CHAPTER 46

Configuring Cisco Mobility Advantage

This chapter describes how to configure the adaptive security appliance for Cisco Unified Communications Mobility Advantage Proxy features.

This chapter includes the following sections:

Information about the Cisco Mobility Advantage Proxy Feature

This section contains the following topics:

Cisco Mobility Advantage Proxy Functionality

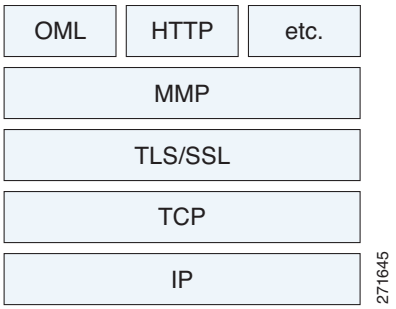
To support Cisco UMA for the Cisco Mobility Advantage solution, the mobility advantage proxy (implemented as a TLS proxy) includes the following functionality:

- The ability to allow no client authentication during the handshake with clients.
- Allowing an imported PKCS-12 certificate to server as a proxy certificate.

The adaptive security appliance includes an inspection engine to validate the Cisco UMA Mobile Multiplexing Protocol (MMP).

MMP is a data transport protocol for transmitting data entities between Cisco UMA clients and servers. As shown in Figure 46-1, MMP must be run on top of a connection-oriented protocol (the underlying transport) and is intended to be run on top of a secure transport protocol such as TLS. The Orative Markup Language (OML) protocol is intended to be run on top of MMP for the purposes of data synchronization, as well as the HTTP protocol for uploading and downloading large files.

Figure 46-1 MMP Stack



The TCP/TLS default port is 5443. There are no embedded NAT or secondary connections.

Cisco UMA client and server communications can be proxied via TLS, which decrypts the data, passes it to the inspect MMP module, and re-encrypt the data before forwarding it to the endpoint. The inspect MMP module verifies the integrity of the MMP headers and passes the OML/HTTP to an appropriate handler. The adaptive security appliance takes the following actions on the MMP headers and data:

- Verifies that client MMP headers are well-formed. Upon detection of a malformed header, the TCP session is terminated.
- Verifies that client to server MMP header lengths are not exceeded. If an MMP header length is exceeded (4096), then the TCP session is terminated.
- Verifies that client to server MMP content lengths are not exceeded. If an entity content length is exceeded (4096), the TCP session is terminated.

Note 4096 is the value currently used in MMP implementations.

Because MMP headers and entities can be split across packets, the adaptive security appliance buffers data to ensure consistent inspection. The SAPI (stream API) handles data buffering for pending inspection opportunities. MMP header text is treated as case insensitive and a space is present between header text and values. Reclaiming of MMP state is performed by monitoring the state of the TCP connection.

Mobility Advantage Proxy Deployment Scenarios

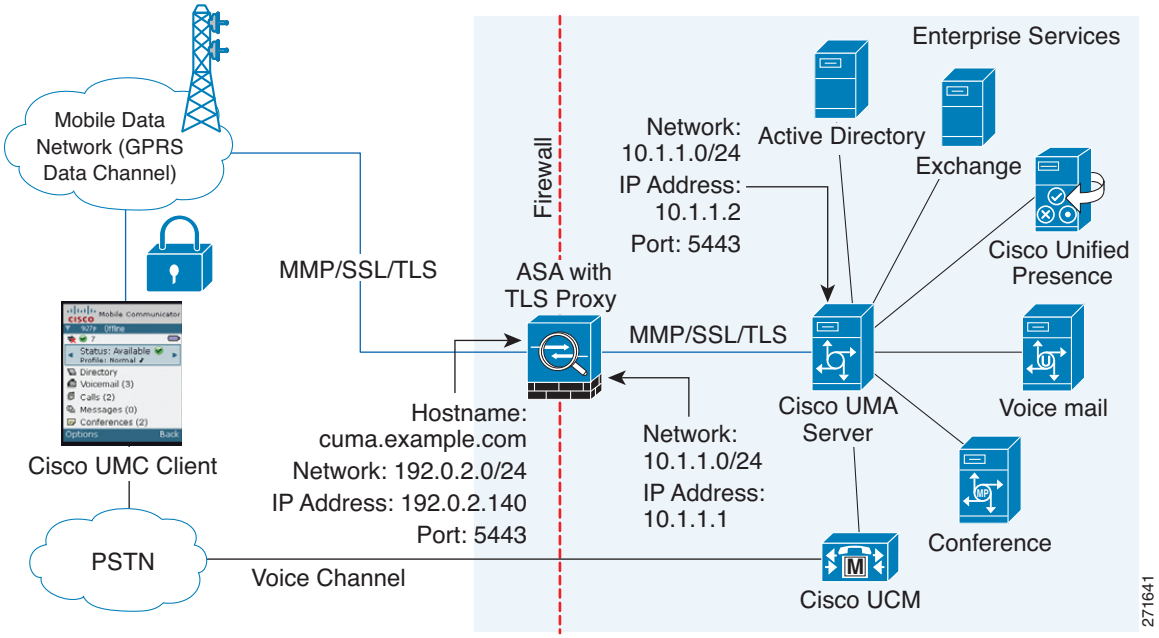
Figure 46-2 and Figure 46-3 show the two deployment scenarios for the TLS proxy used by the Cisco Mobility Advantage solution. In scenario 1 (the recommended deployment architecture), the adaptive security appliance functions as both the firewall and TLS proxy. In scenario 2, the adaptive security appliance functions as the TLS proxy only and works with an existing firewall. In both scenarios, the clients connect from the Internet.

In the scenario 1 deployment, the adaptive security appliance is between a Cisco UMA client and a Cisco UMA server. The Cisco UMA client is an executable that is downloaded to each smartphone. The Cisco UMA client applications establishes a data connection, which is a TLS connection, to the corporate Cisco UMA server. The adaptive security appliance intercepts the connections and inspects the data that the client sends to the Cisco UMA server.

Note The TLS proxy for the Cisco Mobility Advantage solution does not support client authentication because the Cisco UMA client cannot present a certificate. The following commands can be used to disable authentication during the TLS handshake.

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# no server authenticate-client
```

Figure 46-2 Security Appliance as Firewall with Mobility Advantage Proxy and MMP Inspection



In Figure 46-2, the adaptive security appliance performs static NAT by translating the Cisco UMA server 10.1.1.2 IP address to 192.0.2.140.

Figure 46-3 shows deployment scenario 2, where the adaptive security appliance functions as the TLS proxy only and does not function as the corporate firewall. In this scenario, the adaptive security appliance and the corporate firewall are performing NAT. The corporate firewall will not be able to predict which client from the Internet needs to connect to the corporate Cisco UMA server. Therefore, to support this deployment, you can take the following actions:

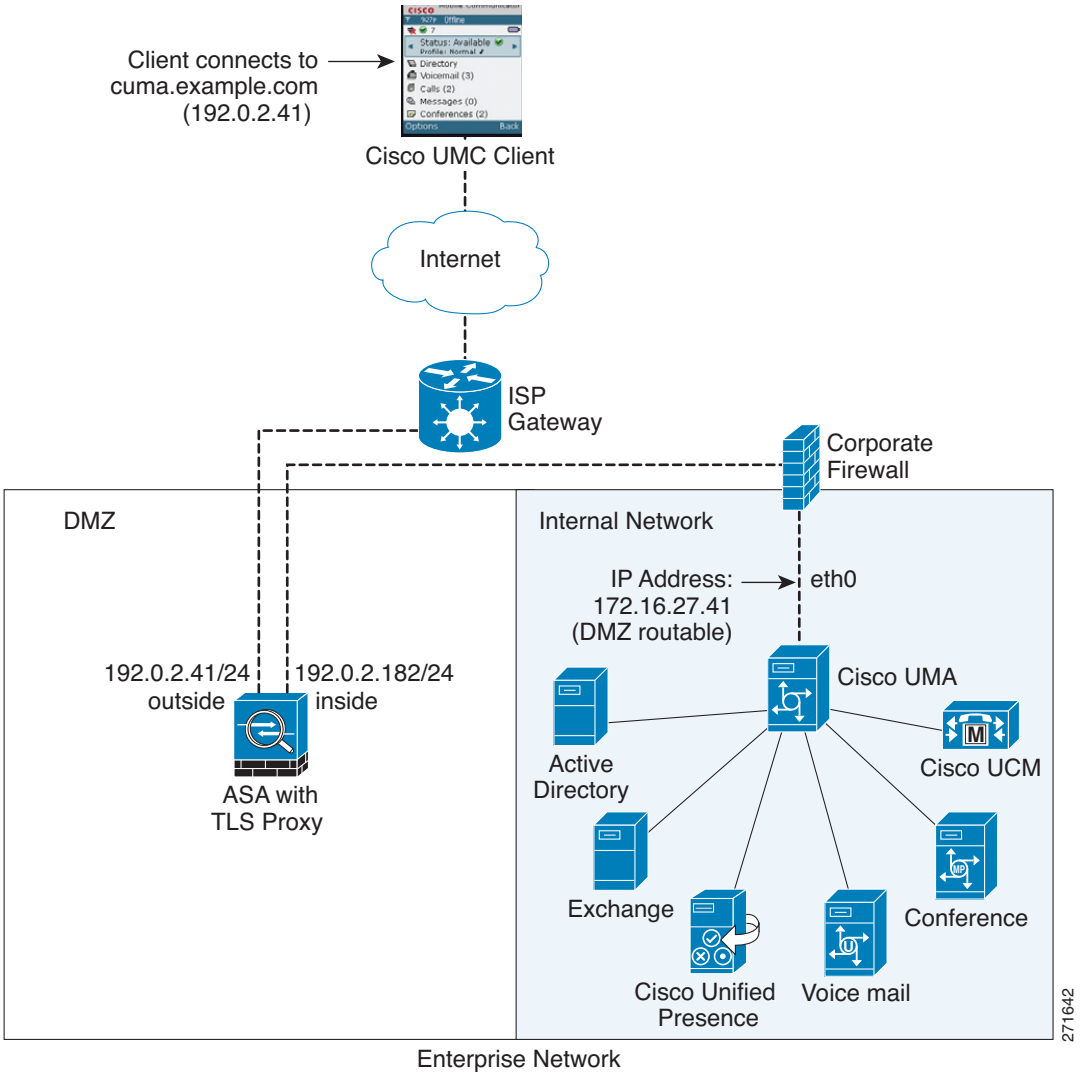
- Set up a NAT rule for inbound traffic that translates the destination IP address 192.0.2.41 to 172.16.27.41.
- Set up an interface PAT rule for inbound traffic translating the source IP address of every packet so that the corporate firewall does not need to open up a wildcard pinhole. The Cisco UMA server receives packets with the source IP address 192.0.12.183.

  ```
  hostname(config)# nat (outside) 1 0.0.0.0 0.0.0.0 outside
  hostname(config)# global (inside) 1 192.0.2.183 netmask 255.255.255.255
  ```

  See Chapter 28, “Configuring Network Object NAT” and Chapter 29, “Configuring Twice NAT” for information.

Note This interface PAT rule converges the Cisco UMA client IP addresses on the outside interface of the adaptive security appliance into a single IP address on the inside interface by using different source ports. Performing this action is often referred as "outside PAT". "Outside PAT" is not recommended when TLS proxy for Cisco Mobility Advantage is enabled on the same interface of the adaptive security appliance with phone proxy, Cisco Unified Presence, or any other features involving application inspection. "Outside PAT" is not supported completely by application inspection when embedded address translation is needed.

Figure 46-3 Cisco UMC/Cisco UMA Architecture – Scenario 2: Security Appliance as Mobility Advantage Proxy Only



Mobility Advantage Proxy Using NAT/PAT

In both scenarios (Figure 46-2 and Figure 46-3), NAT can be used to hide the private address of the Cisco UMA servers.

In scenario 2 (Figure 46-3), PAT can be used to converge all client traffic into one source IP, so that the firewall does not have to open up a wildcard pinhole for inbound traffic.

```
hostname(config)# access-list cumc extended permit tcp any host 172.16.27.41 eq 5443
```

versus

```
hostname(config)# access-list cumc extended permit tcp host 192.0.2.183 host 172.16.27.41
eq 5443
```

Trust Relationships for Cisco UMA Deployments

To establish a trust relationship between the Cisco UMC client and the adaptive security appliance, the adaptive security appliance uses the Cisco UMA server certificate and keypair or the adaptive security appliance obtains a certificate with the Cisco UMA server FQDN (certificate impersonation). Between the adaptive security appliance and the Cisco UMA server, the adaptive security appliance and Cisco UMA server use self-signed certificates or certificates issued by a local certificate authority.

Figure 46-4 shows how you can import the Cisco UMA server certificate onto the adaptive security appliance. When the Cisco UMA server has already enrolled with a third-party CA, you can import the certificate with the private key onto the adaptive security appliance. Then, the adaptive security appliance has the full credentials of the Cisco UMA server. When a Cisco UMA client connects to the Cisco UMA server, the adaptive security appliance intercepts the handshake and uses the Cisco UMA server certificate to perform the handshake with the client. The adaptive security appliance also performs a handshake with the server.

Figure 46-4 How the Security Appliance Represents Cisco UMA – Private Key Sharing

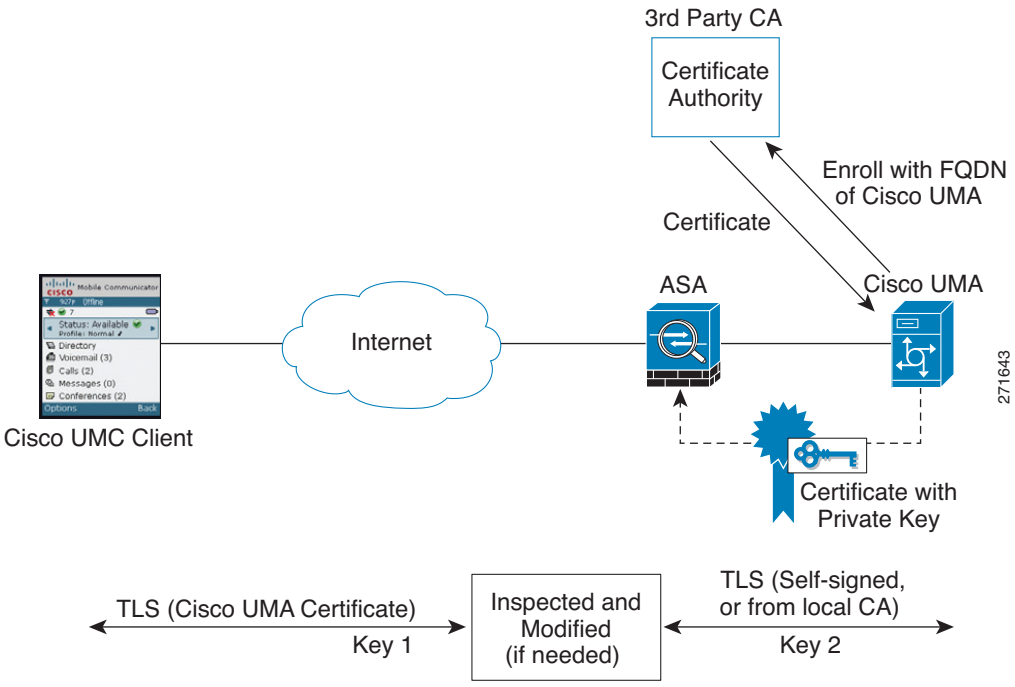
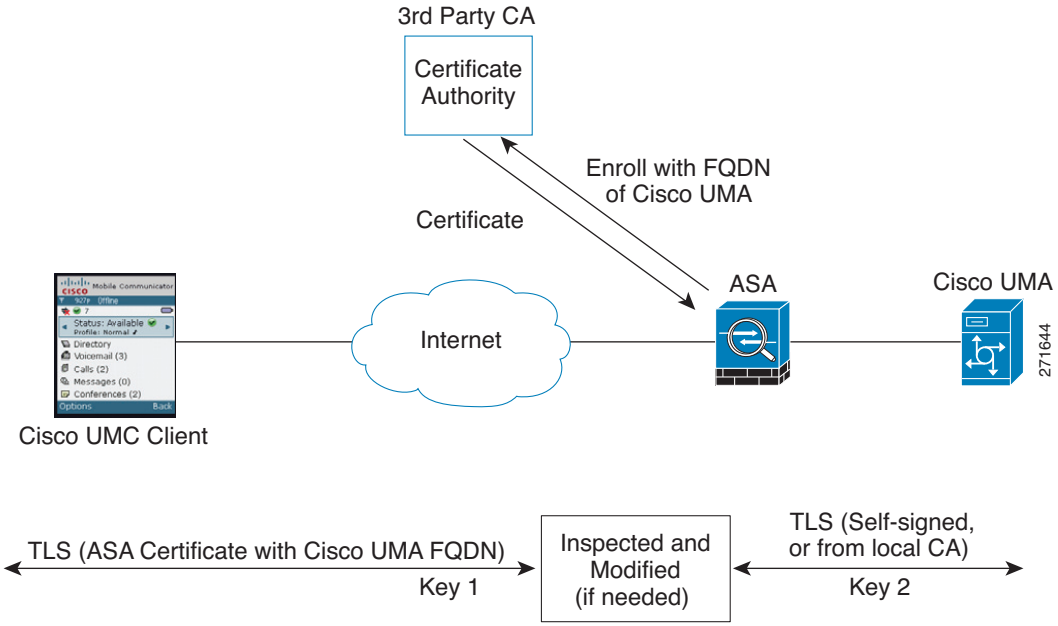


Figure 46-5 shows another way to establish the trust relationship. Figure 46-5 shows a green field deployment, because each component of the deployment has been newly installed. The adaptive security appliance enrolls with the third-party CA by using the Cisco UMA server FQDN as if the adaptive

security appliance is the Cisco UMA server. When the Cisco UMA client connects to the adaptive security appliance, the adaptive security appliance presents the certificate that has the Cisco UMA server FQDN. The Cisco UMA client believes it is communicating to with the Cisco UMA server.

Figure 46-5 How the Security Appliance Represents Cisco UMA – Certificate Impersonation



A trusted relationship between the adaptive security appliance and the Cisco UMA server can be established with self-signed certificates. The adaptive security appliance's identity certificate is exported, and then uploaded on the Cisco UMA server truststore. The Cisco UMA server certificate is downloaded, and then uploaded on the adaptive security appliance truststore by creating a trustpoint and using the **crypto ca authenticate** command.

Licensing for the Cisco Mobility Advantage Proxy Feature

The Cisco Unified Communications proxy features (Cisco Phone Proxy, TLS proxy for encrypted voice inspection, and the Cisco Presence Federation Proxy) supported by the adaptive security appliance require a Unified Communications Proxy license. However, in Version 8.2(2) and later, the Mobility Advantage proxy no longer requires a Unified Communications Proxy license.

The following table shows the licensing requirements for the Mobility Advantage proxy:

Model	License Requirement
All models	Base License.

For more information about licensing, see Chapter 3, “Managing Feature Licenses.”

Configuring Cisco Mobility Advantage

This section includes the following topics:

Task Flow for Configuring Cisco Mobility Advantage

To configure for the adaptive security appliance to perform TLS proxy and MMP inspection as shown in Figure 46-2 and Figure 46-3, perform the following tasks.

It is assumed that self-signed certificates are used between the adaptive security appliance and the Cisco UMA server.

Prerequisites

Export the Cisco UMA server certificate and keypair in PKCS-12 format so that you can import it onto the adaptive security appliance. The certificate will be used during the handshake with the Cisco UMA clients.

Step 1 Create the static NAT for the Cisco UMA server by entering the following commands:

```
hostname(config)# object network name
hostname(config-network-object)# host real_ip
hostname(config-network-object)# nat (real_ifc,mapped_ifc) static mapped_ip
```

Step 2 Import the Cisco UMA server certificate onto the adaptive security appliance by entering the following commands:

```
hostname(config)# crypto ca import trustpoint pkcs12 passphrase
[paste base 64 encoded pkcs12]
hostname(config)# quit
```

Step 3 Install the Cisco UMA server certificate on the adaptive security appliance. See Installing the Cisco UMA Server Certificate, page 46-7.

Step 4 Create the TLS proxy instance for the Cisco UMA clients connecting to the Cisco UMA server. See Creating the TLS Proxy Instance, page 46-8.

Step 5 Enable the TLS proxy for MMP inspection. See Enabling the TLS Proxy for MMP Inspection, page 46-9.

Installing the Cisco UMA Server Certificate

Install the Cisco UMA server self-signed certificate in the adaptive security appliance truststore. This task is necessary for the adaptive security appliance to authenticate the Cisco UMA server during the handshake between the adaptive security appliance proxy and Cisco UMA server.

Prerequisites

Export the Cisco UMA server certificate and keypair in PKCS-12 format so that you can import it onto the adaptive security appliance.

	Command	Purpose
Step 1	`hostname(config)# crypto ca trustpoint` *trustpoint_name* **Example:** `hostname(config)# crypto ca trustpoint cuma_server`	Enters the trustpoint configuration mode for the specified trustpoint so that you can create the trustpoint for the Cisco UMA server. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA.
Step 2	`hostname(config-ca-trustpoint)# enrollment terminal`	Specifies cut and paste enrollment with this trustpoint (also known as manual enrollment).
Step 3	`hostname(config-ca-trustpoint)# exit`	Exits from the CA Trustpoint configuration mode.

Step 4	`hostname(config)# crypto ca authenticate` *trustpoint*
	Example:
	`hostname(config)# crypto ca authenticate cuma_server`
	`Enter the base 64 encoded CA certificate.`
	`End with a blank line or the word "quit" on a line by itself`
	
	`[ certificate data omitted ]`
	
	`Certificate has the following attributes:`
	`Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4`
	`% Do you accept this certificate? [yes/no]: yes`
	`Trustpoint CA certificate accepted.`
	`% Certificate successfully imported`
	`hostname(config)#`
		Installs and authenticates the CA certificates associated with a trustpoint created for the Cisco UMA server.
		Where *trustpoint* specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters.
		The adaptive security appliance prompts you to paste the base-64 formatted CA certificate onto the terminal.

What to Do Next

Once you have created the trustpoints and installed the Cisco UMA certificate on the adaptive security appliance, create the TLS proxy instance. See Creating the TLS Proxy Instance, page 46-8.

Creating the TLS Proxy Instance

Create a TLS proxy instance for the Cisco UMA clients connecting to the Cisco UMA server.

Prerequisites

Before you can create the TLS proxy instance, you must have installed the Cisco UMA server self-signed certificate in the adaptive security appliance truststore.

	Command	Purpose

Step 1	`hostname(config)# tls-proxy proxy_name`
	Example:
	`tls-proxy cuma_tlsproxy`
		Creates the TLS proxy instance.

Step 2	`hostname(config-tlsp)# server trust-point proxy_name`
	Example:
	`hostname(config-tlsp)# server trust-point cuma_proxy`
		Specifies the proxy trustpoint certificate presented during TLS handshake.
		The certificate must be owned by the adaptive security appliance (identity certificate).

Step 3	`hostname(config-tlsp)# client trust-point proxy_name`
	Example:
	`hostname(config-tlsp)# client trust-point cuma_proxy`
		Specifies the trustpoint and associated certificate that the adaptive security appliance uses in the TLS handshake when the adaptive security appliance assumes the role of the TLS client.
		The certificate must be owned by the adaptive security appliance (identity certificate).

Step 4	`hostname(config-tlsp)# no server authenticate-client`	Disables client authentication. Disabling TLS client authentication is required when the adaptive security appliance must interoperate with a Cisco UMA client or clients such as a Web browser that are incapable of sending a client certificate.

Step 5	`hostname(config-tlsp)# client cipher-suite cipher_suite`
	Example:
	`hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1`
		Specifies cipher suite configuration.
		For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suite replaces the default cipher suite.

What to Do Next

Once you have created the TLS proxy instance, enable it for MMP inspection. See Enabling the TLS Proxy for MMP Inspection, page 46-9.

Enabling the TLS Proxy for MMP Inspection

Cisco UMA client and server communications can be proxied via TLS, which decrypts the data, passes it to the inspect MMP module, and re-encrypt the data before forwarding it to the endpoint. The inspect MMP module verifies the integrity of the MMP headers and passes the OML/HTTP to an appropriate handler.

	Command	Purpose
Step 1	hostname(config)# **class-map** *class_map_name* **Example:** hostname(config)# class-map cuma_tlsproxy	Configures the class of traffic to inspect. Traffic between the Cisco UMA server and client uses MMP and is handled by MMP inspection. Where *class_map_name* is the name of the MMP class map.
Step 2	hostname(config-cmap)# **match port tcp eq** *port* **Example:** hostname(config-cmap)# match port tcp eq 5443	Matches the TCP port to which you want to apply actions for MMP inspection. The TCP/TLS default port for MMP inspection is 5443.
Step 3	hostname(config-cmap)# **exit**	Exits from the Class Map configuration mode.
Step 4	hostname(config)# **policy-map** *name* **Example:** hostname(config)# policy-map global_policy	Configures the policy map and attaches the action to the class of traffic.
Step 5	hostname(config-pmap)# **class** *classmap-name* **Example:** hostname(config-pmap)# class cuma_proxy	Assigns a class map to the policy map so that you can assign actions to the class map traffic. Where *classmap_name* is the name of the Skinny class map.
Step 6	hostname(config-pmap)# **inspect mmp tls-proxy** *proxy_name* **Example:** hostname(config-pmap)# inspect mmp tls-proxy cuma_proxy	Enables SCCP (Skinny) application inspection and enables the phone proxy for the specified inspection session.
Step 7	hostname(config-pmap)# **exit**	Exits from the Policy Map configuration mode.
Step 8	hostname(config)# **service-policy** *policy_map_name* **global** **Example:** service-policy global_policy global	Enables the service policy on all interfaces.

Monitoring for Cisco Mobility Advantage

Mobility advantage proxy can be debugged the same way as IP Telephony. You can enable TLS proxy debug flags along with SSL syslogs to debug TLS proxy connection problems.

For example, using the following commands to enable TLS proxy-related debugging and syslog output only:

```
hostname# debug inspect tls-proxy events
hostname# debug inspect tls-proxy errors
hostname# config terminal
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)# logging list loglist message 711001
hostname(config)# logging list loglist message 725001-725014
hostname(config)# logging list loglist message 717001-717038
hostname(config)# logging buffer-size 1000000
hostname(config)# logging buffered loglist
hostname(config)# logging debug-trace
```

For information about TLS proxy debugging techniques and sample output, see the Monitoring the TLS Proxy, page 45-14.

Enable the **debug mmp** command for MMP inspection engine debugging:

```
MMP:: received 60 bytes from outside:1.1.1.1/2000 to inside:2.2.2.2/5443
MMP:: version OLWP-2.0
MMP:: forward 60/60 bytes from outside:1.1.1.1/2000 to inside:2.2.2.2/5443
MMP:: received 100 bytes from inside:2.2.2.2/5443 to outside:1.1.1.1/2000
MMP:: session-id: ABCD_1234
MMP:: status: 201
MMP:: forward 100/100 bytes from inside:2.2.2.2/5443 to outside 1.1.1.1/2000
MMP:: received 80 bytes from outside:1.1.1.1/2000 to inside:2.2.2.2/5443
MMP:: content-type: http/1.1
MMP:: content-length: 40
```

You can also capture the raw and decrypted data by the TLS proxy by entering the following commands:

```
hostname# capture mycap interface outside (capturing raw packets)
hostname# capture mycap-dec type tls-proxy interface outside (capturing decrypted data)
hostname# show capture capture_name
hostname# copy /pcap capture:capture_name tftp://tftp_location
```

Configuration Examples for Cisco Mobility Advantage

This section describes sample configurations that apply to two deployment scenarios for the TLS proxy used by the Cisco Mobility Advantage solution—scenario 1 where the adaptive security appliance functions as both the firewall and TLS proxy and scenario 2 where the adaptive security appliance functions as the TLS proxy only. In both scenarios, the clients connect from the Internet.

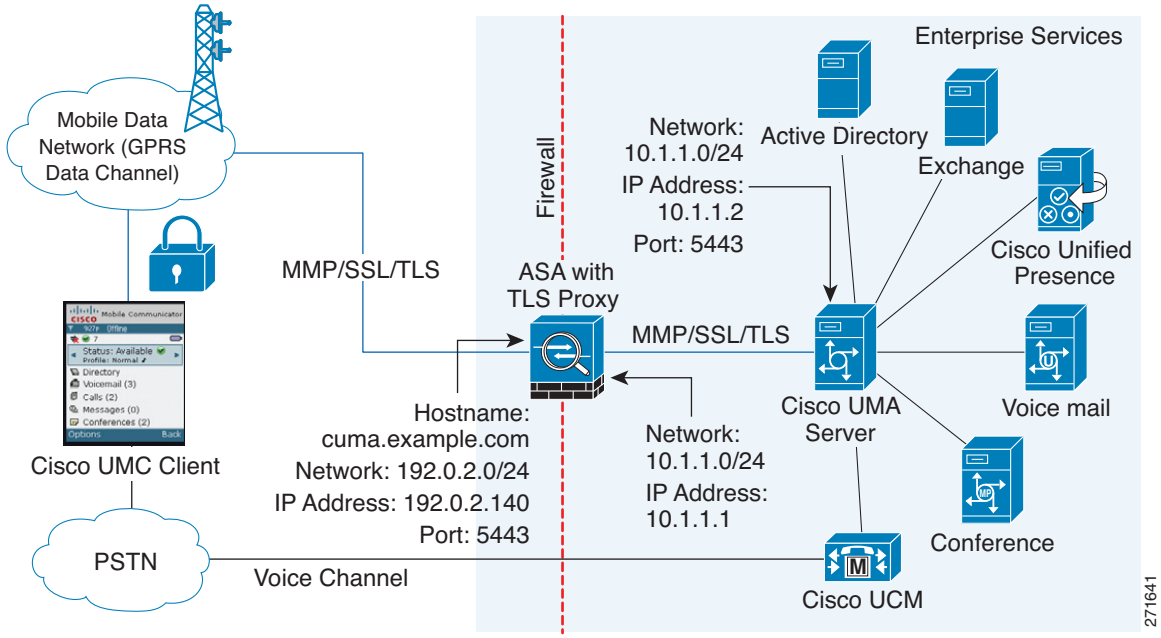
In the samples, you export the Cisco UMA server certificate and key-pair in PKCS-12 format and import it to the adaptive security appliance. The certificate will be used during handshake with the Cisco UMA clients.

Installing the Cisco UMA server self-signed certificate in the adaptive security appliance truststore is necessary for the adaptive security appliance to authenticate the Cisco UMA server during handshake between the adaptive security appliance proxy and Cisco UMA server. You create a TLS proxy instance for the Cisco UMA clients connecting to the Cisco UMA server. Lastly, you must enable TLS proxy for MMP inspection.

Example 1: Cisco UMC/Cisco UMA Architecture – Security Appliance as Firewall with TLS Proxy and MMP Inspection

As shown in Figure 46-6 (scenario 1—the recommended architecture), the adaptive security appliance functions as both the firewall and TLS proxy. In the scenario 1 deployment, the adaptive security appliance is between a Cisco UMA client and a Cisco UMA server. In this scenario, the adaptive security appliance performs static NAT by translating the Cisco UMA server 10.1.1.2 IP address to 192.0.2.140.

Figure 46-6 Cisco UMC/Cisco UMA Architecture – Scenario 1: Security Appliance as Firewall with TLS Proxy and MMP Inspection




```
object network obj-10.1.1.2-01
    host 10.1.1.2
    nat (inside,outside) static 192.0.2.140
crypto ca import cuma_proxy pkcs12 sample_passphrase
    <cut-paste base 64 encoded pkcs12 here>
    quit
! for CUMA server's self-signed certificate
crypto ca trustpoint cuma_server
    enrollment terminal
crypto ca authenticate cuma_server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
    [ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit
tls-proxy cuma_proxy
    server trust-point cuma_proxy
    no server authenticate-client
    client cipher-suite aes128-sha1 aes256-sha1
class-map cuma_proxy
    match port tcp eq 5443
policy-map global_policy
    class cuma_proxy
        inspect mmp tls-proxy cuma_proxy
service-policy global_policy global
```

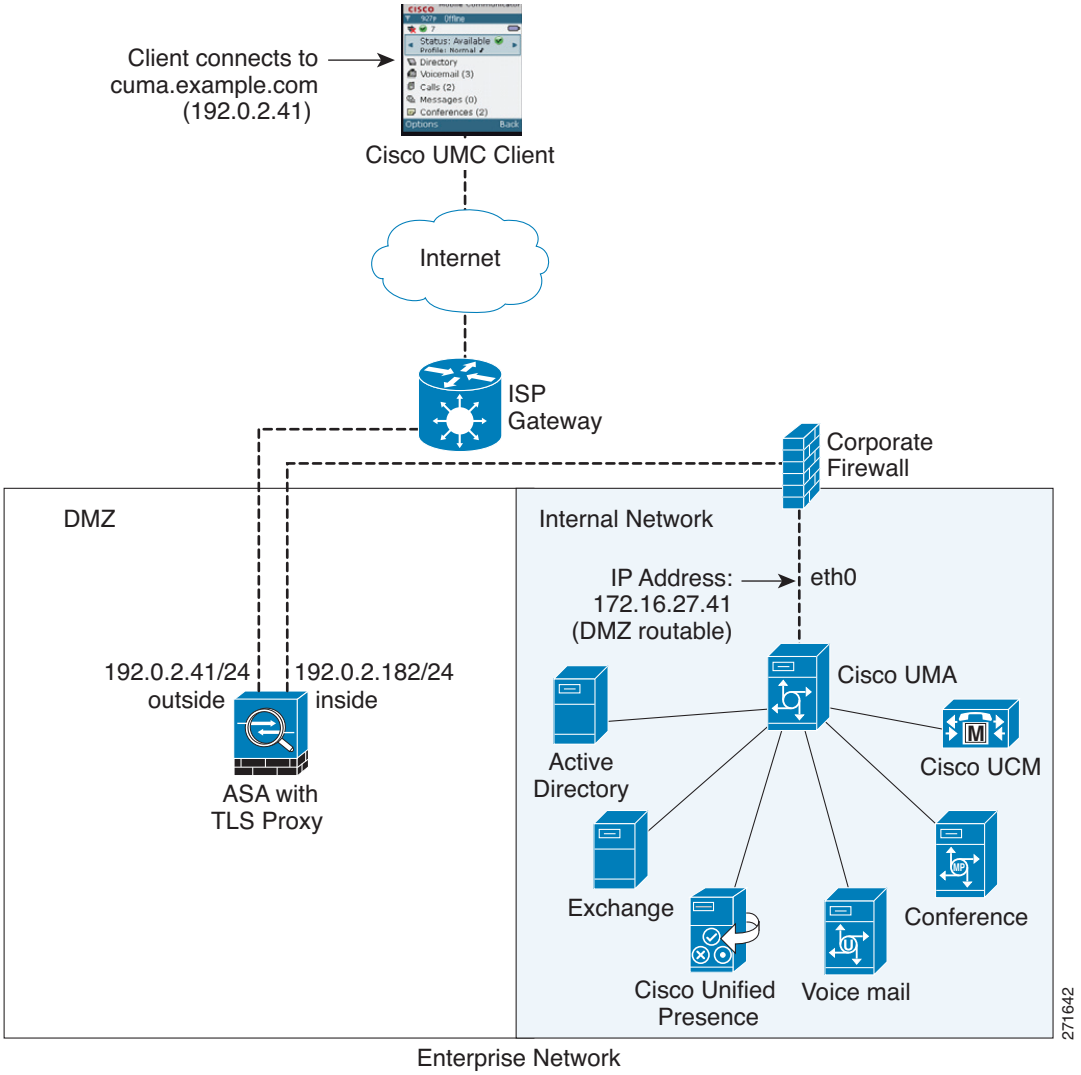
Example 2: Cisco UMC/Cisco UMA Architecture – Security Appliance as TLS Proxy Only

As shown in Figure 46-7 (scenario 2), the adaptive security appliance functions as the TLS proxy only and works with an existing firewall. The adaptive security appliance and the corporate firewall are performing NAT. The corporate firewall will not be able to predict which client from the Internet needs to connect to the corporate Cisco UMA server. Therefore, to support this deployment, you can take the following actions:

- Set up a NAT rule for inbound traffic that translates the destination IP address 192.0.2.41 to 172.16.27.41.
- Set up an interface PAT rule for inbound traffic translating the source IP address of every packet so that the corporate firewall does not need to open up a wildcard pinhole. The Cisco UMA server receives packets with the source IP address 67.11.12.183.

```
hostname(config)# object network obj-0.0.0.0-01
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat (outside,inside) dynamic 192.0.2.183
```

Figure 46-7 Cisco UMC/Cisco UMA Architecture – Scenario 2: Security Appliance as TLS Proxy Only




```
object network obj-172.16.27.41-01
    host 172.16.27.41
    nat (inside,outside) static 192.0.2.140
object network obj-0.0.0.0-01
    subnet 0.0.0.0 0.0.0.0
    nat (outside,inside) dynamic 192.0.2.183
crypto ca import cuma_proxy pkcs12 sample_passphrase
    <cut-paste base 64 encoded pkcs12 here>
    quit
! for CUMA server's self-signed certificate
crypto ca trustpoint cuma_server
    enrollment terminal
crypto ca authenticate cuma_server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
    [ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit
```

```
tls-proxy cuma_proxy
    server trust-point cuma_proxy
    no server authenticate-client
    client cipher-suite aes128-sha1 aes256-sha1
class-map cuma_proxy
    match port tcp eq 5443
policy-map global_policy
    class cuma_proxy
        inspect mmp tls-proxy cuma_proxy
service-policy global_policy global
```

Feature History for Cisco Mobility Advantage

Table 46-1 lists the release history for this feature.

Table 46-1 Feature History for Cisco Phone Proxy

Feature Name	Releases	Feature Information
Cisco Mobility Advantage Proxy	8.0(4)	The Cisco Mobility Advantage Proxy feature was introduced.
Cisco Mobility Advantage Proxy	8.3(1)	The Unified Communications Wizard was added to ASDM. By using the wizard, you can configure the Cisco Mobility Advantage Proxy.