FAQ ASA : Comment interprétez-vous les syslogs générés par l'ASA lorsqu'il crée ou détruit des connexions ?

Contenu

[Introduction](#)
[Comment interprétez-vous les syslogs générés par l'ASA lorsqu'il crée ou détruit des connexions ?](#)
[Topologie du réseau](#)
[Topologie du réseau (interfaces de même sécurité)](#)
[Informations connexes](#)

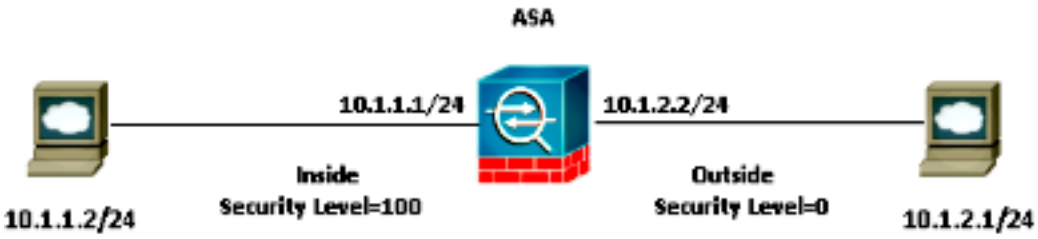
Introduction

Ce document décrit comment interpréter la génération du syslog TCP/UDP sur le périphérique ASA (Adaptive Security Appliance) lorsqu'il crée et déconnecte des connexions.

Comment interprétez-vous les syslogs générés par l'ASA lorsqu'il crée ou détruit des connexions ?

Tous les Syslogs présentés dans ce document sont basés sur les topologies de réseau présentées ici.

Topologie du réseau



Scénario 1 : Le trafic de gestion vers l'interface interne ASA (identité) provient de l'hôte interne

```
%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
```

Scénario 2 : Le trafic via l'ASA provient de l'hôte interne et est destiné à l'hôte externe

```
%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
```

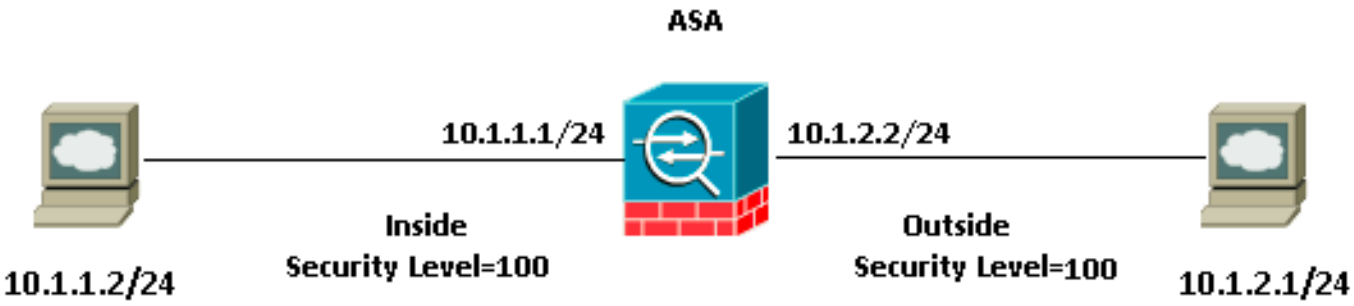
Scénario 3 : Le trafic de gestion vers l'interface externe ASA (identité) provient de l'hôte externe

```
%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
```

Scénario 4 : Le trafic via l'ASA provient de l'hôte externe et est destiné à l'hôte interne

```
%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
```

Topologie du réseau (interfaces de même sécurité)



Scénario 1 : Le trafic via l'ASA provient de l'hôte interne et est destiné à l'hôte externe

```
%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
```

Scénario 2 : Le trafic via l'ASA provient de l'hôte externe vers l'hôte interne

```
%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
```

*Où 10.1.2.5 est l'IP Nat statique pour 10.1.1.2

Informations connexes

- Guides de référence des pare-feu de nouvelle génération Cisco ASA 5500
- Guides de configuration des pare-feu de nouvelle génération de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems