使用IP電話的SSLVPN配置示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[設定](#)
[基本ASA SSL VPN配置](#)
[CUCM:具有自簽名證書的ASA SSL VPN配置](#)
[CUCM:採用第三方證書的ASA SSL VPN配置](#)
[基本IOS SSL VPN配置](#)
[CUCM:採用自簽名證書的IOS SSL VPN配置](#)
[CUCM:使用第三方證書的IOS SSL VPN配置](#)
[Unified CME:帶有自簽名證書/第三方證書配置的ASA/路由器SSL VPN](#)
[採用SSL VPN組態的UC 520 IP電話](#)
[驗證](#)
[疑難排解](#)

簡介

本文檔介紹如何通過安全套接字層VPN(SSL VPN)（也稱為WebVPN）配置IP電話。此解決方案使用兩個思科統一通訊管理器(CallManager)和三種型別的證書。CallManager包括：

- 思科整合通訊管理員(CUCM)
- Cisco Unified Communications Manager Express(Cisco Unified CME)

證書型別為：

- 自簽名證書
- 第三方證書，如Entrust、Thawte和GoDaddy
- Cisco IOS®/調適型安全裝置(ASA)憑證授權單位(CA)

要瞭解的關鍵概念是，一旦完成SSL VPN網關和CallManager上的配置，您必須在本地加入IP電話。這使電話能夠加入CUCM並使用正確的VPN資訊和證書。如果電話未在本地加入，則它們無法找到SSL VPN網關，並且沒有完成SSL VPN握手的正確證書。

最常見的配置是具有ASA自簽名證書和Cisco IOS自簽名證書的CUCM/Unified CME。因此，它們是最容易配置的。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unified Communications Manager(CUCM)或Cisco Unified Communications Manager Express(Cisco Unified CME)
- SSL VPN(WebVPN)
- 思科調適型安全裝置(ASA)
- 證書型別，例如自簽名證書頒發機構、第三方證書頒發機構和證書頒發機構

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA高級版許可證。
- AnyConnect VPN電話許可證。
  - 對於ASA 8.0.x版，許可證為Linksys電話的AnyConnect。
  - 對於ASA 8.2.x版或更高版本，許可證為AnyConnect for Cisco VPN Phone。
- SSL VPN網關：ASA 8.0或更高版本（具有AnyConnect for Cisco VPN電話許可證）或Cisco IOS軟體版本12.4T或更高版本。
  - 如SSL VPN配置指南中所述，正式不支援Cisco IOS軟體版本12.4T或更高版本。
  - 在Cisco IOS軟體版本15.0(1)M中，SSL VPN網關是Cisco 880、Cisco 890、Cisco 1900、Cisco 2900和Cisco 3900平台上的座席數許可功能。成功的SSL VPN會話需要有效的許可證。
- CallManager:CUCM 8.0.1或更高版本，或者Unified CME 8.5或更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

> **附註**：
>
> 使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。
>
> 輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

基本ASA SSL VPN配置

以下文檔中介紹了基本ASA SSL VPN配置：

- ASA 8.x:使用AnyConnect VPN客戶端使用自簽名證書的VPN訪問配置示例
- 配置AnyConnect VPN客戶端連線

完成此配置後，遠端測試PC應該能夠連線到SSL VPN網關，通過AnyConnect連線，然後對CUCM執行ping操作。確保ASA具有AnyConnect for Cisco IP電話許可證。(使用**show ver**命令。)網關和客戶端之間的TCP和UDP埠443都必須開啟。

附註：VPN電話不支援負載平衡SSL VPN。

CUCM:具有自簽名證書的ASA SSL VPN配置

有關詳細資訊，請參閱使用AnyConnect的IP電話SSL VPN到ASA。

ASA必須具有適用於Cisco VPN電話的AnyConnect許可證。配置SSL VPN後，為VPN配置CUCM。

1. 使用以下命令從ASA匯出自簽名證書：

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

此命令向終端顯示一個pem編碼的身份證書。
2. 將憑證複製貼上到文字編輯器中，並將其另存為.pem檔案。請務必包括BEGIN CERTIFICATE和END CERTIFICATE行，否則證書將無法正確匯入。請勿修改證書格式，因為這將導致電話嘗試向ASA進行身份驗證時出現問題。
3. 導覽至**Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain**，以便將憑證檔案載入到CUCM的CERTIFICATE MANAGEMENT區段。
4. 從用於從ASA載入自簽名證書的同一區域下載CallManager.pem、CAPF.pem和Cisco_Manufacturing_CA.pem證書（請參閱步驟1），然後將它們儲存到案頭。
   1. 例如，要將CallManager.pem匯入ASA，請使用以下命令：

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

   2. 當系統提示您複製並貼上信任點的相應證書時，請開啟從CUCM儲存的檔案，然後複製並貼上Base64編碼的證書。請務必包括BEGIN CERTIFICATE和END CERTIFICATE行（使用連字元）。
   3. 鍵入**end**，然後按**Return**。
   4. 系統提示接受憑證時，輸入**yes**，然後按**Enter**。
   5. 對CUCM中的其它兩個證書(CAPF.pem、Cisco_Manufacturing_CA.pem)重複步驟1至4。
5. 按照CUCM IPphone VPN config.pdf所述，為CUCM配置正確的VPN配置。

附註：CUCM上配置的VPN網關必須與VPN網關上配置的URL匹配。如果網關和URL不匹配，電話無法解析地址，並且您在VPN網關上看不到任何調試。

- 在CUCM上：VPN網關URL為https://192.168.1.1/VPNPhone
- 在ASA上，使用以下命令：

```
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
```

- 可以在自適應安全裝置管理器(ASDM)或連線配置檔案下使用這些命令。

CUCM:採用第三方證書的ASA SSL VPN配置

此組態與CUCM中所述的組態非常相似：ASA SSLVPN with Self-Signed Certificates Configuration部分，除非您使用的是第三方證書。使用第三方證書在ASA上配置SSL VPN，如ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例中所述。

> **附註**：必須將完整證書鏈從ASA複製到CUCM並包括所有中間和根證書。如果CUCM不包括全鏈，則電話沒有進行身份驗證所需的證書，SSL VPN握手將失敗。

基本IOS SSL VPN配置

> **附註**：IOS SSL VPN將IP電話指定為不受支援；配置僅盡力而為。

以下文檔中介紹了基本Cisco IOS SSL VPN配置：

- 使用SDM的IOS上的SSL VPN客戶端(SVC)配置示例
- 使用基於IOS區域的策略防火牆的IOS路由器上的AnyConnect VPN客戶端配置示例

完成此配置後，遠端測試PC應該能夠連線到SSL VPN網關，通過AnyConnect連線，然後對CUCM執行ping操作。在Cisco IOS 15.0及更高版本中，您必須擁有有效的SSL VPN許可證才能完成此任務。網關和客戶端之間的TCP和UDP埠443都必須開啟。

CUCM:採用自簽名證書的IOS SSL VPN配置

此組態與CUCM: 中所述的組態類似。ASA SSLVPN，帶第三方證書配置和CUCM:ASA SSLVPN with Self-Signed Certificates配置部分。不同之處在於：

1. 使用以下命令從路由器匯出自簽名的憑證：

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

2. 使用以下命令匯入CUCM證書：

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

WebVPN上下文配置應顯示以下文本：

```
gateway webvpn_gateway domain VPNPhone
```

按照CUCM: 中的說明配置CUCM:ASA SSLVPN with Self-Signed Certificates Configuration部分。

CUCM:使用第三方證書的IOS SSL VPN配置

此組態與CUCM: 中所述的組態類似。ASA SSLVPN with Self-Signed Certificates Configuration部分。使用第三方證書配置WebVPN。

附註：必須將完整的WebVPN證書鏈複製到CUCM並包括所有中間和根證書。如果CUCM不包括全鏈，則電話沒有進行身份驗證所需的證書，SSL VPN握手將失敗。

Unified CME:帶有自簽名證書/第三方證書配置的ASA/路由器SSL VPN

Unified CME的配置與CUCM的配置類似；例如，WebVPN端點配置相同。唯一的顯著差異是Unified CME呼叫代理的配置。按照為SCCP IP電話配置SSL VPN客戶端中所述，為Unified CME配置VPN組和VPN策略。

附註：Unified CME僅支援精簡型呼叫控制協定(SCCP)，不支援VPN電話的會話發起協定(SIP)。

附註：無需將證書從Unified CME匯出到ASA或路由器。您只需要將證書從ASA或路由器WebVPN網關匯出到Unified CME。

要從WebVPN網關匯出證書，請參閱ASA/路由器部分。如果您使用的是第三方證書，則必須包含完整的證書鏈。若要將憑證匯入Unified CME，請使用將憑證匯入路由器所用的相同方法：

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

採用SSL VPN組態的UC 520 IP電話

Cisco Unified Communications 500系列型號UC 520 IP電話與CUCM和CME配置有很大不同。

- 由於UC 520 IP電話既是CallManager又是WebVPN網關，因此無需在兩者之間配置證書。
- 在路由器上配置WebVPN，就像通常使用自簽名證書或第三方證書一樣。
- UC 520 IP電話具有內建的WebVPN客戶端，您可以像配置普通的PC一樣將其連線到WebVPN。輸入網關，然後輸入使用者名稱/密碼組合。
- UC 520 IP電話與Cisco Small Business IP電話SPA 525G電話相容。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。