Konfigurationsbeispiel für SSL VPN mit IP-Telefonen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie IP-Telefone über ein Secure Sockets Layer VPN (SSL VPN), auch als WebVPN bekannt, konfiguriert werden. Für diese Lösung werden zwei Cisco Unified Communications Manager (CallManager) und drei Zertifikatsarten verwendet. CallManager sind:

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

Die Zertifikattypen sind:

- Selbstsignierte Zertifikate
- Zertifikate von Drittanbietern wie Entrust, Thawte und GoDaddy
- Cisco IOS®/Adaptive Security Appliance (ASA) Certificate Authority (CA)

Das Schlüsselkonzept ist, dass Sie nach Abschluss der Konfiguration auf dem SSL VPN-Gateway und CallManager den IP-Telefonen lokal beitreten müssen. Dadurch können die Telefone dem CUCM beitreten und die richtigen VPN-Informationen und -Zertifikate verwenden. Wenn die Telefone nicht lokal verbunden sind, können sie das SSL VPN-Gateway nicht finden und verfügen nicht über die richtigen Zertifikate, um den SSL VPN-Handshake abzuschließen.

Die gängigsten Konfigurationen sind CUCM/Unified CME mit selbstsignierten ASA-Zertifikaten und selbstsignierten Cisco IOS-Zertifikaten. Daher sind sie am einfachsten zu konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Communications Manager (CUCM) oder Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- Cisco Adaptive Security Appliance (ASA)
- Zertifikatstypen wie selbstsignierte, Drittanbieter- und Zertifizierungsstellen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA Premium-Lizenz
- AnyConnect VPN-Telefonlizenz
  - Für die ASA Version 8.0.x ist die Lizenz AnyConnect für Linksys Phone.
  - Für ASA Version 8.2.x oder höher ist die Lizenz AnyConnect für Cisco VPN Phone.
- SSL-VPN-Gateway: ASA 8.0 oder höher (mit AnyConnect für Cisco VPN-Telefonlizenz) oder Cisco IOS Software Release 12.4T oder höher
  - Die Cisco IOS Software Version 12.4T oder höher wird nicht offiziell unterstützt, wie im SSL VPN Configuration Guide beschrieben.
  - In der Cisco IOS Software, Version 15.0(1)M, ist das SSL VPN-Gateway eine Lizenzierungsfunktion zum Anrechnen von Arbeitsplätzen auf den Plattformen Cisco 880, Cisco 890, Cisco 1900, Cisco 2900 und Cisco 3900. Für eine erfolgreiche SSL VPN-Sitzung ist eine gültige Lizenz erforderlich.
- CallManager: CUCM 8.0.1 oder höher oder Unified CME 8.5 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

> **Hinweise**:
>
> Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Grundlegende ASA SSL VPN-Konfiguration

Die grundlegende ASA SSL VPN-Konfiguration wird in den folgenden Dokumenten beschrieben:

- ASA 8.x: Konfigurationsbeispiel für den VPN-Zugriff mit dem AnyConnect VPN-Client mithilfe eines selbstsignierten Zertifikats
- Konfigurieren von AnyConnect VPN Client-Verbindungen

Nach Abschluss dieser Konfiguration sollte ein Remote-Test-PC eine Verbindung zum SSL VPN-Gateway herstellen, eine Verbindung über AnyConnect herstellen und den CUCM pingen können. Stellen Sie sicher, dass die ASA über eine AnyConnect for Cisco IP-Telefonlizenz verfügt. (Verwenden Sie den Befehl **show ver**.) Sowohl der TCP- als auch der UDP-Port 443 müssen zwischen dem Gateway und dem Client offen sein.

Hinweis: SSL VPN mit Lastausgleich wird für VPN-Telefone nicht unterstützt.

CUCM: ASA SSL VPN mit Konfiguration selbstsignierter Zertifikate

Weitere Informationen finden Sie unter IP-Telefon SSL VPN zu ASA mit AnyConnect.

Die ASA muss über eine Lizenz für AnyConnect für das Cisco VPN-Telefon verfügen. Nachdem Sie das SSL VPN konfiguriert haben, konfigurieren Sie den CUCM für das VPN.

1. Verwenden Sie diesen Befehl, um das selbstsignierte Zertifikat von der ASA zu exportieren:

   ```
   ciscoasa(config)# crypto ca export trustpoint name identity-certificate
   ```

   Dieser Befehl zeigt dem Terminal ein pem-kodiertes Identitätszertifikat an.
2. Kopieren Sie das Zertifikat, fügen Sie es in einen Texteditor ein, und speichern Sie es als .pem-Datei. Vergewissern Sie sich, dass Sie die Zeilen "BEGIN CERTIFICATE" und "END CERTIFICATE" (ENDZERTIFIKAT BEGINNEN) angeben, da das Zertifikat nicht korrekt importiert wird. Ändern Sie das Format des Zertifikats nicht, da dies Probleme verursachen wird, wenn das Telefon versucht, sich bei der ASA zu authentifizieren.
3. Navigieren Sie zu **Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain**, um die Zertifikatsdatei in den Abschnitt CERTIFICATE MANAGEMENT des CUCM zu laden.
4. Laden Sie die Zertifikate CallManager.pem, CAPF.pem und Cisco_Manufacturing_CA.pem im gleichen Bereich herunter, in dem Sie die selbstsignierten Zertifikate von der ASA laden (siehe Schritt 1), und speichern Sie sie auf Ihrem Desktop.
   1. Verwenden Sie zum Beispiel die folgenden Befehle, um CallManager.pem in die ASA zu importieren:

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. Wenn Sie aufgefordert werden, das entsprechende Zertifikat für den Vertrauenspunkt zu kopieren und in Ihren Browser einzufügen, öffnen Sie die Datei, die Sie im CUCM gespeichert haben, und kopieren Sie anschließend das Base64-kodierte Zertifikat, und fügen Sie es ein. Stellen Sie sicher, dass Sie die Zeilen BEGIN CERTIFICATE und END CERTIFICATE (mit Bindestrichen) angeben.
3. Geben Sie **end ein**, und drücken Sie dann **Return**.
4. Wenn Sie aufgefordert werden, das Zertifikat zu akzeptieren, geben Sie **yes ein**, und drücken Sie **die Eingabetaste**.
5. Wiederholen Sie die Schritte 1 bis 4 für die beiden anderen Zertifikate (CAPF.pem, Cisco_Manufacturing_CA.pem) vom CUCM.

5. Konfigurieren Sie den CUCM für die korrekten VPN-Konfigurationen, wie in der CUCM-VPN-Konfiguration.pdf beschrieben.

   Hinweis: Das auf dem CUCM konfigurierte VPN-Gateway muss mit der URL übereinstimmen, die auf dem VPN-Gateway konfiguriert wurde. Wenn Gateway und URL nicht übereinstimmen, kann die Adresse nicht vom Telefon aufgelöst werden, und es werden keine Fehlerbehebungen auf dem VPN-Gateway angezeigt.

- Auf CUCM: Die VPN-Gateway-URL lautet https://192.168.1.1/VPNPhone.
- Verwenden Sie für die ASA die folgenden Befehle:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- Sie können diese Befehle im Adaptive Security Device Manager (ASDM) oder im Verbindungsprofil verwenden.

CUCM: ASA SSL VPN mit Zertifizierungskonfiguration für Drittanbieter

Diese Konfiguration ähnelt der Konfiguration in CUCM: Abschnitt "Konfiguration selbstsignierter Zertifikate" für ASA SSLVPN mit selbstsignierter Zertifikatskonfiguration, mit der Ausnahme, dass Sie Zertifikate von Drittanbietern verwenden. Konfigurieren Sie SSL VPN auf der ASA mit Zertifikaten von Drittanbietern, wie in ASA 8.x beschrieben, und installieren Sie Zertifikate von Drittanbietern manuell, um sie mit WebVPN-Konfigurationsbeispiel zu verwenden.

Hinweis: Sie müssen die gesamte Zertifikatskette von der ASA in den CUCM kopieren und alle Zwischen- und Root-Zertifikate einschließen. Wenn der CUCM nicht die vollständige Kette enthält, verfügen die Telefone nicht über die erforderlichen Zertifikate für die Authentifizierung und schlagen beim SSL VPN-Handshake fehl.

Grundlegende IOS SSL VPN-Konfiguration

Hinweis: IP-Telefone werden im IOS SSL VPN als nicht unterstützt eingestuft.

Konfigurationen werden nur nach bestem Wissen durchgeführt.

Die grundlegende Cisco IOS SSL VPN-Konfiguration wird in den folgenden Dokumenten beschrieben:

- SSL VPN Client (SVC) auf IOS mit SDM-Konfigurationsbeispiel
- Konfigurationsbeispiel für einen AnyConnect VPN-Client auf dem IOS-Router mit IOS Zone-basierter Firewall-Richtlinie

Nach Abschluss dieser Konfiguration sollte ein Remote-Test-PC eine Verbindung zum SSL VPN-Gateway herstellen, eine Verbindung über AnyConnect herstellen und den CUCM pingen können. In Cisco IOS 15.0 und höher benötigen Sie eine gültige SSL VPN-Lizenz, um diese Aufgabe durchzuführen. Sowohl der TCP- als auch der UDP-Port 443 müssen zwischen dem Gateway und dem Client offen sein.

CUCM: IOS SSL VPN mit Konfiguration selbstsignierter Zertifikate

Diese Konfiguration ähnelt der Konfiguration in CUCM: ASA SSLVPN mit Drittanbieter-Zertifikatskonfiguration und CUCM: Abschnitte zur Konfiguration von ASA SSLVPN mit selbstsignierten Zertifikaten. Die Unterschiede sind:

1. Verwenden Sie diesen Befehl, um das selbstsignierte Zertifikat vom Router zu exportieren:

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. Verwenden Sie die folgenden Befehle, um die CUCM-Zertifikate zu importieren:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

In der WebVPN-Kontextinformationen sollte folgender Text angezeigt werden:

```
gateway webvpn_gateway domain VPNPhone
```

Konfigurieren Sie den CUCM wie in CUCM beschrieben: Abschnitt "Konfiguration selbstsignierter Zertifikate" für ASA SSLVPN.

CUCM: IOS SSL VPN mit Drittanbieter-Zertifikatskonfiguration

Diese Konfiguration ähnelt der Konfiguration in CUCM: Abschnitt "Konfiguration selbstsignierter Zertifikate" für ASA SSLVPN. Konfigurieren Sie Ihr WebVPN mit einem Zertifikat eines Drittanbieters.

Hinweis: Sie müssen die gesamte WebVPN-Zertifikatskette in den CUCM kopieren und alle Zwischen- und Root-Zertifikate einschließen. Wenn der CUCM nicht die vollständige Kette enthält, verfügen die Telefone nicht über die erforderlichen Zertifikate für die Authentifizierung und schlagen beim SSL VPN-Handshake fehl.

Unified CME: ASA/Router SSL VPN mit selbstsignierter Zertifikatskonfiguration/Konfiguration von Drittanbieterzertifikaten

Die Konfiguration für Unified CME ähnelt der Konfiguration für CUCM. Zum Beispiel sind die WebVPN-Endpunktkonfigurationen identisch. Der einzige wesentliche Unterschied besteht in den Konfigurationen des Unified CME-Anruf-Agenten. Konfigurieren Sie die VPN-Gruppe und die VPN-Richtlinie für Unified CME wie unter Konfigurieren des SSL VPN-Clients für SCCP-IP-Telefone beschrieben.

> **Hinweis**: Unified CME unterstützt nur das Skinny Call Control Protocol (SCCP) und kein Session Initiation Protocol (SIP) für VPN-Telefone.

> **Hinweis**: Die Zertifikate müssen nicht von Unified CME in die ASA oder den Router exportiert werden. Sie müssen die Zertifikate nur vom ASA- oder Router-WebVPN-Gateway in Unified CME exportieren.

Informationen zum Exportieren der Zertifikate vom WebVPN-Gateway finden Sie im Abschnitt zum ASA/Router. Wenn Sie ein Zertifikat eines Drittanbieters verwenden, müssen Sie die gesamte Zertifikatskette einschließen. Verwenden Sie zum Importieren der Zertifikate in Unified CME die gleiche Methode wie zum Importieren von Zertifikaten in einen Router:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

UC 520 IP-Telefone mit SSL VPN-Konfiguration

Das Cisco Unified Communications 500 IP-Telefon mit Modell UC 520 unterscheidet sich erheblich von den CUCM- und CME-Konfigurationen.

- Da das UC 520-IP-Telefon sowohl der CallManager als auch das WebVPN-Gateway ist, müssen keine Zertifikate zwischen den beiden konfiguriert werden.
- Konfigurieren Sie das WebVPN auf einem Router wie gewohnt mit selbstsignierten Zertifikaten oder Zertifikaten von Drittanbietern.
- Das UC520 IP-Telefon verfügt über einen integrierten WebVPN-Client. Sie können diesen so konfigurieren, wie ein normaler PC für die Verbindung mit WebVPN. Geben Sie das Gateway und dann die Kombination aus Benutzername und Kennwort ein.
- Das UC 520 IP-Telefon ist mit den Cisco Small Business IP-Telefonen SPA 525G kompatibel.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.