

# ESA가 syslog 서버와 통신할 때 네트워크 오류가 발생하는 이유는 무엇입니까?

## 목차

### [소개](#)

[ESA가 syslog 서버와 통신할 때 네트워크 오류가 발생하는 이유는 무엇입니까?](#)

## 소개

이 문서에서는 ESA(Email Security Appliance)가 syslog 서버로 데이터를 전송할 수 없는 이유를 설명합니다.

## ESA가 syslog 서버와 통신할 때 네트워크 오류가 발생하는 이유는 무엇입니까?

ESA는 syslog 서버에 로그 서브스크립션을 푸시하도록 구성되었습니다. **파일이 syslog 서버에 성공적으로 푸시될 수도 있고 그렇지 않을 수도 있습니다.** 어떤 경우든 메일 로그 파일에 다음과 유사한 네트워크 오류가 있을 수 있습니다.

```
Log Error: Subscription Mail_Log: Network error while sending log data to syslog server
```

ESA와 syslog 서버 간의 패킷 캡처는 syslog 서버에서 시작된 연결 삭제를 보여줍니다. 이 예에서는 10.44.167.30입니다.

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111889	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=0 SACK_F
279	2015-06-25 08:50:04.114360	10.44.167.30	10.229.24.230	TCP	shell > 26040 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1350
280	2015-06-25 08:50:04.114375	10.229.24.230	10.44.167.30	TCP	26040 > shell [ACK] Seq=1 Ack=1 Win=17550 Len=0
281	2015-06-25 08:50:04.114518	10.229.24.230	10.44.167.30	RSH	Client -> Server data
282	2015-06-25 08:50:04.114877	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=48 Win=32073 Len=0
283	2015-06-25 08:50:04.114883	10.229.24.230	10.44.167.30	RSH	Client -> Server data
284	2015-06-25 08:50:04.115362	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=413 Win=31755 Len=0
285	2015-06-25 08:50:04.116192	10.44.167.30	10.229.24.230	TCP	shell > 26040 [RST, ACK] Seq=1 Ack=413 Win=32120 Len=0

패킷 캡처에서 TCP 스트림을 따라가면 다음과 같은 내용이 표시됩니다.

```
<22>Jun 25 08:50:03 example.com: Info: Begin Logfile
<22>Jun 25 08:50:03 example.com: Info: Version: 8.0.1-023 SN: A4BADB4712A9-511AA1E
<22>Jun 25 08:50:03 example.com: Info: Time offset from UTC: 7200 seconds
<22>Jun 25 08:50:03 example.com: Info: A System/Critical alert was sent to
alerts@ironport.com with subject "Critical <System> mail.example.com: Log Error:
Subscription Mail_Log: Network error while sending l..."
```

**이 오류는 IP 주소에서 syslog 서버에 대한 액세스를 차단하는 방화벽 또는 IPS(Intrusion Prevention System)가 있음을 나타냅니다.** 트래픽을 허용하기 위해 사이에 있는 모든 디바이스를 검

사하고 확인한 경우, 이는 syslog 서버가 너무 사용 중이고 연결을 거부했음을 의미할 수도 있습니다. ESA가 로그 파일을 syslog 서버로 전송하도록 구성된 경우, TCP를 사용하도록 구성되지 않은 기본적으로 UDP syslog 포트 514를 사용합니다. 어플라이언스가 구성되면 연결이 거부됨으로 나열되는 유일한 것은 연결이 열릴 때 연결을 닫는 패킷을 수신한 경우입니다.