Probleemoplossing voor IOS Zone gebaseerde beleidsfirewallinspectie voor het PPTP-protocol met GRE

Inhoud

Inleiding

Dit document beschrijft een probleem dat wordt aangetroffen met de Zone-Based Firewall (ZBF), van waar de ZBF het Point-to-Point Tunneling Protocol (PPTP) niet correct inspecteert met Generic Routing Encapsulation (GRE).

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van de Cisco ZBF-configuratie in IOS-routers.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Geïntegreerde services routers (ISR G1)
- IOS 15M&T

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De PPTP is een uitvoeringsmethode van virtuele particuliere netwerken. PPTP gebruikt een

controlekanaal over TCP en een GRE tunnel die om PPP pakketten in te sluiten.

Een PPTP-tunnel wordt gestart met de peer in de TCP-poort 1723. Deze TCP verbinding wordt dan gebruikt om een tweede GRE-tunnel naar dezelfde peer te openen en te beheren.

De GRE-tunnel wordt gebruikt om ingekapselde PPP-pakketten over te brengen, waarmee de tunnel van een protocol kan worden geïnstalleerd dat binnen PPP wordt uitgevoerd. INDIEN zijn NetBEUI en IPX inbegrepen.

Probleem: Probleemoplossing voor IOS Zone gebaseerde beleidsfirewallinspectie voor het PPTP-protocol met GRE

Er wordt bevestigd dat ZBF de PPTP niet met GRE-verkeer inspecteert en dat dit komt doordat de pin-gaten niet worden geopend die nodig zijn om het retourverkeer door te laten gaan, bijvoorbeeld een typische ZBF-configuratie voor de inspectie van het PPTP-protocol met GRE-verkeer:

```
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
```

> Opmerking: Houd er rekening mee dat in het configuratievoorbeeld de PPTP-verbinding van LAN naar WAN wordt gestart.

> Opmerking: Hoewel de TCP-verbinding van de PPTP wordt getoond zoals vastgesteld in de output van de **showbeleid-firewallsessies** van de ZBF, werkt de PPTP-verbinding niet door de router.

Oplossing

Om de PPTP VPN-verbindingen met GRE via de ZBF mogelijk te maken, moet u de actie van de ZBF-regels voor een **doorvoeractie** in beide richtingen van de verkeersstroom in de betrokken

zone-paren wijzigen, en wel als volgt:

```
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
```

Nadat u deze ZBF configuratieverandering hebt toegepast, zal de verbinding van PPTP VPN met GRE fijn door de ZBF werken.

Gerelateerde informatie

Om GRE en Encapsulating Security Payload (ESP) protocolverkeer door een zone-gebaseerde beleidsfirewall toe te staan, gebruik de **pass actie**. De GRE en de ESP protocollen ondersteunen geen stateful inspection en als u de **inspectie** van de actie op de ZBF gebruikt, wordt het verkeer voor deze protocollen ingetrokken.

Security configuratiegids: Zone-Based Policy Firewall, Cisco IOS release 15M&T

Verwante blog

CSCtn52424 ZBF ENH: Uitvoeren van inspectie van PPTP met dynamische GRE-doorgifte