Waarom zijn er netwerkfouten wanneer de ESA communiceert met de syslogserver?

Inhoud

Inleiding

Dit document beschrijft waarom de E-mail security applicatie (ESA) niet in staat is om gegevens naar een syslig server te sturen.

Waarom zijn er netwerkfouten wanneer de ESA communiceert met de syslogserver?

Het ESA is ingesteld om log abonnementen op een syslogserver te drukken. **De bestanden kunnen of kunnen niet met succes naar de syslog server worden geduwd.** In elk geval kunnen er netwerkfouten voorkomen in het postlogbestand die hierop lijken:

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

Een pakketvastlegging tussen het ESA en de syslog server toont verbindingsdruppels geïnitieerd door de syslog server, die in dit voorbeeld 10.44.167.30 is.

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

Als u de TCP-stream in de pakketvastlegging volgt, ziet u dit:

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

De fouten wijzen erop dat er een firewall of een IPS (Inbraakpreventiesysteem) is die de toegang tot de syslogserver op het IP-adres blokkeert. Als alle apparaten die ertussen zitten onderzocht en

bevestigd zijn om het verkeer mogelijk te maken, dan kan dit ook betekenen dat de syslogserver te druk is en de verbindingen weigert. Wanneer het ESA is ingesteld om een logbestand naar een syslogserver te verzenden, dan zal het standaard de UDP syslog poort 514 gebruiken, tenzij geconfigureerd om TCP te gebruiken. Als het apparaat eenmaal is geconfigureerd is het enige waardoor de verbinding wordt vermeld als geweigerd, indien deze wordt ontvangen van pakketten die de aansluiting sluiten wanneer deze wordt geopend.