



Mobile and Remote Access Collaboration with Cisco Expressway Series

Revised: July 11, 2014

What's New: This is a new chapter that describes a new way for mobile devices to connect from any location without the need for a separate VPN client, which simplifies the BYOD user experience and complements security policies.

Overview

Cisco Expressway Series

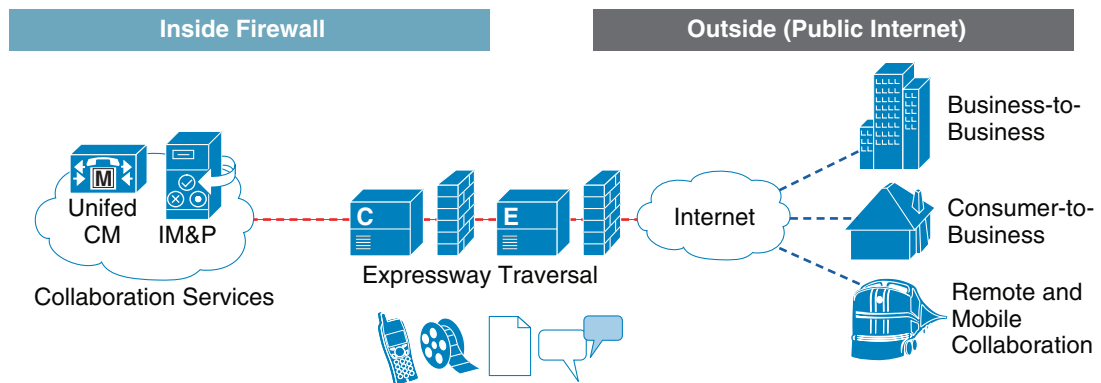
Collaboration should be simple and effective regardless of location. The Cisco Expressway Series helps ensure that collaboration outside the enterprise is as simple and secure as on-premises collaboration. Cisco Expressway provides access to collaboration services from anywhere on a range of devices collaborating with a mix of video, voice, messaging, and presence.

Cisco Expressway provides secure mobile access based on Transport Layer Security (TLS) without the need for a separate VPN client, simplifying the user experience while complementing BYOD security policies.

Some of the benefits of Cisco Expressway include:

- Simple access to video, voice, content, messaging, and presence outside the enterprise firewall so employees are as effective and productive as they are inside the office.
- Highly secure firewall traversal technology to extend organizational reach.
- Improved productivity allowing employees to collaborate with multiple mobile devices.
- Enhance workforce mobility with support for a wide range of devices with Cisco Jabber for smartphones, tablets, and desktops.

Figure 26-1 shows a Cisco Expressway deployment forming a secure traversal link enabling collaboration from outside the firewall.

Figure 26-1 Expressway Deployment

297121

Cisco Expressway Series is a component of the Cisco Collaboration Edge Architecture, which combines the capabilities of Cisco gateway offerings with the core capabilities of Cisco Collaboration solutions to break down barriers and enable effective collaboration. The Collaboration Edge Architecture enables anyone, anywhere, any device collaboration for:

- Remote and mobile workers
- Business-to-business collaboration
- Consumer-to-business collaboration
- Intra-enterprise and cloud connectivity

Jabber Client Connectivity without VPN

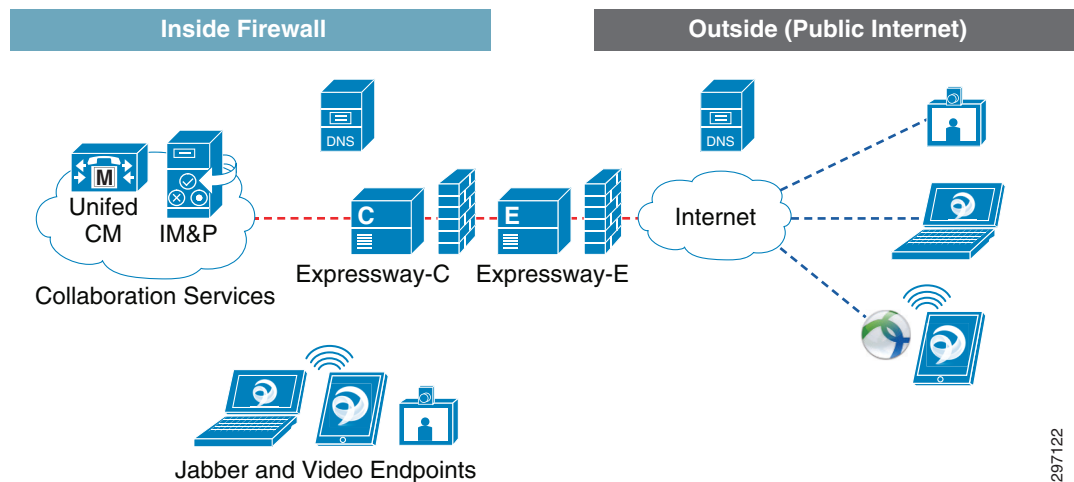
Cisco Expressway provides a secure connection for Cisco Jabber application traffic without having to connect to the corporate network over a VPN tunnel. It is device and operating system agnostic for Windows, Mac, Apple iOS, and Android platforms. It allows Jabber clients that are outside the enterprise to:

- Use instant messaging and presence services.
- Make voice and video calls.
- Search the corporate directory.
- Share content.
- Launch a web conference.
- Access visual voicemail.

Solution Components

Figure 26-2 shows the components tested in this design guide, including the Expressway and Collaboration Services components. These components, in combination with DNS name resolution, allow clients to connect from any location.

Figure 26-2 Solution Components



Cisco Expressway-C and Expressway-E

The Expressway solution builds on the firewall traversal capabilities of the Cisco TelePresence Video Communication Server (VCS) family and explicitly allows mobile and remote access without the need for a separate VPN client.

Two servers are required to provide the firewall traversal features. These may be in the form of virtualized applications, bare-metal appliances, or for deployment on the Cisco ISR Routers using Cisco UCS E-Series. The two servers are:

- Expressway-C or Core—Acts as the traversal client for Expressway-E and is the SIP Proxy and communications gateway for Unified CM.
- Expressway-E or Edge—Resides on the DMZ and is the traversal server that handles incoming calls and issues call requests to Expressway-C. The Expressway-E has a public network domain name and is reachable from the public Internet.

Cisco Unified Communications Manager

The Cisco Unified Communications Manager (Unified CM) serves as the software-based call processing component of the solution.

Endpoint devices register to the Unified CM and the Expressway acts as a Unified Communications Internet gateway/proxy for a full range of collaboration services including video, voice, IM and presence, messaging, and mobility on Cisco as well as third-party devices.

Cisco Unified CM IM and Presence

The Cisco Unified Communications Manager IM and Presence (IM&P) provides native enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications Manager. The service is tightly integrated with Cisco and third-party compatible desktop and mobile clients, including Cisco Jabber.

Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility Client provides a secure connection experience across a broad set of PC and mobile devices. The client automatically selects the optimal network access point and adapts its tunneling protocol to the most efficient method and it may be configured so that the VPN connection remains established during IP address changes or loss of connectivity.

Cisco ASA Firewall

Cisco ASA Adaptive Security Appliances provide a broad span of security technology and solutions to protect critical assets in enterprise networks. A set of modular security services strengthens a proven stateful inspection firewall with next-generation firewall capabilities and network-based security controls for streamlined security operations. The ASA also offers comprehensive endpoint security for AnyConnect VPN clients.

Cisco Jabber Clients

Cisco Jabber is a collaboration client application that streamlines communications and enhances productivity. Cisco Jabber provides the best user experience across the broadest range of platforms via presence, instant messaging (IM), voice, high quality video, voice messaging, and desktop sharing and conferencing. Cisco Jabber is supported across desktop PCs and mobile devices, such as smartphones and tablets.

Cisco TelePresence Endpoints

Cisco TelePresence Endpoints create an immersive, in-person experience over the network, allowing local and remote participants to feel like they are all in the same room. Expressway allows TelePresence endpoints to register to Unified CM over the Internet without VPN or Virtual Office Routers.

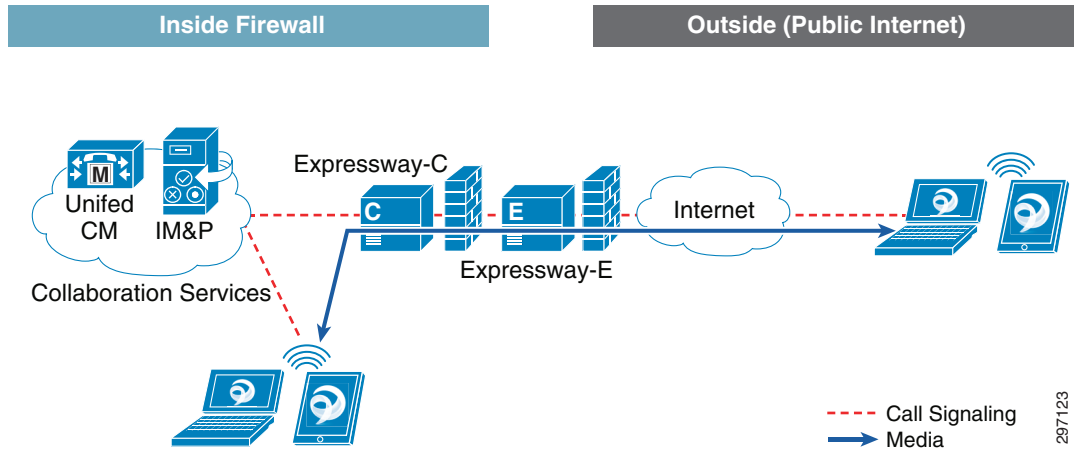
DNS Name Server

The DNS servers are used to perform DNS lookups and resolve network names. The resolution of specific SRV records influences when the client communicates with Expressway-E.

Expressway Traversal

The Expressway traversal enables video, voice, content and IM&P collaboration outside a firewall. The solution works with most firewalls and only requires minimal firewall configuration. [Figure 26-3](#) shows how Expressway-E and Expressway-C allow Jabber clients to connect from the Internet.

Figure 26-3 Expressway Firewall Traversal



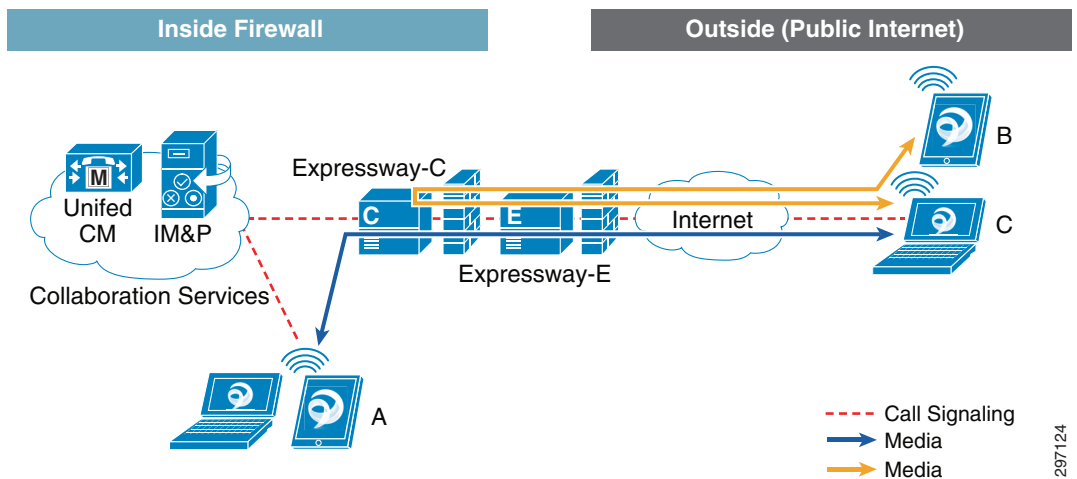
In this deployment, Expressway-E acts as the traversal server and resides in the DMZ, while Expressway-C is the traversal client inside the enterprise network.

- Expressway-C initiates traversal connections outbound through the firewall to specific ports on Expressway-E with secure login credentials and sends keep-alive packets to Expressway-E. This outbound high-to-low connection serves to further minimize the configuration required on the ASA and lowers the risks of an unused, unmonitored ACL from outside to inside.
- When Expressway-E receives incoming call signaling, it sends the signaling to Expressway-C.
- Expressway-C proxies the call signaling to Unified CM, which completes the call process and the call is established, with media traversing the tunnel between Expressway-E and Expressway-C.

Figure 26-4 shows the signaling and media paths between Jabber clients. Unified CM provides call control for both mobile and on-premise endpoints.

- Media traversal—“C” calls “A” while “A” is on-premise. The Expressway solution provides firewall traversal for the media. Expressway-C de-multiplexes media and forwards to “A”.
- Media Relay—“C” calls “B” while both are off-premise. Media is relayed via Expressway-C and the call is established.

Figure 26-4 Signaling and Media Paths



Use Cases in this Document

The use cases presented in this document address several deployment scenarios and explore different combinations of Jabber and TelePresence clients, AnyConnect VPN sessions, and the interaction between them. The use cases are grouped by the client's original location.

Connecting from the Corporate Network

The section focuses on two different ways to allow clients to collaborate:

- Connecting directly to the Unified CM—In this case, the client does not require Expressway services and signs in directly with on-premise collaboration services.
- Providing communication across segments—In this case, clients are separated by some form of segmentation, such as VLANs or Access Control Lists. The BYOD CVD highlights several use cases that cover different deployment models. For example, in the Enhanced use case wireless clients are provided differentiated access based on authorization profiles, but the segmentation enforced on them makes the communication between Jabber clients impossible. This use case facilitates that communication.

Connecting from the Internet

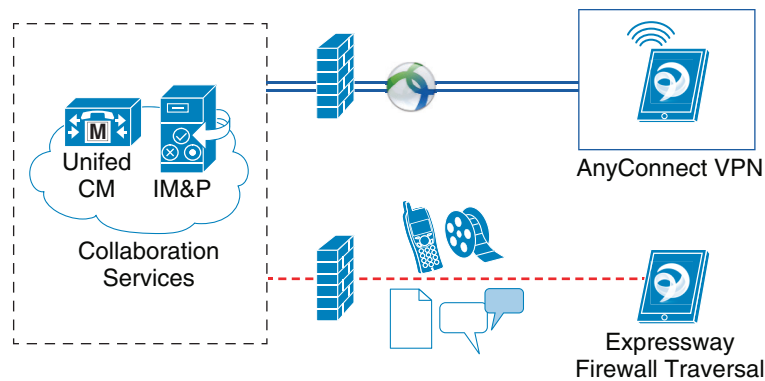
This use case explores how mobile devices can simultaneously use both the Cisco AnyConnect client and Cisco Jabber. While both the AnyConnect client and the Cisco Jabber client work well as designed, their interaction can have a negative impact on collaboration calls between Jabber clients.

This use case focuses on different techniques configured on the ASA, such as split tunneling and filtering that allows the client to always connect to Expressway-E when the connection originates from the Internet.

This use case also explores the option of dedicating a DNS server to provide name resolution for clients connecting from the Internet to guarantee the connection to Expressway-E and reduce the impact to active voice or video calls.

Figure 26-5 shows two different ways for remote clients to connect to the Collaboration Services residing on the corporate network.

- The first one is by establishing a VPN tunnel with the Cisco AnyConnect client. This full-tunneling capability allows mobile devices to access collaboration and other enterprise resources and applications with a consistent LAN-like user experience. This requires installing the Cisco AnyConnect client on the mobile device.
- The second one highlights the firewall traversal capabilities of the Expressway solution to allow remote clients to access collaboration resources without the need for a separate VPN client, making the connection transparent to the user, regardless of location.

Figure 26-5 Remote Access Options

In this use case, the interaction between the Jabber client and AnyConnect VPN client is validated, with a strong focus on providing a positive user experience for collaboration sessions. [Table 26-1](#) highlights some considerations for VPN and Expressway solutions.

Table 26-1 Comparing VPN and Expressway

	Advantages	Challenges
VPN	<ul style="list-style-type: none"> Secure access to all enterprise applications Supports Dial via Office Reverse Callback, Wi-Fi-to-cellular handoff (hand-out), and CTI as well as other non-collaboration work flows. 	With VPN all traffic from connected devices traverses the enterprise network
Expressway Mobile and Remote Access	Only collaboration traffic traverses the enterprise network, everything else goes to the Internet No per-session or user licensing beyond collaboration endpoint/client licensing	No support for Dial via Office Reverse Callback

[Connection Scenarios](#) provides more details on these scenarios.

Discovering Available Services via DNS

When a Jabber client gets a network connection, the device also gets the address of a DNS name server from the DHCP server. Depending on the network connection, the DNS server might be internal or external to the corporate network.

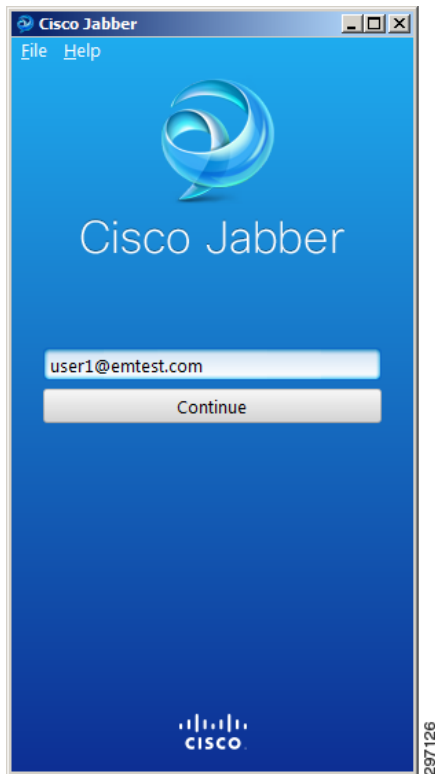
Cisco Jabber clients rely on domain name servers to:

- Automatically discover servers inside the corporate network.
- Locate Expressway servers on the public Internet.
- Determine whether the client is inside or outside the corporate network.

The Jabber client looks for DNS records from internal name servers inside the corporate network and external name servers on the public Internet.

The Jabber client relies on the services domain to query the DNS server for resolution. One way to discover the services domain is by using the user's login credentials, which require the user's ID and domain. The example in Figure 26-6 is from user1 connecting from a Windows Jabber client. The user ID is user1, while emtest.com is used as the services domain to query DNS servers.

Figure 26-6 Services Domain



Collaboration Services—Inside or Outside the Firewall?

To determine whether the client is inside or outside the corporate network and if Expressway is required, the Jabber client queries the DNS server for specific DNS Service (SRV) records. The client sends separate, simultaneous requests to the DNS server for the following SRV records:

- _cisco-uds
- _cuplogin
- _collab-edge

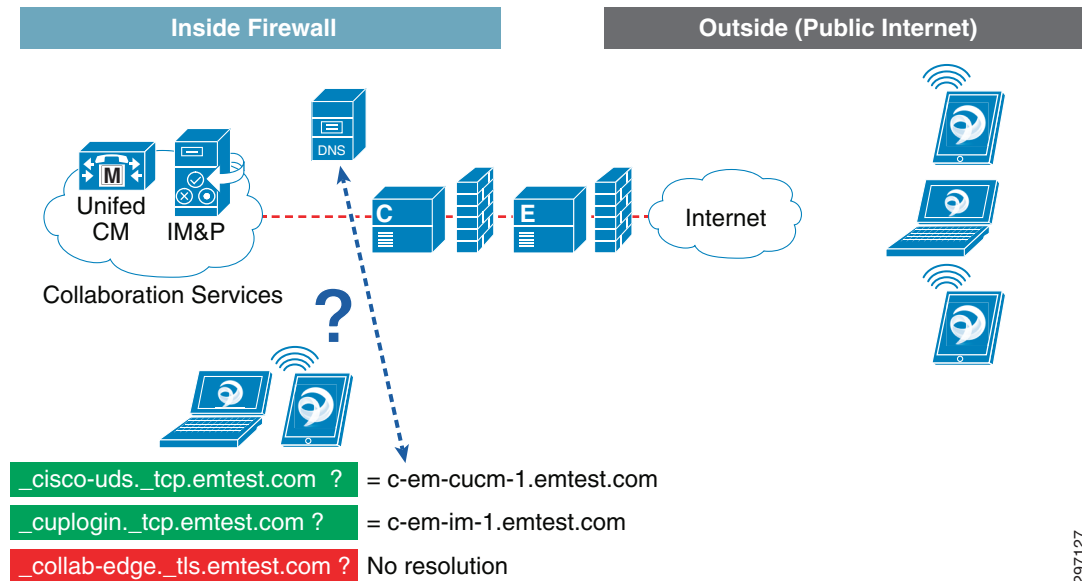
If the name server resolves:

- _cisco-uds or _cuplogin—The client detects it is inside the corporate network and connects to one or both of the following:
 - Cisco Unified Communications Manager—If the name server resolves _cisco-uds.
 - Cisco Unified IM and Presence—If the name server resolves _cuplogin.

- `_collab-edge` and does not resolve `_cisco-uds` or `_cuplogin`—The client attempts to connect to the corporate network through Expressway and discover services.
- None of the SRV records—The client prompts users to manually enter setup and sign-in details.

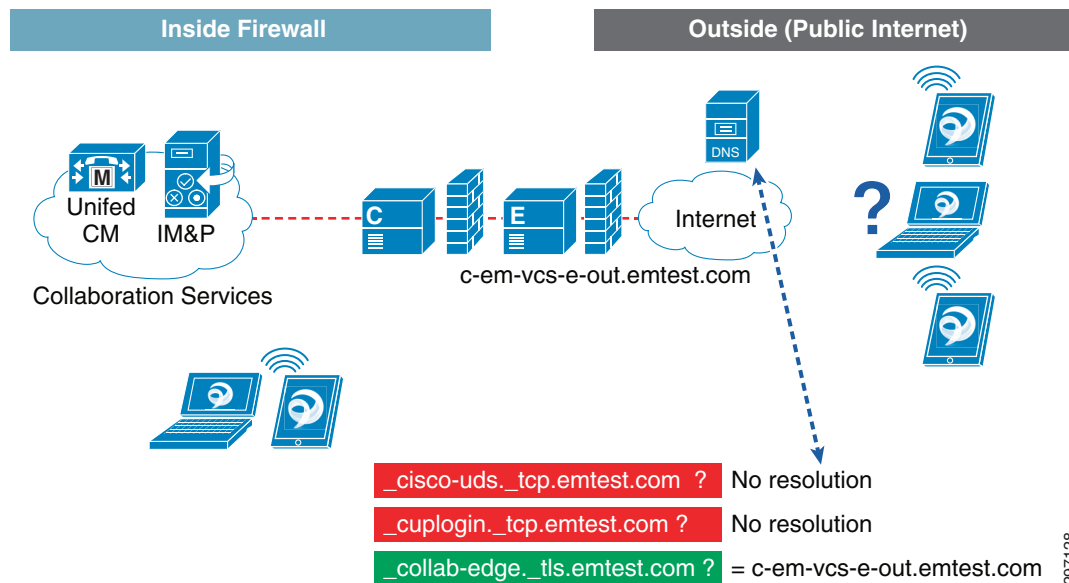
In [Figure 26-7](#) the DNS server resolves the `_cisco-uds` and `_cuplogin` SRV queries and returns the IP address/hostname of the collaboration services nodes. In this case, Expressway mobile and remote access are not required.

Figure 26-7 Connecting to Internal Services



297127

If the name server does not resolve `_cisco-uds` or `_cuplogin`, but does resolve the `_collab-edge` SRV record, the client attempts to connect to internal servers through Expressway. The DNS server in [Figure 26-8](#) returns the `_collab-edge` SRV record and the client connects through Expressway.

Figure 26-8 Connecting through Expressway

SRV Records

Table 26-2 lists the SRV records used by the internal DNS servers to discover internal services.

Table 26-2 Internal SRV Records

Service Record	Description
<code>_cisco-uds</code>	Provides the location of Cisco Unified CM version 9.0 and higher.
<code>_cuplogin</code>	Provides the location of Cisco Unified Presence version 8.x. Supports deployments where all clusters have not yet been upgraded to Cisco Unified CM version 9.

Table 26-3 lists the SRV record provisioned on external name servers.

Table 26-3 External SRV Record

Service Record	Description
<code>_collab-edge</code>	Provides the location of the Cisco Expressway-E server.
	Note The fully qualified domain name (FQDN) must be used in the data field of the SRV record.

The NSLOOKUP command allows Windows clients to discover what SRV records are used by the Jabber client. The example in Figure 26-9 shows resolution for only the `_collab-edge` SRV record and directs the client to connect from outside the firewall to Expressway-E.

Figure 26-9 Verifying SRV Records

```

C:\Windows\system32\cmd.exe
C:\>
C:\>nslookup
Default Server: c-em-dc-1.entest.com
Address: 10.230.1.10

> set type=srv
> collab-edge._tls.entest.com
Server: c-em-dc-1.entest.com
Address: 10.230.1.10

_collab-edge._tls.entest.com SRV service location:
        priority = 10
        weight = 10
        port = 8443
        svr hostname = c-em-ucs-e-out.entest.com
c-em-ucs-e-out.entest.com internet address = 172.26.137.29
>
> cisco-uds._tcp.entest.com
Server: c-em-dc-1.entest.com
Address: 10.230.1.10

DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
*** Request to c-em-dc-1.entest.com timed-out
>
> cuplogin._tcp.entest.com
Server: c-em-dc-1.entest.com
Address: 10.230.1.10

DNS request timed out.
        timeout was 2 seconds.
DNS request timed out.
        timeout was 2 seconds.
*** Request to c-em-dc-1.entest.com timed-out
>
> ^C
C:\>
C:\>

```

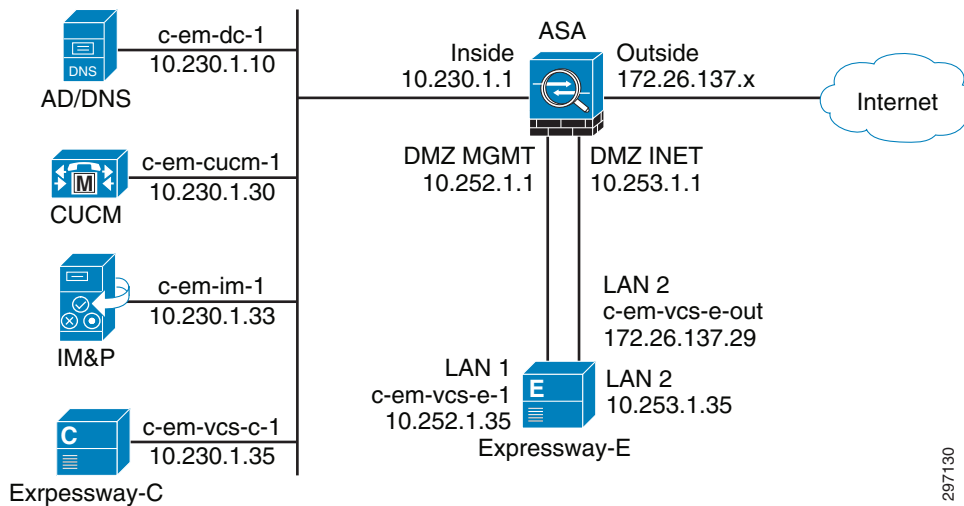
Configuring Cisco Expressway Mobile and Remote Access

This section provides an overview and example of a basic configuration of Cisco Expressway Mobile and Remote Access with Cisco AnyConnect support presented as a stepped example with critical items highlighted throughout. While multiple deployment scenarios exist for Expressway, only one is represented in this section. While multiple deployment scenarios exist for Expressway, only the most common, referred to as “Dual NIC with NAT”, is represented in this section.

Variations in Expressway deployment have little impact on the core configurations. Alternate Expressway deployment models, including high availability deployments, may be found in the Expressway documentation references listed in [Appendix B, “References.”](#)

Expressway Configuration—Network Topology Diagram

The diagram in [Figure 26-10](#) is used as a reference for the rest of this section. The entire configuration example is based on a working lab as depicted in this figure. All host names and IP addresses are consistent throughout the example.

Figure 26-10 Expressway Configuration—Network Topology Diagram

DNS Configuration

Proper DNS implementation is one of the most critical parts of an Expressway implementation. Both the Expressway basic implementation as well as additional configuration for AnyConnect support relies heavily on proper DNS implementation. Issues and inconsistencies with DNS may render the implementation non-functional. Two different DNS systems are utilized to enable Expressway, the internal corporate DNS system and external, or Internet, DNS system.

Table 26-4 and Table 26-5 show the significant DNS records that are used in this section.

Table 26-4 Internal (Corporate) DNS

Record Name (emtest.com)	Record Type	Record Data	Description
c-em-dc-1	Host (A)	10.230.1.10	AD/DNS
c-em-cucm-1	Host (A)	10.230.1.30	Unified CM
c-em-im-1	Host (A)	10.230.1.33	IM&P
c-em-vcs-c-1	Host (A)	10.230.1.35	Expressway-C
c-em-vcs-e-1	Host (A)	10.252.1.35	Expressway-E inside
c-em-vcs-e-out	Host (A)	172.26.137.29	Expressway-E outside NAT
_cisco-uds._tcp	SRV	c-em-cucm-1.emtest.com	SRV record for Unified CM
_collab-edge._tls	SRV	c-em-vcs-e-out.emtest.com	SRV record for Expressway

Table 26-5 External (Internet) DNS

Record Name (emtest.com)	Record Type	Record Data	Description
c-em-vcs-e-out	Host (A)	172.26.137.29	Expressway-E outside NAT
_collab-edge._tls	SRV	c-em-vcs-e-out.emtest.com	SRV record for Expressway

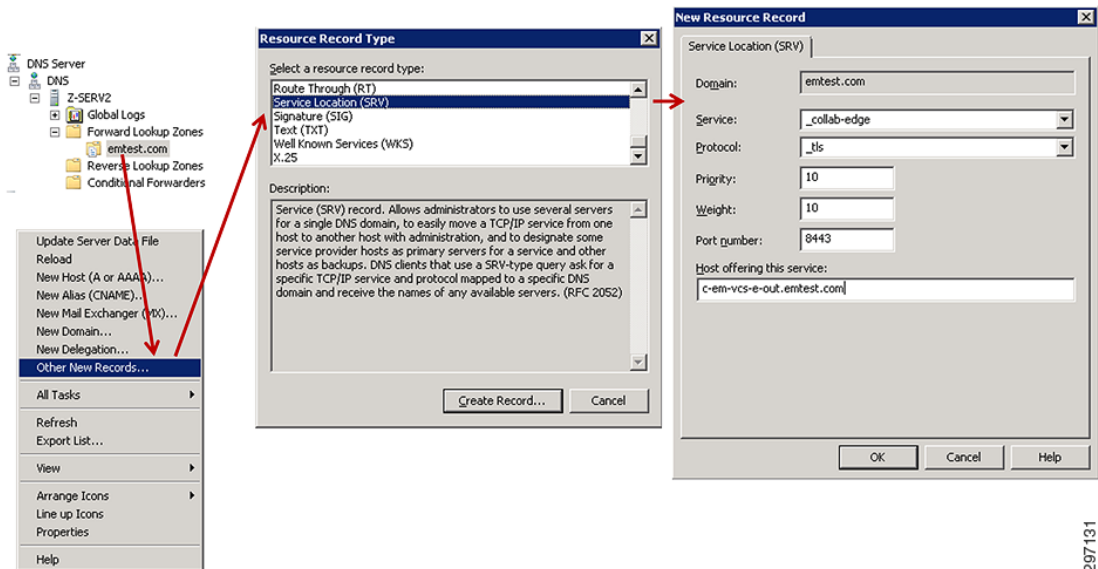


Note

The external DNS records must match the internal DNS records exactly! Specifically the “_collab-edge._tls” SRV record must reference the same A record and that A record must resolve to the same IP address internally and externally. Non-matching records may cause significant functionality issues, especially when using Cisco AnyConnect.

Figure 26-11 shows the creation steps for the _collab-edge DNS SRV record used in this example.

Figure 26-11 DNS SRV Creation Example



287131

Unified CM and IM and Presence Configuration

Very little unique configuration is required for Unified CM and IM&P to have them work with Expressway. Configuring for an internal deployment of Jabber users is the same as deploying Jabber externally through Expressway, allowing existing implementations to add the Expressway component with little alteration of existing Unified CM and IM&P configurations.

For continuity, the basic setup of LDAP, users, and devices in Unified CM is shown in this section. All references are consistent with the overall example configuration.

LDAP Integration

For existing collaboration deployments, LDAP integration is most likely already enabled. [Appendix B, “References”](#) provides links to documentation that extensively covers LDAP integration. [Figure 26-12](#) is simply a brief summary of the LDAP Active Directory integration enabled for this configuration example.

Figure 26-12 LDAP Integration

The screenshot displays the Cisco Unified CM Administration interface for LDAP configuration. The left sidebar shows the navigation menu with 'LDAP' selected. The main content area is divided into three sections:

- LDAP System Configuration:**
 - Status:** Includes informational messages: "Please Delete All LDAP Directories Before Making Changes on This Page" and "Please Disable LDAP Authentication Before Making Changes on This Page".
 - LDAP System Information:**
 - Enable Synchronizing from LDAP Server
 - LDAP Server Type: Microsoft Active Directory
 - LDAP Attribute for User ID: sAMAccountName
- LDAP Directory:**
 - Buttons: Save, Delete, Copy, Perform Full Sync Now (highlighted with a red box), Add New.
 - Status:** Status: Ready
 - LDAP Directory Information:**
 - LDAP Configuration Name*: LDAP sync
 - LDAP Manager Distinguished Name*: CN=Administrator,CN=Users,DC=emtest,DC=com
 - LDAP Password*: [Redacted]
 - Confirm Password*: [Redacted]
 - LDAP User Search Base*: CN=Users,DC=emtest,DC=com
 - LDAP Server Information:**
 - Host Name or IP Address for Server*: 10.230.1.10
 - LDAP Port*: 389
- LDAP Authentication:**
 - Buttons: Save
 - Status:** Status: Ready
 - LDAP Authentication for End Users:**
 - Use LDAP Authentication for End Users
 - LDAP Manager Distinguished Name*: CN=Administrator,CN=Users,DC=emtest,DC=com
 - LDAP Password*: [Redacted]
 - Confirm Password*: [Redacted]
 - LDAP User Search Base*: CN=Users,DC=emtest,DC=com
 - LDAP Server Information:**
 - Host Name or IP Address for Server*: 10.230.1.10
 - LDAP Port*: 389

Red arrows indicate the flow from the 'LDAP' menu item to 'LDAP System', then to 'LDAP Directory', and finally to 'LDAP Authentication'.

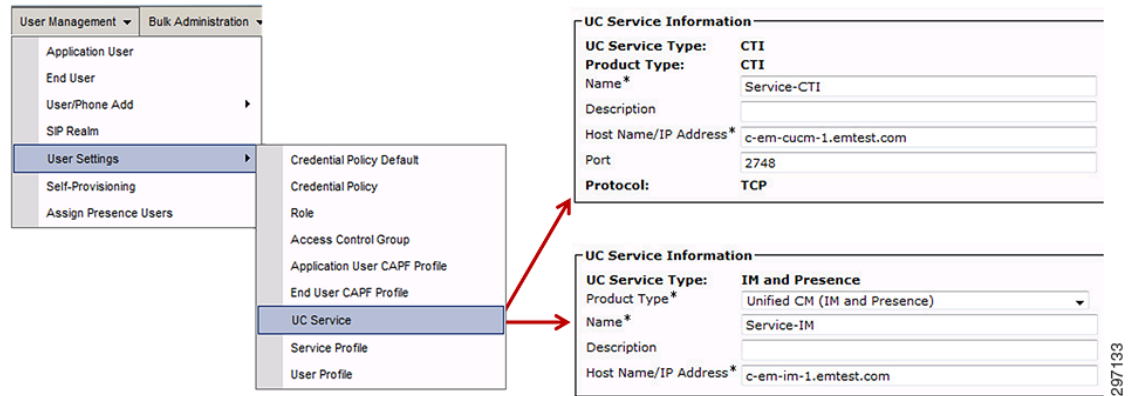
297132

After completing LDAP configuration, be sure to click **Perform Full Sync Now**, shown in the “LDAP Directory” box in [Figure 26-12](#), to ensure all user accounts are synchronized.

User Configuration

Users are synchronized from LDAP and must have a service profile applied and associated with one or more devices. To begin, two basic UC Services are created, as shown in [Figure 26-13](#).

Figure 26-13 UC Services

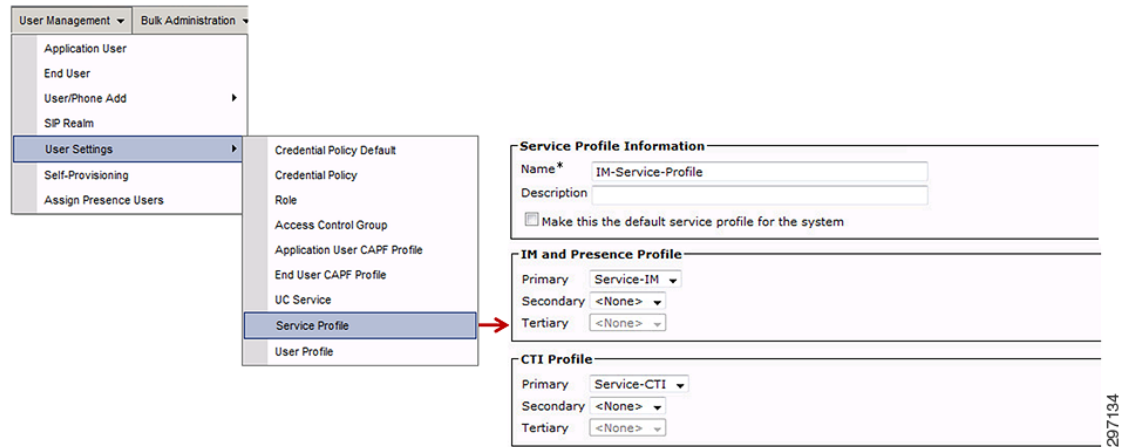


Note

CTI service is shown being created in the above example. Only desktop Jabber clients support CTI services and only when not using Expressway. CTI services configuration are ignored by mobile and Expressway clients, but the same profile may be used for all clients.

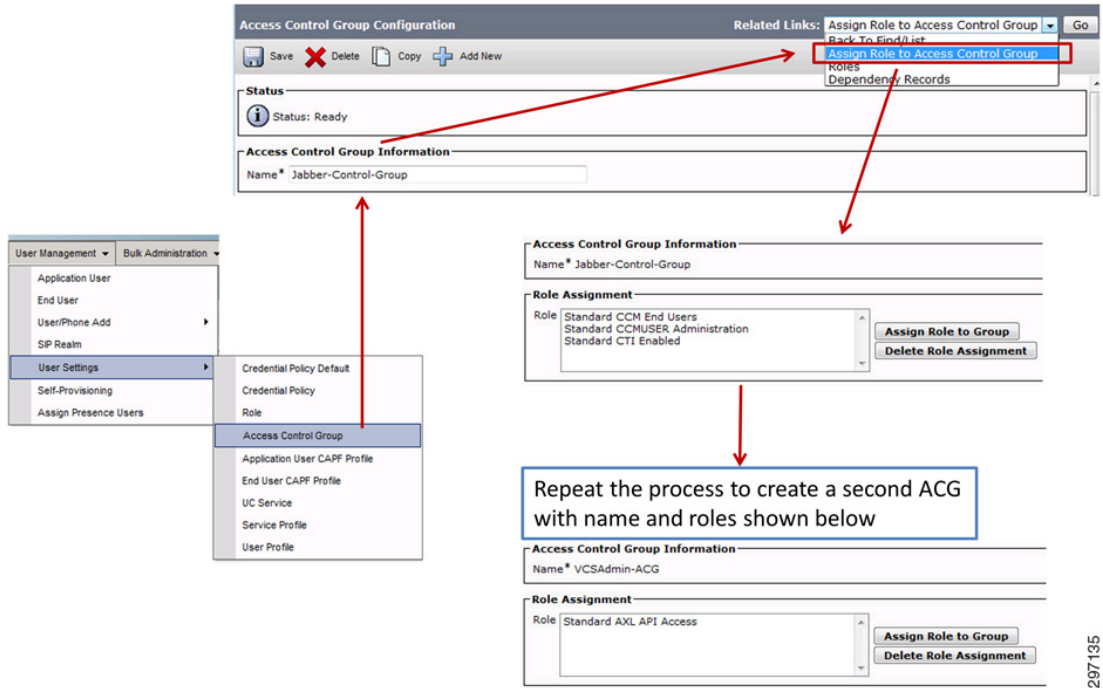
Next a Service Profile is created and the three services are associated with it, as shown in Figure 26-14.

Figure 26-14 UC Service Profile



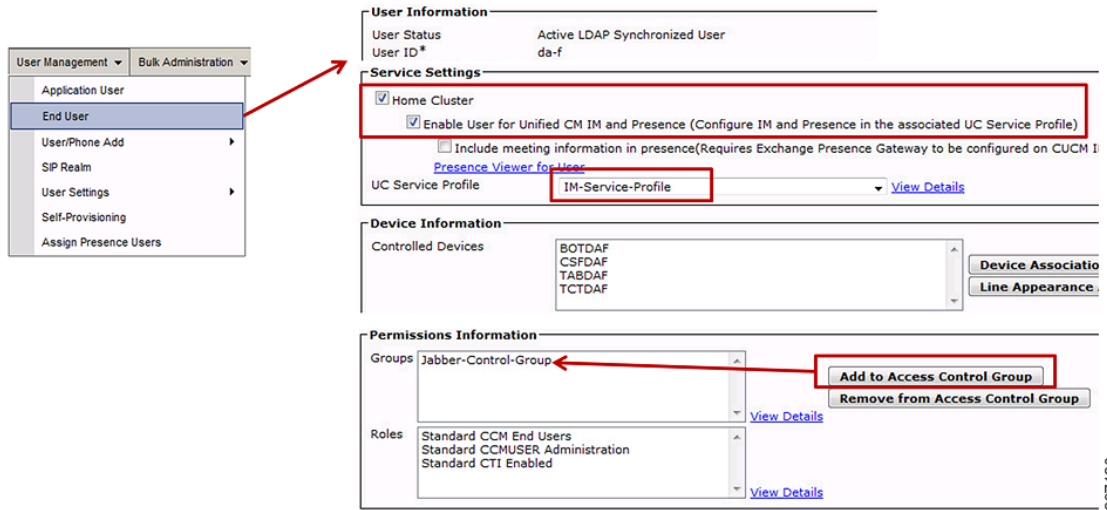
An Access Control Group (ACG) for all Jabber users is created, followed by another ACG for the Expressway Control server, which is used later in the configuration.

Figure 26-15 Access Control Group



The users are then enabled for IM and Presence, associated with the UC Service Profile, and Jabber Access Control Group created earlier.

Figure 26-16 End User Association



Finally, an application user account is created for Expressway-C to access the Unified CM and IM&P servers. This account is created locally on Unified CM. The Access Control Group (VCSAdmin-ACG) created earlier is applied.

Figure 26-17 Expressway Admin User

The screenshot displays the configuration interface for an Expressway Admin User. On the left, a navigation menu includes 'User Management' and 'Bulk Administration' tabs, with 'Application User' selected. The main configuration area is split into two sections: 'Application User Information' and 'Permissions Information'. In the first section, the 'User ID*' is set to 'vcsadmin', and both 'Password' and 'Confirm Password' fields are masked with dots. The second section, 'Permissions Information', shows 'Groups' set to 'VCSAdmin-ACG' and 'Roles' set to 'Standard AXL API Access'. To the right of the Groups list are two buttons: 'Add to Access Control Group' and 'Remove from Access Control Group'. Below both the Groups and Roles lists are 'View Details' links. A vertical page number '297137' is located on the right edge of the screenshot.

Device Configuration

Devices are created for multiple Jabber types. In the example in [Figure 26-18](#), a Dual Mode for Android Jabber type is used for the device, but multiple devices such as Android, iPhone, iPad, Windows, and some other endpoints may all be associated with the same user and directory number/line.

Figure 26-18 Device Configuration

Phone Type
 Product Type: Cisco Dual Mode for Android
 Device Protocol: SIP

Real-time Device Status
 Registration: Unknown
 IPv4 Address: None

Device Information

Device is Active
 Device is trusted

Device Name* BOTDAF

Description Android - da-f

Device Pool* Default

Common Device Configuration < None >

Phone Button Template* Standard Dual Mode for Android

Softkey Template < None >

Common Phone Profile* Standard Common Phone Profile

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List < None >

User Hold MOH Audio Source < None >

Network Hold MOH Audio Source < None >

Location* Hub_None

AAR Group < None >

User Locale < None >

Network Locale < None >

Privacy* Default

Device Mobility Mode* Default

Owner User Anonymous (Public/Shared Space)

Owner User ID* da-f

Users Associated with Line

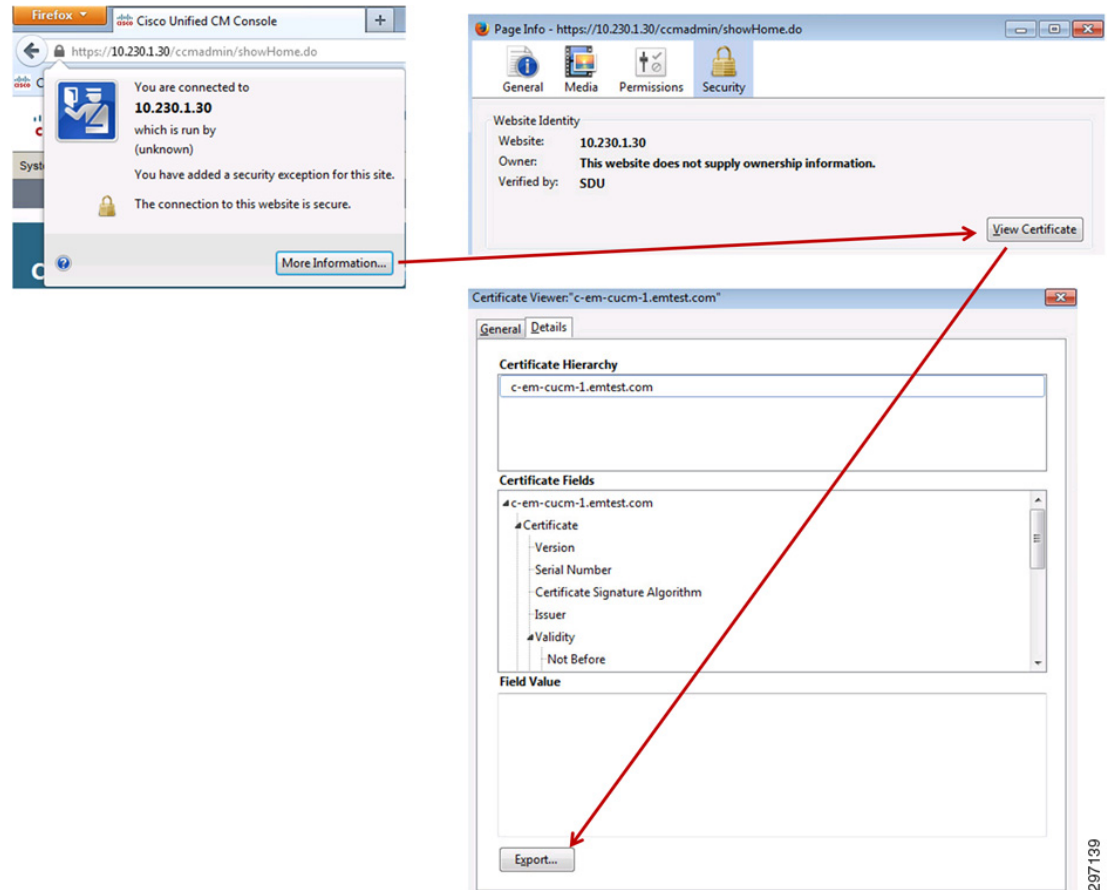
	Full Name	User ID
<input type="checkbox"/>	da-f	da-f

Associate End Users Select All Clear All Delete Selected

When creating a device to be used with IM and Presence as well as with Expressway, associating the User ID with both the Device and Directory Number/Line is essential for proper operation and is an easily overlooked item.

Certificate Export

Communication between UC components and Expressway-C requires certificates. This process usually involves creating unique self-signed certificates. A quick way to get the implementation up initially is to export the existing Unified CM and IM &P web server certificates to be imported to the Expressway-C. In this example, one Unified CM and one IM&P server exist. An easy way to quickly export the cert is to simply use a web browser pointed at the server, as shown in Figure 26-19.

Figure 26-19 Public Certificate Export

Using Firefox, the public cert is easily exported and saved locally to be imported into the Expressway Control server, as described in the next section.

Expressway Configuration

To begin, the basic IP connectivity of the Expressway servers is assumed completed. While part of basic connectivity, it is worth mentioning that accurate NTP synchronization is essential for proper operation. Expressway will not function without all components properly synchronized to one or more reliable NTP sources. The Expressway solution relies heavily on X.509 Certificates for the TLS connections and, if the time gets out of synchronization, this can have a significantly negative affect on the ability of the endpoints/Expressway servers to validate the exchanged certificates, greatly increasing the possibility of an outage.

Importing Certificates for Unified CM and IM&P

As shown in [Figure 26-20](#), the certificates exported from Unified CM and IM&P are imported into the Expressway-C server as Trusted CA certificates. There is no need to import these certificates into the Expressway-E server.

Figure 26-20 Certificate Import

The screenshot displays the 'Trusted CA certificate' configuration page. On the left, a navigation menu is open to 'Security certificates' > 'Trusted CA certificate'. The main content area features a table of certificates:

Type	Issuer
<input type="checkbox"/> Certificate	O=Temporary CA 35cfa4c6-bfdb-11e3-b553-005056a3e603, OU=Temporary CA 35cfa4c6-bfdb-11
<input type="checkbox"/> Certificate	O=SDU, OU=ST, CN=c-em-cucm-1.emtest.com
<input type="checkbox"/> Certificate	O=SDU, OU=ST, CN=c-em-in-1.emtest.com
<input type="checkbox"/> Certificate	CN=emtest-C-EM-CA-1-CA

Below the table are buttons: 'Show all (decoded)', 'Show all (PEM file)', 'Delete', 'Select all', and 'Unselect all'. An 'Upload' section contains a 'Browse...' button. At the bottom, there are buttons for 'Append CA certificate' and 'Reset to default CA certificate'.

297140

Basic Networking (DNS, Routing)

Figure 26-21 and Figure 26-22 show the basic IP configuration of Expressway-C and E for reference.

Figure 26-21 Expressway-C IP Configuration

The screenshot displays the 'IP Configuration' page. The 'IP' section is active, and the 'Configuration' tab is selected. The page shows settings for IP protocol (IPv4), Use dual network interfaces (No), IPv4 gateway (10.230.1.1), and IPv6 gateway. Below this, the 'LAN 1' section is active, showing settings for IPv4 address (10.230.1.35), IPv4 subnet mask (255.255.255.0), IPv4 subnet range (10.230.1.0 - 10.230.1.255), IPv6 address, and Maximum transmission unit (MTU) (1500).

297141

Figure 26-22 Expressway-E IP Configuration

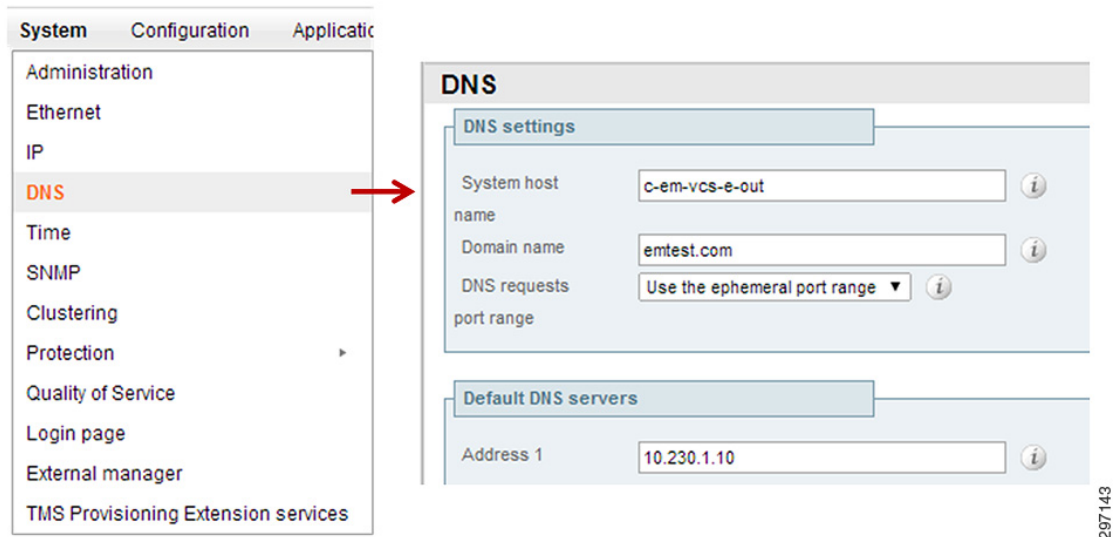
Status	System	Configuration	Applications	Users	Maintenance
IP					
Configuration					
IP protocol		↑ IPv4			
Use dual network interfaces		Yes			
External LAN interface		LAN2			
IPv4 gateway		↑ 10.253.1.1			
IPv6 gateway		↑			
LAN 1 - Internal					
IPv4 address		↑ 10.252.1.35			
IPv4 subnet mask		↑ 255.255.255.0			
IPv4 subnet range		10.252.1.0 - 10.252.1.255			
IPv4 static NAT mode		↑ Off			
IPv6 address		↑			
Maximum transmission unit (MTU)		* ↑ 1500			
LAN 2 - External					
IPv4 address		↑ 10.253.1.35			
IPv4 subnet mask		↑ 255.255.255.0			
IPv4 subnet range		10.253.1.0 - 10.253.1.255			
IPv4 static NAT mode		↑ On			
IPv4 static NAT address		↑ 172.26.137.29			
IPv6 address		↑			
Maximum transmission unit (MTU)		* ↑ 1500			

297142

Expressway DNS and Domain

Figure 26-23 shows the DNS configuration for Expressway-E. Both Expressway-E and Expressway-C must have the System Host Name and Domain Name properly assigned in the DNS settings shown below. The values in these fields are used during the creation of certificates for communication between Expressway servers and for configuration files sent to Jabber clients.

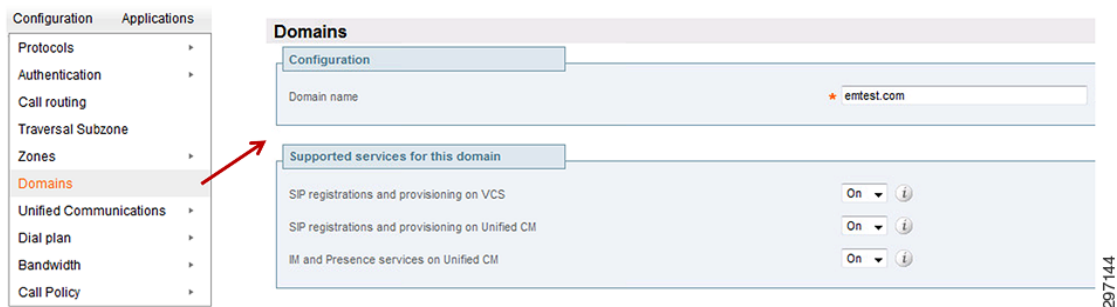
The system host name for Expressway-E must be the DNS host name of the outside NAT address the Jabber clients use to communicate with Expressway. In this example c-em-vcs-e-out is the correct hostname to use here.

Figure 26-23 Expressway-E DNS Settings

Expressway-C system host name is c-em-vcs-c-1.

Expressway-C Domain

Expressway-C also needs the domain defined in a separate section, as shown in [Figure 26-24](#). This is not required for Expressway-E.

Figure 26-24 Expressway-C Domain Configuration

Expressway-E Routing

While basic IP connectivity and routing is defined in the graphical interface shown previously, one piece must be completed via command line for this deployment model. The Expressway-E has a default route to 10.253.1.1, but no route back into the internal network through 10.252.1.1. This route must be statically defined.

Below is the Cisco ip route command, followed by the route statement that would be executed on the Expressway CLI to accomplish the same.

Cisco route statement as an example:

```
ip route 10.230.1.0 255.255.255.0 10.252.1.1
```

Equivalent Expressway static route statement:

```
xCommand RouteAdd Address: "10.230.1.0" PrefixLength: 24 Gateway: "10.252.1.1"
```

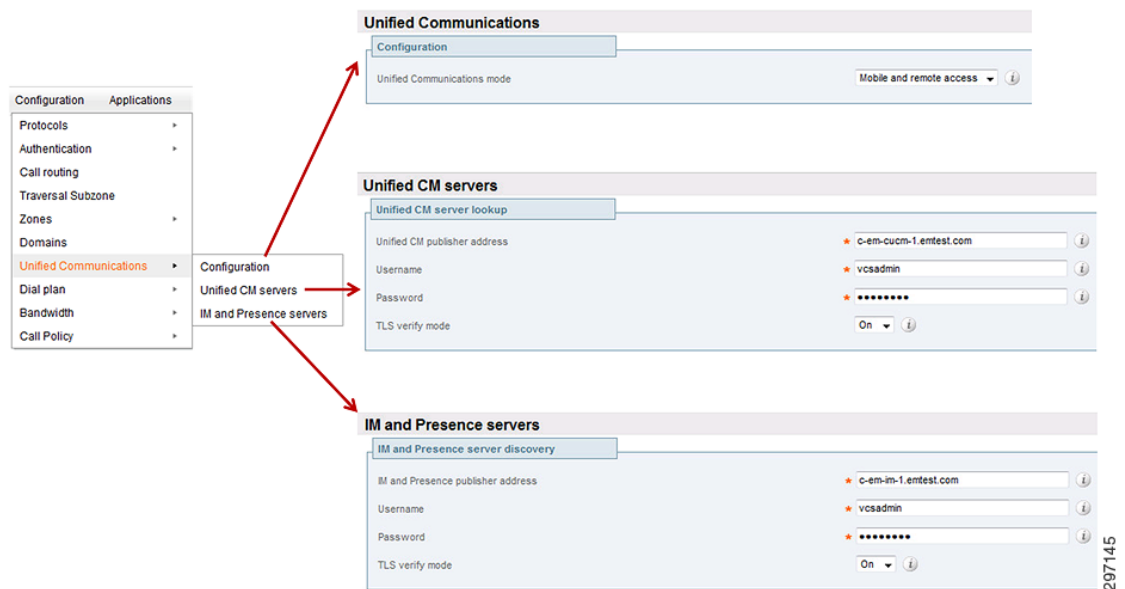
Additional Expressway route statements:

```
xConfiguration ip route (list all static routes)
xCommand RouteDelete RouteId: 1 (delete a static route #1)
```

Expressway-C to Unified CM + IM&P Configuration

With public certificates installed for Unified CM and IM&P, the next step is to configure Expressway-C to communicate with those servers, as shown in [Figure 26-25](#). The account used is the local user account “vcsadmin” created earlier on Unified CM.

Figure 26-25 Expressway-C UC Configuration



Expressway-C to Expressway-E Configuration

Certificate Creation

The first step to establishing communication between Expressway-C and Expressway-E is to generate certificates used for this communication. [Figure 26-26](#) and [Figure 26-27](#) show the screen for generating a certificate signing request for Expressway-C and Expressway-E. Refer to the documentation referenced in [Appendix B, “References”](#) for specific information related to certificate creation.



Note

Before generating the certificate signing request on the Expressway-C server, copy the contents of the field entitled “IM and Presence Chat Node Aliases” to the same field on the Expressway-E certificate signing request page. This value is auto-generated on Expressway-C, but must be manually entered on Expressway-E.

Figure 26-26 Expressway-C Certificate Signing Request

Maintenance

- Upgrade
- Logging
- Option keys
- Tools
- Security certificates
 - Trusted CA certificate
 - Server certificate
 - CRL management
 - Client certificate testing
 - Certificate-based authentication configuration
- Backup and restore
- Diagnostics
- Maintenance mode
- Language
- Restart options

Generate CSR

Common name

Common name: FQDN of VCS
Common name as it will appear: c-em-vcs-c-1.emtest.com

Alternative name

Additional alternative names (comma separated):
IM and Presence chat node aliases: conference-2-StandAloneCluster8b025.emtest.com
Unified CM phone security profile names:
Alternative name as it will appear: c-em-vcs-c-1.emtest.com,conference-2-StandAloneCluster8b025.emtest.com

Additional information

Key length (in bits): 2048
Country: US
State or province: North Carolina
Locality (town name): RTP
Organization (company name): Cisco
Organizational unit: SDU

Generate CSR

297146

Expressway-E requires the FQDN of the internal interface, c-em-vcs-e-1.emtest.com, to be used as an alternative name in the CSR to allow communication between Expressway-C and Expressway-E.

Figure 26-27 Expressway-E Certificate Signing Request

Generate CSR You are here: [Main](#)

Common name

Common name	FQDN of Expressway
Common name as it will appear	c-em-vcs-e-out.emtest.com

Alternative name

Additional alternative names (comma separated)	c-em-vcs-e-1.emtest.com <i>i</i>
Unified Communications domains	emtest.com <i>i</i>
IM and Presence chat node aliases	conference-2-StandAloneCluster8b025.emtest.com <i>i</i>
Alternative name as it will appear	c-em-vcs-e-out.emtest.com,c-em-vcs-e-1.emtest.com,emtest.com,conference-2-StandAloneCluster8b025.emtest.com

Additional information

Key length (in bits)	2048 <i>i</i>
Country	* US <i>i</i>
State or province	* North Carolina <i>i</i>
Locality (town name)	* RTP <i>i</i>
Organization (company name)	* Cisco <i>i</i>
Organizational unit	* SDU <i>i</i>

297147

Traversal Zone

A traversal zone is defined on both the Expressway-C and Expressway-E servers. Expressway-C establishes a TCP connection to Expressway-E using an account defined locally on Expressway-E. Since Expressway-E receives the connection, it is shown being configured first.

Expressway-E is shown configured as the receiver of the Traversal Zone connection. The local user account used to establish this connection may be created from a link within the zone configuration screen, as shown in [Figure 26-28](#).

Figure 26-28 Expressway-E Traversal Zone

The screenshot displays the configuration for a Traversal Zone on a Cisco Expressway-E device. The main configuration area is divided into several sections:

- Configuration:** Name is set to "Traversal Zone", Type is "Traversal server", and Hop count is "15".
- Connection credentials:** Username is "vcstraversal" and Password is "*****". A link "Add/Edit local authentication database" is provided.
- H.323:** Mode is "Off", Protocol is "Assent", and H.460.19 demultiplexing mode is "Off".
- SIP:** Mode is "On", Port is "7001", Transport is "TLS", Unified Communications services is "Yes", TLS verify mode is "On", TLS verify subject name is "c-em-vcs-c-1.emtest.com", Accept proxied registrations is "Allow", Media encryption mode is "Force encrypted", ICE support is "Off", and Poison mode is "Off".

A sidebar on the left shows the navigation menu with "Zones" selected. A "Local authentication database" window is also visible, showing the configuration for the "vcstraversal" user with Name "vcstraversal" and Password "*****".

297148

Following that, the Expressway-C is configured as the originator of the Traversal Zone connection, as shown in [Figure 26-29](#), using the same account credentials just created in the previous step.

Figure 26-29 Expressway-C Traversal Zone

The screenshot displays the configuration interface for a Traversal Zone on Expressway-C. The left sidebar shows a navigation menu with 'Zones' selected. The main content area is divided into sections: Configuration, Connection credentials, H.323, SIP, and Location. A red arrow points from the 'Zones' menu item to the 'Configuration' section. The Configuration section shows Name: Traversal Zone, Type: Traversal client, and Hop count: 15. Connection credentials show Username: vc traversal and Password: [redacted]. H.323 shows Mode: Off and Protocol: Assent. SIP shows Mode: On, Port: 7001, Transport: TLS, Unified Communications services: Yes, TLS verify mode: On, Accept proxied registrations: Allow, Media encryption mode: Force encrypted, ICE support: Off, and Poison mode: Off. The Location section shows Peer 1 address: c-em-vcs-e-1.emtest.com.

Once communication is established, the Location field at the bottom of the Traversal Zone screen shows a “reachable” message, as shown in [Figure 26-30](#).

Figure 26-30 Expressway-E Traversal Zone Status

The screenshot shows the status of the Traversal Zone on Expressway-E. The Location section displays the Peer 1 address as c-em-vcs-e-1.emtest.com and the status as SIP: Reachable: 10.252.1.35:7001.

Note that this message may display “reachable” while other issues still exist between Expressway-C and Expressway-E, such as improper firewall configuration. Also, in certain configurations, this status may show reachable with the peer address pointing to the incorrect interface on Expressway-E. A status of “reachable” does not necessarily mean “functional”.

Firewall Configuration

The Cisco ASA configuration is the most critical piece for proper AnyConnect compatibility with Expressway clients running Cisco Jabber. The Cisco ASA is used for termination of AnyConnect tunnels as well as filtering key DNS records that prevent Jabber clients from consistently connecting through Expressway when AnyConnect is on the same device.

Port requirements for communication between Expressway-C and Expressway-E, as well as between clients and Expressway-E, are well documented in the documentation listed in [Appendix B, “References.”](#) The following section covers how SRV record filtering is enabled on the Cisco ASA used in the example configuration.

ASA SRV Filtering for AnyConnect Support

SRV filtering is achieved through implementation of a regular expression match within the Cisco ASA firewall. This match will match against key SRV DNS requests coming from the client and drop them, preventing them from reaching the internal DNS servers. The Jabber client is looking for responses from three key SRV records:

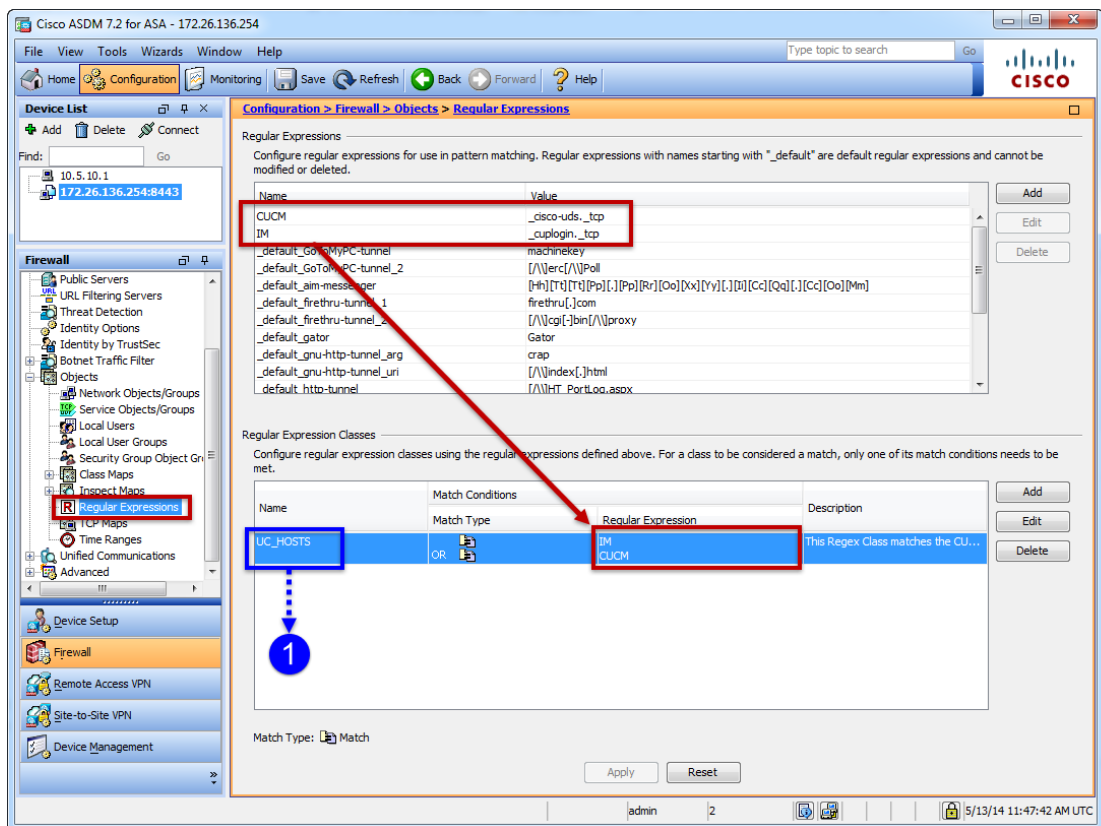
- `_cisco-uds._tcp`—Unified CM
- `_cuplogin._tcp`—Cisco Unified Presence (CUP) 8.X¹
- `_collab-edge._tls`—Expressway-E outside interface

If the Jabber client receives either of the first two SRV records, `_cisco-uds` or `_cuplogin`, it does not attempt to connect to the Expressway server even when the Expressway SRV record, `_collab-ede`, is present.

Regular Expressions

Two regular expressions are created, CUCM and IM. These are applied to a Regular Expression Class, UC_HOSTS.

Figure 26-31 ASA Regular Expression Configuration

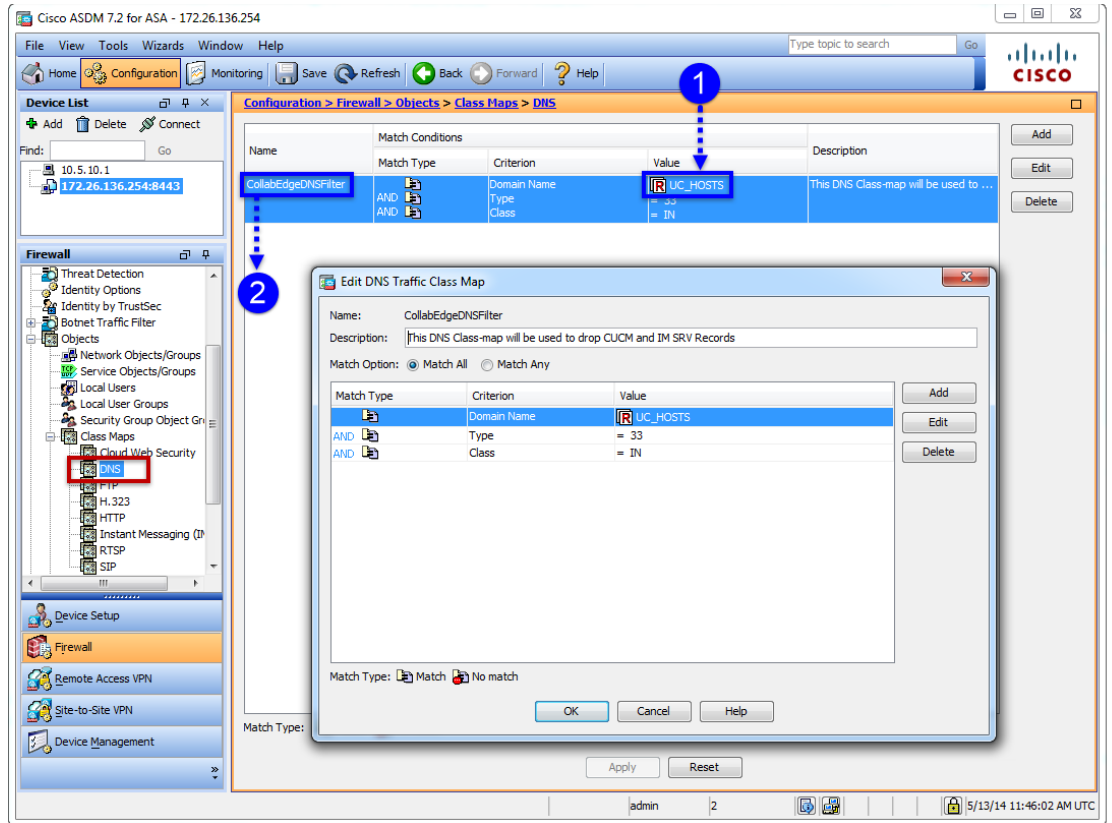


1. SRV record `_cuplogin._tcp` is only used for CUP 8.X implementations. CUP 8.X is not compatible with the Expressway solution, but the existence of this record could cause issues and should be filtered as a preventative measure. This record may exist due to a previous implementation of CUP.

DNS Class Map

UC_HOSTS is applied as a match condition to a DNS Class Map, CollabEdgeDNSFilter. Also contained in the Class Map are matches against the Type=33 (SRV) and Class=IN (Internet origin).

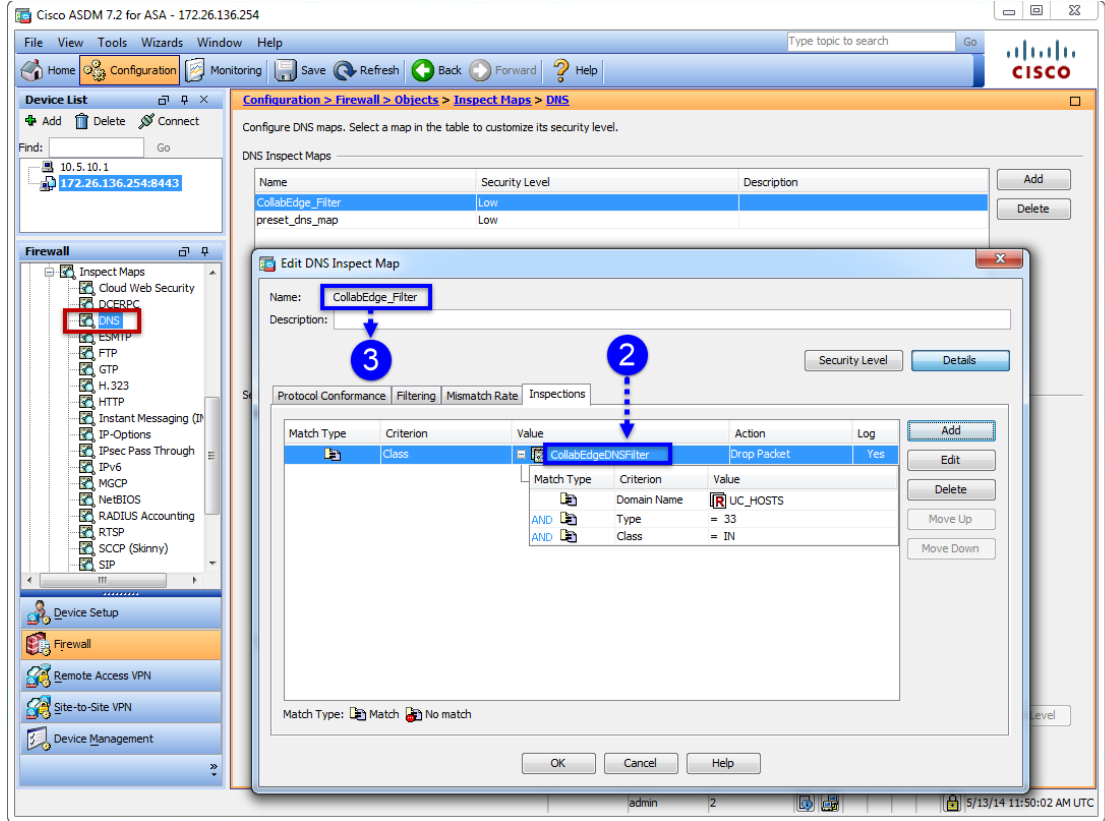
Figure 26-32 ASA DNS Class Map Configuration



DNS Inspect Map

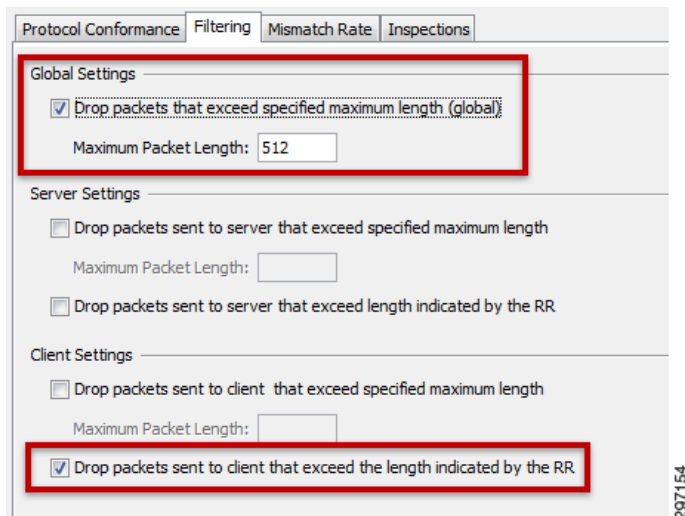
DNS Class Map, CollabEdgeDNSFilter, is applied to a DNS Inspect Map, CollabEdge_Filter.

Figure 26-33 ASA DNS Inspect Map Configuration—1 of 2



Additional default settings under the Filtering tab on the DNS Inspect Map need to be confirmed as selected, as shown in Figure 26-34.

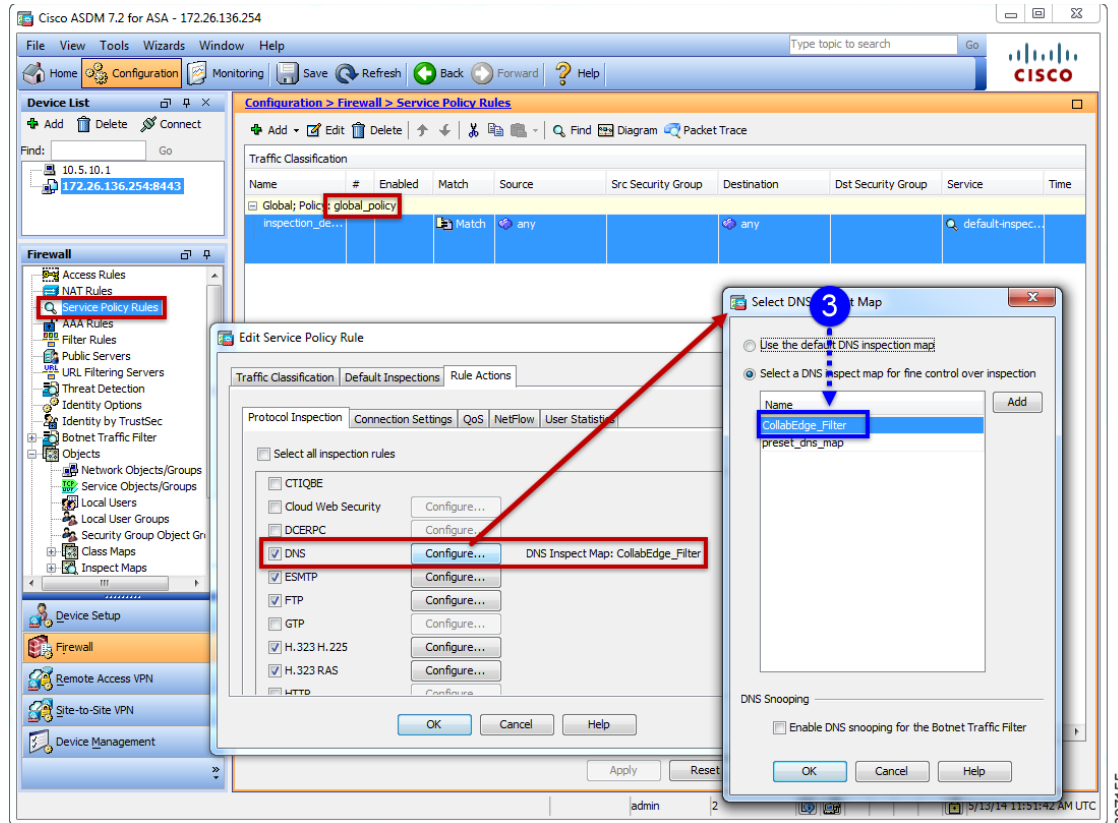
Figure 26-34 ASA DNS Inspect Map Configuration—2 of 2



Service Policy Rule

DNS Inspect Map, CollabEdge_Filter, is applied to a Service Policy, inspection_default, which is applied as a Global Service Policy.

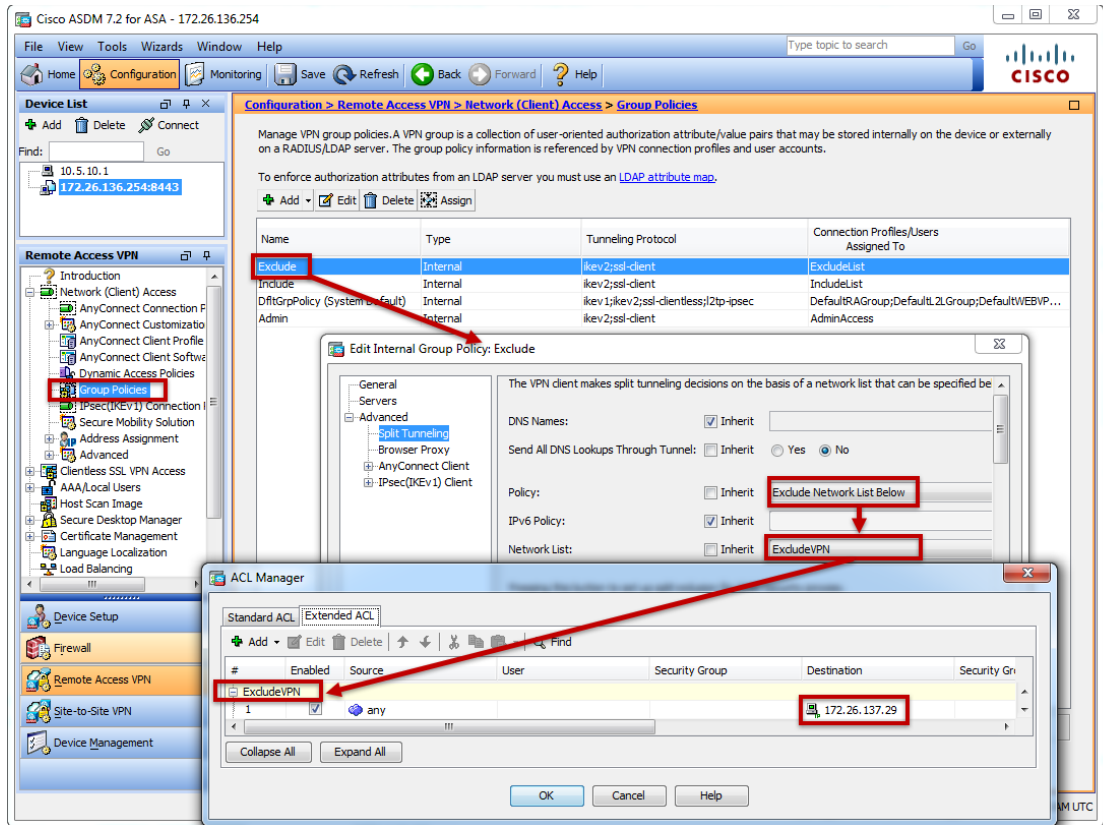
Figure 26-35 ASA Service Policy Rule



Split-Tunnel Exclude for Expressway-E server

The split-tunnel exclude illustrated in Figure 26-36 excludes the external NAT address of the Expressway-E server, 172.26.137.29, allowing clients to maintain an external connection to Expressway-E when the Cisco AnyConnect tunnel is active.

Figure 26-36 ASA Split-Tunnel Exclude



Note

The AnyConnect client for Android devices that are not Samsung branded does not support split-tunnel exclude. All other AnyConnect clients, including the Android client for Samsung devices, supports split-tunnel exclude. Non-Samsung Android devices do support split-tunnel include, so an alternate group policy may be implemented using split-tunnel include instead of split-tunnel exclude.

Note

For split-exclude to work properly with The AnyConnect client for Samsung Android devices, an “AnyConnect Client Profile” may need to be defined on the ASA with “Allow Local LAN Access” enabled.

Relevant configuration excerpts from Cisco ASA are shown below:

```

regex CUCM "_cisco-uds._tcp"
regex IM "_cuplogin._tcp"
!
access-list ExcludeVPN extended permit ip any host 172.26.137.29
!
group-policy Exclude internal
group-policy Exclude attributes
wins-server none
dns-server value 10.230.1.10
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy excludespecified
split-tunnel-network-list value ExcludeVPN
default-domain value emtest.com

```



```
address-pools value Exclude
webvpn
  anyconnect profiles value CollabEdgeScenarios type user
  anyconnect ask none default anyconnect
!
class-map type regex match-any UC_HOSTS
  description This Regex Class matches the CUCM or IM servers.
  match regex IM
  match regex CUCM
class-map inspection_default
  match default-inspection-traffic
class-map type inspect dns match-all CollabEdgeDNSFilter
  description This DNS Class-map will be used to drop CUCM and IM SRV Records
  match domain-name regex class UC_HOSTS
  match dns-type eq 33
  match dns-class eq IN
!
!
policy-map type inspect dns CollabEdge_Filter
  parameters
    message-length maximum client auto
    message-length maximum 512
  class CollabEdgeDNSFilter
    drop log
policy-map global_policy
  class inspection_default
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect dns CollabEdge_Filter
!
service-policy global_policy global
```

Figure 26-37 shows DNS-SRV filtering configuration excerpts from the ASA with referencing annotation.

Figure 26-37 ASA Configuration Excerpts

```

regex CUCM "_cisco-uds._tcp"
regex IM "_cuplogin._tcp"
!
class-map type regex match-any UC_HOSTS
description This Regex Class matches the CUCM or IM servers.
match regex IM
match regex CUCM
class-map inspection_default
match default-inspection-traffic
class-map type inspect dns match-all CollabEdgeDNSFilter
description This DNS Class-map will be used to drop CUCM and IM SRV Records
match domain-name regex class UC_HOSTS
match dns-type eq 33
match dns-class eq IN
!
!
policy-map type inspect dns CollabEdge_Filter
parameters
message-length maximum client auto
message-length maximum 512
class CollabEdgeDNSFilter
drop log
policy-map global_policy
class inspection default
inspect dns CollabEdge_Filter
!
service-policy global_policy global

```

297157

**Note**

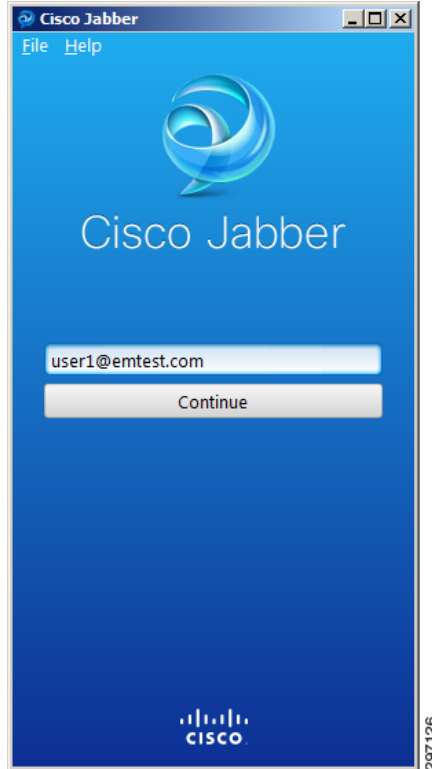
Some version of ASDM may not apply the “inspect dns” command correctly to the global policy-map. In the example above, “inspect dns CollabEdge_Filter” may be applied as “inspect dns”, leaving off “CollabEdge_Filter”. It is advisable to check the configuration for this issue if configuring through ASDM.

Connection Scenarios

When a Jabber client gets a network connection, the device gets the address of a DNS name server from the DHCP server. Depending on the network connection, the DNS server might be internal or external to the corporate network.

This Cisco Jabber client uses the DNS name server received from the DHCP server. The user’s ID and domain is used to log in to Jabber and to determine the services domain, which is used in combination with DNS SRV records to query the DNS server. The login screen shown in [Figure 26-38](#), taken from an Android Jabber client, shows the services domain as emtest.com.

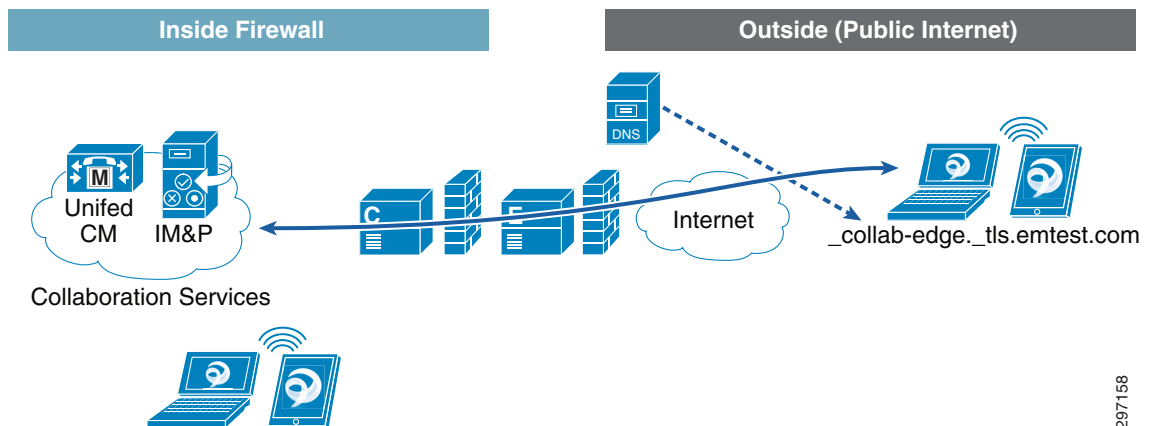
Figure 26-38 Jabber Login Screen



From the Internet

Cisco Jabber clients connecting from outside the corporate network (or public Internet) query their public DNS server for the SRV records. The DNS server resolves the `_collab-edge` SRV record and allows the Jabber client to connect through Expressway.

Figure 26-39 Jabber Client Connecting from the Internet



In this configuration the client connects to the Collaboration Services servers through Expressway. This VPN-less service is attractive for users that require seamless Jabber collaboration from any location without the need for a VPN session.

Cisco AnyConnect Secure Mobility Client

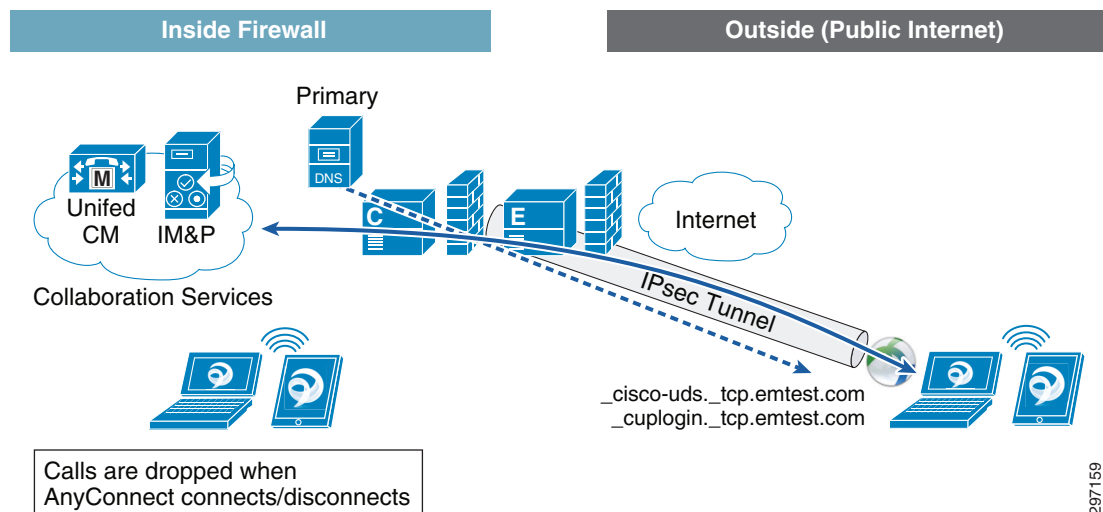
The Cisco AnyConnect Secure Mobility Client provides secure connectivity across a broad set of desktop and mobile devices. This is ideal for mobile users requiring connectivity from different locations and the always-on, intelligent VPN offered by the AnyConnect client. The AnyConnect client selects the optimal network access location and adapts its tunneling protocol to the most efficient method.

The AnyConnect client is designed for mobile users and can be configured so that a VPN connection remains established during IP address changes or loss of connectivity. It is also able to automatically connect when the user is at a remote location and disconnect when the user is in the office.

The AnyConnect client provides full-tunneling access to enterprise resources and applications, providing a consistent LAN-like user experience and is supported in Windows PC, Macs, and Android and iOS devices.

The Jabber client shown in [Figure 26-40](#) is connecting from the public Internet and has established a VPN connection that securely tunnels all traffic from the device into the enterprise. This allows the client to access resources from the enterprise and use the internal DNS name server for resolution.

Figure 26-40 Cisco AnyConnect Client VPN Tunnel



AnyConnect and Expressway Co-existence

In the scenario shown in [Figure 26-40](#), a Jabber session is established to allow the client to interact via voice, video, and IM sessions with other Jabber users.

A problem arises when the client disconnects the AnyConnect session, causing an active Jabber session to drop. This has a negative impact on the user's experience, since an active voice or video call is disconnected. The impact to IM sessions is minimal, since the IM session reconnects shortly after.

For AnyConnect and Expressway to coexist, the Jabber client must be able to reach the Expressway-E without relying on the VPN tunnel. By reaching the Expressway-E server independently from the AnyConnect tunnel, Jabber calls remain up and the collaboration experience is maintained.

To achieve this configuration, the following must be in place:

- Enable split tunneling on the ASA firewall to remove the Expressway-E address from the tunnel.
- Control which SRV records are resolved from the client to force the Jabber client to connect through Expressway.

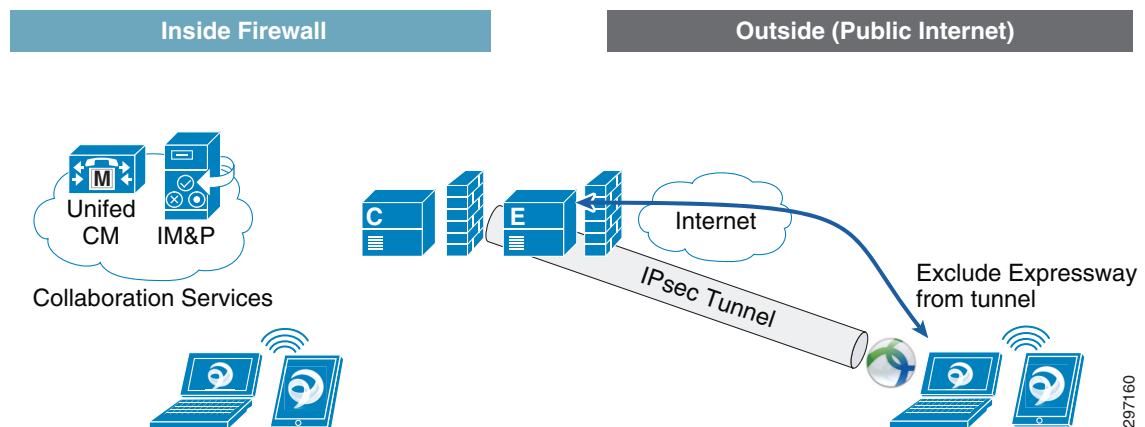
Split Tunneling

The split tunnel feature on the ASA allows administrators to specify which traffic traverses the VPN tunnel and which traffic goes in the clear. In this case, all traffic should traverse the VPN tunnel with the exception of the Expressway server address.

By removing the Expressway IP address from the VPN tunnel, the Jabber client connects through Expressway even when the AnyConnect client connects or disconnects from the ASA, ensuring that the Jabber session remains connected.

Figure 26-41 shows how the Expressway address is removed from the VPN tunnel and traverses the Internet while the rest of the traffic relies on the tunnel to reach corporate resources.

Figure 26-41 Excluding Expressway from Tunnel

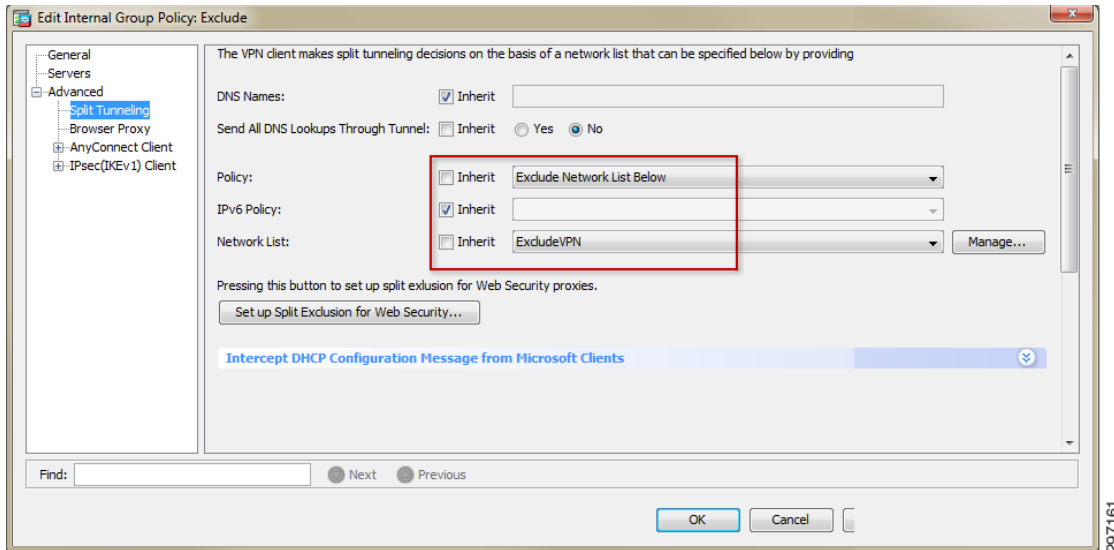


In ASA configuration, the Exclude Network List feature defines a list of networks to which traffic is sent in the clear. The example shown in Figure 26-42 creates an Exclude Network List with the Expressway-E IP address, removing the IP address from the tunnel.



Note

[Configuring Cisco Expressway Mobile and Remote Access](#) provides more details on the ASA configuration.

Figure 26-42 Excluding Expressway from Tunnel

Controlling SRV Records

Since the Jabber client relies on SRV records to determine its service location, the network elements can be configured to filter or deliver the appropriate SRV records. When the client receives a resolution for the `_collab-edge` SRV record, the client uses the Expressway server to reach the Collaboration Services servers.

This document explores a way of controlling what SRV records are provided to the client, assuming split tunneling has been configured on the ASA.

Filtering SRV Records at the ASA

The Cisco ASA may be configured to prevent `_cuplogin` and `_cisco-uds` SRV requests from reaching the DNS server. A regular expression is configured to match the content of certain traffic. In this case, the ASA looks for the strings `_cisco-uds` or `_cuplogin`.

Once the regular expression is defined, a class-map is used to identify traffic based on the regular expression and prevent DNS SRV requests records from reaching the server. [Figure 26-43](#) shows how the regular expression is defined on the ASA.

Figure 26-43 Regular Expressions in ASA

The screenshot shows the Cisco ASDM 7.2 for ASA configuration page for Regular Expressions. The left sidebar shows the navigation tree with 'Regular Expressions' selected under 'Objects'. The main content area is divided into two sections: 'Regular Expressions' and 'Regular Expression Classes'.

Regular Expressions

Configure regular expressions for use in pattern matching. Regular expressions with names starting with "_default" are default regular expressions and cannot be modified or deleted.

Name	Value
CUCM	_cisco-uds._tcp
IM	_cuplogin._tcp
_default_GoToMyPC-tunnel	machinekey
_default_GoToMyPC-tunnel_2	[A\\]erc[A\\]Poll
_default_aim-messenger	[h][t][t][p][.]([p][r][o][x][y])
_default_frethru-tunnel_1	frethru[.]com
_default_frethru-tunnel_2	[A\\]cp[.]bin[A\\]proxy
_default_gator	Gator
_default_gnu-http-tunnel_arg	crap
_default_gnu-http-tunnel_uri	[A\\]index[.]html
default_http-tunnel	[A\\]HT_PortLoc.aspx

Regular Expression Classes

Configure regular expression classes using the regular expressions defined above. For a class to be considered a match, only one of its match conditions needs to be met.

Name	Match Conditions	Regular Expression	Description
Match Type		Regular Expression	Description
UC_HOSTS	OR	IM CUCM	This Regex Class matches the CU...

Match Type: Match

Buttons: Add, Edit, Delete, Apply, Reset

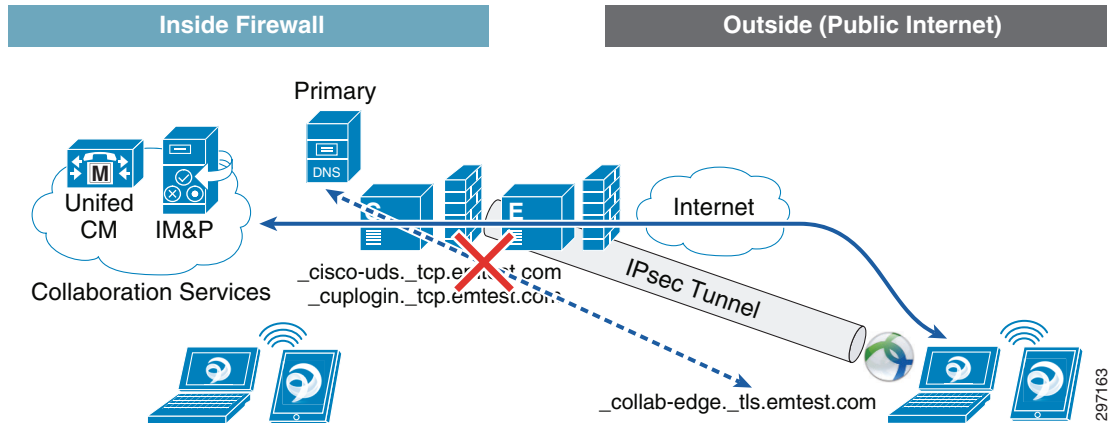
**Note**

Configuring Cisco Expressway Mobile and Remote Access provides more details on the ASA configuration.

Since the Jabber client only receives a response for the _collab-edge SRV record, the client makes use of Expressway independent of VPN to reach the collaboration services and to communicate with other Jabber clients. Changes in AnyConnect client do not impact any active Jabber connections.

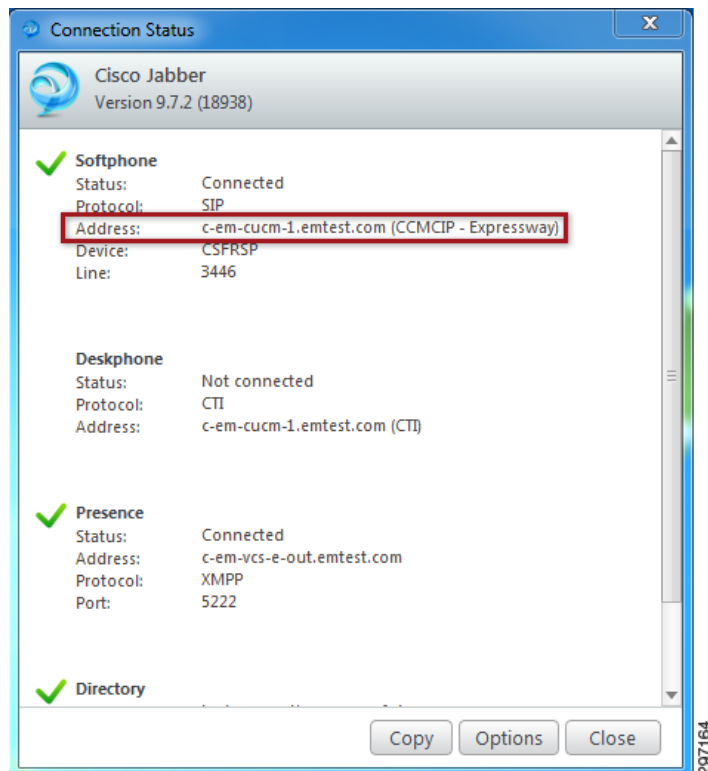
Figure 26-44 shows how the ASA has filtered the internal SRV records and how the client only receives the _collab-edge SRV record.

Figure 26-44 Filtering SRV Records at ASA



A simple way to verify that the Jabber client is connecting through Expressway is by checking the Connection Status in the Windows Jabber client. Figure 26-45 shows the Connection Status from a Windows Jabber client. This information is not available in mobile Jabber clients.

Figure 26-45 Cisco Jabber Status



Filtering DNS SRV records at the ASA leverages existing hardware and software and does not require additional servers to manage or deploy.

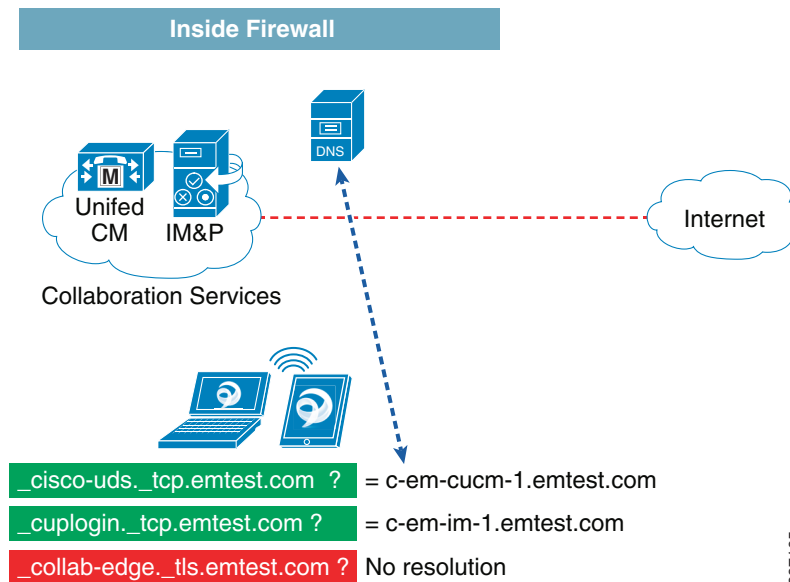
From the Corporate Network

A Cisco Jabber connection initiated from inside the corporate network does not require Expressway services and signs in directly with on-premise collaboration services (e.g., Cisco Unified Communications Manager and IM & Presence).

Primary DNS Server

Figure 26-46 shows a Jabber client receiving the two internal SRV records (`_cisco-uds` and `_cuplogin`) that allow the client to reach the collaboration services servers. By getting a valid response from the DNS server, the client communicates directly with servers and other Jabber clients and does not require Expressway services.

Figure 26-46 Jabber Client inside the Corporate Network



Alternate DNS Server for Differentiated Access

Internal Cisco Jabber clients segmented by internal VLANs/ACLs or other type of filtering can benefit from using Expressway to enable communication.

The BYOD CVD highlights several use cases that provide differentiated access to endpoints, e.g., some clients are granted Partial Access or Internet-Only access based on ISE's authorization profiles. To enforce this Partial or Internet access, Access Control Lists (ACLs) are used to allow/block access to internal resources.

In the case of Partial Access, an ACL, named `ACL_Partial_Access`, provides a way to allow users to reach only the Internet and some internal resources and denies access to all other resources. This can have a negative impact on Cisco Jabber clients, since clients may be connecting from many different segments or VLANs in the network and may need to reach clients on a different VLAN.

The Expressway solution provides an attractive solution to allow Cisco Jabber clients to communicate with each other, bypassing any filtering or network segmentation. By allowing the client to receive only the `_collab-edge` SRV record, the client relies on the Expressway solution, which acts as a proxy for collaboration between two Jabber clients.

A possible way to ensure that the client only gets the `_collab-edge` SRV record is to introduce an Alternate DNS server, which only returns the `_collab-edge` SRV record and not the internal `_cuplogin` and `_cisco-uds` records. Since the DNS server address is provided by the DHCP server, unique DHCP scopes can be created for clients that deserve Full, Partial Access, or Internet Only access.

**Note**

In this scenario, it is not necessary to filter SRV records at the ASA.

VLANs

For devices connecting from the campus location, the VLANs in [Table 26-6](#) were assigned. The VLANs are preconfigured on the switching infrastructure.

Table 26-6 **Virtual LANs**

VLAN	Access Granted
2	Full Access
5	Partial Access
5	Internet Only

To support the VLAN definition shown in [Table 26-6](#), the Wireless LAN Controller is configured with a default VLAN (VLAN 2) to which clients originally connect. The ISE may determine that the client belongs to a different VLAN and can dynamically move the client to a different VLAN.

In addition to an IP address, clients receive the address of a DNS server from the DHCP server. [Figure 26-47](#) shows how clients connecting to VLAN2 receive the IP address of the internal DNS server while clients connecting to VLAN 5 receive the IP address of the Alternate DNS server.

Figure 26-47 DHCP Providing DNS Server

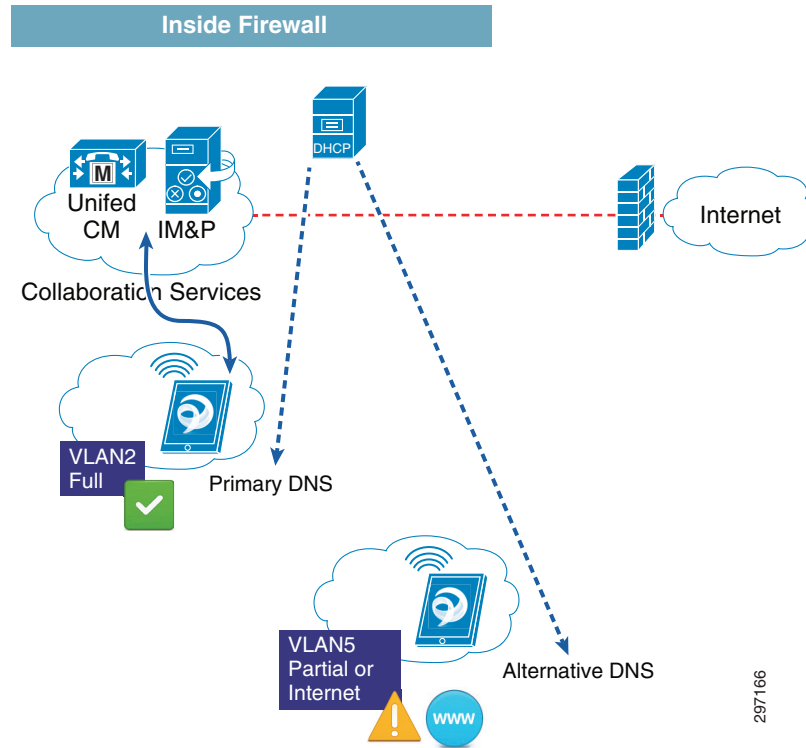
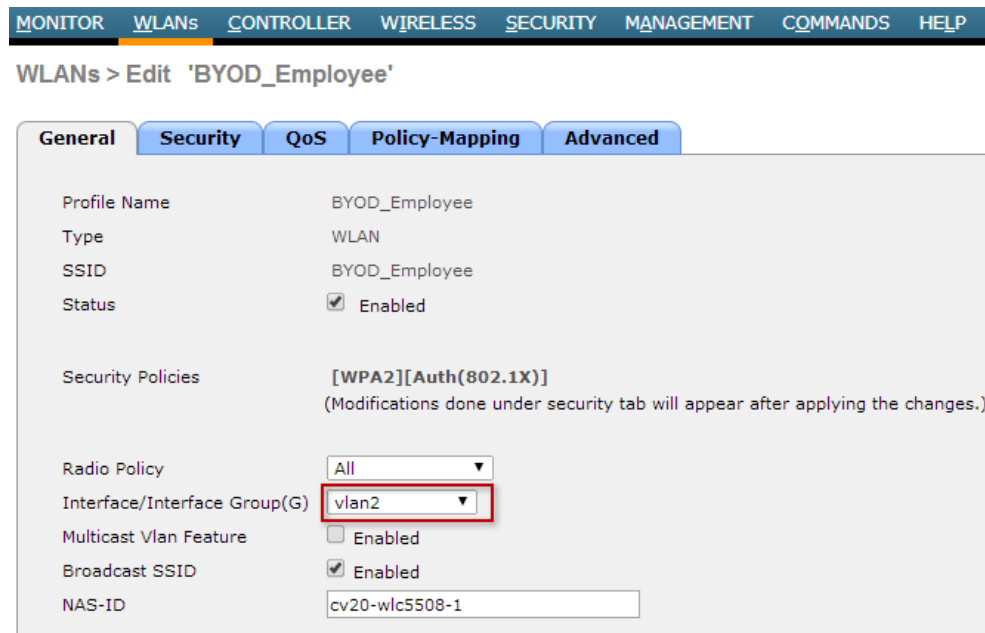


Figure 26-48 shows how the WLC is configured to assign devices connecting to the BYOD_Employee SSID to VLAN 2 by default.

Figure 26-48 BYOD_Employee SSID

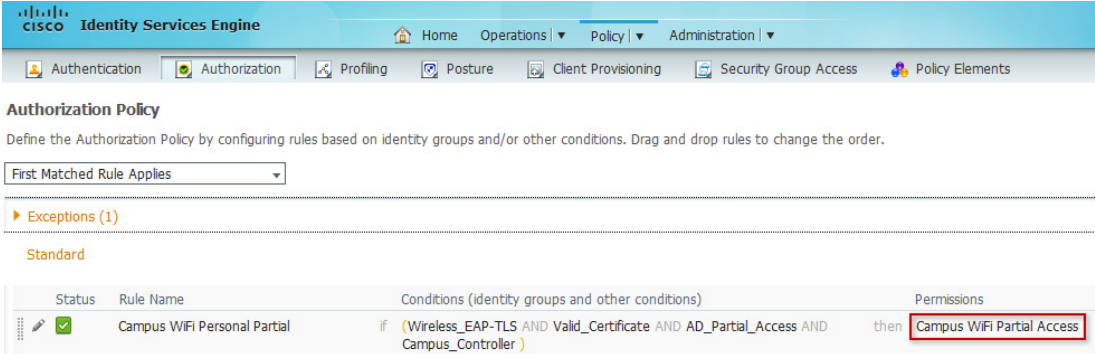


The AAA Override feature (Dynamic VLAN assignment) is used to move clients to specific VLANs based on the returned RADIUS attributes from the ISE. This feature is already highlighted several times throughout the CVD.

Partial Access

To grant Partial Access to devices connecting from the campus, the ISE authorization policy shown in [Figure 26-49](#) was used. If all the conditions in this rule match, the Campus WiFi Partial Access authorization profile is invoked. More details on this rule can be found in [Chapter 15, “BYOD Enhanced Use Case—Personal and Corporate Devices.”](#)

Figure 26-49 *Campus WiFi Personal Partial*



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes Home, Operations, Policy, and Administration. The main menu has tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The 'Authorization Policy' section is active, showing a dropdown for 'First Matched Rule Applies'. Below this, there is a section for 'Exceptions (1)' and a 'Standard' section. A table lists the authorization policy rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Campus WiFi Personal Partial	if (Wireless_EAP-TLS AND Valid_Certificate AND AD_Partial_Access AND Campus_Controller)	Campus WiFi Partial Access

The Campus WiFi Partial Access authorization profile shown in [Figure 26-50](#) has been modified to dynamically move Partial Access clients to VLAN5 in addition to enforcing the ACL_Partial_Access permissions.

Figure 26-50 Partial Access Authorization Profile

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main content area displays the configuration for an Authorization Profile named "Campus WiFi Partial Access". The profile name and description are both "Campus WiFi Partial Access". The Access Type is set to "ACCESS_ACCEPT". Under the "Common Tasks" section, the "VLAN" task is checked, with a Tag ID of 1 and an ID/Name of 5. The "Airespace ACL Name" task is also checked, with a value of "ACL_Partial_Access". The "Attributes Details" section shows the following values: Access Type = ACCESS_ACCEPT, Tunnel-Private-Group-ID = 1:5, Tunnel-Type=1:13, Tunnel-Medium-Type=1:6, and Airespace-ACL-Name = ACL_Partial_Access. A vertical ID number "297169" is visible on the right side of the configuration area.

The ACL_Partial_Access ACL shown in [Figure 26-51](#) is configured to allow access to the alternate DNS server, other internal resources, and the Internet. The ACL is also configured to block access to the primary DNS server.

Figure 26-51 ACL_Partial_Access ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port
1	Deny	0.0.0.0 / 0.0.0.0	10.230.1.10 / 255.255.255.255	Any	Any	Any
2	Deny	10.230.1.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	10.230.1.14 / 255.255.255.255	UDP	Any	DNS
4	Permit	10.230.1.14 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any
5	Permit	0.0.0.0 / 0.0.0.0	10.230.1.12 / 255.255.255.255	Any	Any	Any
6	Permit	10.230.1.12 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
7	Permit	0.0.0.0 / 0.0.0.0	10.230.1.22 / 255.255.255.255	Any	Any	Any
8	Permit	10.230.1.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0 / 0.0.0.0	10.230.1.17 / 255.255.255.255	Any	Any	Any
10	Permit	10.230.1.17 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
11	Permit	0.0.0.0 / 0.0.0.0	172.26.137.31 / 255.255.255.255	TCP	Any	HTTP
12	Permit	172.26.137.31 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any
13	Permit	0.0.0.0 / 0.0.0.0	10.230.1.5 / 255.255.255.255	TCP	Any	HTTP
14	Permit	10.230.1.5 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any
15	Deny	0.0.0.0 / 0.0.0.0	10.230.0.0 / 255.255.0.0	Any	Any	Any
16	Deny	10.230.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any
17	Deny	0.0.0.0 / 0.0.0.0	10.225.0.0 / 255.255.0.0	Any	Any	Any
18	Deny	10.225.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any
19	Deny	0.0.0.0 / 0.0.0.0	10.200.0.0 / 255.255.0.0	Any	Any	Any
20	Deny	10.200.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any
21	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any

287170

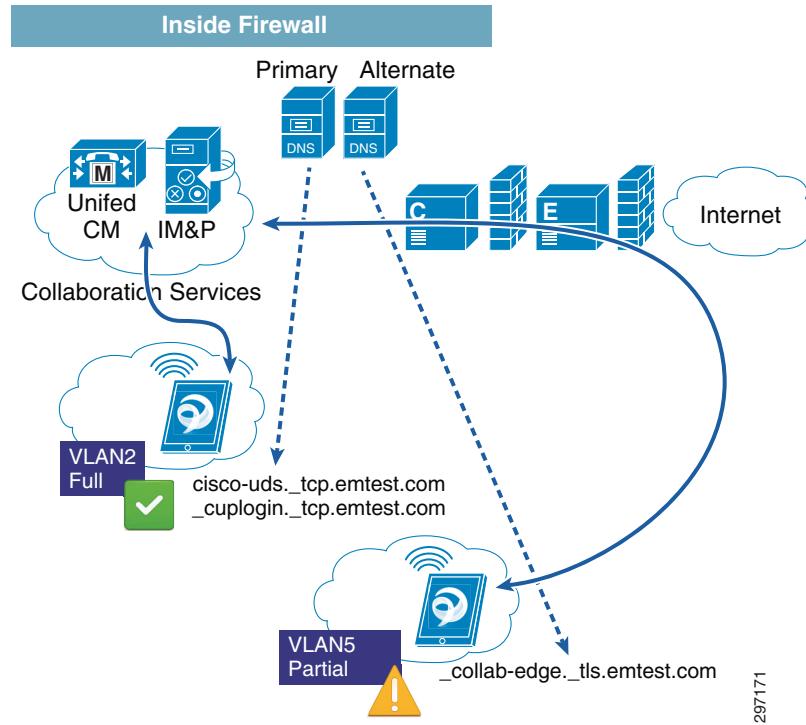
The ACL_Partial_Access ACL specifies the following access:

- Deny access to the primary DNS server (10.230.1.10).
- Allow access to alternate DNS server (10.230.1.14).
- Allow access to some internal resources and the Internet.

By moving clients dynamically to VLAN5 and allowing access to the alternate DNS server, endpoints that have been granted Partial Access query the Alternate DNS server and receive the _collab-edge SRV record, allowing them to connect through Expressway.

Figure 26-52 shows two Jabber clients connecting from different VLANs.

Figure 26-52 Jabber Across Segments—Partial Access

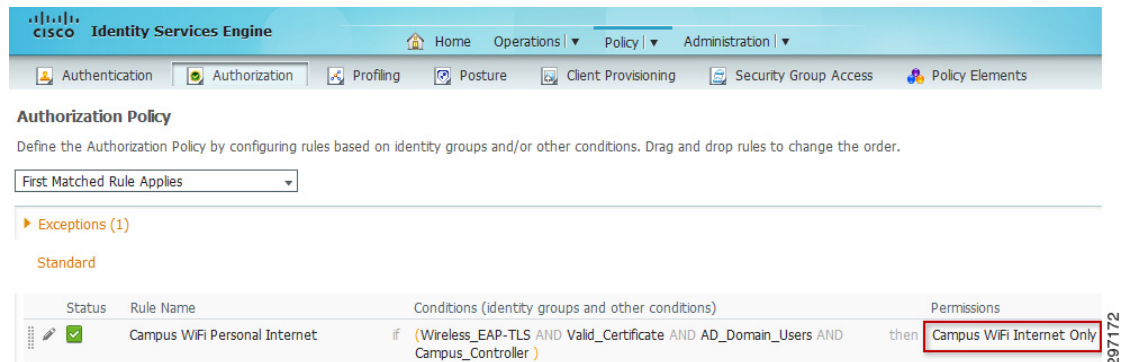


Expressway acts facilitates the communication between clients on VLANs 2 and 5.

Internet Only Access

To grant Internet Only access to devices connecting from the campus, the ISE authorization policy shown in Figure 26-53 was used. If all the conditions in this rule match, the Campus WiFi Internet Only authorization profile is invoked. More details on this rule can be found in Chapter 15, “BYOD Enhanced Use Case—Personal and Corporate Devices.”

Figure 26-53 Campus WiFi Internet Only



The Campus WiFi Internet Only authorization profile shown in Figure 26-54 has been modified to dynamically move Internet Only clients to VLAN5 in addition to enforcing the ACL_Internet_Only permissions.

Figure 26-54 Internet Only Authorization Profile

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main content area is titled "Authorization Profile" and displays the configuration for a profile named "Campus WiFi Internet Only".

Authorization Profile Configuration:

- Name:** Campus WiFi Internet Only
- Description:** Campus WiFi Internet Only
- Access Type:** ACCESS_ACCEPT
- Service Template:** (unchecked)

Common Tasks:

- VLAN: Tag ID 1, ID/Name 5
- Voice Domain Permission
- Web Redirection (CWA, DRW, MDM, NSP, CPP)
- Web Authentication (Local Web Auth)
- Airespace ACL Name: ACL_Internet_Only

Attributes Details:

```

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:5
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
Airespace-ACL-Name = ACL_Internet_Only

```

The left sidebar shows a navigation tree with categories: Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access. The "Results" tab is selected in the top navigation bar.

The ACL_Internet_Only ACL shown in Figure 26-55 is configured to allow access to the alternate DNS server, other internal resources, and the Internet. The ACL is also configured to allow access to the primary DNS server since access to the DNS server is required for the Advanced Use case for Mobile Device Management (MDM) remediation rules (see Chapter 17, “BYOD Advanced Use Case—Mobile Device Manager Integration”).

Figure 26-55 ACL_Internet_Only ACL

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK								
Access Control Lists > Edit								
General								
Access List Name	ACL_Internet_Only							
Deny Counters	0							
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port		
1	Permit	0.0.0.0 / 0.0.0.0	10.230.1.10 / 255.255.255.255	UDP	Any	DNS		
2	Permit	10.230.1.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any		
3	Permit	0.0.0.0 / 0.0.0.0	10.230.1.14 / 255.255.255.255	UDP	Any	DNS		
4	Permit	10.230.1.14 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any		
5	Permit	0.0.0.0 / 0.0.0.0	10.230.1.12 / 255.255.255.255	Any	Any	Any		
6	Permit	10.230.1.12 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any		
7	Permit	0.0.0.0 / 0.0.0.0	10.230.1.22 / 255.255.255.255	Any	Any	Any		
8	Permit	10.230.1.22 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any		
9	Permit	0.0.0.0 / 0.0.0.0	10.230.1.17 / 255.255.255.255	Any	Any	Any		
10	Permit	10.230.1.17 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any		
11	Permit	0.0.0.0 / 0.0.0.0	172.26.137.31 / 255.255.255.255	TCP	Any	HTTP		
12	Permit	172.26.137.31 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any		
13	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any		
14	Deny	10.0.0.0 / 255.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any		
15	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any		
16	Deny	172.16.0.0 / 255.240.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any		
17	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any		
18	Deny	192.168.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any		
19	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any		

287174

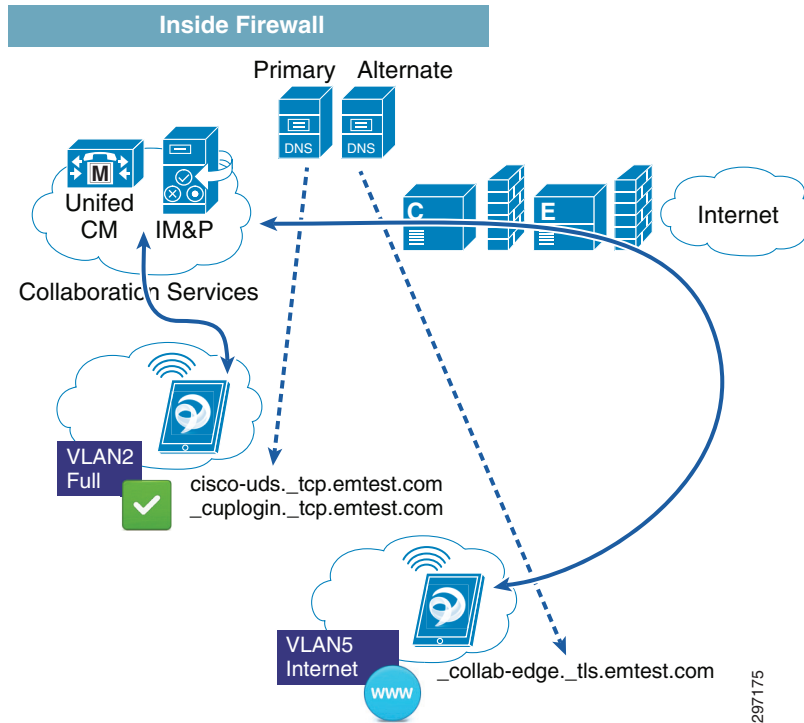
The ACL_Internet_Only ACL specifies the following access:

- Allow access to alternate DNS server (10.230.1.14).
- Allow access to some internal resources and the Internet.

By moving clients dynamically to VLAN5 and allowing access to the alternate DNS server, endpoints that have been granted Internet Only Access query the Alternate DNS server and receive the _collab-edge SRV record, allowing them to connect through Expressway.

Figure 26-56 shows two Jabber clients connecting from different VLANs.

Figure 26-56 Jabber Across Segments—Internet Only



Expressway facilitates the communication between clients on VLANs 2 and 5.