TLS configureren voor versleuteling van inkomende verbinding op een ESA-server

Inhoud

Inleiding

In dit document wordt beschreven hoe u Transport Layer Security (TLS) via een luisteraar kunt inschakelen voor de e-mail security applicatie (ESA).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op het ESA met elke AsyncOS-versie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

U moet TLS voor om het even welke luisteraars inschakelen waar u encryptie voor inkomende verbindingen vereist. Mogelijk wilt u TLS op luisteraars inschakelen die op het internet staan (openbare luisteraars), maar niet voor luisteraars voor interne systemen (privé-luisteraars). Of, u zou encryptie voor alle luisteraars kunnen willen toelaten. Standaard staan noch particuliere noch publieke luisteraars TLS-verbindingen toe. U moet TLS in de Host Access Table (HAT) van een luisteraar inschakelen om TLS in te schakelen voor inkomende of uitgaande (verzendende) e-mail. Bovendien zijn de beleidsinstellingen voor de poststroom van particuliere en publieke luisteraars voor TLS standaard 'uit' gezet.

Configureren

U kunt drie verschillende instellingen voor TLS op een luisteraar instellen:

Instelling	Betekenis
Nee	TLS is niet toegestaan voor inkomende verbindingen. Voor verbindingen met de luisteraar z geen versleutelde Simple Mail Transfer Protocol (MSTP)-gesprekken nodig. Dit is de standaardinstelling voor alle luisteraars die u op het apparaat configureren.
voorbestemd	TLS is toegestaan voor inkomende verbindingen naar de luisteraar van Message Transfer Agents (MTA's).
Vereist	TLS is toegestaan voor inkomende verbindingen van MTA's naar de luisteraar, en totdat ee STARTTLS-opdracht is ontvangen, reageert de ESA met een foutmelding naar elke opdrac anders dan No Option (NOOP), EHLO of QUIT. Indien TLS "Vereiste" is, betekent dit dat e- die de afzender niet wil versleutelen met TLS, door de ESA wordt geweigerd voordat deze v verzonden, waardoor de overdracht ervan niet duidelijk kan zijn.

TLS op een HAT Mail Flow Policy voor een luisteraar inschakelen via GUI

Voer de volgende stappen uit:

1. Kies een luisteraar wiens beleid u wilt aanpassen en klik vervolgens op de link voor de naam van het te bewerken beleid. (U kunt ook de parameters Standaardbeleid bewerken.) De pagina Mail Flow Policy wordt weergegeven.
2. Kies in het gedeelte "Encryption and Authentication" voor het veld "Use TLS:" het niveau van TLS dat u wilt voor de luisteraar.
3. Klik op **Inzenden**.
4. Klik op **Aanmelden**, voeg indien nodig een optioneel commentaar toe en klik vervolgens op **Aanmelden** om de wijzigingen op te slaan.

   Opmerking: U kunt een specifiek certificaat voor TLS-verbindingen toewijzen aan afzonderlijke openbare luisteraars wanneer u een luisteraar maakt.

TLS op een HAT Mail Flow Policy voor een luisteraar inschakelen via CLI

1. Gebruik de **listenerfig > bewerk** opdracht om een luisteraar te kiezen die u wilt configureren.

2. Gebruik de **hostaccess > standaard** opdracht om de standaard HAT-instellingen van de luisteraar te bewerken.
3. Voer een van deze opties in om de instelling voor TLS te wijzigen wanneer u wordt gevraagd:

```
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.
```

   Merk op dat dit voorbeeld u vraagt om het bevel te gebruiken certfig om te verzekeren dat er een geldig certificaat is dat met de luisteraar kan worden gebruikt. Als u geen certificaten hebt aangemaakt, gebruikt de luisteraar het demonstratiecertificaat dat al op het apparaat is geïnstalleerd. U kunt TLS met het demonstratiecertificaat inschakelen voor testdoeleinden, maar dit is niet veilig en wordt niet aanbevolen voor algemeen gebruik. Gebruik de **listenerfig > bewerk > certificaat** opdracht om een certificaat aan de luisteraar toe te wijzen.Zodra u TLS hebt ingesteld, wordt de instelling weergegeven in de samenvatting van de luisteraar in de 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. Voer de opdracht **in** om de wijziging in te schakelen.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- Gebruik het logbestand van de tekst en zie dit document: Bepaal of ESA TLS gebruikt voor levering of ontvangst
- Berichttracering gebruiken: GUI: Monitor > Berichttracering
- Rapportage gebruiken: GUI: monitor > TLS-verbindingen
- Gebruik een website van een derde partij zoals check tls.com

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

U kunt specificeren of de ESA een waarschuwing verstuurt indien de TLS onderhandeling mislukt wanneer berichten worden geleverd aan een domein dat een TLS-verbinding vereist. Het waarschuwingsbericht bevat de naam van het doeldomein voor de mislukte TLS-onderhandeling. De ESA stuurt het waarschuwingsbericht naar alle ontvangers die zijn ingesteld voor het ontvangen van alarmsignalen van het alarmniveau met de ernst van het systeem. U kunt alarmontvangers beheren via de pagina Systeembeheer > Waarschuwingen in de GUI (of via de opdracht **alertfig** in de CLI).

Gerelateerde informatie

- Eindgebruikershandleidingen - AsyncOS voor e-mail
- Technische ondersteuning en documentatie – Cisco Systems