ASA FAQ: How do you interpret the syslogs generated by the ASA when it builds or tears down connections?

Contents

Introduction

This document describes how to interpret the generation for the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) syslog on the Adaptive Security Appliance (ASA) device when it builds and tears down connections.

How do you interpret the syslogs generated by the ASA when it builds or tears down connections?

All the syslogs discussed in this document are based on the network topologies shown here.

Network Topology
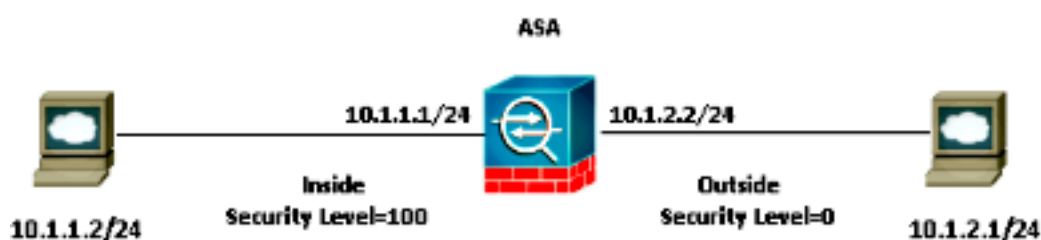
Scenario 1: Management traffic to the ASA inside interface (identity) is sourced from the inside host

```
%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
```
Scenario 2: Traffic through the ASA is sourced from the inside host and is destined to the

outside host

```
%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
```

Scenario 3: Management traffic to the ASA outside interface (identity) is sourced from the outside host

```
%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
```

Scenario 4: Traffic through the ASA is sourced from the outside host and is destined to the inside host

```
%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
```

Network Topology (Same-Security Interfaces)
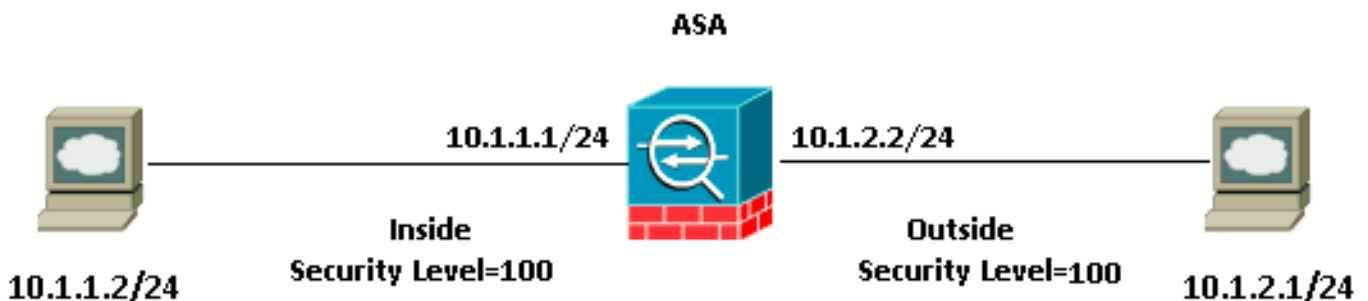
Scenario 1: Traffic through the ASA is sourced from the inside host and is destined to the outside host

```
%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
```

Scenario 2: Traffic through the ASA is sourced from the outside host to the inside host

```
%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
```

*Where 10.1.2.5 is the Static Nat IP for 10.1.1.2

Related Information

- **Cisco ASA 5500 Series Next Generation Firewalls Reference Guides**
- **Cisco ASA 5500 Series Next Generation Firewalls Configuration Guides**
- **Technical Support & Documentation - Cisco Systems**