Fehlerbehebung bei Problemen mit der IOS Zone Based Policy Firewall Inspection für das PPTP-Protokoll mit GRE

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem mit der zonenbasierten Firewall (ZBF), von der aus das ZBF das Point-to-Point Tunneling Protocol (PPTP) mit Generic Routing Encapsulation (GRE) nicht ordnungsgemäß überprüft.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco ZBF-Konfiguration in IOS-Routern verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Integrated Services Router (ISR G1)
- IOS 15M&T

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

PPTP ist eine Implementierungsmethode für virtuelle private Netzwerke. PPTP verwendet einen Kontrollkanal über TCP und einen GRE-Tunnel, der PPP-Pakete kapselt.

Ein PPTP-Tunnel wird zum Peer am TCP-Port 1723 initiiert. Diese TCP-Verbindung wird dann verwendet, um einen zweiten GRE-Tunnel zum gleichen Peer zu initiieren und zu verwalten.

Der GRE-Tunnel wird verwendet, um gekapselte PPP-Pakete zu übertragen, wodurch der Tunnel jedes Protokolls ermöglicht wird, das innerhalb von PPP übertragen werden kann. IF, NetBEUI und IPX sind enthalten.

Problem: Fehlerbehebung bei Problemen mit der IOS Zone Based Policy Firewall Inspection für das PPTP-Protokoll mit GRE

Es wird bestätigt, dass das ZBF das PPTP nicht mit GRE-Datenverkehr überprüft, und zwar deshalb, weil es nicht die Pin-Löcher öffnet, die erforderlich sind, damit der Rückverkehr weitergeleitet werden kann. Hier ein Beispiel einer typischen ZBF-Konfiguration für die Prüfung des PPTP-Protokolls mit GRE-Datenverkehr:

```
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
```

> **Hinweis**: Beachten Sie, dass im Konfigurationsbeispiel die PPTP-Verbindung vom LAN zur WAN-Zone initiiert wird.

> **Hinweis**: Obwohl die TCP-Verbindung des PPTP in der Ausgabe von **Richtlinien-Firewall-Sitzungen** des ZBF wie festgelegt angezeigt wird, funktioniert die PPTP-Verbindung nicht über den Router.

Lösung

Um die PPTP VPN-Verbindungen mit GRE über das ZBF zu ermöglichen, müssen Sie die Aktion

inspect der ZBF-Regeln für eine **Pass-**Aktion in beide Richtungen des Datenverkehrs in den beteiligten Zonenpaaren wie folgt ändern:

```
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
```

Nachdem Sie diese ZBF-Konfigurationsänderung vorgenommen haben, funktioniert die PPTP VPN-Verbindung mit GRE über das ZBF.

Zugehörige Informationen

Verwenden Sie die **Aktion "pass"**, um den Datenverkehr des GRE- und Encapsulating Security Payload (ESP)-Protokolls durch eine zonenbasierte Richtlinien-Firewall zuzulassen. Die GRE- und die ESP-Protokolle unterstützen keine Stateful Inspection. Wenn Sie die **Inspect-**Aktion auf dem ZBF verwenden, wird der Datenverkehr für diese Protokolle verworfen.

Leitfaden zur Sicherheitskonfiguration: Zonenbasierte Firewall, Cisco IOS-Version 15M&T

Verwandter Fehler

CSCtn52424 ZBF ENH: Implementieren der PPTP-Prüfung mit dynamischem GRE-Passthrough