Configurazione di TLS per la crittografia delle connessioni in entrata su un listener ESA

Sommario

Introduzione

In questo documento viene descritto come abilitare Transport Layer Security (TLS) su un listener su Email Security Appliance (ESA).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sull'ESA con qualsiasi versione AsyncOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Ènecessario abilitare TLS per tutti i listener in cui è richiesta la crittografia per le connessioni in entrata. È possibile abilitare TLS sui listener che si trovano su Internet (listener pubblici), ma non sui listener per sistemi interni (listener privati). In alternativa, è possibile abilitare la crittografia per tutti i listener. Per impostazione predefinita, i listener privati o pubblici non consentono le connessioni TLS. È necessario abilitare TLS nella tabella HAT (Host Access Table) di un listener per abilitare TLS per la posta in entrata (ricezione) o in uscita (invio). Inoltre, per impostazione predefinita, TLS è disattivato per i listener privati e pubblici.

Configurazione

Èpossibile specificare tre diverse impostazioni per TLS su un listener:

Impostazione	Significato
No	TLS non consentito per le connessioni in ingresso. Le connessioni al listener non richiedono conversazioni SMTP (Simple Mail Transfer Protocol) crittografate. Si tratta dell'impostazione predefinita per tutti i listener configurati sull'accessorio.
Preferred (Preferito)	TLS è consentito per le connessioni in ingresso al listener dagli agenti di trasferimento messaggi (MTA).
Obbligatorio	Il protocollo TLS è consentito per le connessioni in ingresso al listener dagli MTA e, finché n viene ricevuto un comando STARTTLS, l'ESA risponde con un messaggio di errore a tutti i comandi diversi da No Option (NOOP), EHLO o QUIT. Se TLS è 'Obbligatorio' significa che l'ESA rifiuterà i messaggi e-mail che il mittente non desidera siano crittografati con TLS prim dell'invio, impedendo in tal modo che vengano trasmessi in chiaro.

Abilitare TLS su un criterio del flusso di posta HAT per un listener tramite GUI

Attenersi alla seguente procedura:

1. Nella pagina Criteri di flusso della posta, scegliere un listener di cui si desidera modificare i criteri, quindi fare clic sul collegamento del nome del criterio da modificare. È inoltre possibile modificare i parametri dei criteri predefiniti. Viene visualizzata la pagina Modifica criteri flusso di posta.
2. Nella sezione "Crittografia e autenticazione", per il campo "Usa TLS:", scegliere il livello di TLS desiderato per il listener.
3. Fare clic su **Invia**.
4. Per salvare le modifiche, fare clic su **Commit modifiche**, aggiungere un commento facoltativo se necessario e quindi fare clic su **Commit modifiche**.

Nota: Quando si crea un listener, è possibile assegnare un certificato specifico per le connessioni TLS a singoli listener pubblici.

Abilitare TLS su una policy di flusso di posta HAT per un listener tramite CLI

1. Per scegliere un listener da configurare, usare il comando **listener config > edit**.

2. Usare il comando **hostaccess > default** per modificare le impostazioni HAT predefinite del listener.
3. Immettere una di queste scelte per modificare l'impostazione TLS quando richiesto:

```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
 [1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```

   In questo esempio viene richiesto di utilizzare il comando **certconfig** per verificare che sia disponibile un certificato valido utilizzabile con il listener. Se non sono stati creati certificati, il listener utilizza il certificato dimostrativo preinstallato sull'accessorio. È possibile attivare TLS con il certificato dimostrativo a scopo di test, ma non è sicuro e non è consigliato per un uso generico. Per assegnare un certificato al listener, usare il comando **listener config > edit > certificate**.Dopo aver configurato TLS, l'impostazione viene riflessa nel riepilogo del listener nella CLI:

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```

4. Immettere il comando **commit** per abilitare la modifica.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- Utilizzare il file di log di posta di testo e vedere questo documento: Determine if ESA is Using TLS for Delivery or Receive
- Usa verifica messaggi: GUI: Monitor > Verifica messaggi
- Usa report: GUI: Monitor > Connessioni TLS
- Utilizzare un sito Web di terze parti come checktls.com

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Èpossibile specificare se l'ESA invia un avviso se la negoziazione TLS non riesce quando i messaggi vengono recapitati a un dominio che richiede una connessione TLS. Il messaggio di avviso contiene il nome del dominio di destinazione per la negoziazione TLS non riuscita. L'ESA invia il messaggio di avviso a tutti i destinatari impostati per ricevere gli avvisi relativi al livello di gravità dell'avviso per i tipi di avviso di sistema. È possibile gestire i destinatari degli alert nella pagina Amministrazione del sistema > Alert della GUI (o tramite il comando **alertconfig** della CLI).

Informazioni correlate

- Guide per l'utente finale AsyncOS per la posta elettronica
- Documentazione e supporto tecnico – Cisco Systems