ASA Häufig gestellte Fragen: Wie interpretieren Sie die von der ASA generierten Syslogs, wenn sie Verbindungen aufbaut oder löscht?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Generierung des Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)-Syslog auf dem ASA-Gerät beim Erstellen und Beenden von Verbindungen interpretiert wird.

Wie interpretieren Sie die von der ASA generierten Syslogs, wenn sie Verbindungen aufbaut oder löscht?

Alle in diesem Dokument vorgestellten Syslogs basieren auf den hier gezeigten Netzwerktopologien.

Netzwerktopologie

Szenario 1: Der Management-Datenverkehr zur ASA-Inside-Schnittstelle (Identität) wird vom internen Host übernommen.

```
%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
```

Szenario 2: Datenverkehr über die ASA wird vom internen Host bezogen und ist für den externen Host bestimmt

```
%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
```

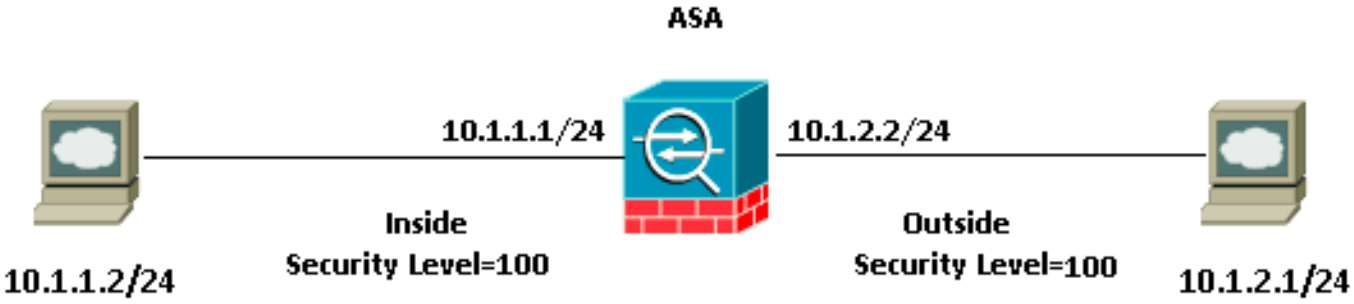
Szenario 3: Der Management-Datenverkehr zur ASA-externen Schnittstelle (Identität) wird vom externen Host übernommen.

```
%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
```

Szenario 4: Datenverkehr über die ASA wird vom externen Host bezogen und ist für den internen Host bestimmt

```
%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
```

Netzwerktopologie (gleiche Sicherheitsschnittstellen)



Szenario 1: Datenverkehr über die ASA wird vom internen Host bezogen und ist für den externen Host bestimmt

```
%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
```

Szenario 2: Der Datenverkehr über die ASA wird vom externen Host zum internen Host geleitet.

```
%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
```

*wobei 10.1.2.5 die statische NAT-IP für 10.1.1.2 ist.

Zugehörige Informationen

- Cisco Firewalls der nächsten Generation der Serie ASA 5500 - Referenzhandbücher
- Konfigurationsanleitungen für die Firewalls der nächsten Generation der Cisco Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems