Pourquoi y a-t-il des erreurs réseau quand l'ESA communique avec le serveur de Syslog ?

Contenu

Introduction

Ce document décrit pourquoi l'appliance de sécurité du courrier électronique (ESA) ne peut pas envoyer des données à un serveur de Syslog.

Pourquoi y a-t-il des erreurs réseau quand l'ESA communique avec le serveur de Syslog ?

L'ESA a été configuré pour pousser des abonnements de log à un serveur de Syslog. **Les fichiers pourraient ou ne pourraient pas être avec succès poussés au serveur de Syslog.** En tous cas, il peut y avoir des erreurs réseau dans le fichier journal de messagerie semblable à ceci :

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

Une capture de paquet entre l'ESA et le serveur de Syslog affiche des baisses de connexion initiées par le serveur de Syslog, qui dans cet exemple est 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

Si vous suivez le flot de TCP dans la capture de paquet vous verrez ceci :

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

Les erreurs indiquent qu'il y a un Pare-feu ou de Système de prévention d'intrusion (IPS) qui bloque l'accès au serveur de Syslog à l'adresse IP. Si tous les périphériques ont été examinés et

dans l'intervalle confirmés afin de permettre le trafic, alors ceci pourrait également signifier que le serveur de Syslog est trop occupé et a refusé les connexions. Quand l'ESA est configuré pour envoyer un fichier journal à un serveur de Syslog, alors par défaut il utilisera le port 514 de Syslog d'UDP à moins que configuré pour utiliser le TCP. Une fois que l'appliance est configurée, la seule chose qui cause la connexion d'être répertoriée en tant que refusé est si elle reçoit les paquets qui ferment la connexion quand ils sont ouverts.