

Preguntas frecuentes sobre ASA: ¿Cómo interpreta los syslogs generados por el ASA cuando construye o destruye las conexiones?

Contenido

[Introducción](#)

[¿Cómo interpreta los syslogs generados por el ASA cuando construye o destruye las conexiones?](#)

[Topología de red](#)

[Topología de red \(Interfaces de la misma seguridad\)](#)

[Información Relacionada](#)

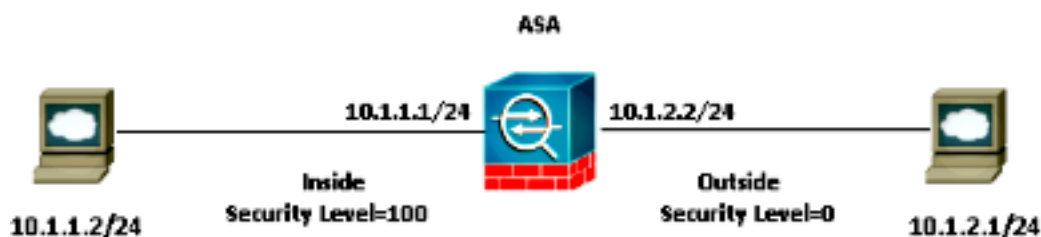
Introducción

Este documento describe cómo interpretar la generación para el syslog del protocolo de control de transmisión (TCP)/protocolo de datagramas de usuario (UDP) en el dispositivo Adaptive Security Appliance (ASA) cuando se construyen y destruyen conexiones.

¿Cómo interpreta los syslogs generados por el ASA cuando construye o destruye las conexiones?

Todos los registros del sistema que se describen en este documento se basan en las topologías de red que se muestran aquí.

Topología de red



Escenario 1: El tráfico de administración a la interfaz interna (identidad) de ASA se origina desde el 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
```

Escenario 2: El tráfico a través del ASA se origina desde el host interno y se dirige al host externo

```
%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
```

Escenario 3: El tráfico de administración a la interfaz externa de ASA (identidad) se origina desde el host externo

```
%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)
```

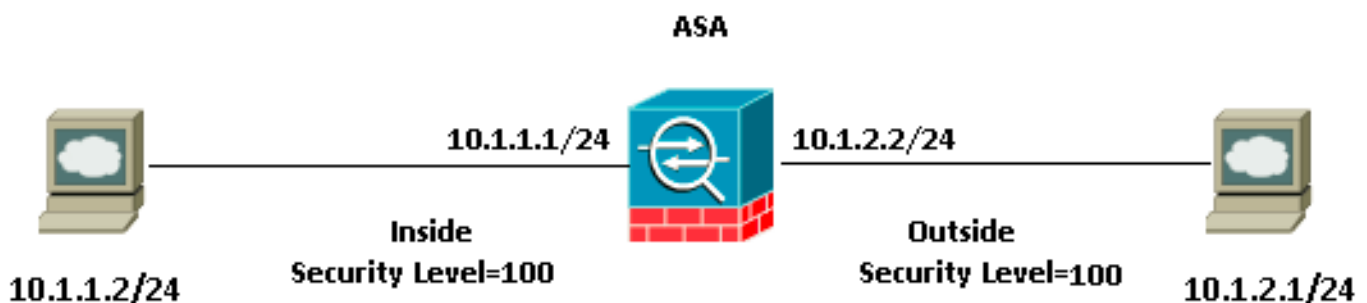
```
%ASA-6-302014: Teardown TCP connection 10 for outside:10.1.2.1/28218 to NP
Identity Ifc:10.1.2.2/22 duration 0:00:33 bytes 968 TCP Reset=0
```

Escenario 4: El tráfico a través del ASA se origina en el host exterior y está destinado al 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
```

Topología de red (Interfaces de la misma seguridad)



Escenario 1: El tráfico a través del ASA se origina desde el host interno y se dirige al host externo

```
%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
```

Escenario 2: El tráfico a través del ASA se origina desde el host exterior al 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
```

*Donde 10.1.2.5 es la IP estática de NAT para 10.1.1.2

Información Relacionada

- [Guías de referencia de los firewalls de última generación Cisco ASA serie 5500](#)
- [Guías de configuración de firewalls de última generación Cisco ASA serie 5500](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)