CHAPTER 8

Securing Unified CCE

Last revised on: August 18, 2009

This chapter describes the importance of securing the Unified CCE solution and points to the various security resources available. It includes the following sections:

Introduction to Security

Achieving Unified CCE system security requires an effective security policy that accurately defines access, connection requirements, and systems management within your contact center. Once you have a good security policy, you can use many state-of-the-art Cisco technologies and products to protect your data center resources from internal and external threats and to ensure data privacy, integrity, and system availability.

An essential security resource is the Unified Communications Security Solution portal, accessible at

http://www.cisco.com/go/ipcsecurity

This site contains important documents and references that are meant to aid the application architect in designing a secure and reliable Cisco Unified Communications environment with its endpoints, call control systems, transport networks, and applications.

As one of those applications in the Cisco Unified Communications network, Unified CCE security considerations at a high level are not very different than those of other applications making up a Cisco Unified Communications solution. Deployments of Unified CCE vary greatly and often call for complex network designs that require competence in all areas of Layer 2 and Layer 3 networking as well as voice, VPN, QoS, Microsoft Windows Active Directory, and so forth. While this chapter provides some guidance that may touch on these various areas, it is not meant to be an all-inclusive guide for deploying a secure Unified CCE network.

Along with the Unified Communications Security Solution portal, you should use other Cisco solution reference network design guides (SRNDs) in addition to this document to answer many design and deployment questions. The SRNDs provide proven best practices for building a network infrastructure for Cisco Unified Communications. The SRNDs are available at

http://www.cisco.com/go/designzone

Among the SRNDs at this site are the following relevant documents relating to security and Cisco Unified Communications, which you should use in order to deploy a Unified CCE network successfully:

- *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*

Updates and additions to these documents are posted periodically, so frequent visits to the SRND website are recommended.

This chapter provides limited guidance on the intricacies of designing and deploying a Windows Active Directory. Additional information is available from Microsoft on designing a new Active Directory logical structure, deploying Active Directory for the first time, upgrading an existing Windows environment to Windows Server 2000 or 2003 Active Directory, and restructuring your current environment to a Windows Active Directory environment. In particular, the *Designing and Deploying Directory and Security Services* section of the *Microsoft Windows Server 2003 Deployment Kit* can assist you in meeting all of the Active Directory design and deployment goals for your organization. This development kit and its related documentation are available from Microsoft at

http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

Security Layers

An adequately secure Unified CCE deployment requires a multi-layered approach to protecting systems and networks from targeted attacks and the propagation of viruses, among other threats. The goal of this chapter is to stress the various areas pertinent to securing a Unified CCE deployment, but it does not delve into the details of each area. Specific details can be found in the relevant product documentation.

Cisco strongly recommends that you implement the following security layers and establish policies around them:

- Physical Security

  You must ensure that the servers hosting the Cisco contact center applications are physically secure. They must be located in data centers to which only authorized personnel have access. The cabling plant, routers, and switches should also have controlled access. Implementing a strong physical-layer network security plan also includes utilizing such things as port security on data switches.

- Perimeter Security

  While this document does not delve into the details on how to design and deploy a secure data network, it does provide references to resources that can aid in establishing an effective secure environment for your contact center applications.

- Data Security

  To ensure an increased level of protection from eavesdropping for customer-sensitive information, Unified CCE provides support for Transport Layer Security (TLS) on the CTI OS and Cisco Agent Desktops, and IPSec to secure communication channels between servers.

- Server Hardening

  On top of support of a more hardened Windows Server 2003, you can configure the server automatically with security settings specifically designed for the application.

- Host-Based Firewall

  Users wishing to take advantage of the Windows Firewall to protect from malicious users and programs that use unsolicited incoming traffic to attack servers can use the Windows Firewall Configuration Utility on servers or the Agent Desktop Installers to integrate with the firewall component of Windows Server 2003 SP1 and Windows XP SP2, respectively.

- Virus Protection

  All servers must be running antivirus applications with the latest virus definition files (scheduled for daily updates). The *Hardware and System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise & Hosted Editions* contains a list of all the tested and supported antivirus applications, and it is available at

  > http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html

- Intrusion Prevention

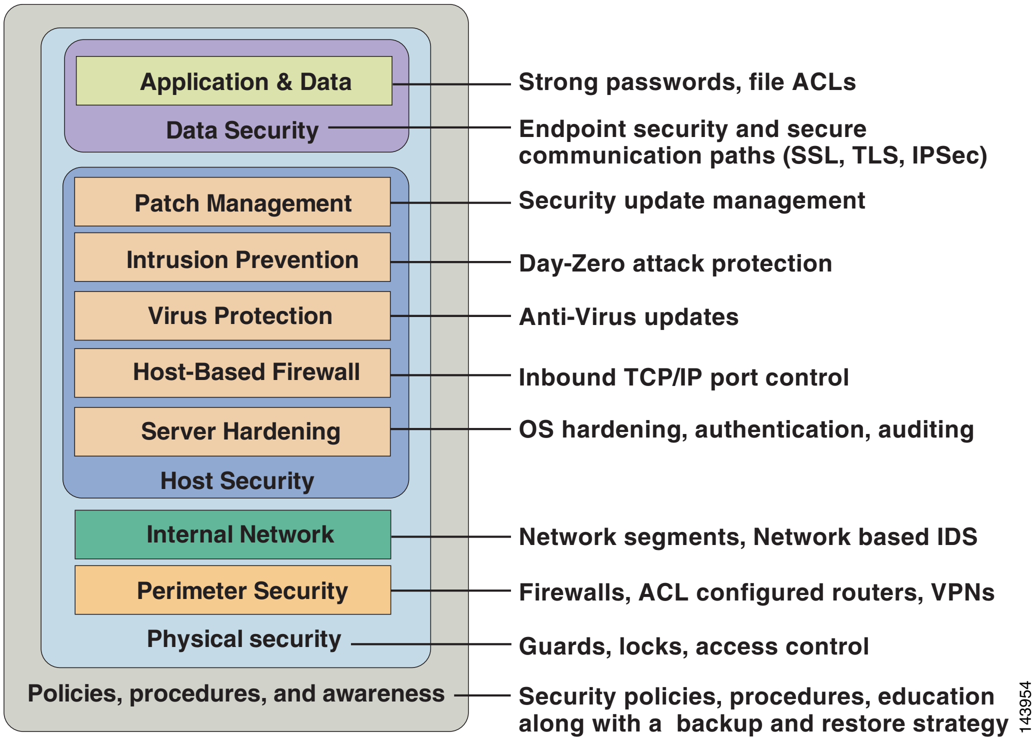
  As an important defense layer, the Unified CCE Cisco Security Agent policy can be used to provide "day-zero" threat protection for servers. It helps to reduce operational costs by identifying, preventing, and eliminating known and unknown security threats.

- Patch Management

  A system typically should not be connected to a live network until all security updates have been applied. It is important for all hosts to be kept up-to-date with Microsoft (Windows, SQL Server, Internet Explorer, and so forth) and other third-party security patches.

For most of these security layers, the Unified CCE solution supports a number of capabilities to enforce the defense-in-depth paradigm illustrated in Figure 8-1. However, what Cisco cannot control or enforce is your enterprise policies and procedures for deploying and maintaining a secure Unified CCE solution.

Figure 8-1 Defense-In-Depth


Application & Data
Data Security
Patch Management
Intrusion Prevention
Virus Protection
Host-Based Firewall
Server Hardening
Host Security
Internal Network
Perimeter Security
Physical security
Policies, procedures, and awareness
Strong passwords, file ACLs
Endpoint security and secure communication paths (SSL, TLS, IPSec)
Security update management
Day-Zero attack protection
Anti-Virus updates
Inbound TCP/IP port control
OS hardening, authentication, auditing
Network segments, Network based IDS
Firewalls, ACL configured routers, VPNs
Guards, locks, access control
Security policies, procedures, education along with a backup and restore strategy
143954

Platform Differences

Before discussing how to design the various security layers required for a Unified CCE network, this section introduces the differences that are inherent in the applications making up the Unified CCE solution.

The Unified CCE solution consists of a number of application servers that are managed differently. The primary servers, those with the most focus in this document, are the Routers, Loggers (also known as Central Controllers), Peripheral Gateways (or Agent/IVR Controllers, as they are called in a System Unified CCE deployment), Administrative Workstations, Historical Data Servers, WebView Servers, and so forth. These application servers can be installed only on a standard (default) operating system installation. For upgrades, these applications can remain (for a limited migration period) on a Windows 2000 Server or Advanced Server, but all new installations must be done on Windows Server 2003 Standard or Enterprise Edition. The maintenance of this operating system in terms of device drivers, security updates, and so forth, is the responsibility of the customer, as is acquiring the necessary software from the appropriate vendors. This category of application servers is the primary focus of this chapter.

The secondary group of servers, those running applications that are part of the solution but are deployed differently, are Cisco Unified Communications Manager (Unified CM), Cisco Unified IP IVR or Cisco IP QM, Cisco Unified Customer Voice Portal (Unified CVP, formerly ISN), and so forth. These servers support and, in some cases (except for Unified CVP), require installation on the Cisco Unified Communications Operating System (CIPT OS). This operating system is configured especially for those applications. It is hardened by default and is shipped and maintained by Cisco. Customers are required to obtain all relevant patches and updates to this operating system from Cisco. The security hardening specifications for this operating system can be found in the *Cisco Unified Communications Solution Reference Network Design (SRND)* guide and other Unified CM product documentation, available at

http://www.cisco.com/

The approach to securing the Unified CCE solution as it pertains to the various layers listed above differs from one group of servers to another. It is useful to keep this in mind as you design, deploy, and maintain these servers in your environment. Cisco is constantly enhancing 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. Some examples of these enhancements include the support of Cisco's host-based intrusion prevention software (Cisco Security Agent) and default server hardening provided by the customized operating system or applications.

Security Best Practices

As part of the Unified CCE 7.0 documentation set, Cisco has released a best-practices guide for the primary group of servers, which covers a number of areas pertaining to the new implementation in the release along with some general guidance for securing a Unified CCE deployment. The best-practices 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
- Intrusion Prevention (CSA)
- Microsoft Baseline Security Analysis
- Auditing
- Anti-Virus Guidelines and Recommendations
- Secure Remote Administration
- Additional Security Best Practices
  - WebView and IIS Hardening (Windows 2000)
  - Sybase EAServer (Jaguar) Hardening
  - RMS Listener Hardening
  - WMI Service Hardening
  - SNMP Hardening
  - Other

For the most current security best practices, refer to the latest version of the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

The recommendations contained in the *Security Best Practices* guide are based in part on hardening guidelines published by Microsoft, such as those found in the *Windows Server 2003 Security Guide*, as well as other third-party vendors' hardening recommendations. It also serves as a reference point for most of the security functionality in the product. The guide is also the installation guide for the Automated Security Hardening bundled with the application installer, Windows Firewall Configuration Utility, and the SSL Configuration Utility.

Because of the existence of the *Security Best Practices* guide, this chapter discusses many areas at a high level without further detail in order to avoid duplicating information available in other sources.

Other Security Guides

Other documents containing security guidance include, but are not limited to, the documents listed Table 8-1.

Table 8-1 Other Security Documentation

Security Topic	Document and URL
Server staging and Active Directory deployment	*Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html
Cisco Security Agent	*Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html
CTI OS encryption	*CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html
	Cisco CAD Installation Guide http://www.cisco.com/en/US/products/sw/custcosw/ps427/prod_installation_guides_list.html
WebView User authentication and administration	*WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* http://www.cisco.com/en/US/products/sw/custcosw/ps4145/prod_installation_guides_list.html
SNMPv3 authentication and encryption	*SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html
Unified ICM partitioning (Database object/access control)	*ICM Administration Guide for Cisco ICM Enterprise* http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_maintenance_guides_list.html **Note** Partitioning is supported only for Unified ICM Enterprise. It is not supported in Unified CCE, Unified ICM Hosted Edition, or Unified CCH Edition.

Table 8-1 Other Security Documentation (continued)

Security Topic	Document and URL
Feature control (Software access control)	*ICM Configuration Guide for Cisco ICM Enterprise* http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html
Validating real-time clients	*Setup and Configuration Guide for Cisco IPCC Hosted Edition* http://www.cisco.com/en/US/products/sw/custcosw/ps5053/prod_installation_guides_list.html

Network Firewalls

There are several important factors to consider when deploying firewalls in an Unified CCE network. The application servers making up a Unified CCE solution (with the exception of Cisco Collaboration Servers) are not meant to reside in a demilitarized zone (DMZ) and should be segmented from any externally visible networks and internal corporate networks. The application servers should be placed in data centers, and the applicable firewalls or routers should be configured with access control lists (ACL) to control the traffic that is targeted to the servers, thereby allowing only designated network traffic to pass through.

Deploying the application in an environment in which firewalls are in place requires the network administrator to be knowledgeable of which TCP/UDP IP ports are used, firewall deployment and topology considerations, and impact of Network Address Translation (NAT).

TCP/IP Ports

For an inventory of the ports used across the contact center suite of applications, refer to the following documentation:

- *Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions,* available at

  http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html
- *Cisco Unified Contact Center Express Port Utilization Guide*, available at

  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- *Cisco Unified Communications Manager TCP and UDP Port Usage Guide*, available at

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_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.

Topology

The deployment in Figure 8-2 represents the recommended placement of firewalls and other network infrastructure components in a Unified CCE deployment. The design model in Figure 8-2 incorporates a parent Unified ICM system with legacy peripheral hosts and a child Cisco Unified System Contact Center (Unified SCC) with a Unified CM cluster. The following best practices apply to this type of deployment:

- Block the following ports at the enterprise perimeter firewall:
  - UDP ports 135, 137, 138, and 445
  - TCP ports 135, 139, 445, and 593
- Deploy Layer-3 and Layer-4 ACLs that are configured as described in the port guides.
- Isolate database and web services by installing dedicated WebView servers and historical data servers.
- Minimize the number of administrative workstation distributors (AWD) and make use of client AWs (no database required) and Internet script editor clients.
- Use the same deployment guidelines when the parent Unified ICM or child system Unified CCE central controllers are geographically distributed.
- Use Windows IPSec to authenticate application servers running the Support Tools Node Agent with the Cisco support tools server that is managing the servers.
- Deploy Windows IPSec (ESP) to encrypt intra-server communications. The use of hardware off-load network cards is required to minimize the impact of encryption on the main CPU and to sustain the load level (including number of agents and call rate) that is supported with the Unified CCE system. See the section on IPSec Deployment, page 8-12, for a more detailed diagram and further information.
- 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 payload of an IP packet experience problems because the IP address that is transmitted in the payload of the IP packet 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 “fixups” for a variety of protocols and applications including SCCP and CTIQBE (TAPI/JTAPI). The fixup 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 IOS or PIX/ASA must be compatible with the Unified CM version.

Unified CCE supports connectivity through a NAT except when CTI OS desktop monitoring/recording is in use. The IP address of the agent phone is seen as the NAT IP address, which causes the agent desktop to improperly filter the IP packets. For more information, consult the *IPSec and NAT Support* section of the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

Active Directory Deployment

This section describes the topology displayed in Figure 8-2. For more detailed Active Directory (AD) deployment guidance, consult the *Staging Guide for Cisco ICM/IPCC & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

While Unified ICM and Unified CCE systems may still be deployed in a dedicated Windows Active Directory domain, it is not a requirement. What makes this possible is the capability of the software security principals to be installed in Organizational Units. This closer integration with AD and the power of security delegation means that corporate AD directories can be used to house application servers (for domain membership), user and service accounts, and groups.

Parent/Child Deployments

The deployment of parent/child systems can be done on the same AD Domain or Forest, but they may also be deployed in totally disparate AD environments. The scenario where this deployment would be common is when the child System Unified CCE system is housed at an outsourced contact center site. In this case, the Gateway PG that is a parent node would be a member of the parent AD domain. (Workgroup membership is supported but not recommended due to the administration limitations.) This type of deployment is common today for having remote branch offices with PGs that are added as members of the central site's domain to which the Routers, Loggers, and Distributors are members.

The topology shown in Figure 8-2 attempts to represent the AD Boundaries for each of the two AD domains involved in this deployment and to which domain the application servers are joined. The parent AD Domain Boundary is extended beyond the central data center site to include the Unified ICM Central Controllers and accompanying servers as well as the ACD PG (at the legacy site) and Gateway PG at the child System Unified CCE site. The child System Unified CCE site and its AD Boundary would have the System Unified CCE servers as members. This may or may not be as part of an outsourcer's corporate AD environment. Of course, it may also be a dedicated AD domain for System Unified CCE.

AD Site Topology

In a geographically distributed deployment of Unified ICM or Unified CCE, redundant domain controllers should be located at each of the sites, and properly configured Inter-Site Replication Connections must be established with a Global Catalog at each site. The Unified CCE application is designed to communicate with the AD servers that are in their site, but this requires an adequately implemented site topology in accordance with Microsoft guidelines.

Organizational Units

Application Created

The installation of Unified ICM or Unified CCE software now requires that the AD Domain in which the servers are members must be in Native Mode. The installation will add a number of OU objects, containers, users, and groups that are necessary for the operation of the software. Adding these objects can be done only in an Organizational Unit in AD over which the user running the install program has been delegated control. The OU can be located anywhere in the domain hierarchy, and the AD Administrator determines how deeply nested the Unified ICM/Unified CCE OU hierarchy is created and populated.

Note Local server accounts and groups are not created on the application servers. 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.

Unified ICM and Unified CCE software installation is integrated with a Domain Manager tool that can be used standalone for pre-installing the OU hierarchies and objects required by the software or can be used 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 server is a member or on a trusted domain. In Cisco Unified System Contact Center (Unified SCC), this function is fulfilled by the Unified CCE machine initializer, which defaults to the machine's joined domain and takes only one input, the <*Facility*> name. The instance name is always **ipcc** in the case of a Unified SCC deployment.

Do not confuse the creation of AD objects with Group Policy Objects (GPO). The Automated Security Hardening, which is provided following the standard Microsoft Security Template format, is *not* added to AD as part of the software installation through the configuration of a GPO. The security policy provided by this customized template (for Unified ICM/Unified CCE applications) is applied locally when a user chooses to apply hardening, or it can be pushed down through a GPO through manual AD configuration using the provided policy file, CiscoICM_Security_Template.inf.

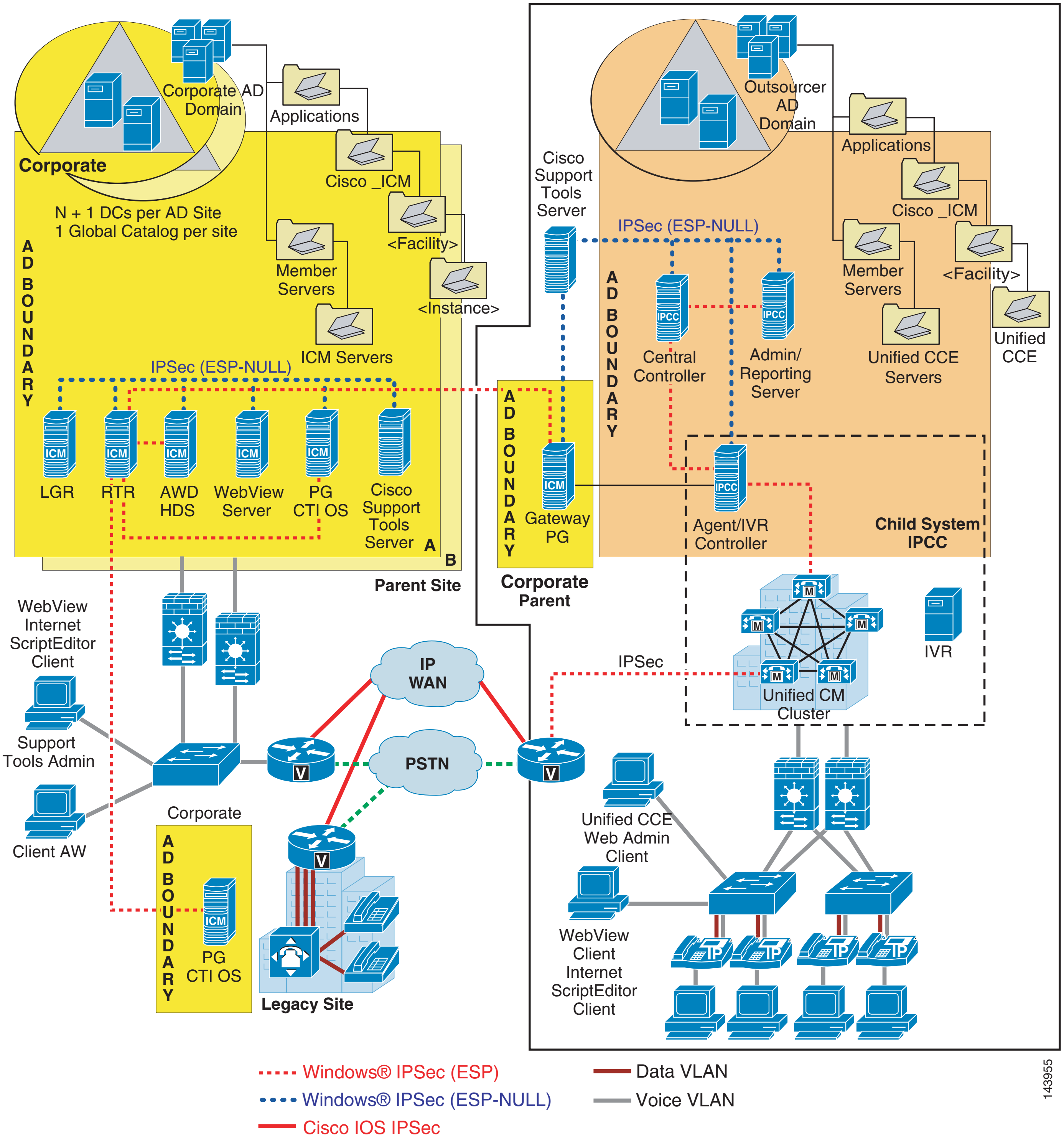
AD Administrator Created

As mentioned, there are certain AD objects that may be created by an administrator. The primary example in Figure 8-2 is represented by an OU container, Unified CCE Servers, which is manually added to contain the servers that are members of a given domain. These servers must be moved to this OU once they are joined to the domain. This ensures that some segregation is applied to control who can or cannot administer the servers (delegation of control) and, most importantly, which AD Domain Security Policy can or cannot be inherited by these application servers that are in the OU.

As noted before, Unified ICM/Unified CCE servers ship with a customized security policy that is modeled after the Microsoft Windows Server 2003 High Security policy. This policy can be applied at this server OU level through a Group Policy Object (GPO), but any differing policies must be blocked from being inherited at the Unified ICM/Unified CCE Servers' OU. Keep in mind that blocking inheritance, a configuration option at the OU object level, can be overridden when the No Override option is selected at a higher hierarchy level. The application of group policies should follow a very well thought-out design that starts with the most common denominator, and those policies should be restrictive only at the appropriate level in the hierarchy. For a more in-depth explanation on how to properly deploy group policies, refer to the *Windows Server 2003 Security Guide*, available at

http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

Figure 8-2 Active Directory and Firewall Deployment Topology



The following notes apply to Figure 8-2:

- Cisco_ICM and ipcc organizational unit object hierarchies are created by the application installer.
- Unified ICM Servers and Unified CCE Servers organizational unit objects must be created by the AD administrators to separately apply custom Cisco Unified ICM Security Policies through a GPO if required.
- Flexible Single Master Operation servers must be distributed across Domain Controllers in the appropriate sites according to Microsoft recommendations.

IPSec Deployment

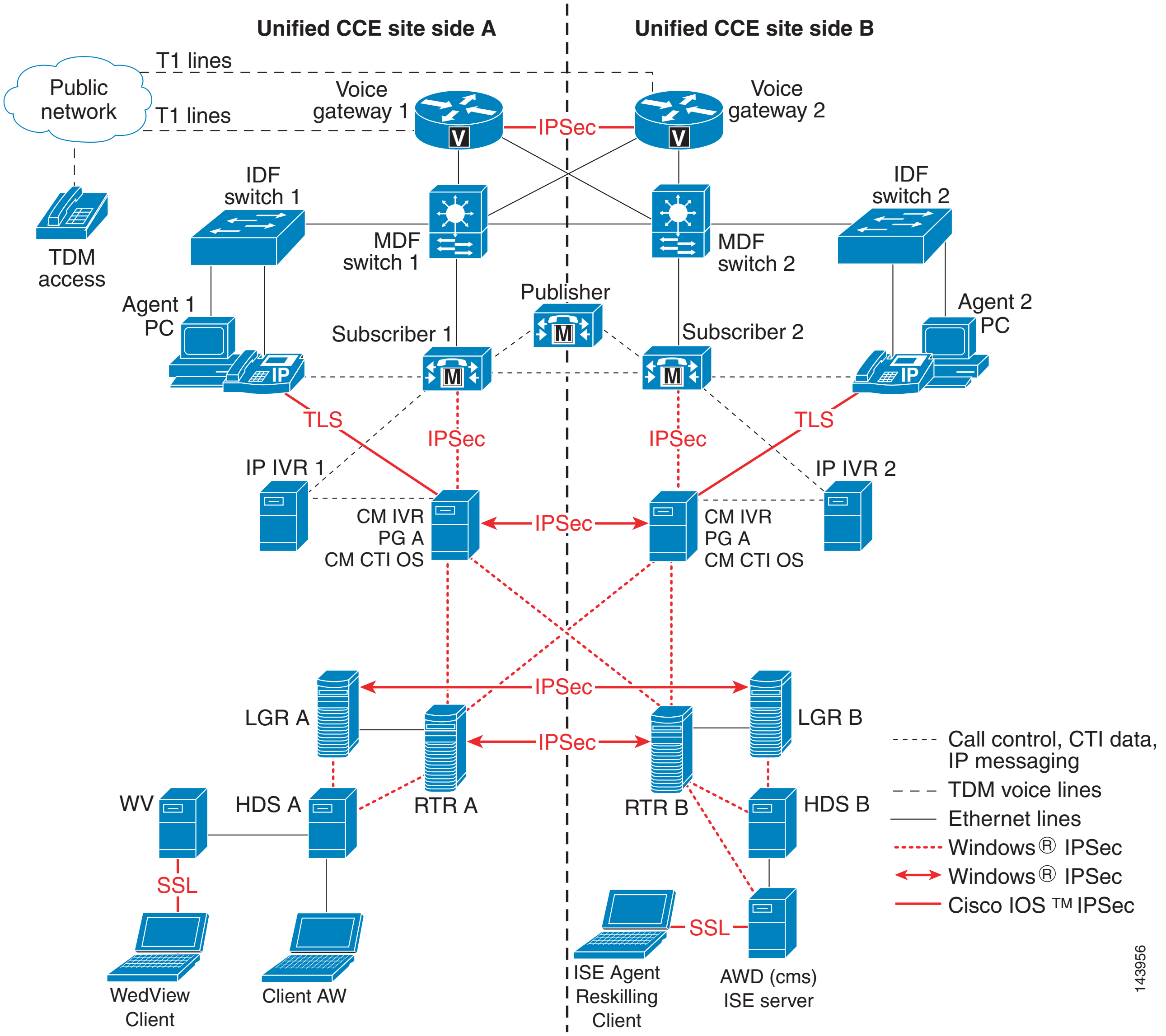
The Unified CCE solution relies on Microsoft Windows IPSec and/or Cisco IOS IPSec to secure critical links between application servers and sites. Figure 8-2 shows a number of connection paths where IPSec is supported. For a more detailed list of supported communication paths, refer to the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

The *Security Best Practices Guide* lists not only the supported paths but also information to help users deploy Windows IPSec, including recommended settings and much more.

Figure 8-3 illustrates the guidelines provided in this chapter and shows the various server interconnections that should be secured with either Windows IPSec or Cisco IOS IPSec. The diagram also shows a number of paths that support SSL and TLS. More information on TLS support can be found in the section on Endpoint Security, page 8-19.

Figure 8-3 IPSec Deployment Example



Host-Based Firewall

By providing host firewall protection on the innermost layer of your network, Windows Firewall, a new security component in Microsoft Windows Server 2003 with Service Pack 1 (SP1), can be an effective part of your defense-in-depth security strategy. Unified CCE supports the deployment of Windows Firewall on the application servers. The *Security Best Practices Guide* contains a chapter on the implementation and configuration of this feature.

In designing an integrated system with many of the security layers discussed in this document, it is important to note the compatibility limitations between the Windows Firewall and the Cisco Security Agent (CSA). For more information on CSA, refer to the section on Cisco Security Agent, page 8-16, and to the *Cisco Security Agent Installation/Deployment Guide for Cisco Unified ICM/CCE & Hosted Editions, Release 7.1*.

Caution The Cisco Security Agent (CSA) version 4.5, which ships with Unified ICM 7.1, disables the Windows Firewall on Windows Server 2003 SP1 when run at the same time. This occurs each time the system is rebooted, even if the Windows firewall has been enabled since the last system startup and configured using the Cisco Unified ICM Firewall Configuration Utility (CiscoICMfwConfig).

Enterprises that want to deploy both the Cisco Security Agent and the Windows Firewall must use Active Directory to enable Windows Firewall using the Windows Firewall Group Policy settings. Because Unified CCE applications require an AD infrastructure, Cisco requires the use of Group Policies to enable Windows Firewall when CSA is deployed along with it.

For details on how to configure an AD Group Policy to enable Windows Firewall when installed with CSA at, refer to *Field Notice: FN-62188 – Cisco Unified ICM Enterprise and Hosted Contact Center Products Notice for Cisco Security Agent 4.5.1.616 Policy 2.0.0*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_field_notices_list.html

The configuration of the exceptions and the opening of the ports required by the application will still be done locally using the Windows Firewall Configuration Utility, which is included with the Unified CCE application.

The Windows Firewall Configuration Utility (CiscoICMfwConfig) uses a configuration file (CiscoICMfwConfig_exc.xml) to determine which ports, applications, or services should be enabled in the Windows Firewall. When deploying CSA in managed mode, hence requiring communication with a CSA Management Center (MC), it is important that this file be changed to add the default UDP port used for the MC to connect to the CSA Agent. This must done before running the Configuration Utility. The following line should be added to the configuration file Ports XML element as needed:

```
<Ports>
..
<Port Number="5401" Protocol="UDP" Name="ManagedCSA" />
</Ports>
```

The Windows Firewall may also be configured afterwards by directly adding the port exception using the Windows Firewall Control Panel Applet or from the command line by using the following commands:

```
netsh firewall add portopening protocol = UDP port = 5401 name = ManagedCSA mode = ENABLE
scope = ALL profile = ALL
```

For more information on the Windows Firewall, see the *Windows Firewall Operations Guide*, available at

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/c52a765e-5a62-4c28-9e3f-d5ed334cadf6.mspx

Virus Protection

Antivirus Applications

A number of third-party antivirus applications are supported for the Unified CCE system. For a list of applications and versions supported on your particular release of the Unified CCE software, refer to the *Hardware and System Software Specifications Guide* (formerly, the *Bill of Materials*) and the *Cisco Voice Portal Bill of Materials* as well as the Cisco Unified CCX and Unified CM product documentation for the applications supported.

Note Deploy only the supported applications for your environment, otherwise a software conflict might arise, especially when an application such as the Cisco Security Agent is installed on the Unified CCE systems.

Configuration Guidelines

Antivirus applications have numerous configuration options that allow very granular control of what and how data should be scanned on a server.

With any antivirus product, configuration is a balance of scanning versus the performance of the server. The more you choose to scan, the greater the potential performance overhead. The role of the system administrator is to determine what the optimal configuration requirements will be for installing an antivirus application within a particular environment. Refer to the *Security Best Practices Guide* and your particular antivirus product documentation for more detailed configuration information on a Unified ICM environment.

The following list highlights some general best practices:

- Upgrade to the latest supported version of the third-party antivirus application. Newer versions improve scanning speed over previous versions, resulting in lower overhead on servers.
- Avoid scanning of any files accessed from remote drives (such as network mappings or UNC connections). Where possible, each of these remote machines should have its own antivirus software installed, thus keeping all scanning local. With a multi-tiered antivirus strategy, scanning across the network and adding to the network load should not be required.
- Due to the higher scanning overhead of heuristics scanning over traditional antivirus scanning, use this advanced scanning option only at key points of data entry from untrusted networks (such as email and Internet gateways).
- Real-time or on-access scanning can be enabled, but only on incoming files (when writing to disk). This is the default setting for most antivirus applications. Implementing on-access scanning on file reads will yield a higher impact on system resources than necessary in a high-performance application environment.
- While on-demand and real-time scanning of all files gives optimum protection, this configuration does have the overhead of scanning those files that cannot support malicious code (for example, ASCII text files). Cisco recommends excluding files or directories of files, in all scanning modes, that are known to present no risk to the system. Also, follow the recommendations for which specific Unified ICM files to exclude in a Unified ICM or Unified CCE implementation, as provided in the *Security Best Practices for Cisco Intelligent Contact Management Software*, available at

  http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/prod_technical_reference_list.html

- 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, refer to the *Security Best Practices* guide listed in the previous item.

Guidelines for configuring antivirus applications for Unified CM are available at the following locations:

- http://cisco.com/en/US/partner/products/sw/voicesw/ps556/products_implementation_design_guides_list.html
- http://cisco.com/en/US/partner/products/sw/voicesw/ps556/products_user_guide_list.html

Intrusion Prevention

Cisco Security Agent

Cisco Security Agent provides threat protection for servers, also known as endpoints. It identifies and prevents malicious behavior, thereby eliminating known and unknown (“day zero”) security risks and helping to reduce operational costs. The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation (in managed mode), all within a single product.

Unlike antivirus applications, Cisco Security Agent analyzes behavior rather than relying on signature matching, but both remain critical components to a multi-layered approach to host security. Cisco Security Agent should not be considered a substitute for antivirus applications.

Deploying Cisco Security Agent on Unified CCE components involves obtaining a number of application-compatible agents and implementing them according to the desired mode.

Note The Cisco Security Agent Policy provided for Unified CCE is limited to servers and may not be deployed on Agent Desktops. Customers may choose to deploy the CSA product in their enterprise and modify the default desktop security policies in the Management Center to allow legitimate application activity on their desktop endpoints, including that of the Agent Desktop software deployed.

Agents Modes

The Cisco Security Agent can be deployed in two modes:

- Standalone mode — A standalone agent can be obtained directly from the Cisco Software Center for each voice application and can be implemented without communication capability to a central Cisco Security Agent Management Center (MC).
- Managed mode — An XML export file specific to the agent and compatible with each voice application in the deployed solution, can be downloaded from the same location and imported into an existing Cisco Unified Operations Management Center for Cisco Security Agents, part of the Cisco Unified Operations VPN/Security Management Solution (VMS) bundle.

The advanced Cisco Unified Operations Management Center for Cisco Security Agents incorporates all management functions for agents in core management software that provides a centralized means of defining and distributing policies, providing software updates, and maintaining communications to the agents. Its role-based, web browser manage-from-anywhere access makes it easy for administrators to control thousands of agents per MC.

Cisco Unified ICM, Unified CCE, and Cisco Voice Portal Agents are available at

http://www.cisco.com/kobayashi/sw-center/contact_center/csa/

Other voice application agents are available at

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Third-Party Applications Dependencies

Cisco Security Agent can reside on the same server with only those supported applications listed in the *Hardware and System Software Specification Guide* or the installation guides for the Cisco Security Agent you are installing. For more details on the installation of Cisco Unified ICM agents, refer to the *Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html

Note Cisco does not test or support other intrusion prevention products by vendors such as Sygate, McAfee, and so forth. Such products are capable of blocking legitimate application functionality if they incorrectly identify that application as a security threat. Just as it is the case with CSA, these products must be specifically configured to allow legitimate operations to execute.

Patch Management

Security Patches

The security updates qualification process for Contact Center products is documented at

http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/prod_bulletins_list.html

This process applies to the application servers running the standard Windows Operating System, not the customized Cisco Unified Communications operating system (CIPT OS).

Upon the release of a Critical or Important security update from Microsoft, Cisco assesses the impact on the Unified ICM-based applications and releases a field notice with this assessment, typically within 24 hours. For the security updates categorized by Cisco as Impacting, Cisco continues to test its products to further determine if there are any potential conflicts. An impact assessment bulletin is published typically a few days after Microsoft releases the security updates. This impact assessment bulletin can be found under *Cisco Event Responses* at:

http://www.cisco.com/security

Customers should follow Microsoft's guidelines regarding when and how to apply these updates. Cisco recommends that Contact Center customers separately assess all security patches released by Microsoft and install those deemed appropriate for their environments. Cisco will continue to provide a service of separately assessing and, where necessary, validating higher-severity security patches that may be relevant to the Contact Center software products.

For all application servers running on the Unified CM Operating System, refer to the *Cisco Unified CallManager Security Patch Process*, available at

> http://www.cisco.com/application/pdf/en/us/guest/products/ps556/c1167/ccmigration_09186a0080157c73.pdf

For information on tracking Cisco-supported operating system files, SQL Server, and security files, refer to *Cisco IP Telephony Operating System, SQL Server, Security Updates*, available at

> http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/win_os/os_srv_sec/osbios.htm

The Security Patch and Hotfix Policy for Unified CM specifies that any applicable patch deemed Severity 1 or Critical must be tested and posted to http://www.cisco.com within 24 hours as Hotfixes. All applicable patches are consolidated and posted once per month as incremental Service Releases.

A notification tool (email service) for providing automatic notification of new fixes, OS updates, and patches for Unified CM and associated products is available at

> http://www.cisco.com/cisco/support/notifications.html

Automated Patch Management

Unified CCE servers (except for the applications installed on the CIPT OS) support integration with Microsoft's Windows Server Update Services, whereby customers control which patches can be deployed to those servers and when the patches can be deployed.

The recommendation is to selectively approve updates and determine when they get deployed on production servers. The Windows Automatic Update Client (installed by default on all Windows hosts) can be configured to retrieve updates by polling a server that is running Microsoft Window Update Services in place of the default Windows Update Web site.

For more configuration and deployment information, refer to the *Deployment Guide* and other step-by-step guides found at

> http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

More information is also available on this topic in the *Security Best Practices Guide for Cisco Unified ICM/CCE & Hosted Editions, Release 7.1*.

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

Endpoint Security

Agent Desktops

The CTI OS (C++/COM toolkit) and CAD agent desktops both support TLS encryption to the server. This encryption protects agent login and CTI data from snooping. A mutual authentication mechanism was implemented for the CTI OS server and client to agree on a cipher suite used for authentication, key exchange, and stream encryption. The Cipher suite used is as follows:

- Protocol: SSLv3
- Key exchange: DH
- Authentication: RSA
- Encryption: AES (128)
- Message digest algorithm: SHA1

Figure 8-4 shows the encryption implementation's use of X.509 certificates on the agent desktops as well as on the servers. The implementation supports the integration with a Public Key Infrastructure (PKI) for the most secure deployment. By default, the application will install and rely on a self-signed certificate authority (CA) used to sign client and server requests. However, Cisco supports integrating with a third-party CA. This is the preferred method due to the increased security provided by a corporate managed CA or external authority such as Verisign.

Figure 8-4 Secure Agent Desktops (Certificate-Based Mutual Authentication)

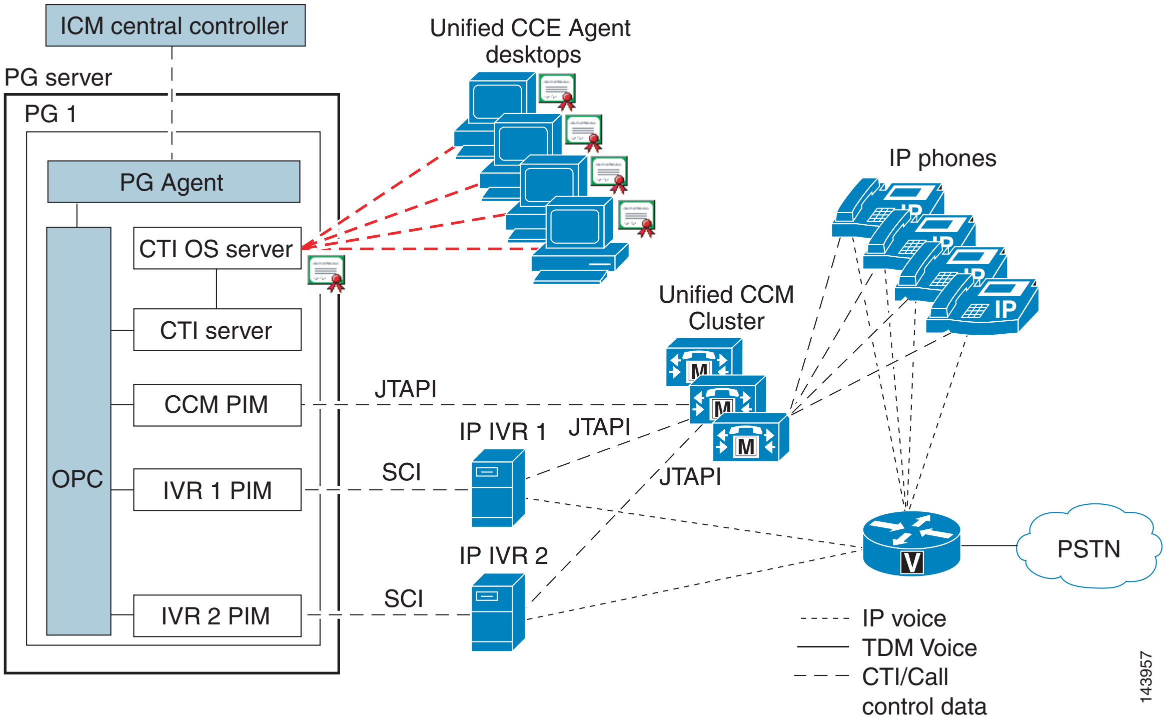
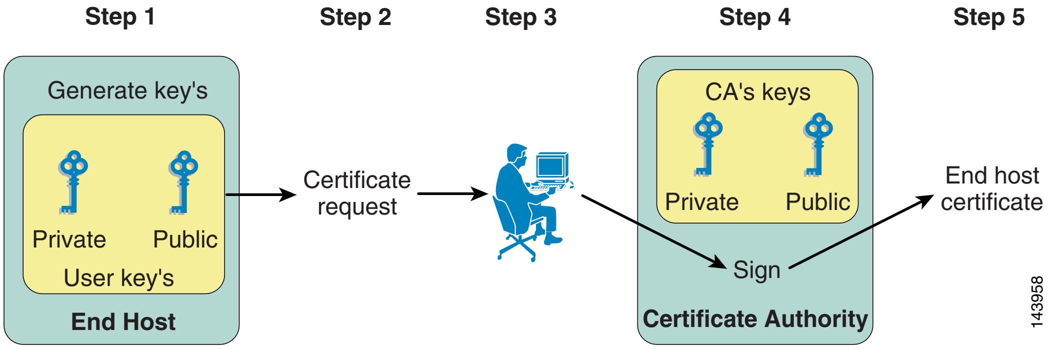


Figure 8-5 shows the Certificate Authority enrollment procedure to generate certificates used by the agent and the servers. The agent desktop certificate enrollment process is manual, requiring the creation of certificate signing requests (CSRs) at each endpoint, which are then transferred to the certificate authority responsible for signing and generating the certificates.

Figure 8-5 Certificate Authority Enrollment Procedure



Unified IP Phone Device Authentication

When designing a Unified CCE solution based on Unified CM Release 4.*x* or 5.0, customers may choose to implement device authentication for the Cisco Unified IP Phones 7940, 7960, or 7970. Unified CCE 7.0 was tested with Unified CM's Authenticated Device Security Mode, which ensures the following:

- Device Identity — Mutual authentication using RSA signatures
- Signaling Integrity — SCCP messages authenticated using HMAC-SHA-1
- Signaling Privacy — SCCP message contents encrypted using AES-128-CBC

Unified IP Phone Media Encryption

Media Encryption may be used with Unified CCE; however, it prevents the use of the silent monitoring feature. Also, if you are deploying a recording system, contact the recording system vendor to verify support for recording in an environment with Secure Real-Time Transport Protocol (SRTP).

IP Phone Hardening

The IP phone device configuration in Unified CM provides the ability to disable a number of phone features to harden the phones, such as disabling the phone's PC port or restricting access of a PC to the voice VLAN. Changing some of these settings can disable the monitoring/recording feature of the Unified CCE solution. The settings are defined as follows:

- PC Voice VLAN Access
  - Indicates whether the phone will allow a device attached to the PC port to access the Voice VLAN. Disabling Voice VLAN Access will prevent the attached PC from sending and receiving data on the Voice VLAN. It will also prevent the PC from receiving data sent and received by the phone. Disabling this feature will disable desktop-based monitoring and recording.
  - Recommended setting: Enabled (default)
- Span to PC Port
  - Indicates whether the phone will forward packets transmitted and received on the Phone Port to the PC Port. To use this feature, PC Voice VLAN access must be enabled. Disabling this feature will disable desktop-based monitoring and recording.
  - Recommend setting: Enabled

The following setting should be disabled to prevent man-in-the-middle (MITM) attacks unless the third-party monitoring and/or recording application deployed uses this mechanism for capturing of voice streams. The CTI OS silent monitoring feature and CAD silent monitoring and recording do not depend on Gratuitous ARP.

- Gratuitous ARP
  - Indicates whether the phone will learn MAC addresses from Gratuitous ARP responses.
  - Recommended setting: Disabled