Cisco IOS防火牆配置故障排除

目錄

簡介

本文提供可用於對Cisco IOS®防火牆配置進行故障排除的資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

疑難排解

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

- 若要反向（移除）存取清單，請在介面組態模式下在**access-group**指令之前加入「no」：

```
int
```

- 如果遭到拒絕的流量過多，請研究您的清單邏輯，或嘗試定義其他更廣泛的清單，然後加以套用。例如：

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int
```

- show ip access-lists命令會顯示應用了哪些存取清單以及哪些流量被它們拒絕。如果您使用源和目標IP地址檢視失敗操作之前和之後被拒絕的資料包計數，則當訪問清單阻止流量時，此數字將增加。
- 如果路由器負載不重，可以在擴展或ip inspect訪問清單的資料包級別進行調試。如果路由器負載過重，則通過路由器的流量會減慢。請謹慎使用調試命令。將no ip route-cache命令臨時新增到介面：

```
int
```

然後，在啟用（但不配置）模式下：

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

生成類似以下的輸出：

```
*Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0),
   g=10.31.1.21, len 100, forward
*Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9,
   len 100, forward
```

- 擴展訪問清單還可以與各種語句末尾的「log」選項一起使用：

```
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，您會在螢幕上看到允許和拒絕流量的消息：

```
*Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100
   -> 10.31.1.161 (0/0), 15 packets
*Mar  1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0)
   -> 10.31.1.161(0), 1 packet
```

- 如果ip inspect list可疑，debug ip inspect <type_of_traffic>命令會產生輸出，例如以下輸出：

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 3195751223
   seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23)
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 3659219378
   seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23)
```

如需這些命令以及其他疑難排解資訊，請參閱驗證代理疑難排解。

相關資訊

- Cisco IOS防火牆產品支援
- 技術支援與文件 - Cisco Systems