¿Por qué hay Errores de red cuando el ESA comunica con el servidor de Syslog?

Contenido

Introducción

Este documento describe porqué el dispositivo de seguridad del correo electrónico (ESA) no puede enviar los datos a un servidor de Syslog.

¿Por qué hay Errores de red cuando el ESA comunica con el servidor de Syslog?

El ESA se ha configurado para avanzar las suscripciones del registro a un servidor de Syslog. **Los archivos pudieron o no se pudieron avanzar con éxito al servidor de Syslog.** En todo caso, puede haber Errores de red en el archivo del registro del correo similar a esto:

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

Una captura de paquetes entre el ESA y el servidor de Syslog muestra los descensos de la conexión iniciados por el servidor de Syslog, que en este ejemplo es 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=0 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

Si usted sigue la secuencia TCP en la captura de paquetes usted verá esto:

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

Los errores indican que hay un Firewall o Sistema de prevención de intrusiones (IPS) que bloquea el acceso al servidor de Syslog en la dirección IP. Si todos los dispositivos se han examinado y se

han confirmado mientras tanto para permitir el tráfico, después éste podría también significar que el servidor de Syslog está demasiado ocupado y rechazó las conexiones. Cuando el ESA se configura para enviar un archivo del registro a un servidor de Syslog, después por abandono utilizará el puerto de Syslog 514 UDP a menos que esté configurado para utilizar el TCP. Una vez que se configura el dispositivo, la única cosa que hace la conexión ser enumerada como rechazado es si recibe los paquetes que cierran la conexión cuando se abren.