

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[无法通过VPN流量](#)

[问题](#)

[解决方案](#)

[无法通过GRE/PPTP](#)

[问题](#)

[解决方案](#)

[网络可达性](#)

[问题](#)

[解决方案](#)

[无法通过DHCP流量—基于区域的防火墙](#)

[问题](#)

[解决方案](#)

[相关信息](#)

简介

本文包含基于区域的防火墙的故障排除信息。

先决条件

要求

Cisco 建议您了解以下主题：

- [使用与基于区域的策略防火墙的VPN](#)
- [区域策略防火墙设计和应用指南](#)

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

无法通过VPN流量

问题

问题是VPN流量无法在基于区域的防火墙间通过。

解决方案

允许基于区域的Cisco IOS防火墙将检查的VPN客户端流量。

例如，这是在路由器配置的线路添加：

无法通过GRE/PPTP

问题

问题是GRE/PPTP流量无法穿过基于区域的防火墙。

解决方案

允许基于区域的Cisco IOS防火墙将检查的VPN客户端流量。

例如，这是在路由器配置的线路添加：

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

检查配置：

```
agw-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
```

网络可达性

问题

在基于区域的防火墙的策略在Cisco IOS路由器后应用，网络不可及的。

解决方案

此问题也许是不对称路由。Cisco IOS防火墙在与不对称路由的环境不工作。数据包没有保证通过同一路由器返回。

Cisco IOS防火墙跟踪TCP/UDP会话的状态。数据包必须从状态信息准确维护的同一路由器离去和

返回。

[无法通过DHCP流量基于区域的防火墙](#)

[问题](#)

您无法通过DHCP流量—基于区域的防火墙。

[解决方案](#)

禁用自身区域流量检查为了解决此问题。

[相关信息](#)

- [技术支持和文档 - Cisco Systems](#)
- [在IOS的AnyConnect与基于区域的防火墙\(ZBFW\)](#)