

ASA FAQ: Como você interpreta os Syslog gerados pelo ASA quando constrói ou rasga para baixo conexões?

Índice

[Introdução](#)

[Como você interpreta os Syslog gerados pelo ASA quando constrói ou rasga para baixo conexões?](#)

[Topologia de rede](#)

[Topologia de rede \(relações da Mesmo-Segurança\)](#)

[Informações Relacionadas](#)

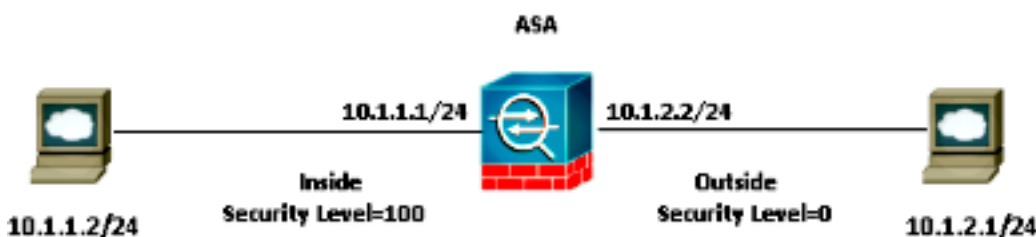
Introdução

Este documento descreve como interpretar a geração para o Syslog do Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) no dispositivo adaptável da ferramenta de segurança (ASA) quando constrói e rasga para baixo conexões.

Como você interpreta os Syslog gerados pelo ASA quando constrói ou rasga para baixo conexões?

Todos os Syslog discutidos neste documento são baseados nas topologias de rede mostradas aqui.

Topologia de rede



Cenário 1: O tráfego de gerenciamento à interface interna ASA (identidade) é originado do host interno

```
%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

Cenário 2: O tráfego com o ASA é originado do host interno e é destinado ao host exterior

```
%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
```

Cenário 3: O tráfego de gerenciamento à interface externa ASA (identidade) é originado do host exterior

```
%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)
```

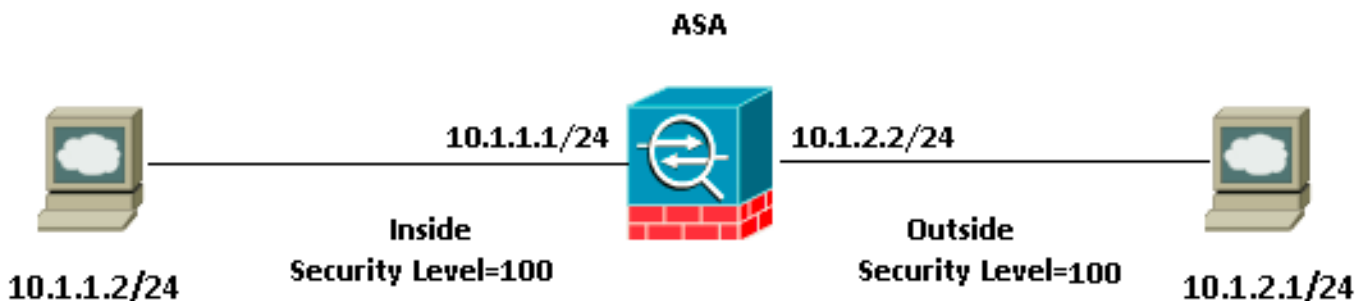
```
%ASA-6-302014: Teardown TCP connection 10 for outside:10.1.2.1/28218 to NP
Identity Ifc:10.1.2.2/22 duration 0:00:33 bytes 968 TCP Reset-O
```

Cenário 4 : O tráfego com o ASA é originado do host exterior e é destinado ao host interno

```
%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
```

Topologia de rede (relações da Mesmo-Segurança)



Cenário 1: O tráfego com o ASA é originado do host interno e é destinado ao host exterior

```
%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
```

Cenário 2: O tráfego com o ASA é originado do host exterior ao host interno

```
%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
```

o *Where 10.1.2.5 é o IP do NAT estático para 10.1.1.2

Informações Relacionadas

- [Guias de referência dos Firewall da próxima geração do 5500 Series de Cisco ASA](#)
- [Manuais de configuração dos Firewall da próxima geração do 5500 Series de Cisco ASA](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)