Когда ESA связывается с сервером системного журнала, почему там ошибки сети?

Содержание

Введение

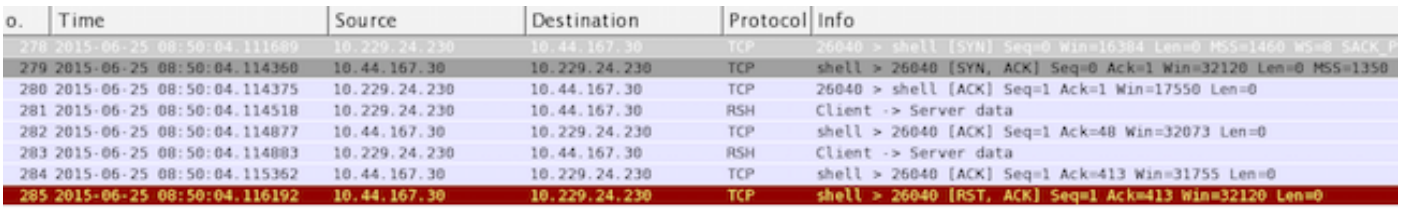
Этот документ описывает, почему Email Security Appliance (ESA) неспособен передать данные к серверу системного журнала.

Когда ESA связывается с сервером системного журнала, почему там ошибки сети?

ESA был настроен для продвижения регистрационных подписок к серверу системного журнала. **Файлы могли бы или не могли бы быть успешно выдвинуты к серверу системного журнала.** В любом случае могут быть ошибки сети в почтовом файле журнала, подобном этому:

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

Захват пакета между ESA и сервером системного журнала показывает отбрасывания соединения, инициируемые сервером системного журнала, который в данном примере является 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

Если вы будете придерживаться потока TCP в захвате пакета, то вы будете видеть это:

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

Ошибки указывают, что существует или межсетевой экран или Система предотвращения вторжений (IPS), которая блокирует доступ к серверу системного журнала в IP-адресе. Если весь промежуток устройств был исследован и подтвержден для разрешения трафика, то это могло также означать, что сервер системного журнала слишком занят и отказался от соединений. Когда ESA будет настроен для передачи файла журнала к серверу системного журнала, тогда по умолчанию он будет использовать порт системного журнала UDP 514, пока не настроено для использования TCP. Как только устройство настроено, единственная вещь, которая заставляет соединение быть перечисленным, как отказано, состоит в том, если это получает пакеты, которые закрывают соединение, когда это открыто.