排除GRE PPTP协议的基于IOS区域的策略防火墙检查问题

目录

简介

本文档介绍基于区域的防火墙(ZBF)发现的问题，ZBF无法通过通用路由封装(GRE)正确检查点对点隧道协议(PPTP)。

先决条件

要求

思科建议您了解IOS路由器中的Cisco ZBF配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 集成多业务路由器(ISR G1)
- IOS 15M&T

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

PPTP是虚拟专用网络的一种实现方法。PPTP使用TCP控制信道和GRE隧道，该隧道用于封装PPP数据包。

PPTP隧道会发起到TCP端口1723上的对等体。然后，此TCP连接用于启动和管理到同一对等体的第二个GRE隧道。

GRE隧道用于传输封装的PPP数据包，这允许在PPP内传输任何协议的隧道。 如果包含

NetBEUI和IPX。

问题：排除GRE PPTP协议的基于IOS区域的策略防火墙检查问题

确认ZBF不检查带GRE流量的PPTP，这是因为它不打开允许返回流量通过所需的引脚孔，下面是用于检查带GRE流量的PPTP协议的典型ZBF配置示例：

```
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
```

注意：请注意，在配置示例中，PPTP连接是从LAN发起到WAN区域的。

注意：即使PPTP的TCP连接在ZBF的**show policy-firewall sessions**输出中显示为已建立，PPTP连接也无法通过路由器工作。

解决方案

要允许通过ZBF与GRE的PPTP VPN连接，您需要更改ZBF规则的**inspect**操作，以便在涉及的区域对中的流量双向执行**pass** 操作，如下所示：

```
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
```

应用此ZBF配置更改后，与GRE的PPTP VPN连接将通过ZBF正常工作。

相关信息

要允许GRE和封装安全负载(ESP)协议流量通过基于区域的策略防火墙，请使用**pass 操作**。GRE和ESP协议不支持状态检测，如果您在ZBF上使用**inspect**操作，则这些协议的流量将被丢弃。

安全配置指南：基于区域的策略防火墙，Cisco IOS版本15M&T

相关Bug

CSCtn52424 ZBF增强版：利用动态GRE直通实现PPTP检测