Erstellen einer Zertifikatssignierungsanfrage auf einer ESA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatssignierungsanfrage (CSR) auf einer E-Mail-Security-Appliance (ESA) erstellen.

CSR auf einer ESA erstellen

Ab AsyncOS 7.1.1 kann die ESA ein selbstsigniertes Zertifikat für Ihre eigene Verwendung erstellen und eine CSR-Anfrage erstellen, die an eine Zertifizierungsstelle gesendet und das öffentliche Zertifikat bezieht. Die Zertifizierungsstelle gibt ein vertrauenswürdiges öffentliches Zertifikat zurück, das von einem privaten Schlüssel signiert wird. Verwenden Sie die Seite **Network > Certificates** (Netzwerk > Zertifikate) in der GUI oder den Befehl **certconfig** in der CLI, um das selbstsignierte Zertifikat zu erstellen, den CSR zu generieren und das vertrauenswürdige öffentliche Zertifikat zu installieren.

Wenn Sie zum ersten Mal ein Zertifikat erwerben oder erstellen, suchen Sie im Internet nach "Certificate Authority Services SSL Server Certificates" (Zertifikaten der Zertifizierungsstelle für SSL-Server) und wählen Sie den Service aus, der am besten die Anforderungen Ihres Unternehmens erfüllt. Befolgen Sie die Anweisungen des Service, um ein Zertifikat zu erhalten.

Konfigurationsschritte in der GUI

1. Um ein selbstsigniertes Zertifikat zu erstellen, klicken Sie in der GUI auf der Seite Network > Certificates (Netzwerk > Zertifikate) auf **Zertifikat hinzufügen** (oder auf den Befehl **certconfig** in der CLI). Wählen Sie auf der Seite Zertifikat hinzufügen die Option **Selbstsigniertes Zertifikat erstellen aus**.
2. Geben Sie diese Informationen für das selbstsignierte Zertifikat ein: Allgemeiner Name: Der vollqualifizierte Domänenname.Organisation - Der genaue rechtliche Name der Organisation.Organisationseinheit - Bereich der Organisation.Stadt (Stadt) - Die Stadt, in der sich die Organisation rechtmäßig befindet.Bundesland (Provinz) - Bundesland, Bezirk oder Region, in dem die Organisation ihren rechtmäßigen Sitz hat.Land - Die Abkürzung

"International Organization for Standardization" (ISO) des Landes, in dem sich die Organisation rechtmäßig befindet.Laufzeit vor Ablauf - Die Anzahl der Tage, die vor Ablauf des Zertifikats vergehen.Größe des privaten Schlüssels: Die Größe des privaten Schlüssels, der für den CSR generiert werden soll. Nur 2048-Bit und 1024-Bit werden unterstützt.

3. Klicken Sie auf **Weiter**, um die Zertifikats- und Signaturinformationen anzuzeigen.
4. Geben Sie einen Namen für das Zertifikat ein. AsyncOS weist den allgemeinen Namen standardmäßig zu.
5. Wenn Sie eine CSR-Anfrage für das selbstsignierte Zertifikat an eine Zertifizierungsstelle senden möchten, klicken Sie auf **Zertifikatssignierungsanfrage herunterladen**, um den CSR im Privacy Enhanced Mail (PEM)-Format auf einem lokalen oder einem Netzwerkcomputer zu speichern.
6. Klicken Sie auf **Senden**, um das Zertifikat zu speichern und Ihre Änderungen zu bestätigen. Wenn Sie die Änderungen nicht übernommen lassen, geht der private Schlüssel verloren, und das signierte Zertifikat kann nicht installiert werden.

Wenn die Zertifizierungsstelle das von einem privaten Schlüssel signierte vertrauenswürdige öffentliche Zertifikat zurückgibt, klicken Sie auf der Zertifikatsseite auf den Namen des Zertifikats, und geben Sie den Pfad zur Datei auf Ihrem lokalen Computer oder Netzwerk ein, um das Zertifikat hochzuladen. Stellen Sie sicher, dass das öffentliche Zertifikat, das Sie erhalten, im PEM-Format oder in einem Format vorliegt, das Sie in PEM konvertieren können, bevor es auf die Appliance hochgeladen wird. Tools, um dies abzuschließen, sind im Lieferumfang von OpenSSL enthalten, einer kostenlosen Software, die unter http://www.openssl.org zur Verfügung steht.

Wenn Sie das Zertifikat von der Zertifizierungsstelle hochladen, wird das vorhandene Zertifikat überschrieben. Sie können auch ein Zwischenzertifikat hochladen, das sich auf das selbstsignierte Zertifikat bezieht. Sie können das Zertifikat mit einem öffentlichen oder privaten Listener, den HTTPS-Diensten einer IP-Schnittstelle, der LDAP-Schnittstelle (Lightweight Directory Access Protocol) oder allen ausgehenden TLS-Verbindungen mit Zieldomänen verwenden.

Zugehörige Informationen

- Umfassender Einrichtungsleitfaden für TLS auf ESA
- Technischer Support und Dokumentation - Cisco Systems