

Cisco Systems TLS Proxy Application Note

Version 1.0

Introduction

Application inspection allows a firewall to open pinholes and perform Network Address Translation (NAT) rewrite for Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) signaling. However, when signaling encryption is enabled, the firewall can no longer parse the signaling information and the ability to open pinholes and rewrite IP addresses for NAT is lost.

The Transport Layer Security (TLS) Proxy function allows a Cisco® ASA appliance to decrypt and re-encrypt signaling traffic, which allows it to provide application inspection services within secured unified communications environments. The TLS Proxy is transparent to voice users.

This document starts by briefly explaining how TLS works. It then explains how TLS Proxy allows the Cisco ASA appliance to be inserted into a secure unified communications architecture. It then describes how to configure Cisco Unified Communications Manager and the Cisco ASA appliance to enable the TLS Proxy feature.

It is assumed that the reader has experience configuring cryptography on Cisco Unified Communications Manager.

TLS in a Unified Communications Environment

The TLS protocol allows applications to communicate across a network in a way that is designed to prevent eavesdropping, tampering, and message forgery. TLS uses cryptography to provide endpoint authentication and communications privacy over a network.

Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure about whom they are communicating with (i.e., a user connecting to online banking).

The next level of security is known as mutual authentication, in which both parties of the "conversation" are sure about whom they are communicating with. Mutual authentication requires public key infrastructure (PKI) deployment to clients.

The Cisco Unified Communications telephony environment uses mutual authentication, meaning that a phone only communicates with an authorized Cisco Unified Communications Manager server, and Cisco Unified Communications Manager servers only communicate with authorized phones.

The current appliance versions of Cisco Unified Communications Manager do not support Simple Certificate Enrollment Protocol (SCEP) or a third-party Certificate Authority. The Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) client is used to manage the PKI. The CAPF tool is used to generate and sign locally significant certificates (LSCs) for the phones.

For more information on CAPF, go to

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/5_0_2/secucapf.html#wp1120076

When a phone attempts to establish a TLS session with Cisco Unified Communications Manager, the server is able to check the identity of the phone by checking the phone certificate, and is able to trust this certificate because it is signed by CAPF. The phone validates the identity of Cisco Unified Communications Manager through a Certificate Trust List (CTL). This file is downloaded from the Trivial File Transfer Protocol (TFTP) server and contains the certificates of the trusted elements of the Cisco Unified Communications Manager cluster.

The important point to understand for TLS Proxy is that certificates are the means by which trust is established between the different devices. The important components of a digital certificate are the key pair (private and public) and the Certificate Authority.

In summary:

- How does a phone trust Cisco Unified Communications Manager?

A Certificate Trust List (CTL) is composed offline and stored on the phones.

The phones trust all of the entities on this list.

Cisco Unified Communications Manager's certificate (X.509v3) is contained within the CTL.

Cisco Unified Communications Manager's certificate is self-signed.

- How does Cisco Unified Communications Manager trust a phone?

The phone's certificate is signed by the CAPF service. The CAPF certificate is installed in the Cisco Unified Communications Manager certificate store.

When a phone registers, its certificate is stored in a dynamic trust list on Cisco Unified Communications Manager.

TLS Proxy Solution

When using TLS Proxy, the Cisco ASA appliance is inserted between the phones and Cisco Unified Communications Manager. The phones will now establish a TLS session with the ASA appliance. The appliance will, in turn, establish a proxy TLS connection with Cisco Unified Communications Manager on the phone's behalf. This function generates two TLS sessions (Figure 1).

Figure 1. TLS Sessions



For correct operation of the TLS Proxy feature, phones and Cisco Unified Communications Manager need to trust the Cisco ASA appliance, and the appliance needs to trust them.

Trusted Relationship between a Cisco Unified IP Phone and the Cisco ASA Adaptive Security Appliance

- The Cisco ASA appliance presents a certificate to the phone on behalf of Cisco Unified Communications Manager.

- The certificate is generated on the Cisco ASA appliance. This certificate can be self-signed like the original one from Cisco Unified Communications Manager, or signed by an external Certificate Authority.
- The certificate will be pushed to the phone in the CTL so the phone can trust the ASA appliance. The CTL client is used to add the ASA appliance's certificate to the trust list.
- The ASA administrator needs to create a trust point for the Certificate Authority that issued phone's certificate (CAPF).

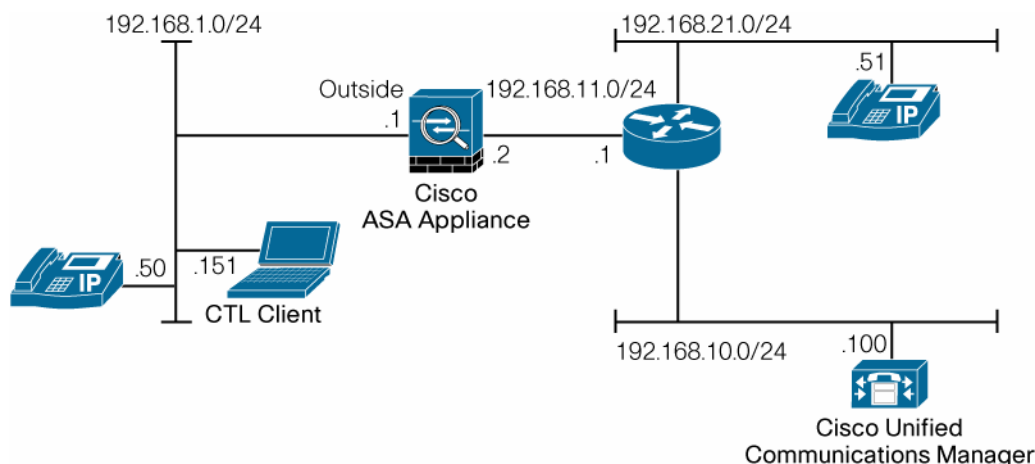
Trusted Relationship Between Cisco Unified Communications Manager and the Cisco ASA Adaptive Security Appliance

- The Cisco ASA appliance presents a unique certificate to Cisco Unified Communications Manager on behalf of the phone. Phone certificates are dynamically created by the ASA appliance and are called local dynamic certificates (LDCs).
- In order to for Cisco Unified Communications Manager to trust the ASA appliance certificates, it needs to trust the Certificate Authority that signed them.
- The system administrator configures a Certificate Authority on the ASA appliance whose role will be to sign the LDCs. The Certificate Authority certificate is uploaded into Cisco Unified Communications Manager's certificate store, which allows the establishment of a trust relationship between Cisco Unified Communications Manager and the ASA appliance.
- The system administrator also creates a trust point on the ASA appliance so it trusts Cisco Unified Communications Manager. The trust points for both Cisco Unified Communications Manager and CAPF may be created manually or installed by the CTL provider on the ASA appliance (described in the next section).

TLS Proxy Lab Overview

The schematic of the lab used for the TLS Proxy is configured below. The ASA and Cisco Unified Communications Manager code releases used were Cisco ASA Software Release 8.0(2) and Cisco Unified Communications Manager 6.0, respectively.

Figure 2. TLS Proxy Lab Configuration



Two phone models were used in the lab: a Cisco Unified IP Phone 7970 with a manufacturing installed certificate and a Cisco Unified IP Phone 7940 with an LSC generated using the Cisco Unified Communications Manager CAPF tool.

TLS Proxy Configuration

Following are instructions on how to configure TLS Proxy from the Cisco ASA appliance command-line interface (CLI).

Step 1. Create RSA key pairs on the Cisco ASA appliance

```
hostname(config)# crypto key generate rsa label ccm_proxy_key modulus
1024
hostname(config)# crypto key generate rsa label ldc_signer_key modulus
1024
hostname(config)# crypto key generate rsa label phone_common modulus
1024
```

This creates the cryptographic material to be used for generating certificates.

The first entry is used to create the **CCM_proxy** Certificate Authority trust point. Its certificate will be presented to the phone on behalf of Cisco Unified Communications Manager (Step 2).

The second entry is used to create the **LDC_server** Certificate Authority trust point and is used to sign the LDC certificates presented to Cisco Unified Communications Manager (Step 3).

The third entry is used to create all the LDCs (Step 5).

Step 2. Create the proxy certificate for the Cisco Unified Communications Manager cluster

```
hostname(config)# ! for self-signed CCM proxy certificate
hostname(config)# crypto ca trustpoint ccm_proxy
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# fqdn none
hostname(config-ca-trustpoint)# subject-name cn=tlspoxytest
hostname(config-ca-trustpoint)# keypair ccm_proxy_key
hostname(config)# crypto ca enroll ccm_proxy
```

The Certificate Authority trust point is used to present a certificate to the phone on behalf of Cisco Unified Communications Manager (configured in Step 5).

This is the proxy Cisco Unified Communications Manager certificate. It is self-signed (enrollment self).

The fully qualified domain name (FQDN) is not really used; it can be left as "none."

The subject name has to be configured but doesn't have any real significance. However, Cisco Unified IP Phones require certain fields from the X.509v3 certificate to be present to validate the certificate by consulting the CTL file. The subject name must be composed of the ordered concatenation of the CN, OU, and O fields. The CN field is mandatory; the others are optional.

The concatenated fields (when present) are separated by a semicolon, yielding one of the following forms:

```
CN=xxx;OU=yyy;O=zzz
CN=xxx;OU=yyy
```

```
CN=xxx;O=zzz
CN=xxx
```

This certificate is exported to the CTL. The relevant configuration parameters are specified within the **ctl-provider** subcommand (Step 4).

Step 3. Create an internal local Certificate Authority to sign the LDC for Cisco Unified IP Phones

```
hostname(config)# ! for the internal local LDC issuer
hostname(config)# crypto ca trustpoint ldc_server
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# proxy-ldc-issuer
hostname(config-ca-trustpoint)# fqdn my_ldc_ca.exmaple.com
hostname(config-ca-trustpoint)# subject-name cn=tlspoxytest
hostname(config-ca-trustpoint)# keypair ldc_signer_key
hostname(config)# crypto ca enroll ldc_server klc
```

These commands create the Certificate Authority trust point that is used to sign the LDCs presented to Cisco Unified Communications Manager on behalf of each phone (Step 5).

Proxy-ldc-issuer defines the local Certificate Authority role for the trust point to issue dynamic certificates for TLS Proxy. This command can only be configured under a trust point with “enrollment self”.

The FQDN is not really used; it can be left as “none.”

The subject name has to be configured but doesn't have any real significance.

The certificate has to be imported manually to Cisco Unified Communications Manager to allow Cisco Unified Communications Manager to trust the LDCs presented by the Cisco ASA appliance (Step 7).

Step 4. Create a CTL provider instance in preparation for a connection from the CTL client

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface outside address
192.168.1.151
hostname(config-ctl-provider)# client username admin password XXXXXX
encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

This configuration lets the ASA appliance accept a connection from the CTL client. For security reasons, the configuration defines which hosts are able to connect; in a production environment, numerous clients may be configured. In this lab environment, the CTL client was connected on the outside interface. In a production environment, we recommend connecting it from the inside interface for security reasons.

The username and password must match the Cisco Unified Communications Manager credentials.

The syntax specifies which certificate will be exported to the phones (created in Step 2) using the **export certificate** command. When the CTL client connects, it will retrieve the certificate and add it to the list of servers in the CTL.

The "CTL install" command tells the ASA appliance to parse the CTL file provided by the CTL client and install trust points. The trust points installed are those for the Cisco Unified Communications Manager server and CAPF. Any trust points installed by this command will have names prefixed with "**_internal_CTL_<ctl_name>**". This is an optional command and is enabled by default. If this command is disabled, each Cisco Unified Communications Manager server's and CAPF's certificate must be manually imported and installed using the **crypto ca trustpoint** and **crypto ca authenticate** commands.

By default, the connection will be made on port 2444; however, it can be changed with the service port **<listening_port>** command. This port number must match the one configured on Cisco Unified Communications Manager (defined under Enterprise Parameters on the Unified Communications Manager administration page).

Step 5. Create a TLS Proxy instance

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1
```

The **server trust point** specifies the proxy trustpoint certificate that is presented to the phones during the TLS handshake (created in Step 2). This is the certificate that was added to the CTL in Step 4.

Client ldc issuer defines the Certificate Authority that issues the dynamic certificates to Cisco Unified Communications Manager on behalf of the phones. This is the certificate created in Step 3.

Client ldc keypair specifies which key pair to use to create the LDCs. It should be noted that the same pair is used for all the LDCs. This key pair was created in Step 1.

Client cipher-suite defines the cipher suite that is announced during the TLS handshake. These are used to replace the original ciphers in the phone's Hello message to Cisco Unified Communications Manager. This allows the system administrator to configure asymmetric encryption. For example, if the link between the ASA appliance and Cisco Unified Communications Manager was over a trusted network, a weaker cipher could be used between the ASA appliance and Cisco Unified Communications Manager to reduce the overhead on Cisco Unified Communications Manager. However, a NULL cipher is not currently supported with the version tested.

The LDCs are created dynamically.

Step 6. Enable TLS Proxy in SCCP or SIP inspection

```
hostname(config)# class-map sec_skinny
hostname(config-cmap)# match port tcp eq 2443
```

This syntax defines which specific type of traffic the Cisco ASA appliance will inspect for a specific class. In this case, the system matches all the TCP traffic for port 2443 (secure SCCP signaling).

```
hostname(config)# policy-map type inspect skinny skinny_inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ! Skinny inspection parameters
```

Entering the above creates a new inspection map for SCCP. This allows the administrator to tune the default inspection "rules" he/she may want to enforce, such as RTP conformance, signaling timeout, media timeout, registration, or filtering the message ID. The lab used default parameters.

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class sec_skinny
hostname(config-pmap-c)# inspect skinny skinny_inspect tls-proxy
my_proxy
```

With these commands, the system adds a new class **sec_skinny** to the policy **global_policy**. It specifies that the inspection map **skinny_inspect** created during the previous step is used for the new class. The optional **tls-proxy** attribute enables the TLS Proxy feature and identifies which TLS Proxy instance to use (in this case, **my_proxy** created in Step 5).

```
hostname(config)# service-policy global_policy global
```

This configures the **global_policy** to be used by the Cisco ASA appliance.

Step 7. Export the local Certificate Authority certificate (ldc_server) and install it as a trusted certificate on the Cisco Unified Communications Manager server

To allow Cisco Unified Communications Manager to trust the proxy phone certificates created dynamically by the ASA appliance, the certificate of the Certificate Authority created on the ASA appliance needs to be imported into Cisco Unified Communications Manager. Use the following command to display the certificate on the screen:

```
hostname(config)# crypto ca export ldc_server identity-certificate (replace
ldc_server by the name that was used in Step 2)
```

```
-----BEGIN CERTIFICATE-----
MIICVTCCAb6gAwIBAgIBMTANBgkqhkiG9w0BAQQFADA+MRUwEwYDVQQDEwxbHNw
cm94eXRlc3QxJTAjBgkqhkiG9w0BCQIWFnRsc3Byb3h5dGVzdC5jaXNjb3Y5b20w
HhcNMDcxMjIwMTAxODU0WWhcNMTcxMjE3MTAxODU0WjA+MRUwEwYDVQQDEwxbHNw
cm94eXRlc3QxJTAjBgkqhkiG9w0BCQIWFnRsc3Byb3h5dGVzdC5jaXNjb3Y5b20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM6NnAGdWkjedL/bfXVf0yEGet2c
BzpPyZg/pCLyqX/bFVzVS7jqU0cKDExxZX9mdezBANgyp0JMMwMD0lvf9z/j0Dcl
d5LDdzlKfwsxH8fx7FcPLcee1ea8acIfiFhM/Fh+tkT9XYU920W+TzRbj0bluojz
9roITuGbPfmrXDKPAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBaAFBstSKYak3Bx1q1Kcrnh94n0D66DMB0GA1UdDgQW
```

```

BBQbLbCmGitwcdatSnK54feJzg+ugzANBgkqhkiG9w0BAQQFAA0BgQB2GvvEM7IS
SqPVi9h8SUoQaZup+ONnw5b1JMyURm80Xm37dpZTf/1PQVRuR2xyid1vsbF7jQHE
JAZHnogI5JepqxmUuqCUBXv2zTRDSGLKLNHX6AfwQFUKs6hEZkKV3o+UKh1/B1K
6FG8rsH1Ckgny7jhud3zR5XiKyUkNSVFLw==
-----END CERTIFICATE-----

```

Copy the output, including the “Begin Certificate” and “End Certificate” lines, to a text file.

Step 1 Under **CUCM OS administration** page, **Navigate to Security>Certificate Management>**

Step 2 Select **Upload Certificate**

Step 3 Select *CallManager-trust* under **Certificate name**

Step 4 Click **Browse** and navigate to the ASA certificate

Step 5 To upload the certificate, click **Upload**

Step 8. Configure the CTL client

Run the CTL client on one of the machines that was defined on the Cisco ASA appliance in Step 4. If the CTL client is not on this machine, it can be downloaded from Cisco Unified Communications Manager under the CUCM administration page by selecting Application/plugins. Click Find, then Download. Alternatively, go directly to:

```

https://x.x.x.x:8443/plugins/CiscoCTLClient.exe
(where x.x.x.x is the IP address of Cisco Unified Communications
Manager)

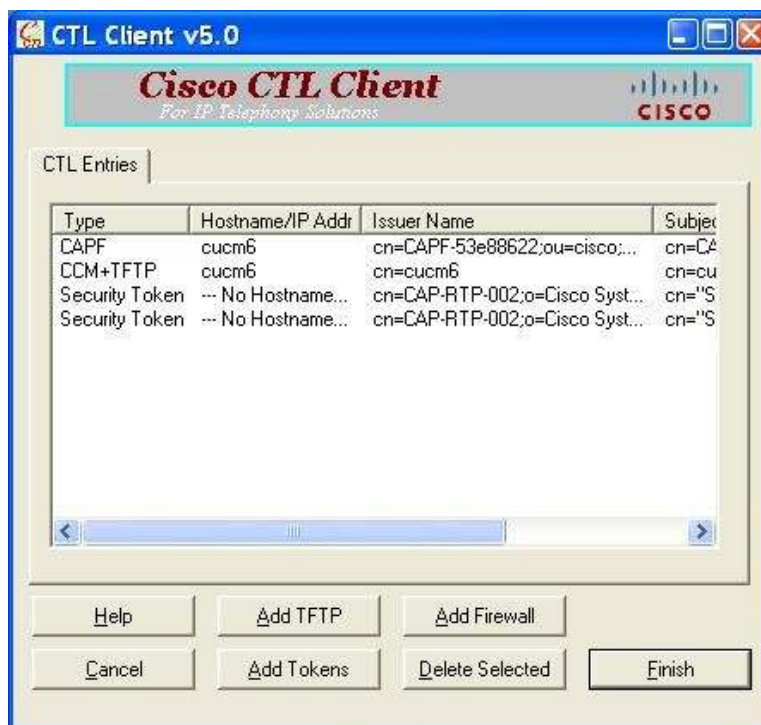
```

Run the CTL client application to add the server proxy certificate (**ccm_proxy**) to the CTL file and install the CTL file on the security appliance. Refer to the Cisco Unified Communications Manager document to learn how to configure and use the CTL client http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sec_vir/ae/sec504/secuauth.htm.

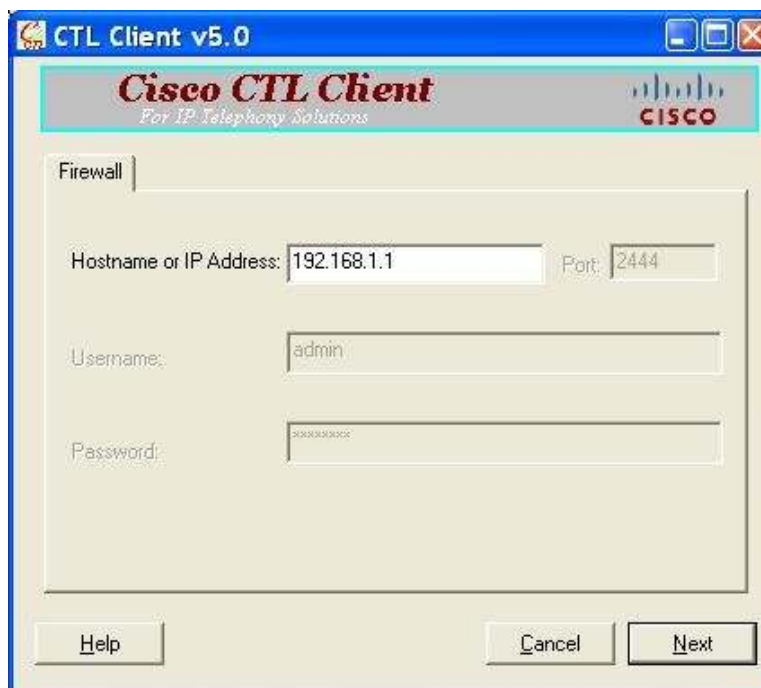
One of the USB security tokens used to initially configure the CTL client will be required to update it.

In the following diagram, the CTL client contains the two security tokens that were used to turn on Cisco Unified Communications Manager security, the certificate for CAPF, and the certificate for Cisco Unified Communications Manager and TFTP.

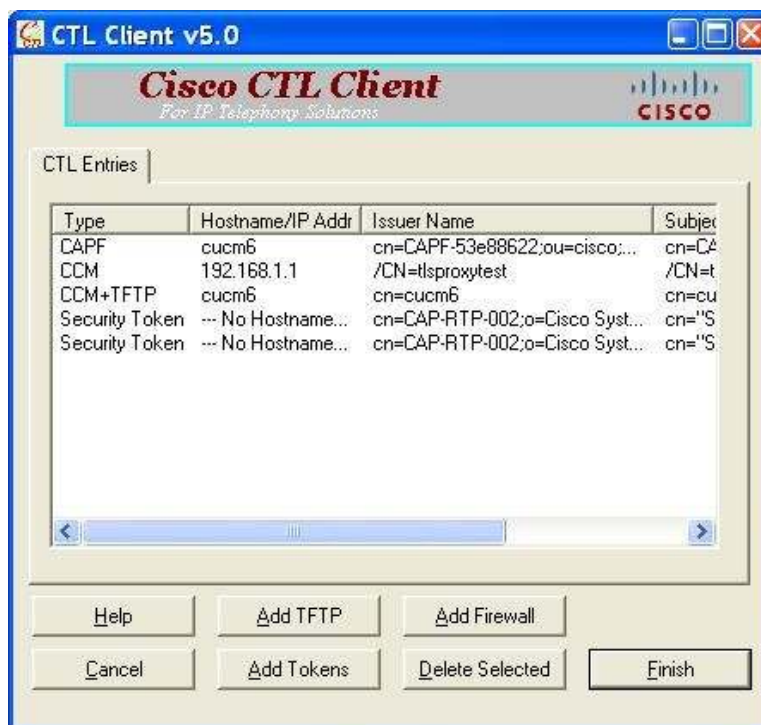
Select **Add Firewall**.



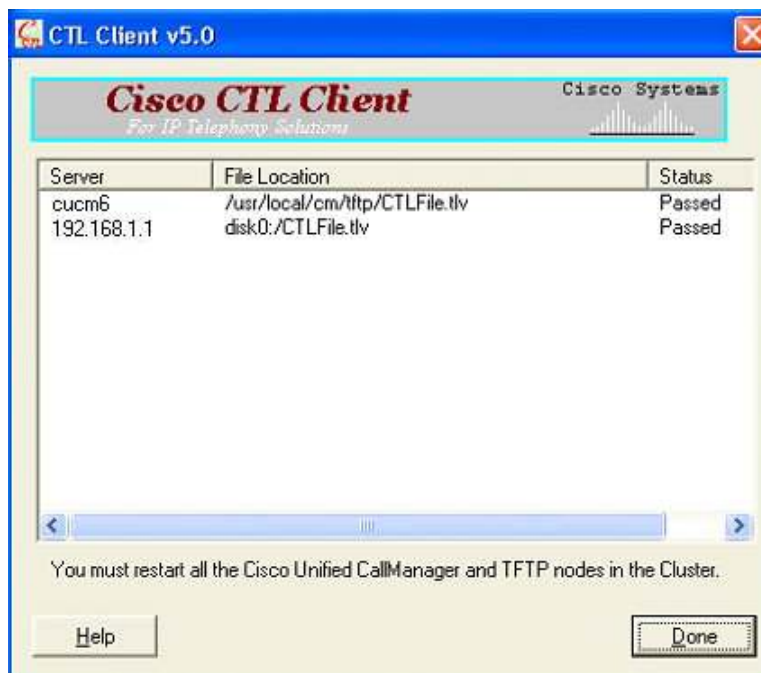
Provide the IP address or the name of the Cisco ASA appliance. Ensure the host used to run the CTL client is able to resolve the name of Cisco Unified Communications Manager and that the IP address is reachable. It should be the IP address of the interface that was used while configuring the CTL provider in Step 4. The login and the password must be the same as the one configured on the ASA appliance in Step 4.



As can be seen in the following screenshot, the Cisco ASA appliance is added as a Cisco Unified Communications Manager. This is because the ASA appliance is acting as a proxy Cisco Unified Communications Manager for the phones.



The CTL will also be downloaded to the ASA appliance so it can be parsed to configure the CAPF and Cisco Unified Communications Manager as Certificate Authority trust points. This is shown in the following screenshot:



The reference that was used for the Cisco ASA appliance configuration can be found at <http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/inspect.html#wp1529598>.

Appendix

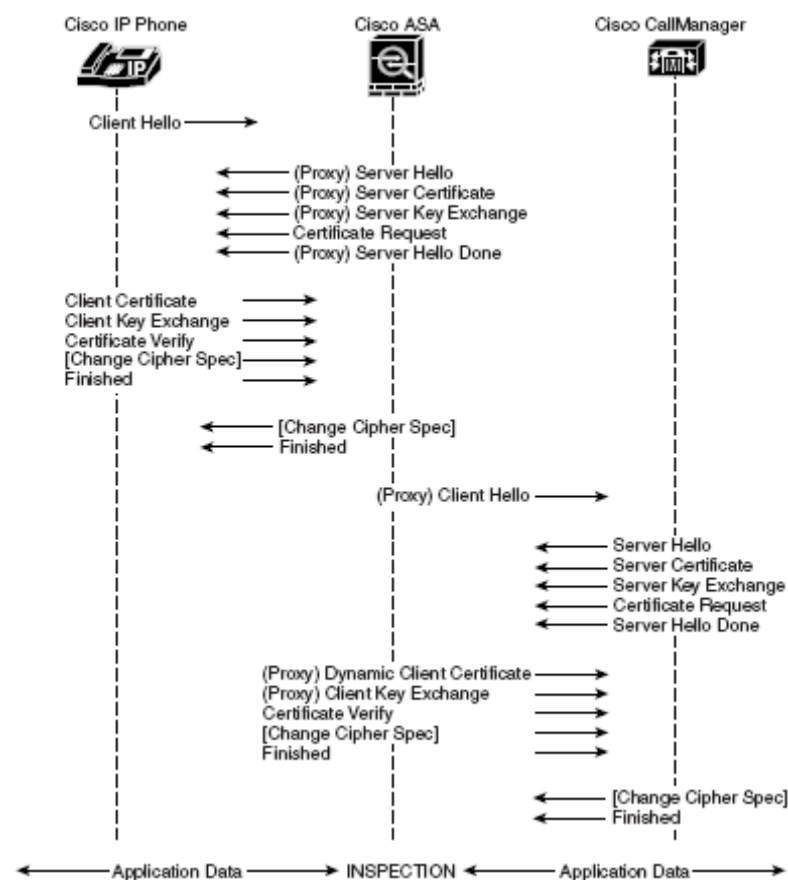
Performances

Table 1.

Firewall	Default Sessions	Maximum Sessions
ASA 5505	10	80
ASA 5510	100	200
ASA 5520	300	1200
ASA 5540	1000	4500
ASA 5550	2000	4500
ASA 5580	4000	13,000

Signaling Flow for the TLS Handshake

Figure 3. TLS Handshake Diagram



Sample Configuration

Cisco ASA Software Version 8.0(2)

```
hostname ciscoasa
domain-name tlsproxytest.cisco.com
enable password whatever encrypted
```

```
names
name 192.168.10.100 CCM6
!
interface Vlan1
  nameif inside
  security-level 100
  ip address 192.168.11.2 255.255.255.0
!
interface Vlan2
  nameif outside
  security-level 0
  ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
  shutdown
!
interface Ethernet0/3
  shutdown
!
interface Ethernet0/4
  shutdown
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
passwd whatever encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
  domain-name tlsproxystest.cisco.com
object-group protocol TCPUDP
  protocol-object udp
  protocol-object tcp
access-list inside_access_in extended permit ip any any
access-list inside_access_in extended deny ip any any
access-list outside_access_in remark Access to CUP server
access-list outside_access_in extended permit tcp host 192.168.1.51
range 1 65000 host 192.168.10.110 eq 8081
access-list outside_access_in remark Access to CUCM list of services
access-list outside_access_in extended permit tcp 192.168.1.0
255.255.255.0 range 1 65000 host CCM6 eq 8080
```

```
access-list outside_access_in extended permit tcp host 192.168.1.111
range 1 65535 host CCM6 eq sip
access-list outside_access_in remark allow SIP
access-list outside_access_in extended permit udp any host CCM6 eq sip
access-list outside_access_in extended permit tcp 192.168.1.0
255.255.255.0 range 1 65000 host CCM6 eq 3804
access-list outside_access_in extended permit udp host 192.168.1.51
range 1 65000 any inactive
access-list outside_access_in extended permit tcp host 192.168.1.50
range 1 65000 host CCM6 eq 3804
access-list outside_access_in extended permit ip any any inactive
access-list outside_access_in extended permit tcp host 192.168.1.151
range 1 65255 host CCM6 eq 2444
access-list outside_access_in remark phone boot connection
access-list outside_access_in extended permit tcp any range 1 65355
host CCM6 eq 2443
access-list outside_access_in extended permit udp host 192.168.1.50
host 192.168.21.51 inactive
access-list outside_access_in extended permit udp any host
192.168.10.10 eq domain
access-list outside_access_in remark permit skinny
access-list outside_access_in extended permit tcp any host CCM6 eq
2000
access-list outside_access_in remark access to CCM6 management
access-list outside_access_in extended permit tcp any host CCM6 eq
8443
access-list outside_access_in extended permit udp any host CCM6 eq
tftp
access-list outside_access_in extended permit ip host 192.168.1.151
any
access-list outside_access_in extended deny ip any any log warnings
access-list global_mpc extended permit object-group TCPUDP any any eq
sip
pager lines 24 logging enable
logging timestamp
logging list loglist message 711001
logging list loglist message 725001-725014
logging list loglist message 717001-717038
logging buffer-size 1000000
logging console loglist
logging trap debugging
logging asdm debugging
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
route inside 0.0.0.0 0.0.0.0 192.168.11.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

```

timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.11.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ca trustpoint ccm_proxy
enrollment self
  fqdn none
  subject-name cn=tlspoxytest
  keypair ccm_proxy_key
  crl configure
crypto ca trustpoint ldc_server
enrollment self
  fqdn tlspoxytest.cisco.com
  subject-name cn=tlspoxytest
  keypair ldc_signer_key
  proxy-ldc-issuer
  crl configure
crypto ca trustpoint _internal_CTL_my_ctl_cn=cucm6
enrollment terminal
  crl configure
crypto ca trustpoint _internal_CTL_my_ctl_cn=CAPF-
53e88622;ou=cisco;o=cisco
enrollment terminal
  crl configure
crypto ca certificate chain ccm_proxy
certificate 31
  308201a2 3082010b a0030201 02020131 300d0609 2a864886 f70d0101
04050030
  17311530 13060355 0403130c 746c7370 726f7879 74657374 301e170d
30373132
  32303130 30313132 5a170d31 37313231 37313030 3131325a 30173115
30130603
  55040313 0c746c73 70726f78 79746573 7430819f 300d0609 2a864886
f70d0101
  01050003 818d0030 81890281 8100ca87 eae574c0 5b160d70 e14cab9a
ccaecb67
  a913a5f8 8745d6d7 0fb9d33c a48c807c 9adf5172 e8b6064f a084334f
0e872d53
  89801969 466bcd0d 33ac62bd eafc142a cbd00184 075c4c35 d846a283
5806ff36
  4fe8930b 80104533 720f5a3b 607320fb cff1c116 deb92b35 98129560
09a33e4f
  7dc9dc6d 02e97a73 5ecc3753 f8270203 01000130 0d06092a 864886f7
0d010104

```

```
05000381 8100c4d7 f87ec703 3233b427 f3b08c56 4b852960 713b043a
ce04ca77
48e642db 5d38c849 c35292d4 c832c916 bdbb01ac c93f5a64 1847e910
0dd1eeea
38ce2bc2 e180f979 5ef2728e 1d9f4d65 aab2b0e8 dbd96e8d f97a31d7
827e659e
dee02a7a 82862ef2 980cd6ca a403fc52 d4061a58 cc4c97d0 8575ad7e
7ab5e482
a33e6244 d9cd
quit
crypto ca certificate chain ldc_server
certificate 31
30820255 308201be a0030201 02020131 300d0609 2a864886 f70d0101
04050030
3e311530 13060355 0403130c 746c7370 726f7879 74657374 31253023
06092a86
4886f70d 01090216 16746c73 70726f78 79746573 742e6369 73636f2e
636f6d30
1e170d30 37313232 30313031 3835385a 170d3137 31323137 31303138
35385a30
3e311530 13060355 0403130c 746c7370 726f7879 74657374 31253023
06092a86
4886f70d 01090216 16746c73 70726f78 79746573 742e6369 73636f2e
636f6d30
819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100
ce8d9c01
9d5a48de 74bdfdb7d 755f3b21 067add9c 073a4fc9 983fa422 f2a97fdb
155cd54b
b8ea5347 0a0c4c57 657f6675 ecc10271 b2a7424c 9b0303d2 5bdf7f3f
e3383725
7792c377 394a7f0b 311fc7f1 ec570f2d c79ed5e6 bc69c21f 88584cfc
587eb644
fd5d853d d8e5be4f 345b8ce6 e5ba88f3 f6ba084e e19b3df9 ab5c328f
02030100
01a36330 61300f06 03551d13 0101ff04 05300301 01ff300e 0603551d
0f0101ff
04040302 0186301f 0603551d 23041830 1680141b 2db0a61a 2b7071d6
ad4a72b9
e1f789ce 0fae8330 1d060355 1d0e0416 04141b2d b0a61a2b 7071d6ad
4a72b9e1
f789ce0f ae83300d 06092a86 4886f70d 01010405 00038181 00761afb
c433b212
4aa3d58b d87c494a 10699ba9 f8e3675b 96e524cc 94466f34 5e6dfb76
96537ff9
4f41546e 476c7289 dd6fb1b1 7b8d01c4 2406479e 8808e497 a9ab1994
baa094ac
15efdb34 d10d218b 28b3475f a01fc101 542acea1 11990a57 7a3e50a8
65fc194a
e851bcae c1f50a48 27cbb8e1 b9ddf347 95e22b25 24352545 2f
quit
crypto ca certificate chain _internal_CTL_my_ctl_cn=cucm6
certificate ca 7238e20f3e56fe65
3082020d 30820176 a0030201 02020872 38e20f3e 56fe6530 0d06092a
864886f7
0d010105 05003010 310e300c 06035504 03130563 75636d36 301e170d
30373132
```

```
32303032 34393039 5a170d31 32313232 30303234 3930395a 3010310e
300c0603
55040313 05637563 6d363081 9f300d06 092a8648 86f70d01 01010500
03818d00
30818902 818100b6 7d7d0a9c a88877c4 270eaf0f d93449b9 b748762e
3a02399d
f8ff21b0 0146b7d0 9c2a755e 7dd1aed4 f0071cd8 bfd6c540 91a58e26
c6416a36
c38f5f7e 925ec32a b3cbeccf a15584b0 cb85174d 6ddfb7e0 8d465705
8ab79df1
0b7aa195 527087c6 711a1e65 46d0970b 92dd2166 de5bfefe d8a3a80b
b1bd27af
d217a98e bbd02702 03010001 a370306e 300b0603 551d0f04 04030202
bc302706
03551d25 0420301e 06082b06 01050507 03010608 2b060105 05070302
06082b06
01050507 03053017 0603551d 11041030 0e860c73 69703a43 4e3d6375
636d3630
1d060355 1d0e0416 041452b9 e2d495cf 987f9ad0 eb2484d8 6a5c0f6b
e03a300d
06092a86 4886f70d 01010505 00038181 009fcfd7 54ce1d2a 707c766c
5ba83104
362b33f8 65cf1034 5d960d97 93ad724b 956d8e2f 647b1c5a 9acb6070
556dd5da
68aa5c3a d10ce388 1527a919 12079074 40f95acf 48290fee 312fb570
6cddd727
e1357109 f512efd3 46299581 ec0bdb8a 85677e6a b243a83e 2b1b479a
d1679a95
9e5df9d4 d72ff98a 4465b69f 5b407b33 39
quit
crypto ca certificate chain _internal_CTL_my_ctl_cn=CAPF-
53e88622;ou=cisco;o=cisco
certificate ca 77096b00cbc79410
30820294 308201fd a0030201 02020877 096b00cb c7941030 0d06092a
864886f7
0d010105 05003065 310e300c 06035504 0a130563 6973636f 310e300c
06035504
08130563 6973636f 310e300c 06035504 07130563 6973636f 310b3009
06035504
06130247 42311630 14060355 0403130d 43415046 2d353365 38383632
32310e30
0c060355 040b1305 63697363 6f301e17 0d303731 32323030 32343931
365a170d
31323132 32303032 34393136 5a306531 0e300c06 0355040a 13056369
73636f31
0e300c06 03550408 13056369 73636f31 0e300c06 03550407 13056369
73636f31
0b300906 03550406 13024742 31163014 06035504 03130d43 4150462d
35336538
38363232 310e300c 06035504 0b130563 6973636f 30819f30 0d06092a
864886f7
0d010101 05000381 8d003081 89028181 00b1e21b 4a2e2b57 26b4b849
433058a8
277459cb ed300c37 0bc4befa 1a9e8c7d 5b3ca891 208bf6fe 38f67995
50291c49
dad78df2 3b8f58e3 9ae1a1de ad23d8ce 690dddc0 778475b8 eeb117e1
56832618
```

```

a12eff01 cccfa662 a287854e 40b60300 d6af0626 1180d1cc 622aee4a
73e5cfa5
f9addeb5 604daa25 9dd02f58 00f7a449 47020301 0001a34d 304b300b
0603551d
0f040403 02028430 1d060355 1d250416 30140608 2b060105 05070301
06082b06
01050507 0305301d 0603551d 0e041604 14297e66 29220fc0 b94e7293
486dee43
557a5027 ff300d06 092a8648 86f70d01 01050500 03818100 a98f4bb4
b4660425
a69cfde2 a46fa532 8dea8dfb 7b4bbcfb 6ce69878 e0df75c0 6957349a
0741420d
aaaa7798 fb5737ad a34d52cb dcf76706 24bc3d71 178523a2 f2c67c6e
4a921e0a
af5b3ed7 2a69189f 7887ee48 0b4c1df9 47e41422 ed9612f8 3ef0c13c
5260402a
526af832 814694f6 14dc7fcd 5fb634cb b58906b6 25d8953b
quit
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpcd address 192.168.1.51-192.168.1.60 outside
dhcpcd dns 192.168.10.10 interface outside
dhcpcd domain tlsproxytest.cisco.com interface outside
dhcpcd option 150 ip CCM6 interface outside
dhcpcd enable outside!

!
tls-proxy my_proxy
server trust-point ccm_proxy
client ldc issuer ldc_server
client ldc key-pair phone_common
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 des-sha1 null-
sha1
no threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
ssl encryption aes128-sha1 aes256-sha1 rc4-sha1
!
ctl-provider my_ctl
client interface outside address 192.168.1.151
client username admin password /YyLq098TvZD3GNj encrypted
export certificate ccm_proxy
!
!
class-map sec_skinny
match port tcp eq 2443
class-map inspection_default
match default-inspection-traffic
!

```

```
!  
policy-map type inspect dns preset_dns_map  
  parameters  
    message-length maximum 512  
policy-map type inspect skinny skinny_inspect  
  parameters  
policy-map global_policy  
  class inspection_default  
    inspect dns preset_dns_map  
    inspect esmtp  
    inspect ftp  
    inspect h323 h225  
    inspect h323 ras  
    inspect netbios  
    inspect rsh  
    inspect rtsp  
    inspect skinny  
    inspect sqlnet  
    inspect sunrpc  
    inspect tftp  
    inspect xdmcp  
  class sec_skinny  
    inspect skinny skinny_inspect tls-proxy my_proxy  
!  
service-policy global_policy global  
prompt hostname context
```



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0804R)