CHAPTER 1

Overview

Cisco Intercompany Media Engine (Cisco IME) provides a technique for establishing direct IP connectivity between enterprises by combining peer-to-peer technologies with the existing public switched telephone network (PSTN) infrastructure. Cisco IME allows companies that have deployed Cisco Unified Communications Manager to communicate securely over the Internet rather than the PSTN by creating dynamic Session Initiation Protocol (SIP) trunks between the enterprises. By enabling traffic outside of the enterprise to travel over the Internet, Cisco IME extends features and functionality to external calls that have previously worked exclusively within the enterprise, such as video enabled calls, wideband audio support, rich caller ID, presence, and others.

Cisco IME allows you to more effectively communicate with external partners that you rely on to run your business, including consultants, manufacturers, suppliers, outsourcing firms, distributors, and supply chain partners.

This section contains the following information:

Features and Benefits

Cisco Intercompany Media Engine (Cisco IME) gradually creates dynamic SIP trunks between businesses, so that a collection of enterprises that work together appears to be one large business with intercluster trunks between the enterprises. Cisco IME allows companies to interconnect on demand over the Internet. This feature has many important properties for the customer:

- Works with phone numbers—Cisco IME works with the phone numbers customers have today. Cisco IME does not require customers to learn new numbers nor change providers.
- Works with existing phones—Cisco IME works with the existing phones within an enterprise. No need to change phones unless you want a more feature-rich phone.
- No new services to purchase—Cisco IME does not require any new services from any service providers. You continue to use your current PSTN and Internet connectivity. Cisco IME gradually moves calls off the PSTN and onto the Internet.
- Brings full Unified Communications experience—Because Cisco IME creates intercluster SIP trunks between businesses, any feature that works over the SIP trunk and only requires a SIP trunk will now work between businesses.

- Works on the Internet—Cisco IME allows you to send calls over the Internet or on managed extranets.
- Worldwide reach—Cisco IME can connect to any enterprise in the world, as long as the enterprise is running Cisco IME technology.
- Unlimited Scale—Cisco IME can work with any number of enterprises.
- Self-learning—After you configure information about your own networks, Cisco IME learns IP routes to other businesses automatically. You never have to enter information about other businesses, including phone prefixes, IP addresses, ports, domain names, and certificates.
- QoS Management—Cisco IME provides features that help you manage the quality of service (QoS) of the Internet connections. Cisco IME monitors the QoS of the Real-Time Transport Protocol (RTP) traffic in real time and fallback to PSTN automatically if problems arise.

How It Works

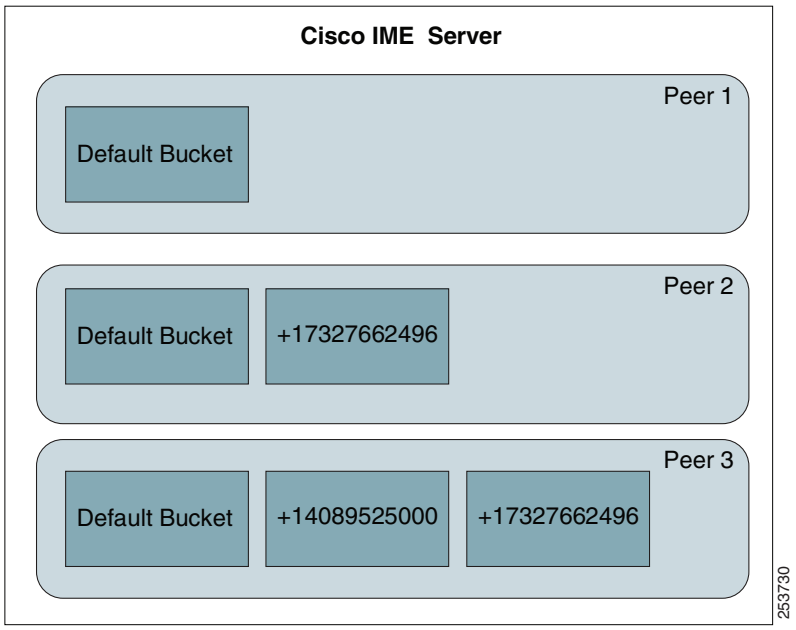
Cisco Intercompany Media Engine (Cisco IME) allows companies that have deployed Cisco Unified Communications Manager to communicate securely over the Internet rather than the PSTN by creating dynamic SIP trunks between the enterprises.

To use Cisco IME, you must deploy the Cisco IME solution, including configuring the direct inward dialing numbers (DIDs) in Cisco Unified Communications Manager that you want to participate in Cisco IME. Cisco Unified Communications Manager publishes these numbers to the Cisco IME server that, in turn, publishes the numbers to a server in the IME distributed cache ring. All Cisco IME (peer) servers participate in the IME distributed cache ring and store data in encrypted form.

Note Cisco IME requires that the system transform the numbers that a user dials to E.164 format numbers that include the international "+" prefix; for example, "+14085551212". This format will be referred to as "+E.164" format throughout this document.

Figure 1-1 provides an illustration of the IME distributed cache ring:

Figure 1-1 IME Distributed Cache Ring



To communicate with another enterprise that has stored numbers in the IME distributed cache ring over the Internet, you must first complete a configurable number of public switched telephone network (PSTN) calls to a number within that enterprise. After each PSTN call terminates, the enterprises that were involved in the call send information about the call to their Cisco IME servers in a voice call record (VCR). The VCR specifies some information about the call, including the start time, stop time, called party number, and calling party number. A validation process begins. The Cisco IME server on the originating side tries to locate the enterprise that claims ownership of the dialed number and begins a validation process to ensure that the terminating enterprise actually owns that phone number. The terminating party verifies that this domain name has not been placed into a set of blacklisted domains.

Once validated, the originating Cisco IME server sends a message to the Cisco Unified Communications Manager server and provides a VoIP route for this number. The originating Cisco Unified Communications Manager learns the route and stores the route and a validation ticket in its database for subsequent use. The ticket specifies the enterprise is authorized to call specific phone numbers at the target enterprise. The route and ticket remains valid for a year. The next time a user places a call to the same number from any number in the originating enterprise, the call travels over the Internet via a dynamic SIP trunk. When the call arrives at the Cisco Intercompany Media Engine-enabled ASA of the terminating enterprise, the Cisco Intercompany Media Engine-enabled ASA verifies the ticket that the SIP message contains. The domain in the ticket must match the domain of the calling enterprise, and the called number must match the number that the ticket permits.

Cisco IME provides security to ensure that only valid routes get sent to the Cisco Unified Communications Manager and methods to preserve quality of service if the Internet connection degrades. For more information on these features, see the following sections:

- Validation Rules, page 1-4
- PSTN Fallback, page 1-5

Validation Rules

To ensure security of the Cisco Unified Communications Manager server, the Cisco Intercompany Media Engine (Cisco IME) feature imposes a set of validation rules to ensure that it passes only valid routes to Cisco Unified Communications Manager.

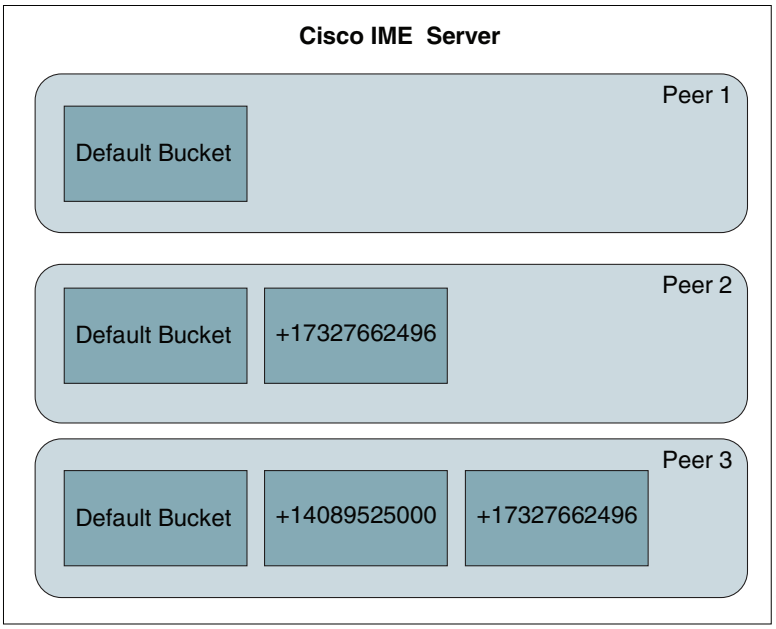
The following list summarizes the validation criteria:

- A number of consecutive successful validations against DIDs owned by a given enterprise (or Cisco IME server) must occur before Cisco Unified Communications Manager receives the learned routes from the Cisco IME server. By default, Cisco Intercompany Media Engine requires 3 validations. The validations can be against different destination numbers. Once three consecutive validations occur, the Cisco IME server passes all three learned routes to the Cisco Unified Communications Manager. You can increase or decrease the number of successful validations required for Cisco Unified Communications Manager to learn a route, depending on your security requirements.
- If validation fails against a particular number, the system requires consecutive validations against that specific number before Cisco IME passes the learned routes to Cisco Unified Communications Manager.
- To ensure that voice call records (VCRs) are uncorrelated, Cisco Unified Communications Manager never validates two VCRs for the same called number that occur within one hour of each other. You can configure the minimum time between validation attempts to the same number, depending on your security requirements.

To track the validation results, the Cisco IME server uses pools, a collection of buckets that are associated with a particular Cisco IME (or peer). Default buckets track successful validations against a Cisco IME server, and the number buckets track successful validations against the same DID.

Figure 1-2 illustrates a Cisco IME server with pools for three different peers.

Figure 1-2 Pools and Buckets



In this example, each pool contains a default bucket. Peer 2 also contains a number-specific bucket for +17327662496. Peer 3 contains two number-specific buckets: one for +1408952500 and one for +17327662496. Because the number +17327662496 exists on two different Cisco IME servers (or peers), a number-specific bucket for that number exists in two different pools, but those buckets have no relation to one another.

Each bucket holds successful validation results. When a validation succeeds against a particular peer, Cisco IME places that validation result into the number-specific bucket that matches the validated number, if one exists; else, into the default bucket. Each validation result also gets associated with a particular value, depending on the method that the Cisco IME server used to validate the call. When a validation result gets placed into a bucket, the value of the bucket increases by the value of that validation result, either 8 or 12.

Each bucket has a configured threshold. The configured threshold applies to both default buckets and number-specific bucket. Once the bucket contains validation result values that exceed the threshold, the validation results in that bucket get removed (or emptied), and the results get passed to Cisco Unified Communications Manager.

Note You can modify the threshold value of the buckets on your Cisco IME server with the set ime validator local bucketentropy CLI command.

When a validation towards a particular peer fails, Cisco IME empties all buckets in the pool that corresponds to that peer and creates a number-specific bucket to the pool for the destination number, if one does not exist. To learn a route after a validation failure, a peer must perform consecutive successful validations to the same number.

The number-specific buckets represent a penalty box. Peers that always have successful validation results never have number-specific buckets and can learn routes after the configured number of consecutive validations against different numbers. Peers that fail validation have number-specific buckets and require the configured number of consecutive validations against the same number.

PSTN Fallback

The Cisco IME feature provides mechanisms to allow calls to fallback to the PSTN, if the quality of service (QoS) degrades below an acceptable level. The Cisco Intercompany Media Engine-enabled ASA on the originating and terminating sides monitor the quality of the traffic. Based on the observed loss and jitter properties, the Cisco Intercompany Media Engine-enabled ASA determines whether the call should fallback to the PSTN. The voice call continues on the PSTN without impacting the call or alerting the users.

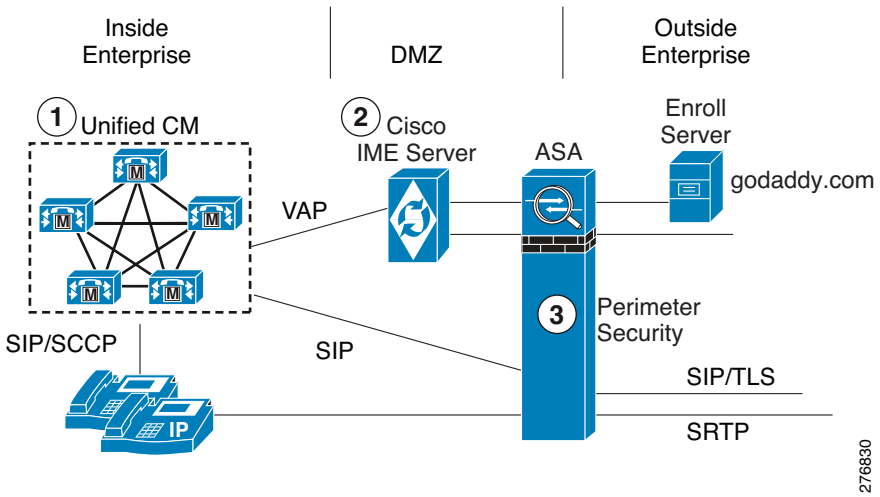
If the call needs to fallback to the PSTN, the originating Cisco Unified Communications Manager sets up a PSTN call in the background while the Cisco IME call remains active. After the Cisco Unified Communications Manager establishes the PSTN call, Cisco Unified Communications Manager seamlessly switches the Internet/RTP stream from the Internet to the PSTN. Any advanced features such as video are lost, but the audio portion of the call remains intact.

Components

Cisco Intercompany Media Engine (Cisco IME) solution consists of several components to allow for the dynamic learning of routes and the secure encryption of call signaling and media between organizations. These components include the Cisco IME server, the Cisco Unified Communications Manager server, the Cisco Intercompany Media Engine-enabled ASA, and certificates from the GoDaddy.com website. The Cisco IME server resides in the demilitarized zone (DMZ) at the customer premise and functions as an automated provisioning service. The server learns VoIP (or Cisco IME) routes to particular phone numbers and pushes those routes to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager server connects to the Cisco IME server through a proprietary protocol called the Validation Access Protocol (VAP). The Cisco Unified Communications Manager performs all call processing functions as in a standard Cisco Unified Communications Manager deployment. The Cisco Intercompany Media Engine-enabled ASA provides perimeter security for the Cisco Intercompany Media Engine solution. The GoDaddy.com website allows you to obtain certificates that are needed to participate in the peer-to-peer network that the ring of Cisco IME servers create.

Figure 1-3 shows the components of the Cisco Intercompany Media Engine network:

Figure 1-3 Cisco Intercompany Media Engine Components



The following sections describe the Cisco IME components in more detail.

Cisco Intercompany Media Engine (Peer) Server

Located in the DMZ, the Cisco IME server communicates with the Cisco Unified Communications Manager server over the Validation Access Protocol (VAP) and communicates with other Cisco IME servers across the Internet. The Cisco IME servers work together to form a peer-to-peer network that creates an IME distributed cache ring across the public Internet.

Each Cisco IME server in the IME distributed cache ring stores a portion of the data owned by the ring. The data gets encrypted so that the Cisco IME server storing the data cannot read the content. Each Cisco IME on the ring can store data into the ring and can fetch data from the ring. The direct inward dialing numbers (DIDs) that get stored in the ring are one-way hashed before they get stored into the DHT. The Cisco IME server does not perform call control. Rather, the Cisco IME server stores direct inward dialing numbers (DIDs) to the IME distributed cache ring and learns routes to remote DIDs that it provides to the Cisco Unified Communications Manager.

You provide local administration and maintenance of the Cisco IME through a command line interface (CLI).

Cisco Intercompany Media Engine (Bootstrap) Server

In order to operate, Cisco IME relies on a set of bootstrap servers that Cisco Systems manages. The bootstrap servers determine which peer servers can join the IME distributed cache ring. Bootstrap servers distribute configuration information. After Cisco makes a configuration change on a bootstrap server, the change propagates around the ring and updates the configuration on all other nodes.

Cisco Unified Communications Manager

Cisco Unified Communications Manager stores the learned VoIP routes from the Cisco IME server and also provides all call processing functions for the Cisco IME solution. Cisco Unified Communications Manager Administration helps you to provision Cisco Unified Communications Manager to use the Cisco IME feature. In Cisco Unified Communications Manager Administration, you identify the Cisco IME servers, the phone numbers that you want to allow to useCisco IME, the domains that you want to trust, and so on. You can also configure parameters to enable Cisco IME calls to fallback to the public switched telephone network (PSTN) if call quality falls below acceptable levels.

ASA

The Cisco Intercompany Media Engine-enabled adaptive security appliance (ASA) plays a key role in the security of the Cisco IME solution. The Cisco Intercompany Media Engine-enabled ASA secures the call control and media interfaces. Enabled with the Cisco Intercompany Media Engine proxy, ASA provides perimeter security functions and inspects SIP signaling between SIP trunks. Specifically, the Cisco Intercompany Media Engine-enabled ASA performs the following functions:

- SIP Application Level Gateway (ALG)—Inspects SIP signaling messages that traverse through the Cisco Intercompany Media Engine-enabled ASA. The Cisco Intercompany Media Engine-enabled ASA patches the SDP and various SIP header fields to handle cases in which network address translation (NAT) is enabled. The SIP ALG also opens pinholes (or create bindings) for media streams so that media can flow in and out of the Cisco Intercompany Media Engine-enabled ASA.
- SIP message verification—Ensures that SIP messages do not crash the Cisco Unified Communications Manager or other components inside the network. The Cisco Intercompany Media Engine-enabled ASA parses and verifies key header fields that allow uniform resource identifiers (URIs). The Cisco Intercompany Media Engine-enabled ASA blocks messages that do not comply with the SIP state diagrams.
- SIP to SIP/TLS—Terminates the SIP/TLS connections towards the Internet and re-initiates a TCP-only connection towards the Cisco Unified Communications Manager when the Cisco Unified Communications Manager is not in secure mode. When the Cisco Unified Communications Manager is in secure mode, the Cisco Intercompany Media Engine-enabled ASA initiates a TLS connection towards the Cisco Unified Communications Manager. The Cisco Intercompany Media Engine-enabled ASA then acts as a TLS proxy, allowing the Cisco Unified Communications Manager to see the SIP messages and process them. The Cisco Intercompany Media Engine-enabled ASA verifies certificates issued from the far-end enterprise against known certificate authorities (CAs.)
- NAT—The ASA frequently provides the NAT and SIP ALG functionality required to work with the Internet.
- RTP/SRTP—Converts RTP on the inside of the Cisco Intercompany Media Engine-enabled ASA to SRTP on the Internet side of the Cisco Intercompany Media Engine-enabled ASA by creating an SRTP key and including the encrypted signaling that gets sent to the other side of the call.
- Ticket Verification—Inspects the Cisco IME ticket header and ensures that all signaling to the Cisco Unified Communications Manager is allowed based on the information in the ticket. The Cisco Intercompany Media Engine-enabled ASA rejects any requests without a valid ticket.
- RTP Monitoring—Inspects the RTP stream for quality of service (QoS).

You can configure your system so that Cisco IME traffic gets sent through a Cisco Intercompany Media Engine-enabled ASA and other corporate traffic gets sent through an existing ASA. For more information, see the "Deployment Models" section on page 1-8.

Enrollment Server (GoDaddy.com)

GoDaddy.com provides certificates to enable Cisco Intercompany Media Engine (Cisco IME) servers to participate in the Cisco IME peer-to-peer network. After you purchase and install the license on the Cisco IME server, go to the GoDaddy.com website to purchase a Cisco IME certificate. During the certificate purchase process, you must provide the Cisco IME server ID to identify the Cisco IME to GoDaddy uniquely. If GoDaddy determines that this server is valid, GoDaddy returns a certificate for the Cisco IME server. The certificates allow for TLS connections between the Cisco IME servers that form the distributed cache ring.

Deployment Models

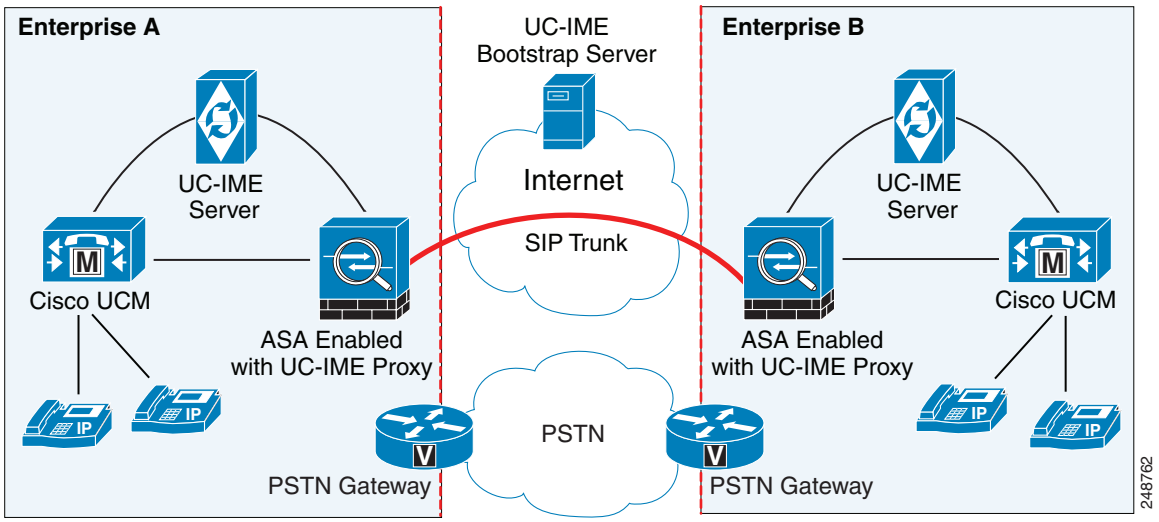
This section includes the descriptions of the available deployment models for Cisco Intercompany Media Engine:

Basic Deployment

In a basic deployment, the Cisco Intercompany Media Engine proxy resides in-line with the Internet firewall so that all Internet traffic traverses the adaptive security appliance (ASA). In this deployment, a single Cisco Unified Communications Manager or a Cisco Unified Communications Manager cluster is centrally deployed within the enterprise, along with a Cisco Intercompany Media Engine (Cisco IME) server. A single Internet connection traverses the ASA that is enabled with the Cisco Intercompany Media Engine proxy.

As shown in Figure 1-4, the ASA resides on the edge of the enterprise and inspects SIP signaling by creating dynamic SIP trunks between enterprises.

Figure 1-4 Basic Deployment Model



Off-path Deployment

In a typical large enterprise that uses two layers of firewalls between the corporate network, customers may not be able to replace/upgrade the existing Internet firewall with Cisco Intercompany Media Engine-enabled ASA or change the existing security architecture by adding Cisco Intercompany Media Engine-enabled ASA inline with the Internet firewall. To resolve this issue, Cisco allows an off-path ASA model for Cisco Intercompany Media Engine.

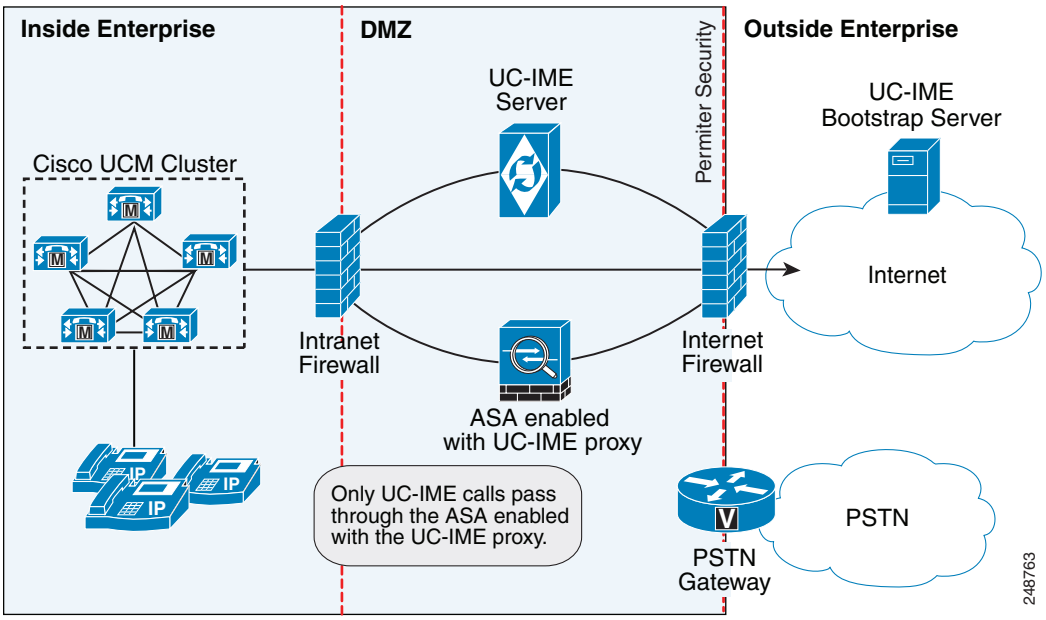
In an off-path deployment, inbound and outbound Cisco Intercompany Media Engine calls pass through an adaptive security appliance (ASA) that is enabled with the Cisco Intercompany Media Engine proxy. You configure the ASA in the DMZ, primarily to provide support for Cisco Intercompany Media Engine. Normal Internet-facing traffic does not flow through this ASA.

For all inbound calls, the signaling gets directed to the ASA because destined Cisco Unified Communications Managers are configured with the global IP address on the ASA. For outbound calls, the called party can specify any IP address on the Internet; therefore, the ASA gets configured with a mapping service that dynamically provides an internal IP address on the ASA for each global IP address of the called party on the Internet.

Cisco Unified Communications Manager sends all outbound calls directly to the mapped internal IP address on the ASA instead of to the global IP address of the called party on the Internet. The ASA then forwards the calls to the global IP address of the called party.

Figure 1-5 illustrates the architecture of the Cisco Intercompany Media Engine in an off-path deployment.

Figure 1-5 Off-path Deployment Model



In the off-path deployment, the Cisco Unified Communications Manager server with the Cisco IME trunk needs to open a TCP connection to the ASA supporting the Cisco IME deployment. This connection exists on a randomly chosen port in the 1024-65535 range. If any firewalls exist between the Cisco Unified Communications Manager server and the ASA supporting Cisco IME, you must open this port range on those firewalls.

The following example shows a sample ACL entry:

access-list SAMPLE extended permit tcp object-group CUCM object-group IME-ASA range 1024 65535

Related Topics

- Features and Benefits, page 1-1
- How It Works, page 1-2
- Deployment Models, page 1-8
- Related Topics, page 1-10