Cisco RES: Verwendung von TLS zum Sichern unverschlüsselter RES-Antworten

Inhalt

[Einführung](#)
[Cisco RES: Verwendung von TLS zum Sichern unverschlüsselter RES-Antworten](#)
[Absenderrichtlinien-Framework](#)
[Hostnamen und IP-Adressen](#)
[Lösung](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie Transport Layer Security (TLS) zum Sichern von Antworten vom Cisco Registered Envelope Service (CRES) verwenden, wodurch ein Benutzer diese in Verbindung mit der Cisco E-Mail Security Appliance (ESA) nicht entschlüsseln muss.

Cisco RES: Verwendung von TLS zum Sichern unverschlüsselter RES-Antworten

Standardmäßig werden Antworten auf eine sichere E-Mail mit Cisco RES verschlüsselt und an Ihr E-Mail-Gateway gesendet. Diese werden dann an Ihre Mail-Server weitergeleitet, die für den Endbenutzer verschlüsselt wurden und mit den Cisco RES-Anmeldeinformationen geöffnet werden können.

Um zu vermeiden, dass sich der Benutzer beim Cisco RES authentifizieren muss, um die sichere Antwort zu öffnen, stellt Cisco RES in einer "unverschlüsselten" Form E-Mail-Gateways bereit, die TLS unterstützen. In den meisten Fällen ist das E-Mail-Gateway die ESA, und dieser Artikel findet Anwendung.

Wenn jedoch ein anderes E-Mail-Gateway vor der ESA installiert ist, z. B. ein externer Spam-Filter, ist die Konfiguration des Zertifikats/TLS/E-Mail-Datenflusses auf der ESA nicht erforderlich. In diesem Fall können Sie die Schritte 1 bis 3 im Abschnitt Projektmappe dieses Dokuments überspringen. Für unverschlüsselte Antworten in dieser Umgebung ist der externe Spam-Filter (Mail-Gateway) die Appliance, die TLS unterstützen muss. Wenn sie TLS unterstützen, können Sie Cisco RES dazu veranlassen, dies zu bestätigen und "unverschlüsselte" Antworten einzurichten, um E-Mails zu sichern.

Absenderrichtlinien-Framework

Um Fehler bei der Verifizierung von Sender Policy Framework (SPF) zu vermeiden, müssen Sie dem SPF-Datensatz mx:res.cisco.com, mxnat1.res.cisco.com und mxnat3.res.cisco.com hinzufügen. Alternativ können Sie "**spfc._spf.cisco.com** in Ihren SPF-Datensatz einfügen.

Beispiel:

```
 ~ dig txt spfc._spf.cisco.com +short
"v=spf1 mx:res.cisco.com mx:sco.cisco.com ~all"
```

Wie und wo Sie Cisco RES zu Ihrem SPF-Datensatz hinzufügen, hängt davon ab, wie Ihr Domain Name System (DNS) mit der Netzwerktopologie implementiert wird. Weitere Informationen erhalten Sie von Ihrem DNS-Administrator.

Wenn der DNS nicht für die Einbindung von Cisco RES konfiguriert ist, wird bei der Erstellung sicherer Komprimierungs- und sicherer Antworten über die gehosteten Schlüsselserver die ausgehende IP-Adresse nicht mit den am Ende des Empfängers aufgelisteten IP-Adressen übereinstimmen, was zu einem Fehler bei der SPF-Verifizierung führt.

Hostnamen und IP-Adressen

Hostname	IP-Adresse	Datensatztyp
res.cisco.com	184,94,241,74	A
mxnat1.res.cisco.com	208,90,57,32	A
mxnat2.res.cisco.com	208,90,57,33	A
mxnat3.res.cisco.com	184,94,241,96	A
mxnat4.res.cisco.com	184,94,241,97	A
mxnat5.res.cisco.com	184,94,241,98	A
mxnat6.res.cisco.com	184,94,241,99	A
mxnat7.res.cisco.com	208,90,57,34	A
mxnat8.res.cisco.com	208,90,57,35	A
esa1.cres.iphmx.com	68 232 140,79	MX
esa2.cres.iphmx.com	68 232 140,57	MX
esa3.cres.iphmx.com	68 232 135 234	MX
esa4.cres.iphmx.com	68 232 135 235	MX

> **Hinweis**: Hostname und IP-Adressen können je nach Service-/Netzwerkwartung oder Wachstum des Service-/Netzwerkes geändert werden. Nicht alle Hostnamen und IP-Adressen werden für den Dienst verwendet. Sie werden hier als Referenz bereitgestellt.

Lösung

1. Ein signiertes Zertifikat und Zwischenzertifikat auf der ESA erhalten und installieren. **Hinweis**: Es ist wichtig, dass Sie das Zwischenzertifikat von Ihrer Signaturautorität erhalten, da das Demozertifikat der Appliance den Ausfall des CRES-Verifizierungsprozesses zur Folge hat.
2. Erstellen einer neuen Mail-Flow-Richtlinie: Wählen Sie in der GUI **Mail Policies > Mail Flow Policies > Add Policy aus...**Geben Sie einen Namen ein, und belassen Sie alle anderen Standardeinstellungen außer *Sicherheitsfunktionen: TLS.* Legen Sie diese Option auf **Erforderlich fest**.
3. Neue Absendergruppe erstellen: Wählen Sie in der GUI **Mail Policies > HAT Overview > Add Sender Group...**Geben Sie einen Namen ein, und legen Sie die Bestellnummer auf Nr. 1 fest. Sie können auch einen optionalen Kommentar eingeben. Wählen Sie die Mail Flow-Richtlinie aus, die Sie in Schritt 2 erstellt haben. Lassen Sie alles andere leer.Klicken Sie auf **Senden und Absender hinzufügen >>**.
4. Geben Sie im Feld Absender die folgenden IP-Bereiche und Hostnamen ein:
   ```
   .res.cisco.com
   .cres.iphmx.com
   208.90.57.0/26 (current CRES IP network range)
   204.15.81.0/26 (old CRES IP network range)
   ```
5. Senden und bestätigen Sie die Änderungen.
6. Wenn Sie sicher sind, dass die ESA für TLS von den Cisco RES-Servern vorbereitet ist, führen Sie die Schritte in How do I test if my domain support TLS with Cisco RES? aus, um die Cisco RES-Server zur Verwendung von TLS anzufordern.

Zugehörige Informationen

- Cisco RES: IP-Adressen und Hostnamen für Schlüsselserver
- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems