排除具有GRE的PPTP協定的IOS基於區域的策略防火牆檢查問題

目錄

簡介

本文說明在區基防火牆(ZBF)中發現的問題，ZBF無法從此問題使用通用路由封裝(GRE)正確檢查點對點通道通訊協定(PPTP)。

必要條件

需求

Cisco建議您瞭解IOS路由器中的Cisco ZBF配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 整合式服務路由器(ISR G1)
- IOS 15M&T

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

PPTP是一種虛擬專用網路的實現方法。PPTP使用TCP上的控制通道和操作來封裝PPP資料包的GRE隧道。

將向TCP埠1723上的對等裝置啟動PPTP隧道。此TCP連線然後用於啟動和管理通向同一對等體的第二個GRE隧道。

GRE通道用於傳輸封裝的PPP封包，這允許在PPP中傳輸的任何通訊協定的通道。 如果包含

NetBEUI和IPX。

問題：排除具有GRE的PPTP協定的IOS基於區域的策略防火牆檢查問題

可以肯定，ZBF不會使用GRE流量檢查PPTP，這是因為它不會開啟允許返回流量通過的針孔。以下是用於使用GRE流量檢查PPTP協定的典型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
```

附註：考慮在配置示例中，從LAN到WAN區域啟動PPTP連線。

附註：即使PPTP的TCP連線在ZBF的**show policy-firewall sessions**輸出中顯示為已建立，PPTP連線仍無法通過路由器工作。

解決方案

為了允許通過ZBF與GRE的PPTP VPN連線，您需要更改ZBF規則的**inspect**操作，該操作用於在所涉及的區域對中資料流兩個方向的**通過**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
```

應用此ZBF配置更改後，通過ZBF與GRE的PPTP VPN連線將正常工作。

相關資訊

要允許GRE和封裝安全負載(ESP)協定流量通過基於區域的策略防火牆，請使用**pass**操作。GRE和ESP協定不支援狀態檢測，如果您在ZBF上使用**inspect**操作，則會丟棄這些協定的流量。

安全配置指南：基於區域的策略防火牆，Cisco IOS版本15M&T

相關錯誤

CSCtn52424 ZBF ENH:利用動態GRE直通實施PPTP檢測