Perché si verificano errori di rete quando l'ESA comunica con il server syslog?

Sommario

Introduzione

In questo documento viene descritto il motivo per cui Email Security Appliance (ESA) non è in grado di inviare dati a un server syslog.

Perché si verificano errori di rete quando l'ESA comunica con il server syslog?

ESA è stato configurato per eseguire il push delle sottoscrizioni dei log in un server syslog. È possibile che il push dei file nel server syslog non sia riuscito. In ogni caso, possono esserci errori di rete nel file di log di posta simili a quanto riportato di seguito:

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

L'acquisizione di un pacchetto tra l'ESA e il server syslog mostra le interruzioni di connessione inizializzate dal server syslog, che nell'esempio riportato è 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

Se si segue il flusso TCP nell'acquisizione dei pacchetti, viene visualizzato quanto segue:

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

Gli errori indicano la presenza di un firewall o di un sistema di prevenzione delle intrusioni (IPS) che blocca l'accesso al server syslog all'indirizzo IP. Se tutti i dispositivi intermedi sono stati esaminati e confermati per autorizzare il traffico, il server syslog potrebbe essere troppo occupato e le connessioni potrebbero essere rifiutate. Quando l'ESA è configurata per inviare un file di log a un server syslog, per impostazione predefinita utilizzerà la porta syslog UDP 514 a meno che non sia configurata per utilizzare il protocollo TCP. Dopo aver configurato l'accessorio, l'unico motivo per cui la connessione viene indicata come rifiutata è la ricezione di pacchetti che chiudono la connessione quando questa viene aperta.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).