação de inspeção** das regras ZBF para uma **ação de passagem** em ambas as direções do fluxo de tráfego

nos pares de zonas envolvidos, da seguinte maneira:

```
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
```

Depois de aplicar essa alteração de configuração de ZBF, a conexão VPN PPTP com GRE funcionará bem através do ZBF.

Informações Relacionadas

Para permitir o tráfego de protocolo GRE e ESP (Encapsulating Security Payload, payload de segurança de encapsulamento) através de um firewall de política baseado em zona, use a ação **pass**. O GRE e os protocolos ESP não suportam inspeção stateful e se você usa a **ação de inspeção** no ZBF, o tráfego desses protocolos é descartado.

Guia de configuração de segurança: Firewall de política baseado em zona, Cisco IOS versão 15M&T

Erro relacionado

CSCtn52424 ZBF ENH: Implementar inspeção de PPTP com passagem de GRE dinâmica