SSLVPN with IP Phones Configuration Example

Contents

Introduction

This document describes how to configure IP phones over a Secure Sockets Layer VPN (SSL VPN), also known as a WebVPN. Two Cisco Unified Communications Managers (CallManagers) and three types of certificates are used with this solution. The CallManagers are:

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

The certificate types are:

- Self-signed certificates
- Third-party certificates, such as Entrust, Thawte, and GoDaddy
- Cisco IOS®/Adaptive Security Appliance (ASA) certificate authority (CA)

The key concept to understand is that, once the configuration on the SSL VPN gateway and CallManager are completed, you must join the IP phones locally. This enables the phones to join the CUCM and to use the correct VPN information and certificates. If the phones are not joined locally, they cannot find the SSL VPN gateway and do not have the correct certificates to complete the SSL VPN handshake.

The most common configurations are CUCM/Unified CME with ASA self-signed certificates and

Cisco IOS self-signed certificates. Consequently, they are the easiest to configure.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM) or Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- Cisco Adaptive Security Appliance (ASA)
- Certificate types, such as self-signed, third-party, and certificate authorities

Components Used

The information in this document is based on these software and hardware versions:

- ASA Premium license.
- AnyConnect VPN phone license.
  - For ASA Release 8.0.x, the license is AnyConnect for Linksys Phone.
  - For ASA Release 8.2.x or later, the license is AnyConnect for Cisco VPN Phone.
- SSL VPN Gateway: ASA 8.0 or later (with an AnyConnect for Cisco VPN Phone License), or Cisco IOS Software Release 12.4T or later.
  - Cisco IOS Software Release 12.4T or later is not formally supported as documented in the SSL VPN Configuration Guide.
  - In Cisco IOS Software Release 15.0(1)M, the SSL VPN gateway is a seat-counted licensing feature on the Cisco 880, Cisco 890, Cisco 1900, Cisco 2900, and Cisco 3900 platforms. A valid license is required for a successful SSL VPN session.
- CallManager: CUCM 8.0.1 or later, or Unified CME 8.5 or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

> **Notes**:
>
> Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.
>
> The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Basic ASA SSL VPN Configuration

The basic ASA SSL VPN configuration is described in these documents:

- ASA 8.x: VPN Access with the AnyConnect VPN Client Using Self-Signed Certificate Configuration Example
- Configuring AnyConnect VPN Client Connections

Once this configuration is complete, a remote test PC should be able to connect to the SSL VPN gateway, connect via AnyConnect, and ping the CUCM. Ensure the ASA has an AnyConnect for Cisco IP phone license. (Use the **show ver** command.) Both TCP and UDP port 443 must be open between the gateway and the client.

> **Note**: Load-balanced SSL VPN is not supported for VPN phones.

CUCM: ASA SSL VPN with Self-Signed Certificates Configuration

Refer to IP Phone SSL VPN to ASA using AnyConnect for more detailed information.

The ASA must have a license for AnyConnect for Cisco VPN Phone. After you configure the SSL VPN, you then configure your CUCM for the VPN.

1. Use this command in order to export the self-signed certificate from the ASA:

   `ciscoasa(config)# crypto ca export trustpoint name identity-certificate` This command displays a pem-encoded identity certificate to the terminal.
2. Copy and paste the certificate to a text editor, and save it as a .pem file. Be sure to include the BEGIN CERTIFICATE and END CERTIFICATE lines, or the certificate will not import correctly. Do not modify the format of the certificate because this will cause problems when the phone tries to authenticate to the ASA.
3. Navigate to **Cisco Unified Operating System Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** in order to load the certificate file to the CERTIFICATE MANAGEMENT section of the CUCM.
4. Download the CallManager.pem, CAPF.pem, and Cisco_Manufacturing_CA.pem certificates from the same area used to load the self-signed certificates from the ASA (see Step 1), and save them to your desktop.
   1. For example, in order to import the CallManager.pem to the ASA, use these commands:

      ```
      ciscoasa(config)# crypto ca trustpoint certificate-name
      ciscoasa(config-ca-trustpoint)# enrollment terminal
      ciscoasa(config)# crypto ca authenticate certificate-name
      ```
   2. When you are prompted to copy and paste the corresponding certificate for the trustpoint, open the file you saved from the CUCM, then copy and paste the Base64-encoded certificate. Be sure to include the BEGIN CERTIFICATE and END CERTIFICATE lines (with hyphens).
   3. Type **end**, then press **Return**.
   4. When prompted to accept the certificate, type **yes**, then press **Enter**.
   5. Repeat steps 1 to 4 for the other two certificates (CAPF.pem,

Cisco_Manufacturing_CA.pem) from the CUCM.

5. Configure the CUCM for the correct VPN configurations, as described in CUCM IPphone VPN config.pdf.

   Note: The VPN gateway configured on the CUCM must match the URL that is configured on the VPN gateway. If the gateway and URL do not match, the phone cannot resolve the address, and you will not see any debugs on the VPN gateway.

- On the CUCM: The VPN gateway URL is https://192.168.1.1/VPNPhone
- On the ASA, use these commands:

```
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
```

- You can use these commands on the Adaptive Security Device Manager (ASDM) or under the connection profile.

CUCM: ASA SSL VPN with Third-Party Certificates Configuration

This configuration is very similar to the configuration described in CUCM: ASA SSLVPN with Self-Signed Certificates Configuration section, except that you are using third-party certificates. Configure SSL VPN on the ASA with third-party certificates as described in ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example.

Note: You must copy the full certificate chain from the ASA to the CUCM and include all intermediate and root certificates. If the CUCM does not include the full chain, the phones do not have the necessary certificates to authenticate and will fail the SSL VPN handshake.

Basic IOS SSL VPN Configuration

Note: IP phones are designated as not supported in IOS SSL VPN; configurations are in best effort only.

The basic Cisco IOS SSL VPN configuration is described in these documents:

- SSL VPN Client (SVC) on IOS with SDM Configuration Example
- AnyConnect VPN Client on IOS Router with IOS Zone Based Policy Firewall Configuration Example

Once this configuration is complete, a remote test PC should be able to connect to the SSL VPN gateway, connect via AnyConnect, and ping the CUCM. In Cisco IOS 15.0 and later, you must have a valid SSL VPN license to complete this task. Both TCP and UDP port 443 must be open between the gateway and the client.

CUCM: IOS SSL VPN with Self-Signed Certificates Configuration

This configuration is similar to the configuration described in CUCM: ASA SSLVPN with Third-Party Certificates Configuration and CUCM: ASA SSLVPN with Self-Signed Certificates Configuration sections. The differences are:

1. Use this command in order to export the self-signed certificate from the router:

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

2. Use these commands in order to import the CUCM certificates:

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

The WebVPN context configuration should show this text:

```
gateway webvpn_gateway domain VPNPhone
```

Configure the CUCM as described in CUCM: ASA SSLVPN with Self-Signed Certificates Configuration section.

CUCM: IOS SSL VPN with Third-Party Certificates Configuration

This configuration is similar to the configuration described in CUCM: ASA SSLVPN with Self-Signed Certificates Configuration section. Configure your WebVPN with a third-party certificate.

> **Note**: You must copy the full WebVPN certificate chain to the CUCM and include all intermediate and root certificates. If the CUCM does not include the full chain, the phones do not have the necessary certificates to authenticate and will fail the SSL VPN handshake.

Unified CME: ASA/Router SSL VPN with Self-Signed Certificates/Third-Party Certificates Configuration

Configuration for the Unified CME is similar to the configurations of the CUCM; for example, the WebVPN endpoint configurations are the same. The only significant difference is the configurations of the Unified CME call agent. Configure the VPN group and the VPN policy for the Unified CME as described in Configuring SSL VPN Client for SCCP IP Phones.

> **Note**: Unified CME supports only Skinny Call Control Protocol (SCCP) and does not support Session Initiation Protocol (SIP) for VPN phones.

> **Note**: There is no need to export the certificates from the Unified CME to the ASA or router. You only need to export the certificates from the ASA or router WebVPN gateway to the Unified CME.

In order to export the certificates from the WebVPN gateway, refer to the ASA/router section. If you are using a third-party certificate, you must include the full certificate chain. In order to import the certificates to the Unified CME, use the same method as used to import certificates into a router:

```
CME(config)# crypto pki trustpoint certificate-name
```

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

UC 520 IP Phones with SSL VPN Configuration

The Cisco Unified Communications 500 Series Model UC 520 IP phone is quite different from the CUCM and CME configurations.

- Since the UC 520 IP phone is both the CallManager and the WebVPN gateway, there is no need to configure certificates between the two.
- Configure the WebVPN on a router as you normally would with self-signed certificates or third-party certificates.
- The UC 520 IP phone has a built in WebVPN client, and you can configure it just as you would a normal PC to connect to WebVPN. Enter the gateway, then the username/password combination.
- The UC 520 IP phone is compatible with the Cisco Small Business IP Phone SPA 525G phones.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.