Konfigurieren von TLS für die Verschlüsselung eingehender Verbindungen auf einem ESA-Listener

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Transport Layer Security (TLS) auf einem Listener der E-Mail Security Appliance (ESA) aktiviert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ESA mit jeder AsyncOS-Version.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Sie müssen TLS für alle Listener aktivieren, für die eine Verschlüsselung für eingehende Verbindungen erforderlich ist. Sie können TLS auf Listener aktivieren, die sich dem Internet gegenüber befinden (öffentliche Listener), jedoch nicht für Listener für interne Systeme (private Listener). Sie können auch die Verschlüsselung für alle Listener aktivieren. Standardmäßig lassen weder private noch öffentliche Listener TLS-Verbindungen zu. Sie müssen TLS in der Host Access Table (HAT) eines Listeners aktivieren, um TLS für eingehende (empfangende) oder ausgehende (sendende) E-Mails zu aktivieren. Darüber hinaus ist die TLS-Funktion in den Mail-Flow-Richtlinieneinstellungen für private und öffentliche Listener standardmäßig deaktiviert.

Konfigurieren

Sie können drei verschiedene Einstellungen für TLS auf einem Listener festlegen:

Einstellung	Bedeutung
Nein	TLS ist für eingehende Verbindungen nicht zulässig. Für Verbindungen mit dem Listener sind keine verschlüsselten SMTP-Konversationen (Simple Mail Transfer Protocol) erforderlich. Die die Standardeinstellung für alle Listener, die Sie auf der Appliance konfigurieren.
Bevorzugt	TLS ist für eingehende Verbindungen mit dem Listener von Message Transfer Agents (MTAs zulässig.
Erforderlich	TLS ist für eingehende Verbindungen mit dem Listener von MTAs zulässig, und bis ein STARTTLS-Befehl empfangen wird, antwortet die ESA mit einer Fehlermeldung für jeden Bef außer No Option (NOOP), EHLO oder QUIT. Wenn TLS 'Erforderlich' ist, bedeutet dies, dass Mails, die der Absender nicht mit TLS verschlüsselt verschlüsseln möchte, von der ESA vor d Senden abgelehnt werden, wodurch die Übermittlung in Klartext verhindert wird.

Aktivieren Sie TLS auf einer HAT-Mail-Flow-Richtlinie für einen Listener über die GUI.

Gehen Sie wie folgt vor:

1. Wählen Sie auf der Seite Mail Flow Policies (Mail-Ablaufrichtlinien) einen Listener aus, dessen Richtlinien Sie ändern möchten, und klicken Sie dann auf den Link, um den Namen der Richtlinie zu bearbeiten. (Sie können auch die Standard-Policy-Parameter bearbeiten.) Die Seite Mail Flow Policies bearbeiten wird angezeigt.
2. Wählen Sie im Abschnitt "Verschlüsselung und Authentifizierung" für das Feld "Use TLS:" (TLS verwenden) die TLS-Ebene aus, die Sie für den Listener verwenden möchten.
3. Klicken Sie auf **Senden**.
4. Klicken Sie auf **Änderungen bestätigen**, fügen Sie ggf. einen optionalen Kommentar hinzu und klicken Sie dann auf **Änderungen bestätigen**, um die Änderungen zu speichern.

   Hinweis: Wenn Sie einen Listener erstellen, können Sie einzelnen öffentlichen Listenern ein bestimmtes Zertifikat für TLS-Verbindungen zuweisen.

Aktivieren von TLS auf einer HAT-Mail-Flow-Richtlinie für einen Listener über die

CLI

1. Verwenden Sie den Befehl **listenerconfig > edit**, um einen Listener auszuwählen, den Sie konfigurieren möchten.
2. Verwenden Sie den Befehl **hostaccess > default**, um die HAT-Standardeinstellungen des Listeners zu bearbeiten.
3. Geben Sie eine der folgenden Optionen ein, um die TLS-Einstellung bei Aufforderung zu ändern:
```
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 diesem Beispiel werden Sie aufgefordert, den Befehl **certconfig** zu verwenden, um sicherzustellen, dass ein gültiges Zertifikat vorhanden ist, das mit dem Listener verwendet werden kann. Wenn Sie keine Zertifikate erstellt haben, verwendet der Listener das auf der Appliance vorinstallierte Demonstrationszertifikat. Sie können TLS mit dem Demonstrationszertifikat zu Testzwecken aktivieren, es ist jedoch nicht sicher und wird nicht für die allgemeine Verwendung empfohlen. Verwenden Sie den Befehl **listenerconfig > edit > certificate**, um dem Listener ein Zertifikat zuzuweisen.Nach der Konfiguration von TLS wird die Einstellung in der Zusammenfassung des Listeners in der CLI angezeigt:
```
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. Geben Sie den Befehl **commit** ein, um die Änderung zu aktivieren.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Verwenden Sie die Text-E-Mail-Protokolldatei, und sehen Sie dieses Dokument: Bestimmen Sie, ob die ESA TLS für die Zustellung oder den Empfang verwendet.
- Nachrichtenverfolgung verwenden: Benutzeroberfläche: Überwachung > Nachrichtenverfolgung
- Reporting verwenden: Benutzeroberfläche: Überwachung > TLS-Verbindungen
- Nutzung einer Website von Drittanbietern, z. B. checktls.com

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Sie können angeben, ob die ESA eine Warnung sendet, wenn die TLS-Aushandlung fehlschlägt,

wenn Nachrichten an eine Domäne gesendet werden, die eine TLS-Verbindung erfordert. Die Warnmeldung enthält den Namen der Zieldomäne für die fehlgeschlagene TLS-Aushandlung. Die ESA sendet die Warnmeldung an alle Empfänger, die für den Empfang von Warnmeldungen mit Schweregrad-Alarmen für Systemwarntypen eingestellt sind. Sie können Alert-Empfänger über die Seite Systemverwaltung > Warnungen in der GUI (oder über den Befehl **alertconfig** in der CLI) verwalten.

Zugehörige Informationen

- Benutzerhandbücher AsyncOS für E-Mail
- Technischer Support und Dokumentation - Cisco Systems