Konfigurieren der DKIM-Signatur auf der ESA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die DomainKeys Identified Mail (DKIM)-Signierung auf einer E-Mail Security Appliance (ESA) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- E-Mail Security Appliance (ESA)-Zugriff.
- DNS-Bearbeitungszugriff zum Hinzufügen/Entfernen von TXT-Datensätzen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Stellen Sie sicher, dass die DKIM-Signatur deaktiviert ist.

Sie müssen sicherstellen, dass die DKIM-Signierung in allen Mail Flow-Richtlinien deaktiviert ist. Auf diese Weise können Sie die DKIM-Signierung ohne Beeinträchtigung des E-Mail-Verkehrs konfigurieren:

1. Navigation zu **Mail-Policys > Mail Flow-Policys**.
2. Navigation zu jeder Mail Flow-Richtlinie und stellen Sie sicher, dass **Domänenschlüssel/DKIM-Signierung** auf "**Aus**" gesetzt ist.

DKIM-Signaturschlüssel erstellen

Sie müssen auf der ESA einen neuen DKIM-Signaturschlüssel erstellen:

1. Navigieren Sie zu **Mail-Policys > Signaturschlüssel,** und wählen Sie **Schlüssel hinzufügen aus.**
2. Nennen Sie den **DKIM-Schlüssel,** und generieren Sie entweder einen neuen privaten Schlüssel, oder fügen Sie ihn in einen aktuellen Schlüssel ein.

   Hinweis: In den meisten Fällen wird empfohlen, eine Größe für den privaten Schlüssel mit 2048 Bit zu wählen.

   ---

3. Bestätigen Sie die Änderungen.

Erstellen eines neuen DKIM-Signaturprofils und Veröffentlichen des DNS-Eintrags in DNS

Als Nächstes müssen Sie ein neues DKIM-Signaturprofil erstellen, einen DKIM-DNS-Eintrag aus diesem DKIM-Signaturprofil generieren und diesen Eintrag in DNS veröffentlichen:

1. Navigieren Sie zu **Mail-Policys > Signaturprofile,** und klicken Sie auf **Profil hinzufügen**.
   1. Geben Sie im Feld **Profilname** einen beschreibenden Namen für das Profil ein.
   2. Geben Sie Ihre Domäne in das Feld **Domain Name (Domänenname) ein**.
   3. Geben Sie eine neue Auswahlzeichenfolge in das Feld **Auswahl ein**.

      Hinweis: Der Selektor ist eine beliebige Zeichenfolge, die verwendet wird, um mehrere DKIM DNS-Einträge für eine bestimmte Domäne zuzulassen.

      ---

   4. Wählen Sie den im vorherigen Abschnitt erstellten DKIM-Signaturschlüssel im Feld **Signaturschlüssel aus**.
   5. Klicken Sie auf **Senden**.
2. Klicken Sie hier in der Spalte **DNS-Textdatensatz** für das gerade erstellte Signaturprofil auf **Generate (Generieren**), und kopieren Sie den generierten DNS-Eintrag. Es muss ähnlich wie folgt aussehen:

   ```
   selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMa
   ```

3. Bestätigen Sie die Änderungen.
4. Senden Sie den DKIM DNS TXT-Eintrag in Schritt 2 an DNS.
5. Warten Sie, bis der DKIM DNS TXT-Datensatz vollständig propagiert wurde.
6. Gehen Sie zu **Mail-Policys > Signaturprofile**.
7. Klicken Sie in der Spalte **Testprofil** auf **Test** (**Test)** für das neue DKIM-Signaturprofil. Wenn der Test erfolgreich war, fahren Sie mit diesem Leitfaden fort. Wenn nicht, stellen Sie sicher, dass der DKIM DNS TXT-Datensatz vollständig propagiert wurde.

Aktivieren der DKIM-Signatur

Nachdem die ESA für DKIM-Signaturnachrichten konfiguriert wurde, können wir die DKIM-Signierung aktivieren:

1. Navigieren Sie zu **Mail-Policys > Mail Flow-Policys**.

2. Wechseln Sie zu jeder Mail Flow-Richtlinie, die das **Verbindungsverhalten** von **Relay** aufweist, und aktivieren Sie **Domänenschlüssel-/DKIM-Signierung** auf **Ein**.

> **Hinweis**: Standardmäßig ist die einzige Mail Flow-Richtlinie mit dem **Verbindungsverhalten** von **Relay** die Mail Flow-Richtlinie **Relayed**. Sie müssen sicherstellen, dass nur ausgehende DKIM-Signaturnachrichten vorhanden sind.

---

3. Bestätigen Sie die Änderungen.

Testen des E-Mail-Flusses zum Bestätigen von DKIM-Durchläufen

Zu diesem Zeitpunkt wird das DKIM konfiguriert. Sie müssen jedoch die DKIM-Signierung testen, um sicherzustellen, dass ausgehende Nachrichten wie erwartet signiert werden und die DKIM-Verifizierung erfolgreich ist:

1. Senden Sie eine Nachricht über die ESA, und stellen Sie sicher, dass DKIM von der ESA signiert und von einem anderen Host verifiziert wird.
2. Nachdem die Nachricht am anderen Ende empfangen wurde, überprüfen Sie die Kopfzeilen der Nachricht auf die **Authentifizierungsergebnisse**. Überprüfen Sie im DKIM-Abschnitt des Headers, ob die DKIM-Verifizierung bestanden hat. Der Header muss ähnlich wie in diesem Beispiel aussehen:

   <#root>

   ```
   Authentication-Results: mx1.domainsite; spf=SoftFail smtp.mailfrom=user1@domainsite;
   ```

   dkim=pass

   ```
    header.i=none; dmarc=fail (p=none dis=none) d=domainsite
   ```

3. Suchen Sie nach dem Header "DKIM-Signature" und vergewissern Sie sich, dass der richtige Selektor und die richtige Domain verwendet werden:

   <#root>

   ```
   DKIM-Signature: a=rsa-sha256;
   ```

   d=domainsite

   ;

   s=selector2

   ;

   ```
      c=simple; q=dns/txt; i=@domainsite;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
                VoG4ZHRNiYzR
   ```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration gibt es derzeit keine spezifische Möglichkeit zur Fehlerbehebung.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.