

# DOMANDE FREQUENTI SULL'APPLIANCE ASA: Come interpretare i syslog generati dall'appliance ASA quando vengono create o interrotte le connessioni?

## Sommario

[Introduzione](#)

[Come interpretare i syslog generati dall'appliance ASA quando vengono create o interrotte le connessioni?](#)

[Topologia della rete](#)

[Topologia di rete \(interfacce con stessa sicurezza\)](#)

[Informazioni correlate](#)

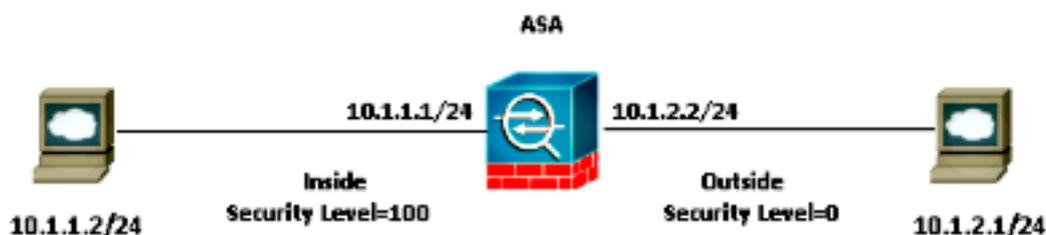
## Introduzione

In questo documento viene descritto come interpretare la generazione del syslog TCP (Transmission Control Protocol)/UDP (User Datagram Protocol) sul dispositivo ASA (Adaptive Security Appliance) quando vengono create e interrotte le connessioni.

## Come interpretare i syslog generati dall'appliance ASA quando vengono create o interrotte le connessioni?

Tutti i syslog discussi in questo documento si basano sulle topologie di rete mostrate di seguito.

### Topologia della rete



**Scenario 1: Il traffico di gestione all'interfaccia interna ASA (identità) ha origine dall'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

## Scenario 2: Il traffico attraverso l'ASA ha origine dall'host interno e è destinato all'host esterno

```
%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
```

## Scenario 3: Il traffico di gestione verso l'interfaccia esterna ASA (identità) ha origine dall'host esterno

```
%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)
```

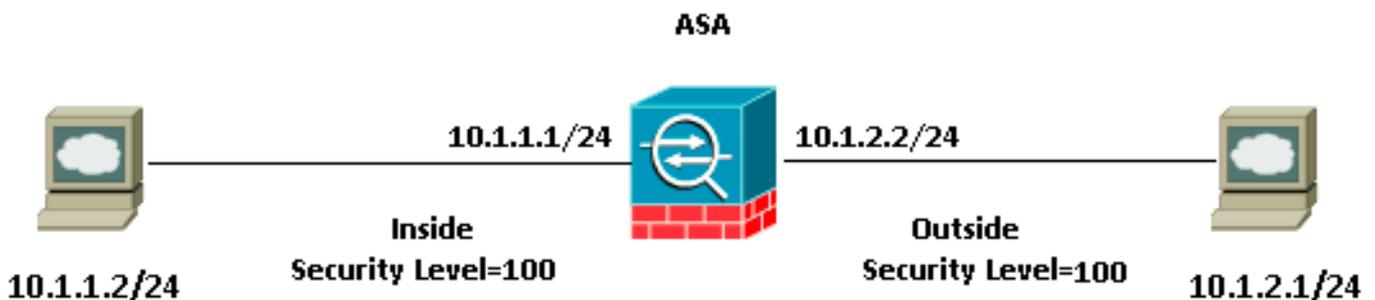
```
%ASA-6-302014: Teardown TCP connection 10 for outside:10.1.2.1/28218 to NP
Identity Ifc:10.1.2.2/22 duration 0:00:33 bytes 968 TCP Reset=0
```

## Scenario 4: Il traffico che attraversa l'ASA proviene dall'host esterno ed è destinato all'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 di rete (interfacce con stessa sicurezza)



## Scenario 1: Il traffico attraverso l'ASA ha origine dall'host interno e è destinato all'host esterno

```
%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
```

## Scenario 2: Il traffico attraverso l'ASA viene indirizzato dall'host esterno all'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
```

\*Dove 10.1.2.5 è il Nat IP statico per 10.1.1.2

## Informazioni correlate

- [Guide di riferimento per i firewall Cisco ASA serie 5500 di nuova generazione](#)
- [Guide alla configurazione dei firewall di nuova generazione Cisco ASA serie 5500](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)