Solution Security

Introduction to Security

Achieving contact center enterprise solution security requires a security policy that accurately defines access, connection requirements, and systems management. A good security policy enables you to use the available Cisco technologies to protect your data center resources from internal and external threats. Security measures ensure data privacy, integrity, and system availability.

The security considerations for contact center enterprise solutions are similar to the considerations for the other applications in a Cisco Unified Communications solution. Contact center enterprise solutions vary greatly and often call for complex network designs. These deployments require competence in Layer 2 and Layer 3 networking as well as voice, VPN, QoS, Microsoft Windows Active Directory, and other networking issues. This chapter provides some guidance in these areas. But, this is not an all-inclusive guide for deploying a secure contact center.

Along with the Unified Communications Security Solution portal, use the design documentation in the *Design Zone* at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html. These documents provide information on properly building a network infrastructure for Cisco Unified Communications. In particular, consult the following relevant documents about security and Cisco Unified Communications:

- *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager*
- *Data Center Networking: Server Farm Security SRNDv2*
- *Site-to-Site IPSec VPN SRND*
- *Voice and Video Enabled IPSec VPN (V3PN) SRND*
- *Business Ready Teleworker SRND*

Updates and additions to these documents are posted periodically, so visit the *Design Zone* frequently.

This chapter provides limited guidance on the intricacies of designing and deploying a Windows Active Directory. More information is available from Microsoft on the following topics:

- Designing a new Active Directory logical structure.
- Deploying Active Directory for the first time.
- Upgrading an existing Windows environment to supported Microsoft Windows Server Active Directory version.
- Restructuring your current environment to a Windows Active Directory environment.

Security Layers

An adequately secure solution requires a multilayered approach to protect it from various threats.

Implement the following security layers and establish policies around them:

- **Physical Security**—Ensure that the servers hosting the contact center applications are physically secure. Locate the server in data centers to which only authorized personnel have access. Also control access to the cabling plant, routers, and switches. Implementing a strong physical-layer network security plan also includes using techniques like port security on data switches.
- **Perimeter Security**—The design and deployment of a secure data network is a complex subject. This guide provides references to resources on establishing an effective perimeter security for your contact center enterprise solution.
- **Data Security**—To ensure an increased level of protection from eavesdropping for customer-sensitive information, contact center enterprise solutions support Transport Layer Security (TLS) for agent desktops. It also supports IPsec to secure communication channels between servers.

Note The contact center enterprise solutions use TLS 1.2 by default. For most components, you can enable earlier versions of TLS if necessary.

- **Host-Based Firewall**—You can use the Windows Firewall to protect from malicious users and programs that attack servers with unsolicited incoming traffic. For more information about the Windows Firewall, see Microsoft documentation.
- **Virus Protection**—Run antivirus applications with the latest virus definition files (scheduled for daily updates) on all VMs. See the *Compatibility Matrix* for your solution for a list of all the tested and supported antivirus applications.
- **Patch Management**—Do not connect your solution to a live network without applying all security updates. Keep all hosts up-to-date with Microsoft (Windows, SQL Server, and so forth) and other third-party security patches. See the third-party patch management policy at http://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.html.

For most of these security layers, contact center enterprise solutions support several capabilities. However, what Cisco cannot control or enforce is your enterprise policies and procedures for deploying and maintaining a secure solution.

Secure Signaling and Media Design and Configuration

TLS-SRTP supports encryption for SIP signal and RTP in Call Server. This illustration displays the comprehensive deployment model.

The communication between VXML server and custom remote server supports TLS for the RPC, HTTP calls and authentication through username / password for running the custom code on remote server.

Deployment Models

1. **Unsecured**

   This deployment model is the model from earlier releases of CVP and VVB. The operations are rendered as they have been before. This is a zero-impact deployment for existing solutions.

2. **Secured signaling only**

   This deployment model introduces signaling security on top of the unsecured model. The operations are enhanced to have secured SIP for call setup. This ensures that all data exchange before any audio is heard is done in a secured manner.

3. **Secured signaling with media security for agent call**

   This deployment model supports signaling security and adds further security for media and audio between the caller and the agent. The spoken content between the caller and the agent that is carried over the IP network within the enterprise is resistant to hacking and snooping.

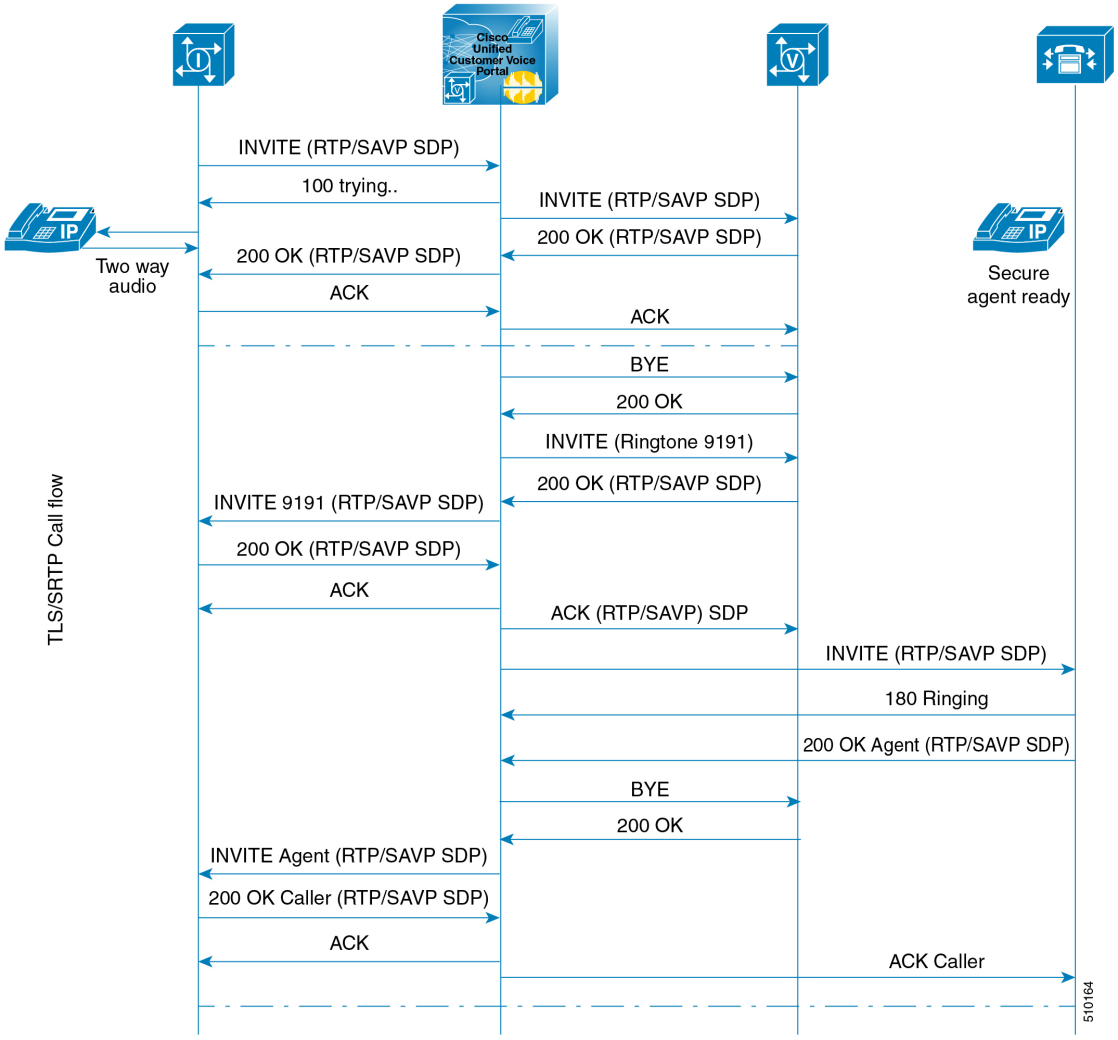
4. **Signaling with end-to-end media security for IVR and agent call**

   This deployment mode offers complete security cover to a call. It ensures that not only is the signaling secured but the media and audio from the caller to IVR and the agent is secured as well.

Note

- In TLS/SRTP deployments:
  - Where CVP and VVB are in G711 mu-law and all agents are in G729, Unified CM does not support secure transcoding in the Whisper Announcement leg. Play the announcement using a VVB in G729 as a workaround to support secure transcoding.

Call Flow



Media Encryption (SRTP) Considerations

Before enabling SRTP in your deployment, consider the following points:

- To use secure media on the agent leg, ensure that the installed IP phones are compatible with SRTP.
- The Virtualized Voice Browser supports SRTP for the VRU leg.
- The IOS VXML Gateway does not support SRTP.
- Mobile Agents cannot use SRTP.
- The Cisco Outbound Option Dialers do not support SRTP. While calls are connected to the Dialer, the calls cannot use SRTP. But, calls can negotiate SRTP once the call is no longer connected to the Dialer.

Platform Differences

The contact center enterprise solution consists of several application servers that are managed differently. The primary servers are for the core components. Install these servers only on a standard (default) operating system installation. For components that you install on Windows Server, use only a default retail version of the Windows Server software. Keep the operating system up to date with the latest device drivers, security updates, and so forth.

Some servers, like Unified Communications Manager (Unified CM), run on the Cisco Voice Operating System (VOS). Obtain all relevant patches and updates to this operating system from Cisco. You can find the security hardening specifications for this operating system in the *Cisco Collaboration System Solution Reference Network Designs* and other Unified CM product documentation at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html.

Appropriate security varies between the servers. Keep this in mind as you design, deploy, and maintain these servers in your environment. Cisco constantly enhances its Unified Communications products with the eventual goal of having them all support the same customized operating system, antivirus applications, and security path management techniques.

Security Design Elements

Unified CCE has the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html. That guide expands on the information in this chapter. The guide covers details of security implementation along with general guidance for securing a Unified CCE deployment. The security guide includes the following topics:

- Encryption Support
- IPsec and NAT Support
- Windows Firewall Configuration
- Automated Security Hardening
- Updating Microsoft Windows
- SQL Server Hardening
- SSL Encryption
- Microsoft Baseline Security Analysis
- Auditing
- Antivirus Guidelines
- Secure Remote Administration
- Single Sign-On

The guidelines are based in part on hardening guidelines published by Microsoft and other third-party vendors. The guide also serves as a reference point for most of the security functionality in the product. The guide covers installation for the Automated OS and SQL Security Hardening bundled with the various contact center enterprise tools.

Other Security Guides

Table 1: Other Security Documentation

Security Topic	Document and URL
Server staging and Active Directory deployment	*Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
SNMPv3 authentication and encryption	*SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html
Feature Control (Software access control)	*Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html
Validating real-time clients	*Setup and Configuration Guide for Cisco Unified ICM* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Network Firewalls

There are several factors to consider when deploying firewalls for your solution. Do not install the application servers for the core components in a demilitarized zone (DMZ). Segment those servers from any externally visible networks and internal corporate networks. Place the VMs in data centers, and configure the applicable firewalls or routers with access control lists (ACL) to control the traffic.

Proper use of firewalls requires a network administrator who knows which TCP/UDP IP ports are used, the firewall deployment and topology considerations, and the impact of Network Address Translation (NAT).

TCP/IP Ports

For an inventory of the ports used across the contact center enterprise solution, see the *Port Utilization Guide for Cisco Unified Contact Center Solutions* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html.

For information on ports used by Unified CM, see the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

To aid in firewall configuration, these guides list the protocols and ports used for agent desktop-to-server communication, application administration, and reporting. They also provide a listing of the ports used for intra-server communication.

Network Firewall Topology

In an Active Directory model where the AD Administrator creates OUs, do the following:

- Block the following ports at the enterprise perimeter firewall:

- UDP ports 135, 137, 138, and 445
- TCP ports 135, 139, 445, and 593

- Deploy properly configured Layer-3 and Layer-4 ACLs.
- Isolate database and web services by installing dedicated historical data servers.
- Minimize the number of Administration & Data Servers (ADS) and use Administration Clients (no database required) and Internet Script Editor clients.
- Deploy Windows IPsec (ESP) to encrypt intraserver communications.
- Use Cisco IOS IPsec for site-to-site VPNs between geographically distributed sites, remote branch sites, or outsourced sites.

Network Address Translation

Network Address Translation (NAT) is a feature that resides on a network router and permits the use of private IP addressing. A private IP address is an IP address that cannot be routed on the Internet. When NAT is enabled, users on the private IP network can access devices on the public network through the NAT router.

When an IP packet reaches the NAT-enabled router, the router replaces the private IP address with a public IP address. For applications such as HTTP or Telnet, NAT does not cause problems. However, applications that exchange IP addresses in the IP packet payload experience problems because the IP address in the IP packet payload is not replaced. Only the IP address in the IP header is replaced.

To overcome this problem, Cisco IOS-based routers and PIX/ASA firewalls implement *fix-ups* for various protocols and applications including CTIQBE (TAPI/JTAPI). The fix-up allows the router to look at the entire packet and replace the necessary addresses when performing the NAT operation. For this process to work, the version of Cisco IOS or PIX/ASA must be compatible with the Unified CM version.

Unified CCE supports connectivity through a NAT. For more information, consult the “IPsec and NAT Support” section of the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html.

ASA NAT and Firewall

The Cisco Adaptive Security Appliance (ASA) Firewall partitions a single security appliance into multiple virtual devices known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Each context keeps customer traffic separate and secure, and also makes configuration easier. All customer traffic is first sent to the firewall before forwarding to the computer resources.

Host-Based Firewall

By providing host firewall protection on the innermost layer of your network, Windows Firewall can be an effective part of your defense-in-depth security strategy. Contact center enterprise solutions support the deployment of Windows Firewall on the VMs. The *Security Guide for Cisco Unified ICM/Contact Center Enterprise* contains a chapter on the implementation and configuration of this feature.

You use the Windows Firewall Configuration Utility to configure the exceptions and open the ports required by the application.

The Windows Firewall is set up during Unified CCE installation, during which required ports are opened.

For more information about the Windows Firewall, see the Microsoft documentation.

Active Directory Deployment

This section describes the Active Directory Deployment topology. For more detailed Active Directory (AD) deployment guidance, consult the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

While you can deploy your solution in a dedicated Windows Active Directory domain, it is not a requirement. Instead, you can use Organizational Units to deploy security principles. This closer integration with AD and the power of security delegation means that your corporate AD directories can house application servers (for domain membership), user and service accounts, and groups.

Global Catalog Requirements

Contact center enterprise solutions use the Global Catalog for Active Directory. All domains in the AD Forest in which the Unified CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookups, and group lookups.

Note This does not imply cross-forest operation. Cross-forest operation is not supported.

Active Directory Site Topology

In a geographically distributed contact center enterprise solution, you locate redundant domain controllers at each of the sites. You establish a Global Catalog at each site to properly configure Inter-Site Replication Connections. Contact center enterprise solutions communicate with the Active Directory servers that are in their site. This requires an adequately implemented site topology in accordance with Microsoft guidelines.

Organizational Units

Application-Created OUs

When you install the solution software, the AD Domain in which the VMs are members must be in Native Mode. The installation adds several OU objects, containers, users, and groups for the solution. You need delegated control over the Organizational Unit in AD to install those objects. You can locate the OU anywhere in the domain hierarchy. The AD Administrator determines how deeply nested the contact center enterprise solution OU hierarchy is created and populated.

Note All created groups are Domain Local Security Groups, and all user accounts are domain accounts. The Service Logon domain account is added to the Local Administrators' group of the application servers.

The contact center enterprise installation integrates with a Domain Manager tool. You can use the tool standalone for preinstalling the OU hierarchies and objects required by the software. You can also use it when the Setup program is invoked to create the same objects in AD. The AD/OU creation can be done on the domain in which the running VM is a member or on a trusted domain.

Active Directory Administrator-Created OUs

An administrator can create certain AD objects. A prime example is the OU container for Unified CCE Servers. This OU container is manually added to contain the VMs that are members of a given domain. You move these VMs to this OU once they are joined to the domain. This segregation controls who can or cannot administer the servers (delegation of control). Most importantly, the segregation controls the AD Domain Security Policies that the application servers in the OU can or cannot inherit.

Decouple CCE Authorizations from Active Directory

Prior to Release 12.0(1), Unified CCE uses Microsoft Active Directory Security Groups to control user access rights to perform setup and configuration tasks. Microsoft AD also grants permissions for system components to interact; for example, it grants permissions to a Distributor to read the Logger database. Microsoft AD manages the user privileges that are associated with the Security Groups - Setup, Config, and Service. Thus, Microsoft AD handled both authentication and authorization. In such cases, Microsoft AD must assign user privileges to the Security Groups. To accomplish this, Unified CCE solution administration requires write permissions to Microsoft AD for authorization.

By default, Unified CCE now decouples authentication and authorization functions.

Decoupling authentication and authorization removes the need to use Microsoft AD to manage authorization in Unified CCE components. The Unified CCE solution requires that you add user IDs to the local user groups on each local machine for authorizations. User privileges are provided by memberships to local user groups in the local machines. Microsoft AD is only used for authentication.

To authorize a user ID that is already present in the Microsoft AD, you associate or add the user ID to the local user groups:

- Associate the user ID with the local `UcceService` security group to provide the SQL server authorizations to the user ID for read/write operations in the SQL database. Use the Service Account Manager tool to assign a domain user as a service account user.
- Add the user ID to the local Administrators group for Unified CCE Setup operations. Add the user ID to the local `UcceService` security group for Unified CCE configuration operations. In the **User List** tool, check the **`Setup`** check box if the user ID is added to the local Administrators group. Check **Config** if the user ID is added to the local `UcceService` group to ensures that the user's security group membership (**`Administrators`** group or **`Config`** group) is indicated in the **User_Role** column in the User Group table in the database schema.

ADSecurityGroupUpdate Registry Key

This Registry key allows or disallows updates to the Config and Setup security groups in the Domain under an instance Organizational Unit (OU).

The key has two values as follows:

- 0—Indicates that the User List tool does not update the Config and Setup security groups in the domain under instance OU.

- 1—Indicates that the User List tool updates the Config and Setup security groups in the domain under instance OU.

The default value is 0.

User Health in Service Account Manager

After upgrade, the Service Account Manager checks the users in the `UcceService` local group. If the users are not in the `UcceService` local group, then the Service Account Manager displays the status as *Unhealthy*. In such a case, run **Fix Group Membership** to make the status healthy. Alternatively, provide the new domain user in the Service Account Manager (SAM) tool or in `Websetup`

For more information about the enhancements, see the following guides:

- The chapter on the Service Account Manager in the Staging Guide for Cisco Unified ICM/Contact Center Enterprise.
- The sections on adding components to Unified CCE instances, configuring permissions in the local machine, and migrating databases in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

Active Directory and Customer Collaboration Platform User Accounts

Customer Collaboration Platform minimizes the storage of agent credentials to reduce the risk of a compromised system. Customer Collaboration Platform only has an administration account for the system setup. Customer Collaboration Platform uses Active Directory (AD) authentication for all agent access. The Customer Collaboration Platform server does not store the agent credentials.

You do not create agent accounts in Customer Collaboration Platform. Any account that your AD authenticates can use Customer Collaboration Platform. To limit who can use the application, set up an AD group and configure Customer Collaboration Platform to only allow access for that group.

In general, AD authenticated agents have access to all Customer Collaboration Platform functions. You can block access to panels by blocking certain URLs.

IPsec Deployment

The contact center enterprise solution relies on one or both of Microsoft Windows IPsec and Cisco IOS IPsec to secure critical links between VMs and sites. You can secure the solution in the following ways:

- By deploying peer-to-peer IPsec tunnels between the VMs and sites
- By deploying a more restrictive and preconfigured Network Isolation IPsec policy
- Using a combination of both

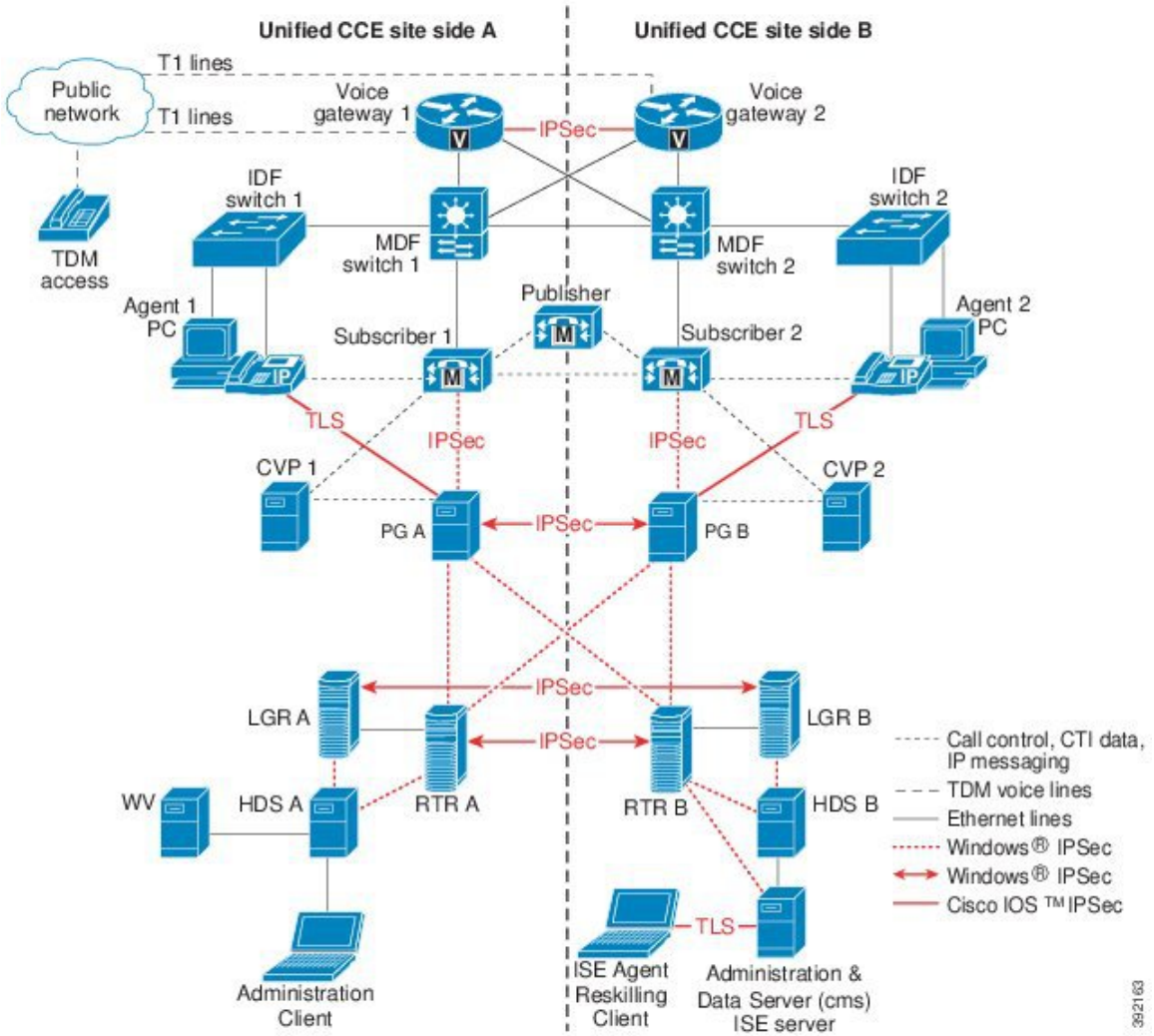
The peer-to-peer IPsec deployment requires manual configuration for each communication path that must be secured, using the tools provided by Microsoft. However, you can automatically deploy the Network Isolation IPsec policy on each VM by using the Network Isolation IPsec utility. The utility secures all communication paths to or from that VM unless an exception is made. The Network Isolation IPsec utility is installed by default on all contact center enterprise servers.

The *Security Guide for Cisco Unified ICM/Contact Center Enterprise* lists the supported paths and information to help you deploy Windows IPsec, including appropriate settings and much more.

Note Enabling IPsec affects scalability in several key areas.

Several connection paths in contact center enterprise solutions support IPsec. This figure shows the various server interconnections that must be secured with either Windows IPsec or Cisco IOS IPsec. The figure also shows several paths that support TLS.

Figure 1: IPsec Deployment Example



Server Security Configuration

Unified Contact Center Security Wizard

The Unified Contact Center Security Wizard allows easy configuration of these security features: SQL Server Hardening, Windows Firewall configuration, and Network Isolation IPsec policy deployment. The Security Wizard encapsulates the functionality of these utilities in an easy-to-use interface that guides the user with the steps involved in configuring the security feature. (This is helpful when deploying the Network Isolation IPsec policy.) The Unified CCE installation includes the Security Wizard by default.

Virus Protection

Antivirus Applications

The contact center enterprise solutions support several third-party antivirus applications. For a list of applications and versions supported for your solution, see the *Compatibility Matrix* for your solution, as well as the Unified Communications Manager product documentation for the supported applications.

Deploy only the supported applications for your environment to avoid a software conflict.

Configuration Guidelines

Antivirus applications have numerous configuration options that allow granular control of what data to scan and how to scan it.

With any antivirus product, configuration is a balance of scanning versus the performance of the VM. The more you choose to scan, the greater the performance overhead. The system administrator determines what the optimal configuration requirements are for installing an antivirus application. See the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html and your particular antivirus product documentation for more detailed configuration information about a contact center enterprise solution.

The following list highlights some general rules:

- Upgrade to the latest supported version of the antivirus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on VMs.
- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Ideally, every machine has antivirus software installed to keep all scanning local. With a multitiered antivirus strategy, scanning across the network and adding to the network load is not required.
- Heuristics scanning has a higher overhead than traditional antivirus scanning. Use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).
- You can enable real-time or on-access scanning, but only on incoming files (when writing to disk). This setting is the default for most antivirus applications. On-access scanning of file reads yields a higher than necessary impact on system resources in a high-performance application environment.
- On-demand and real-time scanning of all files gives optimum protection. But, this configuration imposes the unnecessary overhead of scanning those files that cannot support malicious code (for example, ASCII

text files). Exclude files or directories of files in all scanning modes that are known to present no risk to the system. Also, follow the guidelines for which specific contact center enterprise files to exclude in your solution. The *Security Guide for Cisco Unified ICM/Contact Center Enterprise* covers this.

- Schedule regular disk scans only during low usage times and at times when application activity is lowest. To determine when application purge activity is scheduled, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise*.

Intrusion Prevention

Cisco does not test or support intrusion prevention products by vendors such as Sygate and McAfee. Such products can block legitimate application functionality if they incorrectly identify that application as a security threat. Configure these products carefully to allow legitimate operations to run.

Patch Management

Security Patches

The security updates qualification process for contact center enterprise products is documented at http://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.html. This process applies to the VMs running the standard Windows Operating System.

Follow Microsoft guidelines regarding when and how to apply updates. Assess all security patches released by Microsoft and install those deemed appropriate for your environments.

Automated Patch Management

Contact center enterprise servers (except for the applications installed on VOS) support integration with Microsoft's Windows Server Update Services. Use that service to selectively approve updates and determine when they get deployed on production VMs. You can configure the Windows Automatic Update Client (installed by default on all Windows hosts) to retrieve updates by polling a VM that is running Microsoft Window Update Services in place of the default Windows Update website. Schedule updates to occur during approved maintenance windows.

For more configuration and deployment information, see the Microsoft documentation.

The Cisco Unified Communications VOS configuration and patch process does not currently allow for an automated patch management process.

Endpoint Security

Unified IP Phone Device Authentication

When designing a contact center enterprise solution, you can implement device authentication for the Cisco Unified IP Phones. Contact center enterprise solutions support Unified Communications Manager's Authenticated Device Security Mode, which ensures the following:

- **Device Identity**—Mutual authentication using X.509 certificates

- **Signaling Integrity**—SIP messages authenticated using HMAC-SHA-1
- **Signaling Privacy**—SIP message content encrypted using AES-128-CBC

IP Phone Hardening

With the IP phone device configuration in Unified CM, you can disable certain phone features to harden the phones. For example, you can disable the phone's PC port or restrict a PC from accessing the voice VLAN. Changing some of these settings can disable the monitoring and recording features of the contact center enterprise solution. The settings are defined as follows:

- **PC Voice VLAN Access**—Indicates whether the phone allows a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access prevents the attached PC from sending and receiving data on the Voice VLAN. It also prevents the PC from receiving data sent and received by the phone. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled (the default).

- **Span to PC Port**—Indicates whether the phone forwards packets transmitted and received on the Phone Port to the PC Port. To use this feature, enable PC Voice VLAN access. Disabling this feature disables desktop-based monitoring and recording.

  This setting is Enabled.

Disable the following setting to prevent man-in-the-middle (MITM) attacks. Some third-party monitoring and recording applications use this mechanism for capturing voice streams.

- **Gratuitous ARP**—Indicates whether the phone learns MAC addresses from Gratuitous ARP responses.

  This setting is Disabled.

Secured PII in Transit

The contact center enterprise solution handles customer sensitive information such as Personally Identifiable Information (PII) that is highly susceptible to internal and external exploitation.

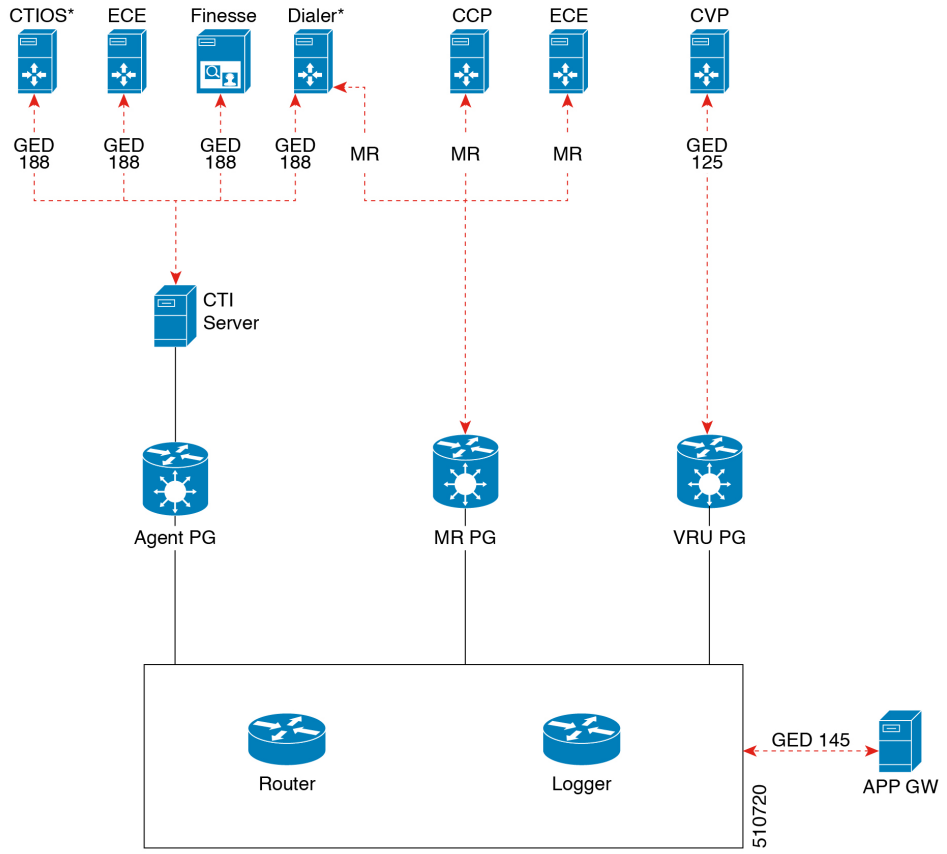
The transport channels such as GED 188, GED 125, GED 145, and MR carry PII and are susceptible to exploitation. The CCE solution uses the TLS protocol to secure the transport channels that carry PII.

The design principles that are used to secure these transport channels are listed below:

- Enabling secured communication channels between client and server components using either self-signed or third-party CA signed certificates.
- No option to fall back to non-secured mode if the connection fails.
- The use of one security certificate per VM.

For more information on secured connections and certificate management, see the Security Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Figure 2: Secured Connection Example



Note The communication channels between the Central Controller and PG are not secure. For end-to-end solution security, use the IPSec Network Isolation Zone.