ASA常见问题：当ASA建立或断开连接时，您如何解释其生成的系统日志？

目录

简介

本文档介绍在自适应安全设备(ASA)设备建立和断开连接时如何解释传输控制协议(TCP)/用户数据报协议(UDP)系统日志的生成。

当ASA建立或断开连接时，您如何解释其生成的系统日志？

本文档中讨论的所有系统日志均基于此处所示的网络拓扑。

网络拓扑

情形 1：发往ASA内部接口（身份）的管理流量源自内部主机

```
%ASA-6-302013: Built inbound TCP connection 8 for
inside:10.1.1.2/12523 (10.1.1.2/12523) to NP Identity
Ifc:10.1.1.1/22 (10.1.1.1/22)

%ASA-6-302014: Teardown TCP connection 8 for inside:
10.1.1.2/12523 to NP Identity Ifc:10.1.1.1/22 duration
0:00:53 bytes 2436 TCP FINs
```

方案 2：通过ASA的流量源自内部主机，并发往外部主机

```
%ASA-6-302013: Built outbound TCP connection 9 for outside:10.1.2.1/22 (10.1.2.1/22)
to inside:10.1.1.2/53496 (10.1.1.2/53496)

%ASA-6-302014: Teardown TCP connection 9 for outside:10.1.2.1/22 to inside:
10.1.1.2/53496 duration 0:00:30 bytes 0 SYN Timeout
```

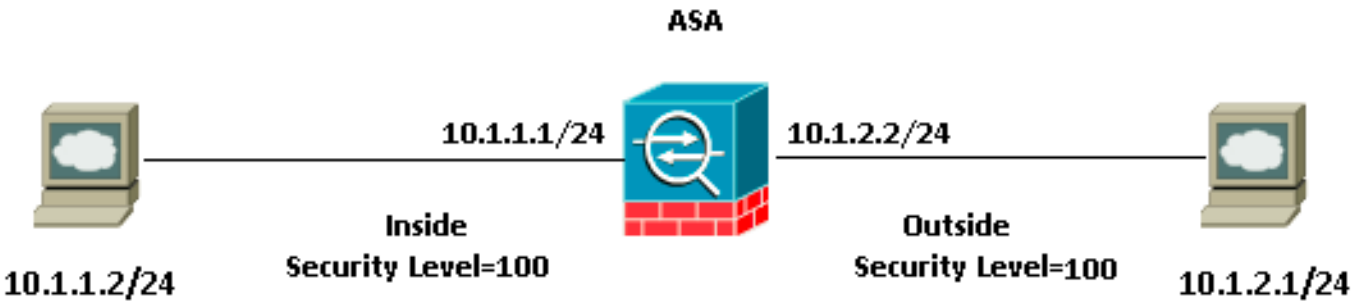
情形 3：发往ASA外部接口（身份）的管理流量来自外部主机

```
%ASA-6-302013: Built inbound TCP connection 10 for outside:10.1.2.1/28218
(10.1.2.1/28218) to NP Identity Ifc:10.1.2.2/22 (10.1.2.2/22)

%ASA-6-302014: Teardown TCP connection 10 for outside:10.1.2.1/28218 to NP
Identity Ifc:10.1.2.2/22 duration 0:00:33 bytes 968 TCP Reset-O
```

场景 4：通过ASA的流量源自外部主机，并发往内部主机

```
%ASA-6-302013: Built inbound TCP connection 11 for outside:10.1.2.1/21647
(10.1.2.1/21647) to inside:10.1.1.2/22 (10.1.1.2/22)

%ASA-6-302014: Teardown TCP connection 11 for outside:10.1.2.1/21647 to
inside:10.1.1.2/22 duration 0:00:00 bytes 0 TCP Reset
```

网络拓扑（同一安全接口）



情形 1：通过ASA的流量源自内部主机，并发往外部主机

```
%ASA-6-302013: Built inbound TCP connection 0 for inside:10.1.1.2/28075 (10.1.1.2/28075)
to outside:10.1.2.1/23 (10.1.2.1/23)

%ASA-6-302014: Teardown TCP connection 0 for inside:10.1.1.2/28075 to outside:10.1.2.1/23
duration 0:00:46 bytes 144 TCP FINs
```

方案 2：通过ASA的流量从外部主机发往内部主机

```
%ASA-6-302013: Built inbound TCP connection 1 for outside:10.1.2.1/17891 (10.1.2.1/17891)
to inside:10.1.1.2/23 (10.1.2.5/23)

%ASA-6-302014: Teardown TCP connection 1 for outside:10.1.2.1/17891 to inside:10.1.1.2/23
duration 0:00:08 bytes 165 TCP FIN
```

*其中10.1.2.5是10.1.1.2的静态NAT IP

相关信息

- Cisco ASA 5500系列下一代防火墙参考指南
- Cisco ASA 5500系列下一代防火墙配置指南
- 技术支持和文档 - Cisco Systems