Entschlüsselungszertifikat in sicherer Web-Appliance konfigurieren

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

HTTPS-Entschlüsselung

Entschlüsselungszertifikat in SWA konfigurieren

- Stammzertifikat und Schlüssel hochladen
- Zertifikat und Schlüssel für den HTTPS-Proxy generieren

Zertifikat importieren

- Upstream-Proxyzertifikat in SWA importieren
- SWA-Zertifikat in ein anderes SWA importieren
- SWA-Zertifikat in Windows-Client importieren
- SWA-Zertifikat in Mac-Client importieren
- SWA-Zertifikat in Ubuntu/Debian importieren
- SWA-Zertifikat in CentOS 6 importieren
- SWA-Zertifikat in CentOS 5 importieren
- SWA-Zertifikat in Mozilla Firefox importieren
- SWA-Zertifikat in Google Chrome importieren
- SWA-Zertifikat in Microsoft Edge/Internet Explorer importieren
- SWA-Zertifikat in Safari importieren
- SWA-Zertifikat von Gruppenrichtlinie in Clients importieren

Verwandte Inhalte

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren von HTTPS-Verschlüsselungszertifikaten in Secure Web Appliances (SWA) und Proxy-Clients beschrieben.

Voraussetzungen

Anforderungen

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

- Administratorzugriff auf die SWA
- Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA

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.

HTTPS-Entschlüsselung

Die sichere (HTTPS)-Entschlüsselung des SWA Hypertext Transfer Protocol verwendet Stammzertifikate und private Schlüsseldateien, die Sie zur Verschlüsselung des Datenverkehrs auf die Appliance hochladen. Das Stammzertifikat und die privaten Schlüsseldateien, die Sie auf die Appliance hochladen, müssen das PEM-Format haben.



Anmerkung: Das DER-Format wird nicht unterstützt.

Sie können auch ein Zwischenzertifikat hochladen, das von einer Stammzertifizierungsstelle signiert wurde. Wenn SWA ein Zertifikat erstellt, das das Serverzertifikat darstellt, sendet es das hochgeladene Zertifikat zusammen mit dem imitierten Zertifikat an die Clientanwendung. Auf diese Weise vertraut die Anwendung dem imitierten Serverzertifikat, solange das Zwischenzertifikat von einer Stammzertifizierungsstelle (Certificate Authority, CA) signiert wird, der die Clientanwendung vertraut.

Entschlüsselungszertifikat in SWA konfigurieren

Der SWA kann ein vorhandenes Zertifikat und einen privaten Schlüssel für die HTTPS-Entschlüsselung verwenden. Es kann jedoch Verwirrung darüber geben, welche Art von Zertifikat verwendet werden muss, da nicht alle x.509-Zertifikate funktionieren.

Es gibt zwei Haupttypen von Zertifikaten: Serverzertifikate und Stammzertifikate. Alle x.509-Zertifikate enthalten ein Feld "Grundbedingungen", in dem der Zertifikatstyp angegeben ist:

- Betrefftyp=Endeinheit - Serverzertifikat
- Betrefftyp=CA - Stammzertifikat

Stammzertifikat und Schlüssel hochladen

Schritt 1: Navigieren Sie in der GUI zu Sicherheitsdienste, und wählen Sie HTTPS-Proxy aus.
Schritt 2: Klicken Sie auf Einstellungen bearbeiten.
Schritt 3. Klicken Sie auf Hochgeladenes Zertifikat und hochgeladenen Schlüssel verwenden.
Schritt 4: Klicken Sie auf das Feld Zertifikat durchsuchen, um zur Zertifikatsdatei zu navigieren, die auf dem lokalen Computer gespeichert ist.



Anmerkung: Wenn die hochgeladene Datei mehrere Zertifikate oder Schlüssel enthält, verwendet der Webproxy das erste Zertifikat oder den ersten Schlüssel in der Datei.

Schritt 5: Klicken Sie im Schlüsselfeld auf Durchsuchen, um zur Datei mit dem privaten Schlüssel zu navigieren.



Anmerkung: Die Schlüssellänge muss 512, 1024 oder 2048 Bit betragen.

Schritt 6. Wählen Sie Schlüssel ist verschlüsselt, wenn der Schlüssel verschlüsselt ist.
Schritt 7: Klicken Sie auf Dateien hochladen, um das Zertifikat und die Schlüsseldateien an die sichere Web-Appliance zu übertragen. Die hochgeladenen Zertifikatinformationen werden auf der Seite HTTPS-Proxy-Einstellungen bearbeiten angezeigt.
Schritt 8. (Optional) Klicken Sie auf Zertifikat herunterladen, um es an die Client-Anwendungen im Netzwerk zu übertragen.

Schritt 9: Änderungen einsenden und bestätigen.

Zertifikat und Schlüssel für den HTTPS-Proxy generieren

Schritt 1: Navigieren Sie in der GUI zu Sicherheitsdienste, und wählen Sie HTTPS-Proxy aus.
Schritt 2: Klicken Sie auf Einstellungen bearbeiten.
Schritt 3. Wählen Sie Generiertes Zertifikat und generierten Schlüssel verwenden aus.
Schritt 4. Klicken Sie auf Neues Zertifikat und neuen Schlüssel generieren.
Schritt 5. Geben Sie im Dialogfeld Zertifikat und Schlüssel generieren die Informationen ein, die für die Anzeige im Stammzertifikat erforderlich sind. Sie können im Feld "Common Name" jedes ASCII-Zeichen außer dem Schrägstrich (/) eingeben.
Schritt 6: Klicken Sie auf Generieren.
Schritt 7: Die generierten Zertifikatinformationen werden auf der Seite HTTPS-Proxyeinstellungen bearbeiten angezeigt.
Schritt 8. (Optional) Klicken Sie auf Zertifikat herunterladen, damit Sie es an die Client-Anwendungen im Netzwerk übertragen können.
Schritt 9: (Optional) Klicken Sie auf den Link Download Certificate Signing Request (Zertifikatssignaturanforderung herunterladen), damit Sie die Zertifikatssignaturanforderung (CSR) an eine Zertifizierungsstelle senden können.
Schritt 10: (Optional) Laden Sie das signierte Zertifikat auf die sichere Web-Appliance hoch, nachdem Sie es von der Zertifizierungsstelle erhalten haben. Sie können dies jederzeit tun, nachdem Sie das Zertifikat auf der Appliance generiert haben.
Schritt 11: Änderungen einsenden und bestätigen.

Zertifikat importieren

Upstream-Proxyzertifikat in SWA importieren

Wenn SWA für die Verwendung eines Upstream-Proxys konfiguriert ist und der Upstream-Proxy für die HTTPS-Entschlüsselung konfiguriert ist, müssen Sie das Zertifikat für die Upstream-Proxyverschlüsselung in SWA importieren. Sie können die Liste der vertrauenswürdigen Zertifikate verwalten, ihr Zertifikate hinzufügen und Zertifikate funktional aus ihr entfernen.

Schritt 1. Wählen Sie in der GUI Network (Netzwerk) und dann Certificate Management (Zertifikatsverwaltung).
Schritt 2: Klicken Sie auf der Seite Zertifikatverwaltung auf Vertrauenswürdige Stammzertifikate verwalten.
Schritt 3: Um ein benutzerdefiniertes vertrauenswürdiges Stammzertifikat mit Signaturberechtigung hinzuzufügen, das nicht in der von Cisco erkannten Liste enthalten ist, klicken Sie auf Importieren und senden die Zertifikatsdatei.

Schritt 4: Änderungen einsenden und bestätigen.

SWA-Zertifikat in ein anderes SWA importieren

Wenn Sie das HTTPS-Zertifikat und den HTTPS-Schlüssel in einem SWA für den HTTPS-Proxy hochgeladen haben und auf die ursprünglichen Dateien zugegriffen werden kann, können Sie sie aus der Konfigurationsdatei in einen anderen SWA importieren.

Schritt 1: Wählen Sie in der GUI beider SWAs Systemverwaltung aus, und klicken Sie auf Konfigurationsdatei.

Schritt 2: Klicken Sie auf Datei auf dem lokalen Computer herunterladen, um sie anzuzeigen oder zu speichern.

Schritt 3: Wählen Sie in den Konfigurationsdateien die Option Kennwörter verschlüsseln aus.

Schritt 4. (Optional) Wählen Sie Benutzerdefinierten Dateinamen verwenden, und fügen Sie den gewünschten Namen zur Konfigurationsdatei hinzu.

Schritt 5: Klicken Sie unter "Aktuelle Konfiguration" auf Senden, um die .xml-Datei herunterzuladen.

Schritt 6. Öffnen Sie heruntergeladene Dateien mit Text-Editoren oder XML-Editoren.

Schritt 7: Kopieren Sie diese Tags aus SWA mit dem Zertifikat, kopieren Sie alle Daten innerhalb der Tags, und ersetzen Sie sie in der Konfigurationsdatei des anderen SWA:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

Schritt 8: Speichern Sie die Änderungen in der .xml-Datei des Ziel-SWA.

Schritt 9: Um die bearbeitete .xml-Konfigurationsdatei in das Ziel-SWA zu importieren, wählen Sie in der GUI die Option Systemverwaltung und klicken auf Konfigurationsdatei.

Schritt 10. Klicken Sie im Abschnitt Konfiguration laden auf Konfigurationsdatei vom lokalen Computer laden.

Schritt 11: Klicken Sie auf Choose file (Datei auswählen), und wählen Sie die bearbeitete .xml-Konfigurationsdatei aus.

Schritt 12: Klicken Sie auf Laden, um die neue Konfigurationsdatei mit dem Zertifikat und dem Schlüssel zu importieren.

Schritt 13. Änderungen bestätigen, wenn das System Sie dazu auffordert.

SWA-Zertifikat in Windows-Client importieren

Gehen Sie wie folgt vor, um das SWA-HTTPS-Proxy-Zertifikat als vertrauenswürdig auf Client-Computern mit Microsoft Windows-Betriebssystem zu importieren:

Schritt 1. Klicken Sie in der Taskleiste auf Start, und geben Sie Computerzertifikate verwalten ein.
Schritt 2. Erweitern Sie auf der Seite Zertifikate - Lokaler Computer die Option Vertrauenswürdige Stammzertifizierung, und klicken Sie mit der rechten Maustaste auf den Ordner Zertifikate.
Schritt 3. Klicken Sie auf Alle Tasks und wählen Sie Importieren aus.
Schritt 4: Klicken Sie auf der Seite "Zertifikatimport-Assistent" auf Weiter.
Schritt 5: Um die SWA-Zertifikatsdatei zu importieren, klicken Sie auf Durchsuchen, und wählen Sie das von SWA heruntergeladene Zertifikat aus.



Tipp: Informationen zum Herunterladen des SWA-Zertifikats finden Sie in Schritt 8 im Abschnitt Hochladen eines Stammzertifikats und Schlüssels oder Generieren eines Zertifikats und Schlüssels für den HTTPS-Proxy.

Schritt 6. Klicken Sie auf Alle Zertifikate in das folgende Kontrollkästchen einfügen.
Schritt 7: Wählen Sie Trusted Root Certification Authorities aus, und klicken Sie auf Next (Weiter).
Schritt 8: Klicken Sie auf Fertig stellen.

Alternativ können Sie diesen Befehl ausführen, um das Zertifikat in vertrauenswürdige Stammzertifizierungsstellen zu importieren.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



Anmerkung: Sie müssen **<**Pfad zu SWA Certificate/CertificateName.crt**>** durch den aktuellen heruntergeladenen Zertifikatpfad und Dateinamen ersetzen.

SWA-Zertifikat in Mac-Client importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA auf den Mac OS-Client herunter.
Schritt 2: Benennen Sie die Dateierweiterung in .crt um.
Schritt 3. Führen Sie diesen Befehl aus, um das Zertifikat als vertrauenswürdiges Zertifikat zu importieren:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```



Anmerkung: Sie müssen es durch den aktuellen heruntergeladenen Zertifikatpfad und Dateinamen ersetzen.

SWA-Zertifikat in Ubuntu/Debian importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2. Öffnen Sie die Zertifikatsdatei im Text-Editor, und kopieren Sie den gesamten Inhalt.
Schritt 3. Erstellen Sie eine neue Datei in /usr/local/share/ca-Certificates/ mit einer .crt Erweiterung.
Schritt 4. Bearbeiten Sie die Datei mit dem gewünschten Texteditor, fügen Sie den kopierten Text in die neue Datei ein, und speichern Sie die Datei.
Schritt 5. Führen Sie diesen Befehl aus, um die Zertifikate im Betriebssystem zu aktualisieren.

```
sudo update-ca-certificates
```



Tipp: Wenn das Zertifikat lokal auf dem Client gespeichert ist, können Sie es in /usr/local/share/ca-Certificates/ kopieren und sudo update-ca-certificats ausführen.



Anmerkung: In einigen Versionen müssen Sie das ca-certificate-Paket mit dem folgenden Befehl installieren: sudo apt-get install -y CA-Zertifikate.

SWA-Zertifikat in CentOS 6 importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2: Öffnen Sie die Zertifikatsdatei im Text-Editor, und kopieren Sie den gesamten Inhalt der Datei.

Schritt 3. Erstellen Sie eine neue Datei in /etc/pki/ca-trust/source/anchors/ mit der Erweiterung .crt.
Schritt 4. Bearbeiten Sie die Datei mit dem gewünschten Texteditor, und speichern Sie den kopierten Text in der neuen Datei.
Schritt 5. Installieren Sie das ca-certificate-Paket:

```
yum install ca-certificates
```

Schritt 6. Führen Sie diesen Befehl aus, um die Zertifikate im Betriebssystem zu aktualisieren:

```
update-ca-trust extract
```



Tipp: Wenn Sie das Zertifikat lokal auf dem Client gespeichert haben, können Sie das Zertifikat nach /etc/pki/ca-trust/source/anchors/ kopieren und update-ca-trust-Extrakt ausführen, nachdem Sie die ca-Zertifikate installiert haben.

SWA-Zertifikat in CentOS 5 importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2: Öffnen Sie die Zertifikatsdatei im Text-Editor, und kopieren Sie den gesamten Inhalt der Datei.
Schritt 3: Erstellen Sie eine neue Datei im aktuellen Ordner mit der Erweiterung .crt (z. B. SWA.crt).
Schritt 4. Bearbeiten Sie die Datei /etc/pki/tls/certs/ca-bundle.crt mit Ihrem gewünschten Texteditor, fügen Sie den kopierten Text am Ende der Datei ein, und speichern Sie ihn.



Tipp: Wenn das Zertifikat lokal auf dem Client gespeichert ist (in diesem Beispiel lautet der Dateiname SWA.crt), können Sie das Zertifikat mit dem folgenden Befehl anhängen: cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

SWA-Zertifikat in Mozilla Firefox importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2: Benennen Sie die Dateierweiterung in .crt um.
Schritt 3. Öffnen Sie Firefox und klicken Sie auf das Menü (drei Leisten in der oberen rechten

Ecke).
Schritt 4. Wählen Sie Einstellungen (in einigen Versionen sind es Optionen).
Schritt 5. Klicken Sie im Menü auf der linken Seite auf Datenschutz und Sicherheit, und scrollen Sie zu Zertifikate.
Schritt 6: Klicken Sie auf Zertifikate anzeigen.
Schritt 7: Klicken Sie auf die Registerkarte Behörden und dann auf Importieren.
Schritt 8. Wählen Sie die Zertifikatsdatei aus, und klicken Sie auf Öffnen.
Schritt 9: Klicken Sie auf OK.

SWA-Zertifikat in Google Chrome importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2: Benennen Sie die Dateierweiterung in .crt um.
Schritt 3. Öffnen Sie Google Chrome und klicken Sie auf Anpassen und steuern Sie Google Chrome (drei Punkte in der rechten oberen Ecke).
Schritt 4. Wählen Sie Einstellungen.
Schritt 5. Klicken Sie im Menü links auf Datenschutz und Sicherheit.
Schritt 6. Wählen Sie Sicherheit.
Schritt 7. Navigieren Sie zu Zertifikate verwalten und klicken Sie auf die Schaltfläche auf der rechten Seite.
Schritt 8: Wählen Sie die Registerkarte Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen), und klicken Sie auf Import (Importieren).
Schritt 9. Wählen Sie die Zertifikatsdatei aus, und klicken Sie auf Öffnen.
Schritt 10: Klicken Sie auf OK.



Anmerkung: Wenn Sie das SWA-Zertifikat im Betriebssystem installieren, vertraut Google Chrome auf dieses Zertifikat, und es besteht keine Notwendigkeit, das Zertifikat separat in Ihren Browser zu importieren.

SWA-Zertifikat in Microsoft Edge/Internet Explorer importieren

Microsoft Edge und Internet Explorer (IE) verwenden Betriebssystemzertifikate. Wenn Sie das SWA-Zertifikat im Betriebssystem installieren, ist es nicht erforderlich, das Zertifikat separat in Ihren Browser zu importieren.

SWA-Zertifikat in Safari importieren

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.

Schritt 2: Benennen Sie die Dateierweiterung in .crt um.
Schritt 3. Wählen Sie im Launchpad Keychain Access aus.
Schritt 4. Klicken Sie im Menü Datei auf Schlüsselbund hinzufügen.
Schritt 5: Wählen Sie die SWA-Zertifikatsdatei aus, und klicken Sie auf Hinzufügen.
Schritt 6. Wählen Sie Sicherheit.
Schritt 7. Navigieren Sie zu Zertifikate verwalten und klicken Sie auf die Schaltfläche auf der rechten Seite.
Schritt 8: Wählen Sie die Registerkarte Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen), und klicken Sie auf Import (Importieren).
Schritt 9. Wählen Sie die Zertifikatsdatei aus, und klicken Sie auf Öffnen.
Schritt 10: Klicken Sie auf OK.

SWA-Zertifikat von Gruppenrichtlinie in Clients importieren

Führen Sie die folgenden Schritte aus, um Zertifikate über die Gruppenrichtlinie von Active Directory an Clientcomputer zu verteilen:

Schritt 1: Laden Sie das HTTPS-Proxy-Zertifikat von SWA herunter.
Schritt 2: Benennen Sie die Dateierweiterung in .crt um.
Schritt 3: Kopieren Sie die Zertifikatsdatei auf Ihren Domänencontroller.
Schritt 4: Klicken Sie auf dem Domänencontroller auf Start, und öffnen Sie das Snap-In Gruppenrichtlinienverwaltung.
Schritt 5: Suchen Sie das gewünschte Gruppenrichtlinienobjekt, oder erstellen Sie ein neues Gruppenrichtlinienobjekt, das das SWA-Zertifikat enthält, das Sie in den Client importieren möchten.
Schritt 6: Klicken Sie mit der rechten Maustaste auf GPO, und klicken Sie auf Bearbeiten.
Schritt 7: Navigieren Sie im Menü auf der linken Seite zu Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel (Public Key Policies).
Schritt 8: Klicken Sie mit der rechten Maustaste auf die vertrauenswürdigen Stammzertifizierungsstellen, und klicken Sie auf Importieren.
Schritt 9: Klicken Sie auf Weiter auf der Seite Willkommen des Zertifikatimport-Assistenten.
Schritt 10: Wählen Sie die SWA-Zertifikatdatei aus, die importiert werden soll, und klicken Sie auf Weiter.
Schritt 11. Klicken Sie auf Alle Zertifikate im folgenden Speicher speichern, und klicken Sie dann auf Weiter.
Schritt 12: Überprüfen Sie die Richtigkeit der bereitgestellten Informationen, und klicken Sie auf Fertig stellen.



Anmerkung: Unter bestimmten Umständen müssen Sie den Client neu starten oder

---

gpupdate /force ausführen, um die Änderungen auf den Active Directory-Clientcomputer anzuwenden.

Verwandte Inhalte

- Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance - GD (Allgemeine Bereitstellung)
- Verteilen von Zertifikaten an Clientcomputer mithilfe der Gruppenrichtlinie | Microsoft - Lernen
- Technischer Support und Dokumentation für Cisco Systeme

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.