Verwendung des WSA-Zertifikats für HTTPS-Entschlüsselung

Inhalt

Einführung

In diesem Dokument wird der Zertifikatstyp beschrieben, der für die HTTPS-Entschlüsselung auf einer Cisco Web Security Appliance (WSA) verwendet werden soll.

Zertifikatsübersicht

Die WSA kann ein aktuelles Zertifikat und einen privaten Schlüssel für die Verwendung mit der HTTPS-Entschlüsselung verwenden. Es kann jedoch zu Unklarheiten hinsichtlich des zu verwendenden Zertifikatstyps kommen, da nicht alle x.509-Zertifikate funktionieren.

Es gibt zwei Arten von Zertifikaten: **Serverzertifikate** und **Stammzertifikate**. Alle x.509-Zertifikate enthalten ein Feld "Basic Constraints" (Grundeinschränkungen), in dem der Zertifikatstyp angegeben ist:

- **Subject Type=Endeinheit** - Serverzertifikat
- **Subject Type=CA** - Stammzertifikat

> **Hinweis**: Sie müssen für die HTTPS-Entschlüsselung auf der WSA ein Root-Zertifikat verwenden, das auch als Zertifizierungsstellen-Signaturzertifikat (Certificate Authority, CA) bezeichnet wird.

Wurzelzertifikate

Ein Root-Zertifikat wird speziell erstellt, um Serverzertifikate zu signieren. Sie können Ihre eigene CA erstellen und betreiben und eigene Serverzertifikate signieren.

Hinweis: Da ein Root-Zertifikat nur andere Zertifikate signiert, kann es nicht auf einem Webserver verwendet werden, um HTTPS-Verschlüsselung und -Entschlüsselung auszuführen.

Die WSA muss ein Root-Zertifikat verwenden, um aktiv Serverzertifikate für die HTTPS-Entschlüsselung zu generieren. Für die Verwendung von Root-Zertifikaten stehen zwei Optionen zur Verfügung:

- Generieren eines Stammzertifikats in der WSA Die WSA erstellt ein eigenes Root-Zertifikat und einen privaten Schlüssel und verwendet dieses Schlüsselpaar zum Signieren von Serverzertifikaten.

- Sie können ein aktuelles Root-Zertifikat und dessen privaten Schlüssel in die WSA hochladen. Das Feld Common Name (CN) in einem Root-Zertifikat gibt die Entität (in der Regel einen Firmennamen) an, die jedem Serverzertifikat vertraut ist, das seine Signatur enthält.

  Hinweis: Bevor ein Serverzertifikat vertrauenswürdig sein kann, muss es von einem Stammzertifikat signiert werden, das einen öffentlichen Schlüssel im Webbrowser enthält.

Serverzertifikate

Ein Serverzertifikat wird speziell erstellt, um in HTTPS-Verschlüsselung und -Entschlüsselung verwendet zu werden und um die Authentizität eines bestimmten Servers zu überprüfen. Serverzertifikate werden von einer CA signiert, die das CA Root-Zertifikat verwendet. Ein häufiges Beispiel für eine CA ist VeriSign oder Thawte.

Hinweis: Ein Serverzertifikat kann nicht zum Signieren anderer Zertifikate verwendet werden. Die HTTPS-Entschlüsselung funktioniert daher nicht, wenn ein Serverzertifikat auf der WSA installiert ist.

Das CN-Feld in einem Server-Zertifikat gibt den Host an, für den das Zertifikat verwendet werden soll. **https://www.verisign.com** verwendet beispielsweise ein Serverzertifikat mit dem CN von **www.verisign.com**.

Zugehörige Informationen

- Verwendung des WSA-Zertifikats (Web Security Appliance) (HTTPS-Entschlüsselung, GUI-Anmeldung, Verschlüsselung der Anmeldeinformationen)
- Schritte zur Aktivierung des HTTPS-Proxys für die Option WSA & Certificate Signing Request (CSR)
- Schritte zur Aktivierung des HTTPS-Proxys für WSA (WSA) und zum Hochladen von Root-/Zwischenzertifikaten
- Technischer Support und Dokumentation - Cisco Systems