ASA FAQ：接続の構築時または切断時に ASA によって生成された syslog を解釈する方法

内容

概要

このドキュメントでは、接続の構築時または切断時に、適応型セキュリティ アプライアンス（ASA）デバイスで Transmission Control Protocol（TCP）/User Datagram Protocol（UDP）に対して生成される syslog を理解する方法について説明します。

接続の構築時または切断時に ASA によって生成された syslog を解釈する方法

このドキュメントに記載されているすべての syslog は、次に示すネットワーク トポロジに基づいています。

Network Topology

シナリオ 1：ASA 内部インターフェイス（識別）への管理トラフィックの送信元が内部ホスト

```
%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
```

シナリオ 2：ASA を通過するトラフィックの送信元が内部ホストで、宛先が外部ホスト

```
%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
```

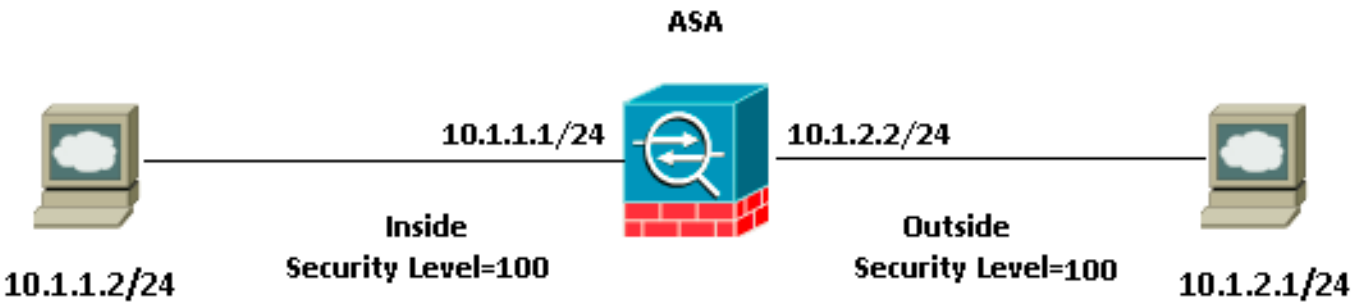
シナリオ 3：ASA 外部インターフェイス（識別）への管理トラフィックの送信元が外部ホスト

```
%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
```

シナリオ 4：ASA を通過するトラフィックの送信元が外部ホストで、宛先が内部ホスト

```
%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
```

ネットワーク トポロジ（同じセキュリティのインターフェイス）



シナリオ 1：ASA を通過するトラフィックの送信元が内部ホストで、宛先が外部ホスト

```
%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
```

シナリオ 2：ASA を通過するトラフィックの送信元が外部ホストで、宛先が内部ホスト

```
%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
```

* ここで、10.1.2.5 は 10.1.1.2 の静的 NAT IP です。

関連情報

- Cisco ASA 5500 シリーズ次世代ファイアウォール レファレンスガイド
- Cisco ASA 5500 シリーズ次世代ファイアウォール設定ガイド
- テクニカル サポートとドキュメント – Cisco Systems