Warum treten Netzwerkfehler auf, wenn die ESA mit dem Syslog-Server kommuniziert?

Inhalt

Einführung

In diesem Dokument wird erläutert, warum die E-Mail Security Appliance (ESA) keine Daten an einen Syslog-Server senden kann.

Warum treten Netzwerkfehler auf, wenn die ESA mit dem Syslog-Server kommuniziert?

Die ESA wurde so konfiguriert, dass Protokoll-Subscriptions an einen Syslog-Server übertragen werden. **Die Dateien werden möglicherweise erfolgreich an den Syslog-Server weitergeleitet.** In jedem Fall können in der E-Mail-Protokolldatei ähnliche Netzwerkfehler auftreten:

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

Eine Paketerfassung zwischen der ESA und dem Syslog-Server zeigt Verbindungsausfälle, die vom Syslog-Server initiiert wurden. In diesem Beispiel ist dies 10.44.167.30.

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111689	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=8 SACK_P
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

Wenn Sie dem TCP-Stream bei der Paketerfassung folgen, wird Folgendes angezeigt:

```
<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...".
```

Die Fehler weisen darauf hin, dass entweder eine Firewall oder ein Intrusion Prevention System (IPS) vorhanden sind, das den Zugriff auf den Syslog-Server an der IP-Adresse blockiert. Wenn

alle Geräte dazwischen überprüft und bestätigt wurden, um den Datenverkehr zuzulassen, kann dies auch bedeuten, dass der Syslog-Server zu beschäftigt ist und die Verbindungen verweigert wurden. Wenn die ESA so konfiguriert ist, dass sie eine Protokolldatei an einen Syslog-Server sendet, verwendet sie standardmäßig den UDP-Syslog-Port 514, es sei denn, sie ist für die Verwendung von TCP konfiguriert. Nach der Konfiguration der Appliance wird die Verbindung nur dann als verweigert aufgelistet, wenn sie Pakete empfängt, die die Verbindung schließen, wenn sie geöffnet wird.