基於區域的防火牆故障排除

目錄

簡介

本文包含基於區域的防火牆的故障排除資訊。

必要條件

需求

思科建議您瞭解以下主題：

- 將VPN與基於區域的策略防火牆配合使用
- 基於區域的策略防火牆設計和應用指南

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

無法傳遞VPN流量

問題

問題是VPN流量無法通過基於區域的防火牆。

解決方案

允許基於區域的Cisco IOS®防火牆檢查VPN客戶端流量。

例如，以下是在路由器配置中新增的線路：

```
access-list 103 permit ip 172.16.1.0 0.0.0.255 172.22.10.0 0.0.0.255

class-map type inspect match-all sdm-cls-VPNOutsideToInside-1
  match access-group 103

policy-map type inspect sdm-inspect-all
  class type inspect sdm-cls-VPNOutsideToInside-1
   inspect

zone-pair security sdm-zp-out-in source out-zone destination in-zone
  service-policy type inspect sdm-inspect-all
```

無法傳遞GRE/PPTP

問題

問題是GRE/PPTP流量無法通過基於區域的防火牆。

解決方案

允許基於區域的Cisco IOS防火牆檢查VPN客戶端流量。

例如，以下是在路由器配置中新增的線路：

```
agw-7206>enable

gw-7206#conf t
gw-7206(config)#policy-map type inspect outside-to-inside
gw-7206(config-pmap)#no class type inspect outside-to-inside
gw-7206(config-pmap)#no class class-default
gw-7206(config-pmap)#class type inspect outside-to-inside
gw-7206(config-pmap-c)#inspect
%No specific protocol configured in class outside-to-inside for inspection.
All protocols will be inspected
gw-7206(config-pmap-c)#class class-default
gw-7206(config-pmap-c)#drop
```

```
gw-7206(config-pmap-c)#exit
gw-7206(config-pmap)#exit
```

檢查設定：

```
gw-7206#show run policy-map outside-to-inside
policy-map type inspect outside-to-inside
 class type inspect PPTP-Pass-Through-Traffic
  pass
 class type inspect outside-to-inside
  inspect
 class class-default
  drop
```

網路連線能力

問題

在Cisco IOS路由器中應用基於區域的防火牆策略後，網路將無法訪問。

解決方案

此問題可能是非對稱路由。Cisco IOS防火牆在非對稱路由環境中無法工作。不能保證資料包通過同一路由器返回。

Cisco IOS防火牆跟蹤TCP/UDP會話的狀態。資料包必須離開並從同一路由器返回才能準確維護狀態資訊。

無法將DHCP流量通過基於區域的防火牆

問題

無法將DHCP流量通過基於區域的防火牆。

解決方案

禁用自區域流量檢測以解決此問題。

相關資訊

- 技術支援與文件 - Cisco Systems
- 使用區域型防火牆(ZBFW)的IOS上的AnyConnect