对 Cisco IOS 防火墙配置进行故障排除

目录

简介

本文提供您能使用为了排除故障Cisco IOS防火墙配置的信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

故障排除

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- 为了倒转(删除)访问列表，请放置在**access-group命令前面的**no在接口配置模式：

```
int <interface>
no ip access-group # in|out
```

- 如果许多个流量拒绝，请研究您的列表逻辑或设法定义一张另外的更加清楚的列表，然后应用它。例如：

```
access-list # permit tcp any any
```

```
access-list # permit udp any any
access-list # permit icmp any any
int <interface>
ip access-group # in|out
```

- **show ip access-lists命令**显示哪访问列表应用，并且什么流量由他们拒绝。如果查看数据包计数拒绝在与源和目的地IP地址的失败的操作前后，此编号增加，如果访问列表阻塞流量。
- 如果路由器没有大量地装载，调试可以进行在数据包级在延长或IP inspect访问列表。如果路由器大量地装载，流量通过路由器减慢。以调试命令使用谨慎。临时地请添加**no ip route-cache命令**到接口：

  ```
  int <interface>
  no ip route-cache
  ```

  然后，在不是enable (event) (但是设置)模式：

  ```
  term mon
  debug ip packet # det
  ```

  生成输出类似于此：

  ```
  term mon
  debug ip packet # det
  ```

- 扩展访问列表可能也与“日志”选项一起使用在多种语句结束时：

  ```
  access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
  access-list 101 permit ip any any
  ```

  因此您为允许看到在屏幕的消息和拒绝的数据流：

  ```
  access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
  access-list 101 permit ip any any
  ```

- 如果IP inspect列表是可疑的， **debug ip inspect <type_of_traffic>命令**生成输出例如此输出：

  ```
  access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
  access-list 101 permit ip any any
  ```

对于这些指令和其他故障排除信息，请参见排错认证代理。

相关信息

- Cisco IOS防火墙产品支持
- 技术支持和文档 - Cisco Systems