ESA が syslog サーバと通信するときに、ネットワーク エラーが発生するのはなぜですか。

目次

概要

このドキュメントでは、E メール セキュリティ アプライアンス (ESA) が syslog サーバにデータを送信できない理由について説明しています。

ESA が syslog サーバと通信するときに、ネットワーク エラーが発生するのはなぜですか。

ESA は、syslog サーバにログ サブスクリプションをプッシュするように設定されています。 **ファイルが正常に syslog サーバにプッシュされる、またはされない場合があります。** いずれの場合も、電子メール ログ ファイルに次のようなネットワーク エラーが含まれることがあります。

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

ESA と syslog サーバ間のパケット キャプチャは、syslog サーバ (この例では 10.44.167.30) によって開始された接続のドロップを表しています。

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

パケット キャプチャ内の TCP ストリームを確認すると、次のように表示されます。

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

このエラーからは、前述の IP アドレスで syslog サーバにアクセスするのをブロックする、ファイアウォールまたは侵入防御システム (IPS) のいずれかが存在するがわかります。 トラフィッ

クを許可するために、間にあるすべてのデバイスを調べ、確認したのであれば、syslog サーバがあまりにもビジー状態で、接続を拒否している可能性があることも考えられます。 ESA が syslog サーバにログ ファイルを送信するように設定されている場合、TCP を使用するように設定しない限り、ESA はデフォルトで UDP の syslog ポート 514 を使用します。 アプライアンスを設定すると、接続が拒否されたとしてリストされる唯一の原因は、接続が開かれている際にその接続を閉じるパケットを受信した場合です。