# Contents

1 Getting Started with the Secure Gateway ................................................. 9  
   About This Guide .................................................................................. 9  
   Accessing Product Documentation ....................................................... 10  

2 Introducing the Secure Gateway .............................................................. 13  
   Overview ............................................................................................... 13  
   Why Use the Secure Gateway .............................................................. 13  
   The Secure Gateway and Secure Gateway Proxy .................................... 14  
      The Secure Gateway ......................................................................... 14  
      The Secure Gateway Proxy ............................................................. 14  
   Citrix Presentation Server .................................................................... 15  
      Web Interface .................................................................................... 15  
      Secure Ticket Authority (STA) .......................................................... 15  
      Citrix XML Service ......................................................................... 15  
   The Secure Gateway Features ............................................................. 16  

3 Planning a Secure Gateway Deployment .................................................. 21  
   How the Secure Gateway Works ........................................................... 21  
   How the Secure Gateway Secures Your Environment .......................... 22  
   Securing Citrix presentation Server ..................................................... 23  
      Establishing a Secure Connection to a Server Farm ......................... 24  
   The Secure Gateway in a Double-Hop DMZ ......................................... 26  
      Establishing a Secure Connection .................................................... 27  
   Upgrading the Secure Gateway ......................................................... 28  
      Upgrading with Citrix Presentation Server ....................................... 28  

4 System Requirements .............................................................................. 31  
   System Software Requirements .......................................................... 32  
   System Hardware Requirements ......................................................... 32
6 Installing the Secure Gateway .......................................................... 55
   Guidelines for Installing and Configuring the Secure Gateway .......... 56
   Preparing for Installation .............................................................. 56
   The Secure Gateway Pre-Installation Checklist ............................... 56
   Installation Sequence ................................................................. 56
   Certificate Requirements ............................................................ 57
      Certificate Requirements for a Single-Hop DMZ Deployment .......... 57
      Certificate Requirements for a Double-Hop DMZ Deployment ......... 58
   Which Components You Need to Install ....................................... 58
   Configuring the Secure Gateway .................................................. 60
   Installing the Secure Gateway Proxy ......................................... 62
   Configuring the Secure Gateway Proxy ....................................... 63
   Upgrading the Secure Gateway .................................................... 64
   Uninstalling the Secure Gateway ................................................ 65

7 Managing the Secure Gateway ..................................................... 67
   The Secure Gateway Tools ........................................................... 68
   The Secure Gateway Configuration Wizard .................................. 68
   Using the Secure Gateway Management Console ............................ 68
      Session and Connection Information ...................................... 69
   The Secure Gateway Performance Statistics ................................ 70
      Performance Counters Available for the Secure Gateway .......... 71
   Viewing the Secure Gateway Diagnostics Report .......................... 74
      Global Settings ................................................................. 75
      Interfaces ............................................................................. 75
   The Secure Gateway Proxy .......................................................... 76
   Authority Servers ..................................................................... 76
   Certificate Check ..................................................................... 76
   Event Logging and Access Logs ................................................... 77
      Event Logging ................................................................. 77
      Access Logs ...................................................................... 77
         HTTP Access Log ......................................................... 78
         CGP Access Log .......................................................... 78
         SOCKS Access Log ....................................................... 78

8 Optimization and Security Guidelines .......................................... 81
   Configuring Firewalls ................................................................. 82
Planning for High Availability ................................................................. 83
Load Balancing Multiple Secure Gateway Servers ............................... 84
Load Balancing an Array of the Secure Gateway Proxy ....................... 84
Certificate Requirements ...................................................................... 85
Load Balancers and SSL Accelerator Cards ...................................... 85
Keep–Alive Values and Citrix Presentation Server .............................. 86
Connection Keep–Alive Values and the Secure Gateway .................... 86
Recommendations for Improving Security ............................................ 87
Deploying the Secure Gateway in the DMZ ........................................ 88
Changing or Restricting Ciphersuites ................................................ 88
Restricting Ciphersuite Use to Secure Communication ...................... 89
Using Secure Protocols ....................................................................... 90
Removing Unnecessary User Accounts .............................................. 90
Removing Sample Code Installed with IIS ........................................ 90
Secure Components that Run on IIS .................................................. 91
Stopping and Disabling Unused Services ......................................... 91
Installing Service Packs and Hotfixes .............................................. 91
Following Microsoft Security Guidelines ......................................... 91
Preventing Indexing by Search Engines ............................................ 92

9 Troubleshooting .............................................................................. 93
General Troubleshooting Procedures ................................................. 93
Checking Results Reported by the Secure Gateway Diagnostics .......... 93
Reviewing the Secure Gateway Event Log ........................................ 94
Common Problems ........................................................................... 94
Certificate Problems ......................................................................... 94
The Secure Gateway Fails with a CSG0188 Error ............................. 94
Connection Problems ........................................................................ 95
Client Connections Launched from IP Addresses in the Logging Exclusions List Fail 95
Load Balancers Do Not Report Active Client Sessions if They Are Idle ........ 95
Performance Issues with Transferring Files between a Client and a Computer Running Citrix Presentation Server ......................................................... 96
Gateway Client Connections Fail When Using Windows XP Service Pack 2 .... 96
Other Problems .................................................................................. 97
Failed Client Connections to the Secure Gateway Result in Duplicate Entries in the Secure Gateway Log ...................................................... 97
Placing the Secure Gateway Behind a Reverse Web Proxy Causes an SSL Error 4 ... 97
Run the Secure Gateway Parallel to the Reverse Web Proxy ............... 99
Use a Network Address Translator Instead of a Reverse Web Proxy ...... 100
Index. ......................................................... 137
Getting Started with the Secure Gateway

About This Guide

This manual is designed to help anyone who plans, designs, pilots, or deploys the Secure Gateway for Citrix Presentation Server. It provides information to administrators about features, installation and setup, implementation, and deployment of the Secure Gateway.

The intended audience for this guide comprises experienced Presentation Server administrators responsible for installing, configuring, and maintaining Citrix environments. This guide is not intended for users of the network. This guide assumes knowledge of:

- System administration
- Networking and security technologies
- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003
- Microsoft Internet Information Services (IIS) 5.0 or later
- Internet and network protocols
- Citrix Presentation Server

Use this guide in conjunction with:

- Citrix Presentation Server for Windows Administrator’s Guide
- Citrix Presentation Server for UNIX Operating Systems Administrator’s Guide
- Web Interface Administrator’s Guide
- Appropriate Citrix Presentation Server Client Administrator’s Guides
The following table highlights references to typical administrative tasks and conceptual information in this guide:

<table>
<thead>
<tr>
<th>Task</th>
<th>See This Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Secure Gateway with computers running Citrix Presentation Server</td>
<td>“Deploying the Secure Gateway with Citrix Presentation Server” on page 37</td>
</tr>
<tr>
<td>Installing and configuring the Secure Gateway</td>
<td>“Installing the Secure Gateway” on page 55</td>
</tr>
<tr>
<td>Learning more about the Secure Gateway’s performance counters and error logs</td>
<td>“Managing the Secure Gateway” on page 67</td>
</tr>
<tr>
<td>Getting general recommendations about using network components such as load balancers, SSL accelerator cards, and firewalls</td>
<td>“Optimization and Security Guidelines” on page 81</td>
</tr>
<tr>
<td>Learning more about troubleshooting a Secure Gateway deployment</td>
<td>“Troubleshooting” on page 93</td>
</tr>
<tr>
<td>Learning about digital certificates and certificate installation</td>
<td>“About Digital Certificates” on page 101</td>
</tr>
</tbody>
</table>

**Accessing Product Documentation**

The documentation for the Secure Gateway includes online documentation, known issues information, and application Help, as follows:

- Online documentation is provided as Adobe Portable Document Format (PDF) files. To view, search, and print the PDF documentation, you need Adobe Reader (supported versions include 5.0.5 with Search, Version 6 or 7). Use Welcome to Citrix Presentation Server (Read_Me_First.html) to access the complete set of online guides.

- Known issues information is included in the Citrix Presentation Server readme, also available on the Web. Use Welcome to Citrix Presentation Server (Read_Me_First.html) to access the product readme.

- In many places in the user interface, integrated on-screen assistance is available to help you complete tasks. For example, in the Access Management Console, you can position your mouse over a setting to display help text that explains how to use that control.

- Online Help is available for some tasks. You can access the online Help from the Help menu or Help button.

- For information about terminology related to Presentation Server, see the Citrix Presentation Server Glossary, available from the Knowledge Center at http://support.citrix.com/docs/.
To provide feedback about the documentation, go to http://www.citrix.com and click Support > Knowledge Center > Product Documentation. To access the feedback form, click the Submit Documentation Feedback link.
Introducing the Secure Gateway

Overview

The Secure Gateway is a Citrix component you can use to secure access to Citrix Presentation Server. The Secure Gateway transparently encrypts and authenticates all user connections to protect against data tampering and theft.

This chapter is an overview of the capabilities and components of the Secure Gateway. It includes the following topics:

• “Why Use the Secure Gateway” on page 13
• “The Secure Gateway and Secure Gateway Proxy” on page 14
• “Citrix Presentation Server” on page 15
• “The Secure Gateway Features” on page 16

Why Use the Secure Gateway

Today, enterprises increasingly rely on global networks that link branch offices, telecommuters, and partners. However, the high cost of maintaining and implementing private leased lines is often prohibitive. Using cost-effective public networks—such as the Internet—is a compelling solution to this issue.

Any enterprise that relies on the Internet for connectivity must contend with security issues. Despite the enthusiasm for access at anytime, anywhere, from any device, corporations must be certain that they can protect confidential data from prying eyes as it travels through a public network.

The Secure Gateway eases firewall traversal and provides a secure Internet gateway between Citrix Presentation Server and client devices.

All data traversing the Internet between a remote workstation and the Secure Gateway is encrypted using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol. The Secure Gateway transparently encrypts and authenticates all user connections to protect against eavesdropping and data tampering.
The Secure Gateway is installed in a network’s demilitarized zone (DMZ) to form a secure perimeter around the Citrix components in your enterprise network. The Secure Gateway authenticates users connecting over the Internet and establishes a secure channel for data exchange between the client device and the Citrix Presentation Server.

The Secure Gateway and Secure Gateway Proxy

The following sections briefly describe the Secure Gateway and Secure Gateway Proxy for secure access. For detailed deployment information, see “Deploying the Secure Gateway with Citrix Presentation Server” on page 37.

The Secure Gateway

The Secure Gateway is an application that runs as a service on a server that is deployed in the DMZ. The server running the Secure Gateway represents a single point of access to the secure, enterprise network. The Secure Gateway acts as an intermediary for every connection request originating from the Internet to the enterprise network.

The Secure Gateway Proxy

For increased security, the Secure Gateway Proxy is used with the Secure Gateway in a double-hop DMZ deployment. The Secure Gateway is installed in the first DMZ and the Secure Gateway Proxy is installed in the second DMZ. The Secure Gateway Proxy acts as a conduit for traffic originating from the Secure Gateway to servers in the secure network, and from servers in the secure network to the Secure Gateway.
Citrix Presentation Server

Your enterprise network can contain one or more servers running Citrix Presentation Server. A server farm is used for hosting published resources that users can access over the network. For information about setting up and configuring a server farm, see the *Citrix Presentation Server Administrator’s Guide*.

The Secure Gateway works with components of Citrix Presentation Server for logon and authentication. These include:

- The Web Interface
- Secure Ticket Authority
- Citrix XML Service
- Web Client

Web Interface

The Web Interface provides user access to published resources in a server farm from a Web browser. The Web Interface works with the Secure Gateway to provide a logon interface, and facilitates authentication and authorization of connection requests to the server farm. For more information about the Web Interface, see the *Web Interface Administrator’s Guide*.

Secure Ticket Authority (STA)

The STA is responsible for issuing session tickets in response to connection requests for published resources on Citrix Presentation Server. These session tickets form the basis of authentication and authorization for access to published resources. Earlier versions of the Secure Gateway and Citrix Presentation Server required installation of the STA on a standalone server. During installation of Citrix Presentation Server 4.5, the STA is automatically installed. It is no longer necessary to reserve a separate server for the STA.

Citrix XML Service

When the Secure Gateway provides secure access to published resources available in a server farm, the Citrix XML Service is contacted for published resources availability and location.
The Citrix XML Service is the point of contact for a server farm and provides an HTTP interface to the client device. It uses the TCP protocol instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80. Ensure that this port is configured, functioning correctly, and is accessible through the firewall in front of the secure network. For more information about the Citrix XML Service, see the Citrix Presentation Server Administrator’s Guide.

The Secure Gateway Features

The Secure Gateway has features for enhanced security, certificate management, deployment, scalability, logging and instrumentation, and support for networking protocols, in addition to features that were included in previous versions of the Secure Gateway.

The Secure Gateway has the following features.

- **Improved security**
  The Secure Gateway provides authentication, authorization, and cryptography functionality that is consistent with Microsoft’s best practices for secure software.

- **Increased network protocols**
  The Secure Gateway supports the TCP/IP protocols, such as FTP, HTTP, and Telnet.

- **Simplified deployment**
  The Secure Gateway includes the following deployment improvements:
  - Citrix Presentation Server includes the Secure Ticket Authority (STA) and is merged into a single Windows Installer package resulting in a more efficient deployment
  - The STA is automatically deployed on the same computer as Citrix Presentation Server, resulting in a reduction of the number of computers required for basic deployment
  - Internet Information Server is no longer a requirement for installing the STA
  - Internet Information Server deployment is a supported option during installation of Citrix Presentation Server

- **Improved certificate management**
  The Secure Gateway includes the following certificate management improvements:
• Improved certificate selection. The Secure Gateway Configuration wizard prevents the selection of a certificate that does not have a private key.

• Improved certificate detection. The Secure Gateway Configuration wizard verifies that the appropriate certificate is installed in the local machine certificate store.

• Wildcard certificate support. Wildcard certificates can be deployed on the Secure Gateway, the Secure Gateway Proxy, and on the Citrix Presentation Server hosting the STA.

• Load balancing
The Secure Gateway provides load balancing for the Secure Gateway Proxy. IP addresses are retrieved from the DNS using a domain name or listed individually.

• Improved logging
The Secure Gateway uses the Apache standard access log files and supports log rotation functionality for the access log files. The access log files provide connection information to the Secure Gateway or the Secure Gateway Proxy.

• Improved instrumentation
The Secure Gateway includes a new set of performance counters to analyze the usage and load on the Secure Gateway server. For more information about the performance counters, see “The Secure Gateway Performance Statistics” on page 70.

• Apache Technology
The Apache 2.x code base is used as a foundation for building the Secure Gateway.

• Secure Socket Layer support
The Secure Gateway provides SSL support to secure communication between the client and the Secure Gateway components.

• Section 508 compliance
User interface enhancements ensure the Secure Gateway is compliant with Section 508 of the United States Workforce Rehabilitation Act of 1973. For full Section 508 compliance, the minimum server requirement is the Windows 2000 Server family with Service Pack 4.

• Session reliability
Improvements in session reliability benefit both mobile and local users by having their work items remain open when network connectivity is lost, and then seamlessly resumed when connectivity is restored. This feature is especially useful for mobile users with wireless connections that are interrupted or dropped. When a session connection is interrupted, all open windows to published resources will remain visible while reconnection is automatically attempted in the background. Session reliability is enabled using the common gateway protocol.

- **Relay mode**

Version 3.0 of the Secure Gateway can be installed in relay mode for internal secure communications. Relay mode can be used in secure corporate environments such as intranets, LANs, and WANs. Relay mode is not recommended for external connections from the Internet to a server farm or server access farm. For more information about relay mode, see “Using the Secure Gateway Proxy in Relay Mode” on page 119.

- **Secure connectivity over the Internet; no VPN required**

Providing standards-based encryption over the Internet, the Secure Gateway eliminates the cost and configuration requirements of a traditional virtual private network (VPN). The Secure Gateway provides secure access to company information, corporate applications, intranets, and internal Web sites without the cost and complexity of a VPN.

- **Supports single-hop or double-hop DMZ deployment**

The Secure Gateway can be installed to span a single-hop or a double-hop DMZ. If your DMZ is divided into two stages, install the appropriate Secure Gateway component in each DMZ segment to securely transport HTTP/S and ICA traffic to and from the secure network. For more information about deploying Secure Gateway, see “Deploying the Secure Gateway with Citrix Presentation Server” on page 37.

- **Supports secure communication between the Secure Gateway components.**

The Secure Gateway components support the use of digital certificates, and the task of securing links, using SSL/TLS, between components. This is easily accomplished using the Secure Gateway Configuration wizard.

- **Configuration, management, and diagnostic tools**

The Secure Gateway Management Console is a Microsoft Management Console (MMC) snap-in you can use to manage, analyze, and troubleshoot a Secure Gateway deployment. In addition, the Secure Gateway Diagnostics tool, available from the Secure Gateway Management Console,
Introducing the Secure Gateway 19

• **Minimal client configuration**
When securing an access server farm, client devices require no preinstalled software for security. Remote, secure access is easy to support, requiring little effort from IT staff.

• **Certificate–based security**
The Secure Gateway uses standard Public Key Infrastructure (PKI) technology to provide the framework and trust infrastructure for authentication and authorization.

• **Standard encryption protocols**
The Secure Gateway uses industry-standard SSL or TLS encryption technology to secure Web and application traffic between the client and server. It provides secure access to company information, corporate applications, intranets, and internal Web sites without the cost and complexity of a VPN.

Connections between clients and the Secure Gateway are encrypted using SSL or TLS protocols. You can further enhance security by forcing the Secure Gateway to restrict its use of ciphersuites to commercial or government ciphersuites certified for Federal Information Processing Standard (FIPS) 140 requirements.

• **Authentication**
The Secure Gateway works with the Web Interface to facilitate authentication of users attempting to establish connections to an access server farm or to a server farm.

• **Authorization**
Authorization takes place when the Secure Gateway confirms that the user is authenticated by the enterprise network. The authorization process is entirely transparent to the user.

• **Single point of entry**
The need to publish the address of every computer running Citrix Presentation Server is eliminated and server certificate management is simplified. The Secure Gateway allows a single point of encryption and access to computers running Citrix Presentation Server.
Firewall traversal
Connections from clients are secured with standard protocols using ports typically open on corporate firewalls. This allows easy traversal of firewalls without custom configuration.

Ease of installation and management
Adding the Secure Gateway to an existing server farm is relatively quick and simple, and requires minimal configuration, significantly reducing time and management costs.

Reliability and fault tolerance
The solution allows implementation of duplicate components to enable a redundant system. Large arrays can be built using industry-standard SSL load balancing systems for scalability. Even if hardware fails, the server farm remains protected.

Scalable and extensible solution
A single server running the Secure Gateway can easily support a small corporate site consisting of hundreds of users. You can support medium to large sites catering to thousands of users connecting to an array of load balanced servers running the Secure Gateway. The Secure Gateway components do not require any special hardware devices or network equipment upgrades.

Event and audit logging
Critical and fatal system events are logged to the Secure Gateway application log. This log file provides administrators with a record of systems events and facilitates diagnosis of system problems.

Logging levels are configurable and can be set from the user interface. Depending on the configured logging level, you can retrieve a complete record of network connection attempts to the Secure Gateway. You can also configure the Secure Gateway to omit log entries for polls from network equipment such as load balancers.
In this chapter, you will learn how the Secure Gateway works with Citrix Presentation Server to secure your enterprise network. In addition, this chapter provides information to help you plan your network to include the Secure Gateway and the Secure Gateway Proxy.

This chapter contains the following topics:

- “How the Secure Gateway Works” on page 21
- “How the Secure Gateway Secures Your Environment” on page 22
- “Securing Citrix Presentation Server” on page 23
- “The Secure Gateway in a Double-Hop DMZ” on page 26
- “Upgrading the Secure Gateway” on page 28

How the Secure Gateway Works

The deployment of the Secure Gateway depends on several factors, including which Citrix components you have in your enterprise network. The Secure Gateway is designed to work with Citrix Presentation Server.

If you have a server farm using Citrix Presentation Server, users connect through the Secure Gateway using the Web Interface.

Note: Citrix recommends setting up the Secure Gateway in a test environment before implementation to your production environment to make sure all of the features work correctly.
How the Secure Gateway Secures Your Environment

The Secure Gateway provides secure Internet access to computers running Citrix Presentation Server in an enterprise network.

The following figure shows how an enterprise uses the Secure Gateway to securely access information over the Internet. The network is divided into three segments. The Internet segment contains remote employees, partners, and customers. The DMZ segment contains the Secure Gateway. The secure enterprise network segment contains a server farm hosting enterprise applications and an access server farm that aggregates published resources, internal data, and other information. All data between the Internet and secure enterprise network segments use SSL and pass through the DMZ segment containing the Secure Gateway.

Securing an access server farm and applications with the Secure Gateway

The Secure Gateway uses open standard security protocols and Public Key Infrastructure (PKI) to secure HTTP and/or ICA connections to the secure corporate network.

SSL or TLS is used to encrypt communications between remote client devices and the Secure Gateway.

Users must log on to the secure network with valid user credentials; the Secure Gateway is completely transparent to users.
Securing Citrix Presentation Server

One or more computers running Citrix Presentation Server are referred to as a server farm. To securely access resources published in a server farm, install the Secure Gateway in the DMZ. In this configuration, the Secure Gateway manages authentication and authorization and is responsible for creating a secure channel for data exchanged between the client device and computers running Citrix Presentation Server in the secure network.

In this configuration, the Secure Gateway is deployed to provide secure Internet access directly to computers running Citrix Presentation Server in the enterprise. Mobile workers and partners are allowed to access applications and resources, such as network printers, published on a server farm. In this usage scenario, the Secure Gateway securely transmits ICA traffic over the Internet.
The above figure shows a Secure Gateway deployment used to secure a server farm. The Internet/unsecure network contains a client device running a Web browser and Citrix Presentation Server Client. The demilitarized zone contains the Secure Gateway and Web Interface components that are installed on the same server. The secure network contains a server farm with Citrix Presentation Server with one computer running the Secure Ticket Authority. The Secure Gateway needs to connect to only one server running the STA. A server within the server farm runs the Citrix XML Service. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate devices to enable secure communications.

In this configuration, you need the following software components:

- The Secure Gateway
- Citrix Presentation Server installed on one or more computers
- Web Interface
- Citrix XML Service

**Note:** In previous versions of Citrix Presentation Server, the STA was installed on a separate server in the DMZ. Now, the STA is included and automatically installed with Citrix Presentation Server, which eliminates the need for a separate server for the STA.

For more information about each of these components, see “The Secure Gateway and Secure Gateway Proxy” on page 14.

For information about setting up and configuring a server farm, see the *Citrix Presentation Server Administrator’s Guide*.

### Establishing a Secure Connection to a Server Farm

In this scenario, the Secure Gateway works with the Web Interface to provide secure access to published resources available on a secure enterprise network.

1. A remote user types the address of the server running the Secure Gateway, such as https://www.gateway01.wxyco.com/, in the address field of a Web browser.
2. The Secure Gateway receives the request and relays the request to the Web Interface.
3. The Web Interface responds by sending a logon page to the client browser.
4. The Web Interface sends user credentials to the Citrix XML Service available from the server farm and obtains a list of applications that this user is authorized to use.

5. The Web Interface populates the Web page with the list of published resources that the user is authorized to access.

6. When the user clicks a published application link, the Web Interface sends the IP address and port for the requested computer running Citrix Presentation Server to the STA and requests a session ticket for the user. The STA saves the IP address and issues the requested ticket to the Web Interface.

7. The Web Interface generates an ICA file containing the ticket issued by the STA and sends it to the client browser.

**Important:** The ICA file generated by the Web Interface contains the Fully Qualified Domain Name (FQDN) or Domain Name Server (DNS) name of the server running the Secure Gateway. The address of the server(s) running Citrix Presentation Server is never revealed to the Citrix Presentation Server Client.

8. The client Web browser uses the ICA file to launch the Citrix Presentation Server Client. The client connects to the Secure Gateway using the FQDN or DNS name in the ICA file. Initial SSL/TLS handshaking is performed to establish the identity of the server running the Secure Gateway.

9. The Secure Gateway receives the session ticket from the client and contacts the STA for ticket validation.

10. If the ticket is valid, the STA returns the IP address of the computer running Citrix Presentation Server on which the requested application resides. If the session ticket is invalid or has expired, the STA informs the Secure Gateway and an error message appears on the client device.

11. On receipt of the IP address for the computer running Citrix Presentation Server, the Secure Gateway establishes an ICA connection to the client device. When the ICA connection is established, the Secure Gateway encrypts and decrypts data flowing through the connection.

In this deployment scenario, the Web Interface is installed on the same server as the Secure Gateway. This is a supported configuration; however, you may prefer to install the Web Interface on a separate Web server depending on the hardware resources you have available. See “Deploying the Secure Gateway with Citrix Presentation Server” on page 37 for detailed instructions about deploying the Secure Gateway in this scenario.
The Secure Gateway in a Double-Hop DMZ

Depending on the security and network policies practiced by your organization, you may want to secure your network by using a DMZ that is divided into two stages, referred to as a *double-hop DMZ*. This provides greater security to your enterprise network and the resources located on servers within the network.

The Secure Gateway is designed to fully support deployment in a double-hop scenario. To deploy the Secure Gateway in a double-hop DMZ, install the Secure Gateway in the first DMZ segment and the Web Interface and the Secure Gateway Proxy on separate servers in the second DMZ segment. When a user is authenticated and authorized by the Web Interface, the Secure Gateway Proxy functions as a conduit for traffic originating from the Secure Gateway to servers in the secure network, and from servers in the secure network to the Secure Gateway.
This figure shows a typical double-hop Secure Gateway deployment used to secure published applications within a server farm. The unsecure network contains a client device running a Web browser and Citrix Presentation Server Client. The first stage of the demilitarized zone contains the Secure Gateway. The second stage of the DMZ contains the Secure Gateway Proxy and Web Interface. The secure network contains servers running Citrix Presentation Server and internal Web servers. A server within the server farm runs the Citrix XML Service. A firewall separates the unsecure network from the first stage of the demilitarized zone, a second firewall separates the first stage of the demilitarized zone from the second stage of the demilitarized zone, and a third firewall separates the second stage of the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate computers to enable secure communications.

Establishing a Secure Connection

The illustration above shows a double-hop deployment in which the Secure Gateway provides secure access to a server farm.

All communications between the Secure Gateway and servers within the secure network are routed through the Secure Gateway Proxy. The Secure Gateway Proxy uses an inbound Access Control List (ACL) to accept incoming connections from the Secure Gateway. It uses an outbound ACL to connect to specific servers within the secure network.

The communication flow is similar to that described for single-hop deployment scenarios except that any data exchanged between the Secure Gateway and servers within the secure network is routed through the Secure Gateway Proxy.

In double-hop DMZ deployments, the server running the Web Interface must be located in the second DMZ segment.

_Important:_ If the communications link between the Secure Gateway and the Secure Gateway Proxy is not secured, port 1080 must be open on the firewall between the first and second DMZ segments.

For more information about double-hop deployment scenarios, see “Deploying the Secure Gateway with Citrix Presentation Server” on page 37.
Upgrading the Secure Gateway

If your enterprise network currently has Citrix Presentation Server or MetaFrame Secure Access Manager 2.x with Version 2.0 of the Secure Gateway, you need to plan your upgrade according to the products you are using.

If your enterprise network contains a mixture of MetaFrame Presentation Server 3.0 and Access Gateway 4.0 with Version 3.0 of the Secure Gateway, the Secure Gateway must use the Authentication Service for ticketing and authentication.

**Important:** To use Version 3.0 of the Secure Gateway with Access Gateway, the secure network must have Access Gateway 4.0. The Secure Gateway will not work with earlier versions of MetaFrame Secure Access Manager or with Advanced Access Control 4.2.

Upgrading with Citrix Presentation Server

It is recommended, but not required, that you upgrade Citrix Presentation Server 4.5. When Version 3.0 of the Secure Gateway is used with the latest version of Citrix Presentation Server, all of the features of each product are available. However, Version 3.0 of the Secure Gateway will work with the previous version of Citrix Presentation Server, the STA, and the Web Interface.

**Note:** For session reliability, the Secure Gateway requires the STA that is included with Citrix Presentation Server 4.0 and beyond.

The following components work with the latest version of the Secure Gateway:

- MetaFrame Presentation Server 3.0
- Citrix Presentation Server 4.0 or higher
- Secure Ticket Authority Version 2.0
- Secure Ticket Authority Version 3.0
- Web Interface Version 3.0
- Web Interface Version 4.0 or higher

When upgrading the Secure Gateway without upgrading the server farm, make sure you have the FQDN of the server running the STA and of the server running the Web Interface.
If the server farm is upgraded to Citrix Presentation Server 4.5, upgrade the components for the Secure Gateway in the following order:

1. Remove the standalone server running the STA.
2. Upgrade the server farm to Citrix Presentation Server 4.5.
3. Upgrade the Web Interface to the one included with Citrix Presentation Server 4.5.
4. Upgrade the Secure Gateway.
System Requirements

This chapter describes the minimum requirements for hardware and software for deploying the Secure Gateway and the Secure Gateway Proxy. This includes:

- “System Software Requirements” on page 32
- “System Hardware Requirements” on page 32
- “Client Device System Requirements” on page 32
- “Citrix Components Compatibility” on page 33
- “Certificate Requirements” on page 34
System Software Requirements

You can install the Secure Gateway components on computers running the following Microsoft operating systems:


**Important:** Full Section 508 compliance when using the Secure Gateway Management Console requires Windows 2000 Server Service Pack 4 release or later.

System Hardware Requirements

The Secure Gateway requires the minimum hardware requirements for Windows 2000 Server, as specified by Microsoft:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>266Mhz or higher Pentium-compatible CPU</td>
</tr>
<tr>
<td>Memory</td>
<td>512MB RAM</td>
</tr>
<tr>
<td>Hard drive</td>
<td>4GB with 2GB of free space. Reserve 150MB for Secure Gateway installation.</td>
</tr>
<tr>
<td>Networking</td>
<td>One network adapter</td>
</tr>
<tr>
<td>Display</td>
<td>VGA or higher resolution monitor</td>
</tr>
<tr>
<td>Keyboard</td>
<td>Required</td>
</tr>
<tr>
<td>Pointing device</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Important:** For maximum security, Citrix recommends you reserve a standalone server for the Secure Gateway.

Client Device System Requirements

To access resources published in a server farm using the Secure Gateway, client devices must meet or exceed the following requirements.
Software System Requirements
The following Microsoft operating systems are supported for client devices:

- Windows 95
- Windows 98
- Windows Millennium Edition
- Windows NT 4.0 Workstation
- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional

The Web Interface requires Internet Explorer version 5.0 or later.

Note: If you are running Internet Explorer 5.0, ensure that the Microsoft Internet Explorer High Encryption Pack is installed. Citrix recommends that all critical updates be installed from the Microsoft Windows Update Web site.

Web Interface Compatibility
The Secure Gateway is compatible with the Web Interface for Citrix Presentation Server Version 4.0 and later and the Web Interface for MetaFrame Presentation Server 3.0. Earlier versions of the Web Interface and NFuse Classic are not supported.

Citrix Components Compatibility
The Secure Gateway is compatible with the following Citrix products:

- MetaFrame Presentation Server 3.0
- Citrix Presentation Server 4.0
- Citrix Presentation Server 4.5

Note: If MetaFrame Presentation Server 3.0 is used with Version 3.0 of the Secure Gateway, session reliability is not supported.
Certificate Requirements

All client devices and secure servers in a Secure Gateway deployment use digital certificates to verify each other’s identity and authenticity.

The Secure Gateway supports the use of digital certificates. As the security administrator, you need to decide whether or not the communication links between the Secure Gateway and other servers in the DMZ or secure network need to be encrypted.

For conceptual information about digital certificates and cryptography, see “About Digital Certificates” on page 101.

**Important:** If you purchased server certificates from a commercial certificate authority (CA), support for root certificates for most commercial CAs is built into Internet Explorer and Windows server products. If you obtained server certificates from a private CA or commercial CA whose root certificates are not, by default, supported by the Windows operating system, you must install matching root certificates on all client devices and servers connecting to secure servers.

Certificate Requirements for a Single-Hop DMZ Deployment

If your secure network contains Citrix Presentation Server with the Secure Gateway in the DMZ, servers and clients need the following certificates:

- Root certificates on all client devices that connect to the server running the Secure Gateway.
- Root certificates on every Secure Gateway component that connects to a secure server. For example, a root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running the STA.
- A server certificate on the server running the Secure Gateway.
- **Optional.** A server certificate on the servers running the STA. The STA is installed by default when you install Citrix Presentation Server.

All Secure Gateway components support the use of digital certificates. Citrix recommends that the communication links between the Secure Gateway and other servers in the DMZ or secure network be encrypted.

The Secure Gateway and the client each require one root certificate.
Certificate Requirements for a Double-Hop DMZ Deployment

If your secure network contains Citrix Presentation Server with the Secure Gateway in the first DMZ, and the Secure Gateway Proxy and the Web Interface in the second DMZ, servers and clients need the following certificates:

- Root certificates on all client devices connecting to the server running the Secure Gateway.
- Root certificates on every Secure Gateway server that connects to a secure server or Web server. For example, an appropriate root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running Citrix Presentation Server.
- A server certificate on the server running the Secure Gateway.
- Optional. A server certificate on the server(s) running the Secure Gateway Proxy.
- Optional. A server certificate on the server running the STA.
Deploying the Secure Gateway with Citrix Presentation Server

This chapter describes recommended scenarios for deploying the Secure Gateway to provide secure Internet access to a server farm. Reviewed are choosing how to deploy the Secure Gateway for optimum security, basic concepts of setting up and testing a server farm, and single-hop demilitarized zone (DMZ) or a double-hop DMZ deployment scenarios.

This chapter contains the following topics:

- “Deploying the Secure Gateway with Citrix Presentation Server” on page 37
- “Choosing a Deployment for Your Organization” on page 38
- “Setting Up and Testing a Server Farm” on page 41
- “The Secure Ticket Authority (STA)” on page 41
- “Configuring the Web Interface to Support the Secure Gateway” on page 42
- “Scenario A: Single-Hop DMZ Deployment” on page 42
- “Scenario B: Double-Hop DMZ Deployment” on page 45
- “Scenario C: Upgrading from Earlier Versions of the Secure Gateway” on page 47
- “Testing Your Deployment” on page 53
Choosing a Deployment for Your Organization

Citrix Presentation Server is the world’s most widely deployed presentation server for centrally managing multiple applications and delivering their functionality as a service to employees, wherever they may be. Designed to enhance Windows 2000 and Windows 2003 servers, Citrix Presentation Server provides the exceptional scalability, interoperability, manageability, flexibility and network leverage that the enterprise requires from an access infrastructure solution, while delivering end-to-end security and measurable business and IT benefits.

One or more computers running Citrix Presentation Server creates a server farm. If your enterprise network contains a server farm, you can deploy the Secure Gateway to provide secure Internet access to published resources.

In such deployments, the Secure Gateway works with the Web Interface to provide authentication, authorization, and redirection to published resources hosted on a computer running Citrix Presentation Server.

The following section evaluates recommended topologies in which you can deploy the Secure Gateway and the Web Interface for access to server farms.

Single-Hop DMZ Deployments

In a single-hop deployment, users can connect to the enterprise network in two ways. The first is where the Secure Gateway intercepts the client connection and routes it to the Web Interface. After logging on and authenticating user credentials, the Secure Gateway handles the connection. Alternatively, users can be directed to the Web Interface first, where they logon and then the connection is handled by the Secure Gateway. The first scenario is referred to as “behind the Secure Gateway.” The second scenario is referred to as “parallel to the Secure Gateway.”

Running the Web Interface behind the Secure Gateway in the DMZ

In this scenario, all incoming traffic is intercepted by the Secure Gateway. The Web Interface can be installed on the same server as Secure Gateway or on a separate server. All data exchanged between client devices and the Web Interface is relayed through the Secure Gateway.

The firewall facing the Internet has port 443 open. Users connect to the Secure Gateway using a URL such as https://Secure Gateway FQDN/, where Secure Gateway FQDN, where is the fully qualified domain name for the server running the Secure Gateway.
Why You Would Select this Deployment
Citrix recommends deploying the Secure Gateway in this configuration if your network is small to medium sized, with a usage profile of hundreds of users. This type of deployment is optimal when users are connecting over the Internet to the Secure Gateway.

If any of the limitations described above are a concern and you have a sizeable user base accessing the Secure Gateway over the LAN, consider deploying the Web Interface in the configuration described in “Running the Web Interface Parallel with the Secure Gateway” on page 40.

Locking Down Internet Information Services (IIS)
All traffic to the server running the Web Interface is proxied through the server running the Secure Gateway. You need to lockdown IIS to allow only the Secure Gateway to communicate with the Web Interface.

For instructions about configuring IIS to explicitly grant or deny access to applications or Web sites, refer to the IIS documentation that ships with Microsoft Windows Server 2000 or Microsoft Windows Server 2003.
Running the Web Interface Parallel with the Secure Gateway

In this configuration, the Secure Gateway and the Web Interface are installed on separate servers. Users can connect directly to the Web Interface.

Users connect directly to the Web Interface, using a URL such as https://Web Interface FQDN/citrix/MetaFrame, where Web Interface FQDN is the fully qualified domain name for the server running the Web Interface.

Citrix recommends securing both servers by installing a server certificate on each server running the Secure Gateway and the Web Interface. Open port 443 on the firewall facing the Internet.

Why You Would Select this Deployment

You want to use the features available with the Web Interface, including smart card authentication and firewall and proxy settings that depend on knowing the client IP address.

Double-Hop DMZ Deployments

Deploy the Secure Gateway in a double-hop DMZ configuration if your DMZ is divided into two segments. In this configuration, the server running the Secure Gateway is in the first DMZ segment. The firewall between the first DMZ segment and the Internet has port 443 open.

The Web Interface and the Secure Gateway Proxy are installed on separate servers in the second DMZ segment. The server farm is located in the secure network. The firewall between the first and second DMZ segments has ports 80 and 443 open.

The Secure Gateway, deployed in the first DMZ segment, is responsible for intercepting all incoming traffic. The Web Interface is responsible for user authentication and authorization. After authentication, the Secure Gateway Proxy is responsible for relaying all data exchanged between the Secure Gateway and servers in the secure network. The firewall between the second DMZ segment and the secure network has ports 80, 443, and 1494 open.
Why You Would Select this Deployment

Deploy the Secure Gateway in this configuration if your network contains a double-hop DMZ. A double-hop DMZ provides additional protection because an attacker would need to penetrate multiple security zones to reach servers in the secure network.

If the resources accessible through the Secure Gateway are extremely sensitive and require a high level of security, consider this configuration.

Important: The same limitations described in “Running the Web Interface Parallel with the Secure Gateway” on page 53 apply when you deploy the Secure Gateway in a double-hop DMZ configuration.

Setting Up and Testing a Server Farm

The steps below provide a list of tasks you need to complete prior to installing and configuring the Secure Gateway.

1. Install and configure a server farm in the enterprise network.
2. Install, configure, and publish applications on the server farm.
3. Connect to the server farm using a client device and ensure you can access available published resources.

For detailed instructions about performing these tasks, see the Citrix Presentation Server Administrator’s Guide.

The Secure Ticket Authority (STA)

In previous versions of the Secure Gateway, the STA was installed and configured as a separate component. When Citrix Presentation Server 4.5 for Windows is installed, the STA is automatically installed and configured.

If Citrix Presentation Server 4.5 is installed on a server that has an older version of the STA, the old STA is upgraded to the new version.

The new STA eliminates the requirement for Microsoft’s Internet Information Services (IIS). The STA can be hosted by the Citrix XML Service. If the STA is hosted by the Citrix XML Service, configure the Citrix SSL Relay. For detailed instructions for configuring the Citrix SSL Relay, see the Citrix Presentation Server Administrator’s Guide.
During installation of the Secure Gateway, enter the FQDN of the server running Citrix Presentation Server. If you are using an SSL-enabled connection between the Secure Gateway and the STA, make sure the correct certificates are installed from a certificate authority. If the certificates are not installed, the Secure Gateway might not be able to find the STA during configuration.

**Configuring the Web Interface to Support the Secure Gateway**

You need to configure the Web Interface to interact with the Secure Gateway components to provide authentication and authorization functionality.

Make sure the configuration settings on the server running the Web Interface correctly reflect the details of the STA and the Secure Gateway.

For detailed instructions about configuring the Web Interface to support the Secure Gateway, refer to the *Web Interface Administrator’s Guide*.

**Scenario A: Single-Hop DMZ Deployment**

WXYCo Inc. is an audit firm that recently purchased licenses for Citrix Presentation Server.

The company’s employees are financial auditors who visit client sites and conduct financial audits. They use a proprietary, client-server auditing software application, AuditorX. They publish AuditorX on computers running Citrix Presentation Server. They also deploy the Web Interface for Web access to their published resources. Employees can access AuditorX and other published resources through a Web browser on a client device connected to the LAN.

WXYCo realizes installing the Secure Gateway allows them to provide secure Internet access to published resources on its server farms. Because the workforce is largely mobile, use of the Internet to connect to the enterprise network is expected to dramatically reduce remote access costs.
A secure server farm using a single-hop DMZ.

This figure illustrates a secure enterprise network separated from the Internet by a single-hop DMZ. The enterprise network contains a server farm including one server running Citrix Presentation Server with the Secure Ticket Authority (STA). The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open. If session reliability is enabled, port 2598 is open on the internal firewall.

The DMZ contains a single server running the Secure Gateway, and the Web Interface. Traffic to the Web Interface is proxied through the Secure Gateway which communicates with the Web Interface using HTTP.

The DMZ is separated from the Internet by a firewall that has port 443 open. The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the Citrix Presentation Server Client for 32-bit Windows.

The security analyst recommends securing the communication link between the Secure Gateway and the STA. To do this, the company purchased two server certificates from a commercial certificate authority (CA). The server running the Secure Gateway and the Web Interface have root and server certificates installed. The server running Citrix Presentation Server has a server certificate installed.

For more information about certificates, see “About Digital Certificates” on page 101.

The following sections describe the steps required to deploy the Secure Gateway in this usage scenario.
Setting Up and Testing the Web Interface

In this scenario, the Web Interface and the Secure Gateway are hosted on the same server in the DMZ. Install and configure the Web Interface before you install the Secure Gateway.

1. Install the Web Interface on the server reserved for the Secure Gateway and the Web Interface.

2. Add and configure a server farm(s) for use with the Web Interface.

3. Use a Web browser on a client device to connect and log on to the Web Interface.

4. Verify that you can launch published applications.

5. Configure the Secure Gateway and include the FQDN for the STA.

For detailed instructions about performing these tasks, see the Web Interface Administrator’s Guide.

Installing and Configuring the Secure Gateway

The Secure Gateway is installed on the same server as the Web Interface in the DMZ.

To install and configure the Secure Gateway, see “Installing and Configuring the Secure Gateway” on page 44.

Checking Client Devices

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in “Client Device System Requirements” on page 32.
Scenario B: Double-Hop DMZ Deployment

WXCYCo, Inc. deployed the Web Interface for access to published resources hosted on computers running Citrix Presentation Server. The company plans to deploy the Secure Gateway to provide secure Internet access to published resources.

The security analyst recommended setting up a double-hop DMZ between the Internet and the company’s secure network and securing communications between the Secure Gateway, the Web Interface, and the Secure Gateway Proxy.

![Diagram of a Secure Gateway deployment in a double-hop DMZ environment with a server farm](https://www.gateway3.wxycz.com)

This figure shows a Secure Gateway deployment used to secure a server farm in a double-hop DMZ environment. The secure enterprise network is separated from the Internet by a double-hop DMZ. The enterprise network contains a server farm including a server running Citrix Presentation Server with the Secure Ticket Authority (STA). The firewall separating the secure network from the second DMZ segment has port 443 open. If session reliability is enabled, port 2598 is open.

The second DMZ segment contains a server running the Secure Gateway Proxy and a second server running the Web Interface. The firewall separating the first and second DMZ segments has port 443 open. The first DMZ segment contains a single server running the Secure Gateway. All traffic originating from the Secure Gateway to servers in the secure network is proxied through the Secure Gateway Proxy.
If the communications link between the Secure Gateway and the Secure Gateway Proxy is not secured, open port 1080 on the firewall between the first DMZ segment and the second.

The Secure Gateway communicates directly with the server running the Web Interface in the second DMZ segment, which in turn communicates directly with servers in the secure network. The first DMZ segment is separated from the Internet by a firewall that has port 443 open.

The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the Citrix Presentation Server Client for 32-bit Windows.

The following sections describe the steps required to deploy the Secure Gateway in this usage scenario.

**Installing and Configuring the Secure Gateway**

The Secure Gateway is installed on a standalone server in the first DMZ zone.

To install and configure the Secure Gateway, see “Installing the Secure Gateway” on page 55.

**Installing and Configuring the Secure Gateway Proxy**

The Secure Gateway Proxy is installed on a standalone server in the second DMZ zone.

To install and configure the Secure Gateway Proxy, see “Installing the Secure Gateway” on page 55.

**Setting Up and Testing the Web Interface**

The Web Interface needs to be set up on a Web server in the second DMZ segment. Ensure you complete the following tasks before you install the Secure Gateway.

1. Install the Web Interface on a standalone server in the second DMZ segment.
2. To secure communications between the Secure Gateway and the Web Interface, ensure you install a server certificate on the server running the Web Interface.
3. Add and configure a server farm(s) for use with the Web Interface.
4. Configure the Secure Gateway using the FQDN of the STA.
5. Use a Web browser on a client device to connect and log on to the Web Interface.
6. Verify that you can launch published applications.

For detailed instructions about performing these tasks, see the *Web Interface Administrator’s Guide*.

**Publishing the Web Address to Log on to the Secure Gateway**

Because all traffic to the Web Interface is proxied through the Secure Gateway, users need to type the following Web address to access the logon page:

https://Secure Gateway FQDN/Citrix/MetaFrame

where Secure Gateway FQDN is the fully qualified domain name for the server running the Secure Gateway.

In the case of WXYCo, the Web address for the logon page is:

https://www.gateway01.wxyco.com/Citrix/MetaFrame/

Alternatively, consider changing the default Web root directory in IIS on the server running the Web Interface to point to the Web Interface directory. This enables you to access the logon page by connecting directly to the root Web address; that is, https://Secure Gateway FQDN/.

In this case, the URL that employees of WXYCo use to access the logon page is:

https://www.gateway01.wxyco.com/

**Scenario C: Upgrading from Earlier Versions of the Secure Gateway**

XYZCo, Inc. deployed Version 2.0 of the Secure Gateway to provide secure access to a server farm. Recently, XYZCo purchased Citrix Presentation Server, which includes the newest release of the Secure Gateway.
XYZCo’s network administrator recommended to the management that, in addition to upgrading the Web Interface and Citrix Presentation Server, they upgrade Version 2.0 of the Secure Gateway to Version 3.0 of the Secure Gateway.

A secure enterprise network in a single-hop DMZ.

This figure illustrates a secure enterprise network separated from the Internet by a single-hop DMZ running MetaFrame Presentation Server 3.0. The enterprise network contains a server farm and a secure server running the Secure Ticket Authority (STA). The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open. The DMZ contains a secure server running Version 2.0 of the Secure Gateway and a second secure server running the Web Interface for Citrix Presentation Server.

Users connect directly to the secure server running the Web Interface, which authenticates the user. Authenticated connections then go to the server running the Secure Gateway. The DMZ is separated from the Internet by a firewall that has port 443 open.

The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the Citrix Presentation Server Client.

The following sections describe the steps required to upgrade an existing deployment of the Secure Gateway.
Upgrading the Server Farm

In this scenario, upgrade the server farm to Citrix Presentation Server 4.5 for Windows. For detailed instructions about performing this task, see the Citrix Presentation Server Administrator’s Guide.

Upgrading the Secure Ticket Authority

The Secure Ticket Authority (STA) is included with Citrix Presentation Server 4.5 and is automatically installed when Citrix Presentation Server is installed and configured. This eliminates the need to have a separate server for the STA. If the Secure Ticket Authority is installed on a standalone server, Citrix recommends that it be removed from the network and to use the STA that is included with Citrix Presentation Server 4.5 for Windows.

Important: If you are securing communications between the Secure Gateway and the STA, ensure you install a server certificate on the server running the STA.

Starting the Citrix XML Service Port

Citrix Presentation Server uses the Citrix XML Service to supply servers running the Web Interface and TCP/IP-connected clients with the names of published applications that are available in a server farm. By default, installation of Citrix Presentation Server configures the Citrix XML Service to share port 80 with IIS.

If you intend to send data to the Web Interface over a secure HTTP connection using SSL, be sure that the Citrix XML Service is set to share its port with IIS and that IIS is configured to support HTTPS.

If you do not want the Citrix XML Service to share the TCP port with IIS, make sure the port you plan to use is not used by any other application.

Important: All servers in the server farm must use the same TCP port for the Citrix XML Service.

For a list of ports in use, type `netstat -a` at a command prompt. Make a note of the port number you specify. If you use a port other than the default port 80, you must configure servers running the Web Interface to use the port you choose. See the Web Interface Administrator’s Guide for instructions about configuring the Web Interface to use a different port.

If Citrix Presentation Server is installed and port sharing is not enabled, the scripts directory is not created and the files for the STA are not copied to the Inetpub folder.
Important: Use this procedure only if you do not want to share the port used by IIS. If you enter a port number other than the default “Share with IIS” during Setup, you can change the port to another port number using the Presentation Server Console. However, if you want to change the setting to share the port with IIS after running Setup, you must follow the instructions for manually setting the Citrix XML Service to share the TCP port with IIS.

To change the Citrix XML Service port after installation

1. Use the Services Control Panel to stop the Citrix XML Service.
2. At a command prompt, type `ctxxmlss /u` to unload the Citrix XML Service from memory.
3. Type `ctxxmlss /rnn`, where `nn` is the number of the port you want to use. For example, `ctxxmlss /r88` forces the Citrix XML Service to use TCP/IP port 88.
4. Restart the Citrix XML Service in the Control Panel.

To manually configure the Citrix XML Service to share the TCP port with IIS

1. Use the Services Control Panel to stop the Citrix XML Service.
2. At a command prompt, type `ctxxmlss /u` to unload the Citrix XML Service.
3. Copy Wpnbr.dll and Ctxxmlss.txt to the IIS scripts directory on your Web server. These files are installed in `\Program Files\Citrix\System32` during Citrix Presentation Server installation. The default scripts directory is `\Inetpub\Scripts`.
4. Use Internet Service Manager to give the files read and write access.
5. Stop and restart the Web server.

Upgrading and Configuring the Secure Gateway

To upgrade the Secure Gateway, see “Upgrading the Secure Gateway” on page 64.

If you need to modify the configuration parameters for the Secure Gateway Proxy, you can run the Secure Gateway Proxy Configuration wizard. For more information, see “Configuring the Secure Gateway Proxy” on page 63.
Upgrading the Web Interface

Upgrade the server running the Web Interface. Ensure the configuration settings on the server running the Web Interface correctly reflect details of the STA and the Secure Gateway. For detailed instructions about configuring the Web Interface to support the Secure Gateway operation, see the Web Interface Administrator’s Guide.

**Important:** If you are securing communications between the Secure Gateway and the Web Interface, install a server certificate on the server running the Web Interface.

![Diagram](image)

**Enterprise network upgraded to Citrix Presentation Server 4.5 and Version 3.0 of the Secure Gateway**

This figure illustrates a secure enterprise network separated from the Internet by a single-hop DMZ running Citrix Presentation Server 4.5. The enterprise network contains a server farm. The Secure Ticket Authority (STA) is running on one server in the farm. The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open. The DMZ contains a secure server running Version 3.0 of the Secure Gateway and a second secure server running the Web Interface.

As in the earlier deployment, users connect directly to the secure server running the Web Interface, which authenticates the user. Authenticated connections then go to the server running the Secure Gateway. The DMZ is separated from the Internet by a firewall that has port 443 open.
The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the Citrix Presentation Server Client.

**Publishing the Web Address to Log on to the Secure Gateway**

The Web address that users connect to depends on whether you choose to deploy the Web Interface behind or in parallel with the Secure Gateway.

**Running the Web Interface behind the Secure Gateway**

In this scenario, users connect directly to the Secure Gateway. The Web Interface is not accessible through the Internet. All communications to the Web Interface are proxied through the Secure Gateway.

**Important:** Review the guidance provided in “Running the Web Interface behind the Secure Gateway in the DMZ” on page 38 for information about the advantages and limitations of deploying the Secure Gateway and the Web Interface in this configuration.

Because all traffic to the Web Interface is proxied through the Secure Gateway, users must type the following Web address to load the logon page:

https://Secure Gateway FQDN/citrix/MetaFrame/

where **Secure Gateway FQDN** is the fully qualified domain name for the server running the Secure Gateway. When the Secure Gateway receives a request for a connection, it routes the connection request to the server running the Web Interface.

In the case of XYZCo, users must type the Web address below to access the logon page:

https://www.gateway01.xyzco.com/citrix/MetaFrame/

Alternatively, consider changing the default Web root directory in IIS to point to the Web Interface directory. This enables you to access the logon page by connecting directly to the root Web address; that is, https://Secure Gateway FQDN/.

In this case, the Web address employees of XYZCo use to access the logon page is:

https://www.gateway01.xyzco.com/
To modify the value of the Web root directory in IIS

1. Log on as an administrator to the server running the Web Interface.
2. Create a new file called default.asp and save it to the InetPub\wwwroot directory.
3. Edit the default.asp file and add the following line of code:
   `<% Response.Redirect "\citrix/MetaFrame/" %>`
4. Save and close the file.

Running the Web Interface Parallel with the Secure Gateway

In this configuration, users connect directly to the server running the Web Interface. Therefore, users must type the following Web address to load the logon page:

https://Web Interface FQDN/citrix/MetaFrame/

where Web Interface FQDN is the fully qualified domain name for the server running the Web Interface. In the case of XYZCo, users must type the URL below to access the logon page:

https://www.gateway01.xyzco.com/citrix/MetaFrame/

Alternatively, consider changing the default Web root directory in IIS to point to the Web Interface directory, as described in “To modify the value of the Web root directory in IIS” on page 53.

Depending on the configuration in which you deployed the Secure Gateway and the Web Interface, inform your users about the URL to enter to access published resources.

Testing Your Deployment

After you complete installation and configuration of the Secure Gateway, test your deployment to make sure it works and is accessible through the Internet.

If you encounter problems loading the logon page, try working your way through the deployment steps to figure out the problem.

You can also run the Secure Gateway Diagnostics tool to find a solution. This utility contacts all servers running the Secure Gateway components and generates a report containing configuration and status information for each component. For more information, see “Viewing the Secure Gateway Diagnostics Report” on page 74.
To test your deployment

1. Use a Web browser on a client device to connect to the Secure Gateway; for example, https://www.gateway01.wzyco.com/Citrix/MetaFrame/.

2. Log on using domain credentials. After a brief interval, the Applications page containing icons for published resources appears.

3. Verify that you can launch published applications from this page.
Installing the Secure Gateway

This chapter discusses the installation and configuration of the Secure Gateway. There are individual procedures for installing and configuring the Secure Gateway or the Secure Gateway Proxy to work with a server farm. There are also recommendations for installation of other components, such as Web Interface, which depend on the configuration of your enterprise network.

This chapter contains the following topics:

- “Guidelines for Installing and Configuring the Secure Gateway” on page 56
- “Preparing for Installation” on page 56
- “Which Components You Need to Install” on page 58
- “Configuring the Secure Gateway” on page 60
- “Installing the Secure Gateway Proxy” on page 62
- “Configuring the Secure Gateway Proxy” on page 63
- “Upgrading the Secure Gateway” on page 64
- “Uninstalling the Secure Gateway” on page 65
Guidelines for Installing and Configuring the Secure Gateway

To ensure that the security of the Secure Gateway is not compromised, Citrix recommends:

- Reserving servers for the exclusive use of the Secure Gateway
- Ensuring only users with administrative privileges are allowed to install the Secure Gateway

**Important:** You must be logged on as an administrator to install and configure the Secure Gateway and use the management tools.

Preparing for Installation

Before installing the Secure Gateway or the Secure Gateway Proxy, make sure the hardware and software meet the system requirements described in “System Requirements” on page 31.

**The Secure Gateway Pre-Installation Checklist**

Print and complete the *Secure Gateway Pre-Installation Checklist*. Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing the Secure Gateway components.

**Installation Sequence**

The following steps outline the installation sequence of the Secure Gateway:

1. Install Citrix Presentation Server.
2. Install root and server certificates on the appropriate computers. For more information, see “Certificate Requirements” on page 57 and “About Digital Certificates” on page 101.
3. If using a double-hop DMZ, install the Secure Gateway Proxy in the second DMZ.
4. Install the Secure Gateway in the first, or only, DMZ.

**Important:** The Secure Gateway is designed to discover and verify the existence of the other Citrix components during configuration. For example, during configuration the Secure Gateway verifies that servers running the Logon
Agent, the Authentication Service, the Web Interface, and the STA, if used, are functional. If a required component is not found, the Secure Gateway may fail to start. It is therefore important to follow the recommended installation sequence.

The installation sequence must be in this order:

1. Always install components within the secure network first.
2. **Optional.** If your network contains a double-hop DMZ, install components in the second DMZ segment next.
3. Install components in the first DMZ segment last.

**Certificate Requirements**

All client devices and secure servers in a Secure Gateway deployment use digital certificates to verify each other’s identity and authenticity.

For conceptual information about digital certificates and cryptography, see “About Digital Certificates” on page 101.

**Important:** If you purchased server certificates from a commercial certificate authority (CA), support for root certificates for most commercial CAs is built into Internet Explorer and Windows server products. If you obtained server certificates from a private CA or commercial CA whose root certificates are not, by default, supported by the Windows operating system, you must install matching root certificates on all client devices and servers connecting to secure servers.

**Certificate Requirements for a Single-Hop DMZ Deployment**

If the Secure Gateway is in the DMZ, servers and clients need the following certificates:

- Root certificates on all client devices that connect to the server running the Secure Gateway.
- Root certificates on every Secure Gateway component that connects to a secure server. For example, a root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running the STA.
- A server certificate on the server running the Secure Gateway.
- **Optional.** A server certificate on the servers running the STA. The STA is installed by default when you install Citrix Presentation Server.
All Secure Gateway components support the use of digital certificates. Citrix recommends the communication links between the Secure Gateway and other servers in the DMZ or secure network be encrypted.

**Certificate Requirements for a Double-Hop DMZ Deployment**

If the Secure Gateway is in the first DMZ and the Secure Gateway Proxy in the second DMZ, and the Web Interface is in the second DMZ, servers and clients need the following certificates:

- Root certificates on all client devices connecting to the server running the Secure Gateway.
- Root certificates on every Secure Gateway component that connects to a secure server or Web server. For example, an appropriate root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running Citrix Presentation Server.
- A server certificate on the server running the Secure Gateway.
- **Optional.** A server certificate on the server(s) running the Secure Gateway Proxy.
- **Optional.** A server certificate on the server running the STA.

All Secure Gateway components support the use of digital certificates. It is not a requirement, however Citrix recommends that the communication links between the Secure Gateway and other servers in the DMZ or secure network be encrypted.

**Which Components You Need to Install**

The tables below describe the components required in single and double-hop DMZ deployment scenarios.

The Secure Gateway installer is designed so you can install the Secure Gateway or the Secure Gateway Proxy. When installation is complete, the Secure Gateway Configuration wizard automatically starts so you can configure Secure Gateway.

The Secure Gateway can be installed using the Citrix Presentation Server Components CD-ROM.

**To install the Secure Gateway**

1. From the Autorun screen, click **Network & Security** and then click **Install Secure Gateway**.
2. On the Welcome screen, click **Next**.
3. Read and accept the license agreement, and then click **Next**.
4. In Installation Mode, select **Secure Gateway**.

5. To install the Secure Gateway in the default destination path, click **Next**. To install these components in a different location, click **Browse** and then navigate to the folder you want to use.

6. In **Service Account**, select the user account to determine credentials and privileges. Citrix recommends you select an account that restricts privileges.

7. Click **Next** and follow the instructions in the wizard to complete installation.

8. After installing the Secure Gateway, restart the server on which you installed it.

9. Install the Secure Gateway hotfix SGE300W003 or its replacements on the Secure Gateway server. This hotfix is available from the \Secure Gateway\Windows folder of the Citrix Presentation Server 4.5 Components CD.

   This hotfix is also available from the Citrix Web site. Go to the Hotfixes, Rollups & Service Packs section of the Citrix Knowledge Center and browse to the Secure Gateway 3.0 hotfix (SGE300W003) or its replacements.

---

**Important:** Before clients connect to the Secure Gateway, you must install this hotfix. If you do not install this hotfix on your Secure Gateway server, the ICA Java Client (version 9.3 and higher) and the Presentation Server Client for Windows (version 9.200 and higher) cannot use the Session Reliability feature of Secure Gateway. Session Reliability is enabled by default in Citrix Presentation Server 4.5.

---

**Note:** If you cancel the installation at any point, the selections you made in the installation wizard are not saved. Citrix recommends that you uninstall and reinstall the Secure Gateway if you cancel or abort the installation.
Configuring the Secure Gateway

The Secure Gateway Configuration wizard automatically starts when the installation is complete. The wizard guides you through configuration tasks and provides context-sensitive help describing the procedures and information you need to enter.

To configure the Secure Gateway for use with Citrix Presentation Server, you need to have the following information:

- The FQDN and path of the server running the STA
- The FQDN and path of the server running the Web Interface

To configure the Secure Gateway

1. On the Welcome screen, select Citrix Presentation Server and then click OK.
2. On the Secure Gateway configuration level screen, select Advanced and then click Next.
3. On the Select a server certificate screen, select the server certificate to associate with the Secure Gateway and then click Next.
4. On the Specify secure protocol parameters screen, select the secure protocol and ciphersuite that the Secure Gateway must use for client connections.
5. On the Configure inbound client connections screen:
   - Select the Monitor all IP addresses check box
   - Accept the default value 443 as the TCP port number
   These options configure the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
6. On the Configure outbound connections screen, do one of the following:
   - If there are no outbound traffic restrictions, select No outbound traffic restrictions and then click Next.
   - If you are using a double-hop DMZ, select Use the Secure Gateway Proxy. Click Configure, click Add, and then enter either the FQDN or IP address of the Secure Gateway Proxy. Click OK, and then click Next.
   - To configure an Access Control List, select Use an Access Control List (ACL), and then click Configure. Click Add, and then enter the
IP address range and select a protocol. Click OK twice and then click Next.

The access control list contains IP addresses and DNS names for allowed access to the secure network. Only those listed in the ACL are allowed to connect to the Secure Gateway and the secure network.

7. On the Details of the server running the Secure Ticket Authority (STA) screen, click Add.

8. On the STA details screen, enter the fully qualified domain name of the server running the STA; for example, accesscenter01.uvwco.com.

9. The Secure Gateway Configuration wizard contacts the server running the STA. When the wizard successfully resolves the specified address, the ID field is automatically populated when you click OK.

10. Click OK and then click Next to continue.

11. On the Connection parameters screen, click Next to accept default values for connection time-outs and connection limits.

12. On the Logging Exclusions screen, click Add and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.

13. On the Details of the server running the Web Interface screen, select one of the following:

   - **Indirect**: To access the Web Interface, users enter the URL of the Secure Gateway. Users connect to the Secure Gateway, which routes the request to the Web Interface. If the Web Interface is installed on the same computer as the Secure Gateway, select Installed on this computer. For more information see, “Running the Web Interface behind the Secure Gateway in the DMZ” on page 38.

   - **Direct**: To access the Web Interface, users enter the URL of the Web Interface. Users connect to the Web Interface directly. For more information, see “Running the Web Interface Parallel with the Secure Gateway” on page 40.

14. On the Logging parameters screen, click Next to accept the default logging level for the Secure Gateway. The configuration of the Secure Gateway is complete.

15. Check Start the Secure Gateway and click Finish. The Secure Gateway starts.

If you need to modify configuration parameters for the Secure Gateway, run the configuration wizard again.
To start the Secure Gateway Configuration wizard

1. Click Start > Programs.
2. Click Citrix > Secure Gateway > Secure Gateway Configuration Wizard.

Ensure that you stop the Secure Gateway service before modifying configuration settings.

To stop the Secure Gateway service

1. Log on as an administrator to the Secure Gateway.
2. Click Start > Programs > Management Consoles > Secure Gateway Management Console.
3. In the Secure Gateway Management Console, on the Action menu, click All Tasks and click Stop.

Installing the Secure Gateway Proxy

Install the Secure Gateway Proxy on a standalone server in the second DMZ segment. If you are securing communications between the Secure Gateway and the Secure Gateway Proxy, ensure you install a server certificate on the server running the Secure Gateway Proxy.

To install the Secure Gateway Proxy

1. Insert the Citrix Presentation Server Components CD-ROM. From the Autorun screen, click Network & Security and then click Install Secure Gateway.
2. On the Welcome screen, click Next.
3. Read and accept the license agreement and click Next.
4. In Installation Mode, click Secure Gateway Proxy and click Next.
5. Select the destination folder and click Next. To install these components in a different location, click Browse and then navigate to the folder you want to use.
6. In Service Account, select the user account to determine credentials and privileges. Select an account that restricts privileges.
7. Click Next and follow the instructions in the wizard to complete installation.
Configuring the Secure Gateway Proxy

After installing the Secure Gateway Proxy, the Secure Gateway Proxy Configuration wizard starts.

To configure the Secure Gateway Proxy

1. On the Configuration type screen, select Advanced and check Secure traffic between the Secure Gateway and Secure Gateway Proxy.

2. On the Select a server certificate screen, select the server certificate to associate with the Secure Gateway Proxy and click Next.

3. On the Configure secure protocol settings screen, click Next to accept default values for the secure protocol and ciphersuite that the Secure Gateway Proxy uses for client connections.

4. On the Configure inbound client connections screen:
   A. Select the Monitor all IP addresses check box
   B. Accept the default value 443 as the TCP port number

   These options configure the Secure Gateway Proxy to listen for client connection requests on all IP addresses available on this server.

5. On the Configure outbound connections screen, select No outbound traffic restrictions and then click Next.

6. On the Connection parameters screen, click Next to accept default values for connection time-outs and connection limits.

7. On the Logging Exclusions screen, click Add and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.

8. On the Logging parameters screen, click Next to accept the default logging level for the Secure Gateway. The configuration of the Secure Gateway Proxy is complete.

Upgrading the Secure Gateway

You can upgrade from Version 2.0 of the Secure Gateway to Version 3.0 of the Secure Gateway.

When you run the Secure Gateway installer, it automatically checks for installed versions of the Secure Gateway. If a previously installed version of the Secure Gateway is detected, you are prompted to upgrade or remove the previous version.

For more information about upgrading, see “Upgrading the Secure Gateway” on page 28.

**Important:** If Version 3.0 of the Secure Gateway Proxy is installed in relay mode, upgrading is not supported. Earlier versions of the Secure Gateway Proxy must be uninstalled. Use Add/Remove Programs in Control Panel to uninstall the software before running the Secure Gateway installer.

To upgrade the Secure Gateway

1. Insert the Citrix Presentation Server, Components CD-ROM. From the Autorun screen, click Network & Security and then click Install Secure Gateway.

2. On the Welcome screen, click **Next**.

3. Read and accept the license agreement and click **Next**.

4. On the **Upgrade Notification** screen, click **Next**.

5. On the Installation Mode screen, select either **Secure Gateway** or **Secure Gateway Proxy**.

6. Select the destination folder and click **Next**. To install these components in a different location, click **Browse** and then navigate to the folder you want to use.

7. In **Service Account**, select the user account to determine credentials and privileges. Citrix recommends you select an account that restricts privileges. Click **Next**.

8. Click **Next** to begin installation of the Secure Gateway.

When installation is complete, the Secure Gateway Configuration Wizard starts. After installation, configure the Secure Gateway following the procedure in “Configuring the Secure Gateway” on page 60.
Uninstalling the Secure Gateway

You can uninstall the Secure Gateway using Add/Remove Programs available from Control Panel.

To uninstall the Secure Gateway

1. Exit any applications running on the server.
2. Click Start, click Control Panel, and then click Add/Remove Programs.
Managing the Secure Gateway

This chapter describes using the management and diagnostic tools available for the Secure Gateway. The discussion includes the features of the Secure Gateway Management Console, sessions and connections, performance counters, and reporting tools. These features of the Secure Gateway allow you to monitor the security of your network and to diagnose problems that may occur with a server farm or access server farm.

This chapter contains the following topics:

- “The Secure Gateway Tools” on page 68
- “Using the Secure Gateway Management Console” on page 68
- “The Secure Gateway Performance Statistics” on page 70
- “Viewing the Secure Gateway Diagnostics Report” on page 74
- “Event Logging and Access Logs” on page 77
The Secure Gateway Tools

The following is a description of the management tools used for the Secure Gateway.

The Secure Gateway Configuration Wizard

When you install the Secure Gateway, shortcuts for the Secure Gateway Configuration wizard and the Secure Gateway Diagnostics are added to the Citrix program menu on the Start menu.

The Secure Gateway Configuration wizard helps you configure the Secure Gateway for use with Citrix Presentation Server.

**Important:** If you modify values of parameters such as certificates or the STA, the Secure Gateway or the Secure Gateway Proxy must be restarted for changes to take effect.

To start the Secure Gateway Configuration wizard

1. Click **Start > Programs > Citrix**.
2. Click **Administration Tools > Secure Gateway Configuration Wizard**.

The Secure Gateway configuration tools are wizard driven. To access context-sensitive help at any time, click **Help** or press F1.

Using the Secure Gateway Management Console

The Secure Gateway Management Console is an MMC snap-in and provides an administrator with tools to administer, monitor, and troubleshoot the Secure Gateway.

You can access the Secure Gateway Management Console from the Citrix program menu on the Start menu.

You can start, stop, and restart the Secure Gateway using the icons available on the console toolbar.

**Note:** Version 2.0 of the Secure Gateway allowed the service to be paused. This permitted existing connections to continue communications through the Secure Gateway but new connections could not be created. Version 3.0 of the Secure Gateway does not support this feature.
In addition, the Secure Gateway Management Console displays the following information:

- Session and connection information for the Web Interface that is currently running through the Secure Gateway. To refresh the display, right-click the Session Information node and select Refresh. To disconnect a session, right-click the session in the right pane and select Disconnect. For more information about sessions and connections, see “Session and Connection Information” on page 69.

Note: The sessions for the Web Interface has one connection for one session.

- An instance of the Windows Performance Monitor containing performance statistics applicable to the Secure Gateway. Review this list to obtain detailed information regarding the status of client connections running through the Secure Gateway.

The Secure Gateway Management Console also provides access to the following applications:

- The Secure Gateway Service Configuration wizard, which allows you to configure operating parameters for the Secure Gateway.

- The Secure Gateway Diagnostics tool, which presents configuration information and results of communication checks against servers hosting components such as the STA and the Secure Gateway Proxy in the form of a diagnostics report.

Important: For full section 508 compliance when using the Secure Gateway Management Console, you need Windows 2000 Server Service Pack 4 or later.

Session and Connection Information

The Secure Gateway provides session and connection information in the Secure Gateway Management Console. Session information is displayed in the right pane by clicking Session Information in the tree pane.

The session information shows the client IP address, user, domain, time the connection was established, and how long the client has been connected.

Each session provides detailed connection information. To get connection information, right-click the session and click Properties. The Connection Information dialog box appears.

The connection information provides the following information:
The Secure Gateway Performance Statistics

Monitoring system performance is an important part of maintaining and administering a Secure Gateway deployment. Performance data can be used to:

- Understand the workload on the Secure Gateway and the corresponding effect it has on system resources.
- Observe changes and trends in workloads and resource usage so you can plan system sizing and failover.
- Test changes in configuration or other tuning efforts by monitoring the results.
- Diagnose problems and target components or processes for optimization.

Citrix recommends that you monitor performance of the Secure Gateway as part of your administrative routine.

You can display the Windows Performance monitor from the Secure Gateway Management Console.

To view the Secure Gateway performance statistics

1. Open the Secure Gateway Management Console.
3. Use the Windows Performance Console controls that appear at the top of the right pane to perform tasks such as switching views or adding counters.
Performance Counters Available for the Secure Gateway

The following performance counters are available for the Secure Gateway:

<table>
<thead>
<tr>
<th>Counter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections: Total Successful</td>
<td>This the total number of successful client connections. It is the sum of all successful connections for all protocols: CGP, HTTP/S, and SOCKS.</td>
</tr>
<tr>
<td>CGP Successful Connections</td>
<td>The total number of successful CGP connections.</td>
</tr>
<tr>
<td>SOCKS Successful Connections</td>
<td>The total number of successful SOCKS connections.</td>
</tr>
<tr>
<td>HTTP/S Successful Connections</td>
<td>The total number of successful HTTP/S connections.</td>
</tr>
<tr>
<td>Connections: Total Active</td>
<td>The total number of client connections currently active.</td>
</tr>
<tr>
<td>CGP Active Connections</td>
<td>The total number of CGP client connections currently active.</td>
</tr>
<tr>
<td>SOCKS Active Connections</td>
<td>The total number of SOCKS client connections currently active.</td>
</tr>
<tr>
<td>HTTP/S Active Connections</td>
<td>The total number of HTTP/S connections currently active.</td>
</tr>
<tr>
<td>Connections: Peak Active</td>
<td>The highest number of concurrent connections through the Secure Gateway.</td>
</tr>
<tr>
<td>Connections/Second</td>
<td>The number of successful client connection requests per second.</td>
</tr>
<tr>
<td>Connections/Second: Peak</td>
<td>The highest number of successful client connection requests per second.</td>
</tr>
<tr>
<td>Failed Connections: Total Client</td>
<td>The total number of failed client connection requests. It is the sum of the Failed Connections (Timed Out), Failed Connections (SSL Error), and Failed Connections (General Client Error) counters.</td>
</tr>
<tr>
<td>Failed Connections: Client Timed Out</td>
<td>The total number of client connection requests that were accepted but timed out before completing the protocol handshake.</td>
</tr>
<tr>
<td>Failed Connections: SSL Client Handshake Error</td>
<td>The total number of client connection requests that were accepted but did not successfully complete the SSL handshake.</td>
</tr>
<tr>
<td>Failed Connections: General Client Error</td>
<td>The total number of client connection requests that failed to connect to the Secure Gateway for any reason other than timing out or SSL handshake error.</td>
</tr>
<tr>
<td>Kilobytes to Client</td>
<td>The total number of kilobytes sent from the Secure Gateway to all connected clients.</td>
</tr>
<tr>
<td>CGP Kilobytes to Client</td>
<td>The total number of kilobytes sent from the Secure Gateway to all clients connected using the CGP protocol.</td>
</tr>
<tr>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SOCKS Kilobytes to Client</td>
<td>The total number of kilobytes sent from all connected clients to the Secure Gateway using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Kilobytes to Client</td>
<td>The total number of kilobytes sent from all connected clients to the Secure Gateway using the HTTPS protocol.</td>
</tr>
<tr>
<td>Kilobytes from Client</td>
<td>The total number of kilobytes sent from all connected clients to the Secure Gateway.</td>
</tr>
<tr>
<td>CGP Kilobytes from Client</td>
<td>The total number of kilobytes sent from all clients connected to the Secure Gateway using the CGP protocol.</td>
</tr>
<tr>
<td>SOCKS Kilobytes from Client</td>
<td>The total number of kilobytes sent from all clients connected to Secure Gateway using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Kilobytes from Client</td>
<td>The total number of kilobytes sent from all clients connected to the Secure Gateway using the HTTP/S protocol.</td>
</tr>
<tr>
<td>Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients.</td>
</tr>
<tr>
<td>CGP Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the CGP protocol.</td>
</tr>
<tr>
<td>SOCKS Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the HTTP/S protocol.</td>
</tr>
<tr>
<td>Peak Bytes/Sec to Client</td>
<td>The highest data throughput rate (bytes per second) from the Secure Gateway to all connected clients.</td>
</tr>
<tr>
<td>CGP Peak Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the CGP protocol.</td>
</tr>
<tr>
<td>SOCKS Peak Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Peak Bytes/Sec to Client</td>
<td>The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the HTTP/S protocol.</td>
</tr>
<tr>
<td>Bytes/Sec from Client</td>
<td>The data throughput rate (bytes per second) from all connected clients to the Secure Gateway.</td>
</tr>
<tr>
<td>CGP Bytes/Sec from Client</td>
<td>The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the CGP protocol.</td>
</tr>
<tr>
<td>Counter Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SOCKS Bytes/Sec from Client</td>
<td>The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Bytes/Sec from Client</td>
<td>The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the HTTP/S protocol.</td>
</tr>
<tr>
<td>Peak Bytes/Sec from Client</td>
<td>The highest data throughput rate (bytes per second) from all connected clients to the Secure Gateway.</td>
</tr>
<tr>
<td>CGP Peak Bytes/Sec from Client</td>
<td>The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the CGP protocol.</td>
</tr>
<tr>
<td>SOCKS Peak Bytes/Sec from Client</td>
<td>The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the SOCKS protocol.</td>
</tr>
<tr>
<td>HTTP/S Peak Bytes/Sec from Client</td>
<td>The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the HTTP/S protocol.</td>
</tr>
<tr>
<td>Client Connect Time: Average (in ms)</td>
<td>The average amount of time (in milliseconds) for a client connection request to complete the connection process.</td>
</tr>
<tr>
<td>Client Connect Time: Longest (in ms)</td>
<td>The longest amount of time (in milliseconds) for a client connection request to complete successfully.</td>
</tr>
<tr>
<td>SSL Handshakes: Total</td>
<td>Total number of SSL handshakes that completed successfully between a client and the Secure Gateway.</td>
</tr>
<tr>
<td>SSL Handshakes: Pending</td>
<td>Number of SSL handshakes currently in progress between a client and the Secure Gateway.</td>
</tr>
<tr>
<td>SSL Handshakes/Sec</td>
<td>Number of successful SSL handshakes per second.</td>
</tr>
<tr>
<td>SSL Handshakes/Sec: Peak</td>
<td>Highest number of successful SSL handshakes per second.</td>
</tr>
<tr>
<td>SSL Handshake Time: Average</td>
<td>Average length of time (in milliseconds) for an SSL handshake to complete.</td>
</tr>
<tr>
<td>SSL Handshake Time: Longest</td>
<td>Length of time (in milliseconds) for the longest SSL handshake to complete.</td>
</tr>
<tr>
<td>Failed Backend Connections</td>
<td>The total number of backend connections that failed. Clients that successfully connect to the Secure Gateway may not successfully connect to backend servers, such as a Web server. These connections are not counted as part of the failed client connection count.</td>
</tr>
<tr>
<td>Connections: Pending</td>
<td>Total number of client connection requests accepted, but not yet completed, by the Secure Gateway. Pending connections are still active and have not timed out or failed.</td>
</tr>
</tbody>
</table>
Viewing the Secure Gateway Diagnostics Report

The Secure Gateway Diagnostics tool presents configuration information and results of communication checks against servers hosting components such as the global settings, network protocols, and certificates. It is a quick and easy way of performing a series of checks to ascertain the health and status of the Secure Gateway components.

Note: You can also click the Secure Gateway Diagnostics icon from the Secure Gateway Management Console.

The diagnostics tool scans the registry and reports global settings for the Secure Gateway. It uses the Secure Gateway configuration information to contact servers running the Web Interface, the Secure Gateway Proxy, and the STA, and reports whether or not the communication check passed or failed. It examines the server certificate installed on the server running the Secure Gateway and checks credentials and validity.

In the Secure Gateway Diagnostics window, information icons indicate that a registry or configuration value is present:

<table>
<thead>
<tr>
<th>Information icon</th>
<th>A registry or configuration value is present.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning icon</td>
<td>A registry or configuration value is missing.</td>
</tr>
<tr>
<td>Passed check icon</td>
<td>A communication check for the component passed.</td>
</tr>
<tr>
<td>Failed check icon</td>
<td>A communication check for the component failed.</td>
</tr>
</tbody>
</table>

For any component marked with a warning or failed check icon, verify that you properly installed the component and provided all necessary configuration information.

The information available in a typical Secure Gateway Diagnostics report is described in the following sections.

To start the Secure Gateway Diagnostics

1. Click Start > Programs > Citrix.
2. Click Administration Tools > Secure Gateway Diagnostics.
   The Secure Gateway Diagnostics window appears.
Global Settings

Configuration settings for the Secure Gateway are stored in the Windows registry. The Secure Gateway Diagnostics tool scans the registry and returns the following values:

Secure Gateway Diagnostics Version 3.0.1

Computer NetBIOS Name: GATEWAY01

-----------------------------------------------

Secure Gateway for MetaFrame Global Settings

-----------------------------------------------

Version = 3.0.1
Products Secured = Citrix Presentation Server
Logging Level = 3 (All events including information)
ClientConnectTimeout = 100 seconds
Maximum Concurrent Connections = 250
CertificateFQDN = gateway01.company.com

Interfaces

This section contains values for one or more IP interface and port combinations that the Secure Gateway is configured to use.

Interfaces

----------

All interfaces (0.0.0.0 : 443)

-------------------------------

Protocol = SSL, TLS
Ciphersuites = ALL
Secured = Yes
HTTP = Yes
ICA = Yes
SOCKS = No
Gateway Client = Yes
LoadBalancerIPs = 17.34.124.233
The Secure Gateway Proxy

This section contains information about the Secure Gateway Proxy, if used, and whether or not the Secure Gateway was able to establish a connection to it.

<table>
<thead>
<tr>
<th>Secure Gateway Proxy - All output is directed to a Secure Gateway Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN = gwyproxy.company.com</td>
</tr>
<tr>
<td>Port = 1080</td>
</tr>
<tr>
<td>Secured = No</td>
</tr>
<tr>
<td>Tested OK</td>
</tr>
</tbody>
</table>

Authority Servers

The STA is called an authority servers. This section contains information about the servers running the STA, and whether or not the Secure Gateway was able to establish a connection.

<table>
<thead>
<tr>
<th>Authority Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID = STAFE565EE5A52E</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>FQDN = sta01.company.com</td>
</tr>
<tr>
<td>Port = 443</td>
</tr>
<tr>
<td>Path = /Scripts/CtxSTA.dll</td>
</tr>
<tr>
<td>Type = STA</td>
</tr>
<tr>
<td>Secured = Yes</td>
</tr>
<tr>
<td>Protocol = BOTH</td>
</tr>
<tr>
<td>Ciphersuites = ALL</td>
</tr>
<tr>
<td>Tested OK</td>
</tr>
</tbody>
</table>

Certificate Check

This section contains information about the server certificate installed on the server running the Secure Gateway and whether or not it is valid for the current system date.

<table>
<thead>
<tr>
<th>Certificate Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN = gateway01.company.com</td>
</tr>
<tr>
<td>This certificate is currently valid.</td>
</tr>
</tbody>
</table>
Event Logging and Access Logs

error messages and the Secure Gateway provides access logs. Event logging allows administrators and Citrix support representatives to diagnose problems with the Secure Gateway. The access logs provide connection information to the Secure Gateway and the Secure Gateway Proxy.

Event Logging

The Secure Gateway error messages are logged to the Secure Gateway application log. The error messages include:

- Status messages. These are messages of normal operational events, such as starting or stopping the Secure Gateway.
- Fatal messages. These are messages of operational failure events that prevent the Secure Gateway from starting.
- Service messages. These are messages regarding a partial failure of the Secure Gateway.
- Warning messages. These are messages that are logged as a result of events such as corrupted data requests, data packets received, or ticket time-outs.
- Informational messages. These are messages that are logged as a result of client connection events.

The Secure Gateway error messages can be viewed using Windows Event Viewer.

To view the Secure Gateway error messages

1. Open Event Viewer.
2. Expand the Event Viewer node and click Secure Gateway. A list of all errors and events recorded since the service was started appears.
3. To view the properties of an event, double-click the event. The Description field contains the event ID and a brief description of the Secure Gateway error.

Access Logs

The access logs record connection information. For the Secure Gateway, the access logs record HTTP, SOCKS, and CGP connection information. The Secure Gateway Proxy access log records SOCKS connections. Each access log provides specific information regarding connections.
HTTP Access Log
The HTTP access log provides the following information:

- Remote host
- Remote log name
- Remote user
- Time of access
- First line of request
- Status
- Bytes sent
- Referer header content in the request
- User-agent header content in the request

CGP Access Log
The CGP access log provides the following information:

- Time of access
- Remote IP address
- CGP response code
- Destination host
- Destination port
- Protocol

SOCKS Access Log
The SOCKS access log provides the following information:

- Time of access
- Remote IP address
- SOCKS response code
- Destination host
- Destination port
The access logs are generated by the Secure Gateway service. The default path for the error logs is the installation path for the Secure Gateway or the Secure Gateway Proxy, typically in `%systemroot%\Program Files\Citrix\Secure Gateway\logs`. 
Optimization and Security Guidelines

This chapter provides general compatibility guidelines for deploying the Secure Gateway in complex network environments containing components such as load balancers, SSL accelerator cards, and firewalls. This chapter contains the following topics:

- “Configuring Firewalls” on page 82
- “Planning for High Availability” on page 83
- “Keep–Alive Values and Citrix Presentation Server” on page 86
- “Recommendations for Improving Security” on page 87
- “Preventing Indexing by Search Engines” on page 92
Configuring Firewalls

A firewall is a device designed to stop unauthorized access to a network. It may also protect the network from other kinds of threats, such as network viruses. Firewalls are positioned between a network and the Internet, so that all network traffic flows through the firewall.

The Secure Gateway is designed to facilitate secure Internet access to applications and resources hosted on server farms in a secure, enterprise network. The Secure Gateway is typically deployed in the DMZ, so that traffic originating from a remote client device must traverse firewalls to get to the destination server in the secure network. It is, therefore, crucial to the Secure Gateway operation that firewalls are configured to allow network traffic traversal. Correct firewall configuration can help prevent disconnects and contribute toward better performance of the Secure Gateway.

Of particular concern with regard to firewall traversal is ICA/SSL traffic, a Citrix-proprietary protocol used for communications between client devices and computers running Citrix Presentation Server. Firewalls are not ICA aware and do not make any distinction between HTTPS or ICA/SSL traffic. The ICA protocol is a real-time, interactive protocol that is very sensitive to latency and other network delays. Because ICA traffic typically consists of mouse-clicks and keystrokes, delays in their transmission could result in significantly degraded performance of the connection. In contrast, HTTPS traffic is less sensitive to latency or other types of network delays. Therefore, HTTPS connections to computers running Citrix Presentation Server are less affected than ICA connections to computers running Citrix Presentation Server.

To ensure that users experience usable and reliable sessions when using the Secure Gateway, Citrix recommends configuring your firewall to work in forwarding mode as opposed to proxy mode. Set the firewall to use its maximum inspection level. Configuring your firewall to use forwarding mode ensures that TCP connections are opened directly between remote client devices and the Secure Gateway.

However, if you prefer to configure your firewall to use proxy mode, ensure that your firewall does not:

- Impose any time-outs on ICA/SSL sessions, including idle, absolute, and data traffic time-outs
- Use the Nagle algorithm for ICA/SSL traffic
- Impose any other specific restrictions or filters on ICA/SSL traffic

**Important:** If you use a firewall that is ICA aware, the issues outlined above may not apply.
Planning for High Availability

You can design a Secure Gateway deployment to ensure high availability by deploying multiple servers running the Secure Gateway.

This configuration does not make Secure Gateway sessions fault tolerant, but provides an alternative server if one server fails.

When the number of concurrent sessions exceeds the capacity of a single server running the Secure Gateway, multiple servers running the Secure Gateway must be deployed to support the load. There is no practical limit to the number of servers running the Secure Gateway that can be deployed to service large access server farms or server farms.

To deploy multiple servers running the Secure Gateway, a load balancer is required. The function of the load balancer is to distribute client sessions to one of a number of servers offering a service. This is normally done by implementing a virtual address on the load balancer for a particular service and maintaining a list of servers offering the service. When a client connects to a service, the load balancer uses one of a number of algorithms to select a server from the list and directs the client to the selected server.

The algorithm can be as simple as a “round robin” where each client connect request is assigned to the next server in a circular list of servers, or a more elaborate algorithm based on machine load and response times.

The client response to a server failure depends on which server fails and at what point in the session the server fails. Types of server failure include:

- **Web Interface.** The server running the Web Interface is involved during user sign on, application launch, or application relaunch. Failure of the Web Interface requires you to reconnect to the logon page and sign on again when you want to launch a new application or relaunch an existing application.

- **STA.** The STA is involved in the launch or relaunch of an application. Failure of the STA during application launch requires that you return to the published applications page on the access server farm or the Web Interface to relaunch the application.

- **Secure Gateway.** The Secure Gateway is involved during application launch and the time an application remains active. If a session fails, the client connection goes to another server and the session automatically reconnects without having to logon again.

Intelligent load balancers can detect the failure of a server through server polling, temporarily remove the failed server from the list of available servers, and restore them to the list when they come back online.
Load Balancing Multiple Secure Gateway Servers

A load balancing solution managing an array of servers running the Secure Gateway can provide the following key benefits, including:

- **Scalability.** Performance of a Secure Gateway implementation is optimized by distributing its client requests across multiple servers within the array. As traffic increases, additional servers are added to the array. The only restriction to the maximum number of servers running the Secure Gateway in such an array is imposed by the load balancing solution in use.

- **High availability.** Load balancing provides high availability by automatically detecting the failure of a server running the Secure Gateway and redistributing client traffic among the remaining servers within a matter of seconds.

Load balancing an array of servers running the Secure Gateway is accomplished using a virtual IP address that is dynamically mapped to one of the real IP addresses (for example, 10.4.13.10, 10.4.13.11 and 10.4.13.12) of a server running the Secure Gateway. If you use a virtual IP address such as 10.4.13.15, all your requests are directed to the virtual IP address and then routed to one of the servers. You can set up the virtual IP address through software, such as Windows NT Load Balancing Service, or hardware solutions, such as a Cisco CSS 11000 Series Content Services switch. If you use hardware in a production environment, make sure you use two such devices to avoid a single point of failure.

Load Balancing an Array of the Secure Gateway Proxy

You can load balance an array of servers running the Secure Gateway Proxy in the same way as the Secure Gateway. Instead of using an external load balancer, the Secure Gateway Proxy has built-in support for load balancing.

This is useful in situations where you experience extremely high loads on the Secure Gateway array, in which case, it may help to deploy a second Secure Gateway Proxy and load balance the two servers.

In addition, if the communications link between the Secure Gateway and the Secure Gateway Proxy is secured, you can use a single certificate for the Secure Gateway Proxy array.
Certificate Requirements

Load balancing relies on the use of a virtual IP address. The virtual IP address is bound to an FQDN and all clients request connections from the virtual IP address rather than the individual servers running the Secure Gateway behind it. A single IP address, the virtual IP, acts as an entry point to your servers running the Secure Gateway, simplifying the way clients access Web content, published applications, and services on computers running Citrix Presentation Server.

If you are using a load balancing solution, all servers running the Secure Gateway can be accessed using a common FQDN; for example, csgwy.company.com.

In conclusion, you need a single server certificate, issued to the FQDN (mapped to the virtual IP or DNS name) of the load balancing server. The certificate must be installed on every server running the Secure Gateway in the server array that is being load balanced.

Load Balancers and SSL Accelerator Cards

Load balancing solutions available in the market today may feature built-in SSL accelerator cards. If you are using such a solution to load balance an array of servers running the Secure Gateway, disable the SSL acceleration for traffic directed at the servers running the Secure Gateway. Consult the load balancer documentation for details about how to do this.

Presence of SSL accelerator cards in the network path before the server running the Secure Gateway means the data arriving at the Secure Gateway is decrypted. This conflicts with a basic function of the Secure Gateway, which is to decrypt SSL data before sending it to a computer running Citrix Presentation Server. The Secure Gateway does not expect non–SSL traffic and drops the connection.
Keep–Alive Values and Citrix Presentation Server

If you enable TCP/IP keep–alive parameters on computers running Citrix Presentation Server, Citrix recommends that you modify the parameters on the server running the Secure Gateway in the same manner.

In an environment containing the Secure Gateway, ICA and HTTP/S connections are routed through the Secure Gateway. TCP/IP keep–alive messages from the computer running Citrix Presentation Server to the remote client are intercepted, and responded to, by the server running the Secure Gateway. Similarly, TCP/IP keep–alive packets from the server running the Secure Gateway are sent only to the client device; the server running the Secure Gateway does not transmit keep–alives to the computer running Citrix Presentation Server. Setting the keep–alive values on the server running the Secure Gateway to match the values set on the computer running Citrix Presentation Server ensures that the server farm is aware of the client connection state and can either disconnect or log off from the connection in a timely manner.


Connection Keep–Alive Values and the Secure Gateway

The Secure Gateway establishes connections over the Internet between remote clients and servers running Citrix Presentation Server. When a client connection is dropped without being properly logged off, the Secure Gateway continues to keep the connection to the server open. Accumulation of such “ghost” connections eventually affects Secure Gateway performance.

A Secure Gateway deployment subject to a heavy load may run out of sockets because of these “ghost” connections remaining open. The Secure Gateway uses TCP/IP keep–alives to detect and close broken connections between the Secure Gateway and the client device. The default Windows setting for KeepAliveTime is two hours. This is the duration that TCP/IP waits before verifying whether or not an idle connection is still connected. “Ghost” connections may therefore remain open for up to two hours before the system detects that a connection failed.

To prevent broken connections from remaining open, the Secure Gateway changes the KeepAliveTime to one minute. If a connection is dropped, the Secure Gateway knows within one minute, instead of two hours.
If there is no response, TCP/IP retries the verification process after the interval specified by KeepAliveInterval and for a maximum number of times specified by TcpMaxDataRetransmissions. The default value for KeepAliveInterval is one second and the default value for TcpMaxDataRetransmissions is five seconds.

If the Secure Gateway is under a heavy load and is used predominately to secure HTTP connections to internal Web servers, the Secure Gateway rapidly opens and closes connections. Closed connections stay in the TIME_WAIT state for an interval specified by TcpTimedWaitDelay.

The default value of TcpTimedWaitDelay is four minutes; the Secure Gateway sets this value to 30 seconds. This change enables the Secure Gateway to recycle sockets faster resulting in improved performance. The system cannot reuse sockets in the TIME_WAIT state. MaxUserPort specifies the number of sockets available on the system. By default, the system uses ports between 1024 and 5000; the Secure Gateway modifies this setting to use ports between 1024 and 65000.

The KeepAliveInterval, KeepAliveTime, MaxUserPort, TcpMaxDataRetransmissions, and TcpTimedWaitDelay parameters are stored in the Windows registry at:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\n
---

Caution: Using the Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee resolution of problems resulting from the incorrect use of Registry Editor. Use Registry Editor at your own risk.

---

For more information, see the Microsoft knowledgebase articles, Q120642 - “TCP/IP & NBT Configuration Parameters for Windows 2000 or Windows NT,” Q314053 - “TCP/IP & NBT Configuration Parameters for Windows XP,” and Q196271 - “Unable to Connect from TCP Ports Above 5000” for information about making changes to these parameters. Under normal circumstances, it is not necessary to change these settings.

---

**Recommendations for Improving Security**

The Secure Gateway is an application–specific proxy designed to achieve a corresponding level of security. It is not a firewall and should not be used as such. Citrix recommends that you use a firewall to protect servers running the Secure Gateway, Citrix Presentation Server, and other corporate resources from unauthorized access from the Internet and internal users.
Deploying the Secure Gateway in the DMZ

Place the Secure Gateway in the DMZ between two firewalls for maximum protection. In addition, physically secure the DMZ to prevent access to the firewalls and servers within the DMZ. A breach of your DMZ servers may, at best, create an annoyance in the form of downtime while you recover from the security breach.

**Caution:** Citrix recommends that you configure your firewalls to restrict access to specific TCP ports only. If you configure your firewalls to allow access to TCP ports other than those used for HTTP, ICA, SSL, and XML data, you may allow users to gain access to unauthorized ports on the server.

Changing or Restricting Ciphersuites

The process of establishing a secure connection involves negotiating the ciphersuite that is used during communications. A ciphersuite defines the type of encryption that is used—it defines the cipher algorithm and its parameters, such as the size of the keys.

Negotiation of the ciphersuite involves the client device informing the Secure Gateway which ciphersuites it is capable of handling, and the Secure Gateway informing the client which ciphersuite to use for client-server communications.

The Secure Gateway supports two main categories of ciphersuite: COM (commercial) and GOV (government). The ALL option includes both the commercial and government suites.

The COM ciphersuites are:

- SSL_RSA_WITH_RC4_128_MD5 or {0x00,0x04}
- SSL_RSA_WITH_RC4_128_SHA or {0x00,0x05}

The GOV ciphersuite is:

SSL_RSA_WITH_3DES_EDE_CBC_SHA or {0x00,0x0A}

Some organizations, including U.S. government organizations, require the use of government-approved cryptography to protect sensitive but unclassified data.

**Important:** You must restart the Secure Gateway to let configuration changes take effect.
To change or restrict the ciphersuites

1. Log on as an administrator to the server running the Secure Gateway.

2. Launch the Secure Gateway Configuration Wizard.

3. Select Advanced Configuration and click Next until you see the Configure secure protocol settings screen.

   The default setting for ciphersuites is ALL.

4. To restrict the ciphersuite, change the value to GOV or COM, as required. Click Next.

5. Follow prompts until configuration is complete. Click to exit the configuration wizard.

Restricting Ciphersuite Use to Secure Communication

The ciphersuites used to secure communications between the Secure Gateway and the Secure Gateway Proxy are determined by the configuration settings on the server running the Secure Gateway Proxy. The default setting on the Secure Gateway for outgoing connections to the Secure Gateway Proxy is set to use all ciphersuites.

Security policies of some organizations may require tighter control of the ciphersuites offered by the Secure Gateway for outgoing connections to the Secure Gateway Proxy. This is achieved by modifying the SChannel registry settings.

For instructions about modifying the SChannel registry settings to restrict ciphersuites, refer to the Microsoft Knowledge Base Article Q245030, “How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll.”
Using Secure Protocols
The Secure Gateway is designed to handle both SSL Version 3 and TLS Version 1 protocols. It is important to note the following in this context:

• The Gateway Client is set to use TLS Version 1 as the default
• Internet Explorer is set to use SSL Versions 2 and 3 as the default

You can restrict the Secure Gateway to accept only SSL Version 3 or TLS Version 1 connections. If you decide to change the default protocol setting on the Secure Gateway, ensure you modify protocol settings on the client Web browser as well as the Gateway Client to match the protocol setting on the server running the Secure Gateway.

As a general rule, Citrix recommends against changing the default setting for the secure protocol used by the Secure Gateway.

Removing Unnecessary User Accounts
Citrix recommends removing all unnecessary user accounts on servers running the Secure Gateway.

Avoid creating multiple user accounts on servers running the Secure Gateway and limit the file access privileges granted to each account. Review active user accounts regularly and when personnel leave.

Removing Sample Code Installed with IIS
An important security step is to disable or remove all the IIS-installed sample Web applications. Never install sample sites on production servers because of the many well-identified security risks they present. Some sample Web applications are installed so that you can access them only from http://localhost or the IP address 127.0.0.1. Nevertheless, you should remove the sample sites. The IISSamples, IISHelp, and Data Access virtual directories and their associated folders are good examples of sample sites that should not reside on production servers.
Secure Components that Run on IIS
To ensure that security of the Secure Gateway components is not compromised, you can do the following:

- Set appropriate ACLs on IIS to prevent unauthorized access to executable and script files. For instructions about locking down IIS, refer to current Microsoft product documentation and online resources available from the Microsoft Web site.

- Secure all the Secure Gateway components using SSL or TLS to ensure that data communications between all the Secure Gateway components is encrypted. For instructions about securing the Secure Gateway components, see previous chapters in this guide.

To maximize the security of the servers running the Secure Gateway components hosted by IIS, follow Microsoft security guidelines for locking down Internet Information Services on Windows Servers.

Stopping and Disabling Unused Services
Windows services introduce vulnerabilities to the computer. If a Windows service is not required by your organization, Citrix recommends that the service be disabled. For a complete list of services and their functions, see the Microsoft Web site http://www.microsoft.com/technet/security/guidance/secmod54.mspx.

Caution: Disabling a Windows service could stop the computer from functioning correctly.

Installing Service Packs and Hotfixes
Ensure that you install all operating system-specific service packs and hotfixes, including those applicable to applications and services that you are running on the system.

Ensure you do not install hotfixes for services that are not installed. Ensure you regularly review Security Bulletins from Microsoft. These are available online at http://www.microsoft.com/technet/security/current.asp.

Following Microsoft Security Guidelines
Citrix recommends that you review Microsoft guidelines for securing Windows servers.

In general, refer to the Microsoft Web site for current guidance to help you understand and implement the processes and decisions that must be made to get, and stay, secure.
Preventing Indexing by Search Engines

Search engines use a program that automatically retrieves Web pages and indexes the pages. This includes pages hosted on the Secure Gateway that might potentially be sensitive.

To prevent indexing by most search engines, a global file (robots.txt) can be used. It needs to be installed at the root of the Web server, such as sg.customer.com/robots.txt. The content of robots.txt must be:

```
User-agent: *
Disallow: /
```
Troubleshooting

The Secure Gateway must be configured correctly to prevent connection errors or failures. This section provides basic techniques to assist you in troubleshooting potential problems that could occur with a Secure Gateway deployment.

This chapter contains the following topics:

- “General Troubleshooting Procedures” on page 93
- “Common Problems” on page 94
- “If You Cannot Resolve the Problem” on page 100

General Troubleshooting Procedures

This section contains general guidelines and advice for troubleshooting a Secure Gateway deployment.

Note: Troubleshooting information concerning firewall traversal, Domain Name Service (DNS), and Network Address Translation (NAT) are beyond the scope of this document. This chapter assumes that you correctly configured NAT and packet filtering on your network.

Checking Results Reported by the Secure Gateway Diagnostics

The Secure Gateway Diagnostics tool is designed to perform a quick check to determine that the Secure Gateway is configured correctly and that it is able to resolve addresses and communicate with servers located in the DMZ and the secure network.

Run the Secure Gateway Diagnostics tool on the server running the Secure Gateway and examine the results reported. The report contains configuration values for the Secure Gateway and results of connection attempts to components and services in the DMZ and secure network that the Secure Gateway uses.
The results reported by the Secure Gateway Diagnostics tool are sufficient to narrow down causes of connection failure. Use the information to work out whether configuration settings are incorrect or if the required components or services are unavailable.

For instructions about using the Secure Gateway Diagnostics tool, see “Viewing the Secure Gateway Diagnostics Report” on page 74.

**Reviewing the Secure Gateway Event Log**

Careful review of the Secure Gateway event log can help you identify the sources of system problems. For example, if log warnings show that the Secure Gateway failed because it could not locate the specified certificate, you can conclude that the certificate is missing or installed in the wrong certificate store. In general, information in the event log helps you trace a record of activity leading up to the event of failure.

**Common Problems**

The following sections describe known system problems and preventive measures and possible solutions to resolve them.

**Certificate Problems**

This section describes problems with the Secure Gateway and the installation of certificates from a certificate authority.

**The Secure Gateway Fails with a CSG0188 Error**

This error implies that SChannel could not validate certificate credentials of the server certificate used by the Secure Gateway.

Ensure that the certificate installed was issued by a trusted source, is still valid, and is issued for the correct computer.

**To check your certificates**

1. Log on as an administrator to the server running the Secure Gateway.
2. Click **Start**, click **All Programs**, and then click **Citrix**.
3. Click **Administration Tools** and then click **Secure Gateway Configuration Wizard**.
4. Select the products you want to secure and then click **OK**.
5. On the **Secure Gateway configuration level** screen, select **Advanced**.
6. In the **Select server certificate** dialog box, select the certificate the Secure Gateway is configured to use and click **View**.
7. Check that the value in the **Issued To** field matches the FQDN of this server.

8. When you view the certificate, ensure that it contains a key icon and the caption “You have private key that corresponds to this certificate” at the bottom of the **General** tab. The lack of an associated private key can result in the CSG0188 error.

9. Ensure the certificate is not expired. If it is expired, you need to apply for certificate renewal.
   Contact the appropriate resources in your company for assistance with certificate renewal.

### Connection Problems

This section describes connection issues between the client device and the server computer to and from the Secure Gateway.

**Client Connections Launched from IP Addresses in the Logging Exclusions List Fail**

For security reasons, IP addresses configured in the logging exclusions list are not allowed to establish connections to the Secure Gateway. This measure blocks connections to the Secure Gateway that do not leave an audit trail.

The logging exclusions list is designed to help keep the system log free of redundant data. You can configure the IP address of load balancing devices in the Logging Exclusions list. Configuring an exclusions list enables the Secure Gateway to ignore polling activity from such devices and keeps the log free of this type of data.

**Load Balancers Do Not Report Active Client Sessions if They Are Idle**

Some load balancers stop reporting active client connections flowing through them if the connections are idle for a while because of the way in which certain load balancers treat idle connections.

Connections that are idle for a certain amount of time stop being represented as active connections in the load balancer’s reporting tools even though they are still valid connections.

You can resolve this issue by modifying the keep–alive settings in the Windows registry on the server(s) running the Secure Gateway.

If you have load balanced an array of servers running the Secure Gateway, decrease the keep–alive values to force packets to be sent after a period of session inactivity. For more information about configuring TCP/IP keep–alive settings, see “Keep–Alive Values and Citrix Presentation Server” on page 86.
Performance Issues with Transferring Files between a Client and a Computer Running Citrix Presentation Server

When connecting to MetaFrame XP with Feature Release 2 or later servers, users may experience performance issues with data transfer using client drive mapping on high bandwidth, high latency connections.

As a workaround, you can optimize throughput by increasing the value of TcpWindowSize in the Windows registry of your server running the Secure Gateway.

To modify this setting, edit the following Windows Registry key:

\Caution: Using the Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee resolution of problems resulting from the incorrect use of Registry Editor. Use Registry Editor at your own risk.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip \Parameters\TcpWindowSize

Citrix recommends setting the value of TCPWindowSize to 0xFFFF(64K).

Be aware that this change incurs higher system memory usage. Citrix recommends increasing physical system memory on the server running the Secure Gateway to suit the typical usage profile of the network.

For more information, refer to the Microsoft Knowledgebase Article, “TCP/IP and NBT Configuration Parameters for Windows 2000 or Windows NT (Q120642),” available from the Microsoft Support Web site.

Gateway Client Connections Fail When Using Windows XP Service Pack 2

Windows XP Service Pack 2 (SP2) prevents connections to all IP addresses that are in the loopback address range except for 127.0.0.1. If the Gateway Client is using a loopback address other than 127.0.0.1, the connection to the Secure Gateway fails.

Microsoft provides a patch to fix this issue. For more information, refer to the Microsoft Knowledgebase Article “Programs that connect to IP addresses that in the loopback address range may not work as you expect in Windows XP Service Pack 2 (884020)” available from the Microsoft Support Web site at http://support.microsoft.com/support/kb/articles/.
Other Problems

Failed Client Connections to the Secure Gateway Result in Duplicate Entries in the Secure Gateway Log

You may find duplicate entries for client connection attempts in the Secure Gateway application and performance logs. Duplicate entries can occur in the following situations:

- SSL protocol mismatch between the client device and the server running the Secure Gateway
- Client automatically attempts to reconnect if the first connection attempt fails

The log entries are not duplicates but a record of client behavior. In the above cases, the client attempts to reconnect if it fails the first time.

Placing the Secure Gateway Behind a Reverse Web Proxy Causes an SSL Error 4

If the Web Interface and the Secure Gateway are on the same server, it can create confusion if a reverse Web proxy is placed between the client and the Secure Gateway. Clients can communicate with the enterprise network using HTTPS but traffic for ICA/SSL is refused. When a combination of the Web Interface and the Secure Gateway are placed behind a reverse Web proxy server, users can log on using the Web Interface and enumerate application icons, which is all HTTP communications. When the users attempt to launch a published application, they receive an SSL Error 4. This happens because the ICA/SSL session is terminated by the reverse Web proxy, not by the Secure Gateway.
Incorrect placement of the Secure Gateway and Web Interface behind a reverse Web proxy

The Secure Gateway views the reverse Web proxy as a “man in the middle” that compromises the integrity of the ICA/SSL network stream. This causes the SSL handshake between the client and the Secure Gateway to fail.

There are two possible solutions to correct this problem:

- Run the Secure Gateway parallel to the reverse Web proxy
- Use a network address translator (NAT) in place of the reverse Web proxy
Run the Secure Gateway Parallel to the Reverse Web Proxy

The Secure Gateway and the Web Interface are installed on two separate servers. The server running the Web Interface is behind the reverse Web proxy. The Secure Gateway is parallel to the reverse Web proxy.

Correct placement of the Secure Gateway, which is parallel to the reverse Web proxy.

Placing the Secure Gateway parallel to the reverse Web proxy provides a secure solution. Security policies that are defined on the reverse Web proxy continue to affect all end users of the Secure Gateway. To cross the Secure Gateway, users must first satisfy the reverse Web proxy and log onto the Web Interface to get a ticket from the STA. Any access control rules that are defined on the reverse Web proxy affects users who are also trying to gain entry through the Secure Gateway.
Use a Network Address Translator Instead of a Reverse Web Proxy

If the reverse Web proxy is configured to forward all network traffic (not just HTTP traffic) to the combination Secure Gateway and Web Interface, the SSL connection is not terminated at the proxy and users can connect through the Secure Gateway. The following figure is an example of how different vendors refer to this type of deployment.

Using a network address translator instead of a reverse Web proxy.

This approach has the disadvantage that some control must be sacrificed regarding the type of traffic that is permitted to cross the proxy. Incoming traffic must be routed directly to the Secure Gateway and the Web Interface without being decrypted, authenticated, or inspected. From a security standpoint, this is not much different than exposing the Secure Gateway server directly to the Internet. There is a logical SSL tunnel between the client and the Secure Gateway.

If You Cannot Resolve the Problem

If you are still experiencing problems with a Secure Gateway deployment, see the Citrix Web site http://www.citrix.com/support/ for available technical support options.
About Digital Certificates

This appendix provides conceptual information about the security technologies used in the Secure Gateway solution, helps you identify the number and type of certificates required, and helps you decide how and where to obtain and install them. This appendix contains the following topics:

- “Understanding SSL/TLS, Cryptography, and Digital Certificates” on page 102
- “Getting Certificates” on page 109
- “Server Certificates” on page 110
- “Root Certificates” on page 116
- “Wildcard Certificates” on page 117
Understanding SSL/TLS, Cryptography, and Digital Certificates

This section introduces the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, and provides an overview of cryptography and Public Key Infrastructure (PKI).

SSL and TLS

SSL and TLS are the leading Internet protocols providing security for e-commerce, Web services, and many other network functions.

The SSL protocol is today’s standard for securely exchanging information on the Internet. Originally developed by Netscape, the SSL protocol became crucial to the operation of the Internet. As a result, the Internet Engineering Taskforce (IETF) took over responsibility for the development of SSL as an open standard. To clearly distinguish SSL from other ongoing work, the IETF renamed SSL as TLS. The TLS protocol is the descendant of the third version of SSL; TLS 1.0 is identical to SSL 3.1.

Some organizations, including US government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography. FIPS (Federal Information Processing Standard) 140 is a standard for cryptography.

The SSL/TLS protocol allows sensitive data to be transmitted over public networks such as the Internet by providing the following important security features:

• **Authentication.** A client can determine a server’s identity and ascertain that the server is not an impostor. Optionally, a server can also authenticate the identity of the client requesting connections.

• **Privacy.** Data passed between the client and server is encrypted so that if a third party intercepts messages, it cannot unscramble the data.

• **Data integrity.** The recipient of encrypted data knows if a third party corrupts or modifies that data.

Cryptography

The SSL/TLS protocol uses cryptography to secure communications. Cryptography provides the ability to encode messages to ensure confidentiality. Cryptography is also used to authenticate the identity of a message source and to ensure the integrity of its contents.
A message is sent using a secret code called a cipher. The cipher scrambles the message so that it cannot be understood by anyone other than the sender and receiver. Only the receiver who has the secret code can decipher the original message, thus ensuring confidentiality.

Cryptography allows the sender to include special information in the message that only the sender and receiver know. The receiver can authenticate the message by reviewing the special information.

Cryptography also ensures that the contents of a message are not altered. To do this, the sender includes a cryptographic operation called a hash function in the message. A hash function is a mathematical representation of the information, similar to the checksums found in communication protocols. When the data arrives at its destination, the receiver calculates the hash function. If the receiver’s hash function value is the same as the sender’s, the integrity of the message is assured.

**Types of Cryptography**

There are two main types of cryptography:

- Secret key cryptography
- Public key cryptography

In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely.

Public key cryptography, also called asymmetric encryption, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.
The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key. The following example illustrates how public key cryptography works:

- Ann wants to communicate secretly with Bill. Ann encrypts her message using Bill’s public key (which Bill made available to everyone) and Ann sends the scrambled message to Bill.
- When Bill receives the message, he uses his private key to unscramble the message so that he can read it.
- When Bill sends a reply to Ann, he scrambles the message using Ann’s public key.
- When Ann receives Bill’s reply, she uses her private key to unscramble his message.

The major advantage asymmetric encryption offers over symmetric key cryptography is that senders and receivers do not have to communicate keys up front. Provided the private key is kept secret, confidential communication is possible using the public keys.

Combining Public Key and Secret Key Cryptography. The main disadvantage of public key cryptography is that the process of encrypting a message, using the very large keys common to PKI, can cause performance problems on all but the most powerful computer systems. For this reason, public key and secret key cryptography are often combined. The following example illustrates how this works:

- Bill wants to communicate secretly with Ann, so he obtains Ann’s public key. He also generates random numbers to use just for this session, known as a session key.
- Bill uses Ann’s public key to scramble the session key.
- Bill sends the scrambled message and the scrambled session key to Ann.
- Ann uses her private key to unscramble Bill’s message and extract the session key.

When Bill and Ann successfully exchange the session key, they no longer need public key cryptography—communication can take place using just the session key. For example, public key encryption is used to send the secret key; when the secret key is exchanged, communication takes place using secret key encryption.

This solution offers the advantages of both methods—it provides the speed of secret key encryption and the security of public key encryption.
Digital Certificates and Certificate Authorities

In the above scenarios, how can Ann be sure that Bill is who he says he is and not an impostor? When Ann distributes her public key, Bill needs some assurance that Ann is who she says she is.

The ISO X.509 protocol defines a mechanism called a certificate that contains a user’s public key that is signed by a trusted entity called a certificate authority (CA).

Certificates contain information used to establish identities over a network in a process called authentication. Like a driver’s licence, a passport, or other forms of personal identification, certificates enable servers and clients to authenticate each other before establishing a secure connection.

Certificates are valid only for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

To establish an SSL/TLS connection, you require a server certificate at one end of the connection and a root certificate of the CA that issued the server certificate at the other end.

- **Server certificate.** A server certificate certifies the identity of a server. The type of digital certificate that is required by the Secure Gateway is called a server certificate.

- **Root certificate.** A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the CA. This type of digital certificate is required by a client device to verify the server certificate.

When establishing an SSL connection with a Web browser on a client device, the server sends its certificate to the client.

When receiving a server certificate, the Web browser (for example, Internet Explorer) on the client device checks to see which CA issued the certificate and if the CA is trusted by the client. If the CA is not trusted, the Web browser prompts the user to accept or decline the certificate (effectively accepting or declining the ability to access this site).

Now when Ann receives a message from Bill, the locally stored information about the CA that issued the certificate is used to verify that it did indeed issue the certificate. This information is a copy of the CA’s own certificate and is referred to as a root certificate.

Certificates generally have a common format, usually based on ITU standards. The certificate contains information that includes the:

- **Issuer.** The organization that issues the certificates.

- **Subject.** The party that is identified by the certificate.

- **Period of validity.** The certificate’s start date and expiration date.
• **Public key.** The subject’s public key used to encrypt data.
• **Issuer’s signature.** The CA’s digital signature on the certificate used to guarantee its authenticity.

A number of companies and organizations currently act as CAs, including VeriSign, Baltimore, Entrust, and their respective affiliates.

**Certificate Chains**

Some organizations delegate the responsibility for issuing certificates to resolve the issue of geographical separation between organization units, or that of applying different issuing policies to different sections of the organization.

Responsibility for issuing certificates can be delegated by setting up subordinate CAs. The X.509 standard includes a model for setting up a hierarchy of CAs. In this model, the root CA is at the top of the hierarchy and has a self-signed certificate. The CAs that are directly subordinate to the root CA have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the subordinate CAs.
CA certificate signed by self

Root CA

CA certificate signed by Root CA

Asia CA
Subordinate CA

Europe CA
Subordinate CA

US CA
Subordinate CA

CA certificate signed by US CA

US - 1 CA
Subordinate CA

US - 2 CA
Subordinate CA

US - 3 CA
Subordinate CA

CA certificate signed by US - 3 CA

The hierarchical structure of a typical digital certificate chain.

CAs can sign their own certificates (that is, they are self-signed) or they can be signed by another CA. If the certificate is self-signed, they are called root CAs. If they are not self-signed, they are called subordinate or intermediate CAs.

If a server certificate is signed by a CA with a self-signed certificate, the certificate chain is composed of exactly two certificates: the end entity certificate and the root CA. If a user or server certificate is signed by an intermediate CA, the certificate chain is longer.
The following figure shows the first two elements are the end entity certificate (in this case, gwy01.company.com) and the certificate of the intermediate CA, in that order. The intermediate CA’s certificate is followed by the certificate of its CA. This listing continues until the last certificate in the list is for a root CA. Each certificate in the chain attests to the identity of the previous certificate.

![A typical digital certificate chain.](image)

**Certificate Revocation Lists**

From time to time, CAs issue certificate revocation lists (CRLs). CRLs contain information about certificates that can no longer be trusted. For example, suppose Ann leaves XYZ Corporation. The company can place Ann’s certificate on a CRL to prevent her from signing messages with that key.

Similarly, you can revoke a certificate if a private key is compromised or if that certificate expired and a new one is in use. Before you trust a public key, make sure that the certificate does not appear on a CRL.

**Certificate Expiration and Renewal**

Certificates are issued with a planned lifetime and explicit expiration date. After it is issued, a certificate is considered valid until its expiration date is reached. After the expiration date, the certificate cannot be used to validate a user session. This policy improves security by limiting the damage potential of a compromised certificate. These expiration dates are set by the CA that issued the certificate.

Usually, you need to renew a certificate before it expires. Most CAs offer a well documented process for certificate renewal. Consult the Web site of your CA for detailed instructions about renewing certificates.
Getting Certificates

When you identify the number and type of certificates required for your Secure Gateway deployment, you must decide where to obtain the certificates. Where you choose to obtain certificates depends on a number of factors, including:

- Whether or not your organization is a CA, which is likely to be the case only in very large corporations
- Whether or not your organization has already established a business relationship with a public CA
- The fact that the Windows operating system includes support for many public Certificate Authorities
- The cost of certificates, the reputation of a particular public CA, and so on

If Your Organization Is its Own Certificate Authority

If your organization is running its own CA, you must determine whether or not it is appropriate to use your company’s certificates for the purpose of securing communications in your Secure Gateway installation. Citrix recommends that you contact your corporate security department to discuss this and to get further instructions about how to obtain certificates.

If you are unsure if your organization is a CA, contact your corporate security department or your organization’s security expert.
If Your Organization Is Not its Own Certificate Authority

If your organization is not running its own CA, you need to obtain your certificates from a public CA such as VeriSign.

Obtaining a digital certificate from a public CA involves a verification process in which:

- Your organization provides corporate information so the CA can verify that your organization is who it claims to be. The verification process may involve other departments in your organization, such as accounting, to provide letters of incorporation or similar legal documents.
- Individuals with the appropriate authority in your organization are required to sign legal agreements provided by the CA.
- The CA verifies your organization as a purchaser; therefore your purchasing department is likely to be involved.
- You provide the CA with contact details of suitable individuals who they can call if there are queries.

Server Certificates

Your organization’s security expert should have a procedure for obtaining server certificates. Instructions for generating server certificates using various Web server products are available from the Web sites of popular CAs such as Verisign and others.

Several CAs offer Test Server Certificates for a limited trial period. It might be expedient to obtain a Test Certificate to test the Secure Gateway before deploying it in a production environment. If you do this, be aware that you need to download matching Test Root Certificates that must be installed on each client device that connects through the Secure Gateway.
Obtaining and Installing Server Certificates

To provide secure communications (SSL/TLS), a server certificate is required on the server running the Secure Gateway. The steps required to obtain and install a server certificate on a server running the Secure Gateway are as follows:

1. Create a certificate request.
2. Apply for a server certificate from a valid CA.
3. Save the certificate response file sent by the CA as an X.509 Certificate (.cer format).
4. Import the X.509 certificate into the certificate store.
5. Export the certificate into Personal Information Exchange format (.pfx, also called PKCS #12).
6. Install the server certificate on the server running the Secure Gateway.

Each of the above steps is described in the following sections.

Important: Part of an initial request for a certificate involves generating a public/private key pair that is stored on your server. Because the public key from this key pair is encoded in your certificate, loss of the key pair on your server renders your certificate worthless. Make sure you back up your key pair data on another computer, a floppy disk, or both. The Microsoft IIS Key Manager has a special Export Key function that can be used to generate a backup file.

To create a certificate request

Create a certificate request using the IIS Certificate wizard on any Windows 2000 or Windows 2003 server that has IIS installed. To do this:

1. Click Start, click Programs, click Administrative Tools, and then click Internet Services Manager.
2. On the Internet Information Services console, right-click the entry for Default Web Site and select Properties.
4. Click Server Certificate under Secure Communications.
5. The IIS Server Certificate wizard appears. Click Next.
6. Select Create a new certificate and click Next.
7. Select Prepare the request now, but send it later. Click Next.
8. In Name, type the name for the server certificate.
9. **In Bit Length**, enter the bit length to be used for the certificate’s encryption strength. The greater the bit length, the higher the security. Citrix recommends that you select 1024 or higher. If you are specifying a bit length higher than 1024, ensure that the clients you deploy support it. For information about supported encryption strength on a client device, see the appropriate client’s documentation.

10. Click **Next**.

11. Enter details about your organization. Click **Next**.

12. Enter the FQDN of the server running the Secure Gateway and click **Next**.

13. **In Geographical Information**, enter pertinent geographical information about your location. Click **Next**.

14. Save the certificate request as a text file; for example, certreq.txt. Click **Finish** to exit the wizard.

**To apply for a server certificate**

To apply for a valid server certificate, follow the process specified by the public or private CA you are using.

**To save the certificate response file**

The duration of the certification process can vary, but when the process is complete, you receive a response file from the CA. The response file contains the public key that is signed by the CA.

- Copy the text block that contains the public key and save it to an X.509 format certificate file: filename.cer.

```
-----BEGIN CERTIFICATE-----
MIIDBDCCAgq4CEGTFq6PjvXhFUZjJKoZIlhcNAQEEBQAwgakxFjAU
BgNVBAsTDVZlcm1TaWduLCBJbmxMxRzMFBgNVBAsTHIeL01B
mLjBMaWFibWtVc2l0ZS5jbi5jb20vcmVwb3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVm
X0aXiplZCBvZlJlbmNlQ1BTIEluY29ycC4gQnkgUmVm
------END CERTIFICATE------
```
To import the certificate

When you import a certificate, you copy the certificate from a file that uses a standard certificate storage format to a certificate store for your computer account.

The server certificate must be placed in the certificate store for the local computer. Use the Certificate Import wizard to install the server certificate.

**Important:** Do not attempt to import the file by double-clicking or right-clicking the certificate file within Windows Explorer. Doing so places the certificate in the certificate store for the current user.

1. Log on to the system as an administrator.
2. Click **Start**, click **Run**, in **Open**, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in** and then click **Add**.
4. Under **Snap-in**, double-click **Certificates**, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, select **Local computer** and click **Finish**.
6. Click **Close** in the **Add Standalone Snap-in** dialog box.
7. Click **OK** to close the **Add/Remove Snap-in** dialog box.
8. In the console tree, click **Certificates (Local Computer)**.
9. Right-click the **Personal** folder and then click **All Tasks**, and then click **Import**.
10. Follow the instructions in the **Certificate Import** wizard to import the certificate.
To export the certificate

Before you can install the server certificate on the server running the Secure Gateway, you must export the certificate to PKCS #12 (Personal Information Exchange Syntax Standard) format. The PKCS #12 standard specifies a portable format for storing or transporting a user’s private keys, certificates, and so on.

**Important:** Part of generating a key pair is specifying a password used to encrypt it. This prevents someone with access to the keypair data from extracting the private key and using it to decrypt SSL/TLS traffic to and from your server. Forgetting this password could render your certificate worthless, so be sure to remember it and save it in a secure location.

1. Log onto the system as an administrator.
2. Click **Start**, click **Run**, in **Open**, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in** and then click **Add**.
4. Under **Snap-in**, double-click **Certificates**, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, select **Local computer** and click **Finish**.
6. Click **Close** and then **OK**.
7. In the console tree, click **Certificates**, click **Personal**, and then click **Certificates**. A list of available certificates appears in the right pane.
8. In the **Details** pane, click the certificate you want to export.
9. On the **Action** menu, click **All Tasks**, and then click **Export**. The **Certificate Export** wizard screen appears. Click **Next**.
10. Follow the instructions in the **Certificate Export** wizard to export the certificate.

When the Certificate Export wizard is finished, the certificate remains in the certificate store in addition to being in the newly created file. To remove the certificate from the certificate store, you must delete it.
To install the server certificate

The final step in the process is to install the PKCS #12 file on the server running the Secure Gateway.

**Important:** Do not attempt to import the PFX file by double-clicking or right-clicking the certificate file within Windows Explorer. Doing so places the certificate in the certificate store for the current user.

The server certificate must be placed in the certificate store for the local computer. Instead, use the Certificate Import wizard to install the server certificate. To do this:

1. Copy the PKCS #12 file, filename.pfx, to the server running the Secure Gateway.
2. Open an MMC console that contains the Certificates snap-in.
3. The Certificates snap-in dialog box appears; select **Computer Account** and click **Next**.
4. The **Select Computer** dialog box appears; select **Local Computer** and click **Finish**.
5. Click **Close** and then **OK**.
6. In the console tree, click **Certificates** and then click **Personal**.
7. On the **Action** menu, click **All Tasks** and then click **Import**.
8. In the **Certificate Import** wizard, do the following to import your PFX file:
   - Browse to and select the file containing the certificate you are importing.
   - Type the password used to encrypt the private key.
   - Select if you want the certificate to be placed automatically in a certificate store (based on the type of certificate), or if you want to be able to specify where the certificate is stored.

The certificate, filename.pfx, is now imported and stored in the local certificate store.
Root Certificates

A root certificate must be present on every client device that connects to the secure network through the Secure Gateway.

Support for most trusted root authorities is already built into the Windows operating system and Internet Explorer. Therefore, there is no need to obtain and install root certificates on the client device if you are using these CAs. However, if you decide to use a different CA, you need to obtain and install the root certificates yourself.

Obtaining a Root Certificate from a CA

Root certificates are available from the same CAs that issue server certificates. Well-known or trusted CAs include Verisign, Baltimore, Entrust, and their respective affiliates.

Certificate authorities tend to assume that you already have the appropriate root certificates (this is because most Web browsers have root certificates built-in) so you need to specifically request the root certificate.

Several types of root certificates are available. For example, VeriSign has approximately 12 root certificates that they use for different purposes, so it is important to ensure that you obtain the correct root certificate from the CA.

Installing Root Certificates on a Client Device

To install a root certificate on a client device

1. Double-click the root certificate file. The root certificate file has the extension .cer, .crt, or .der.
2. Verify that you are installing the correct root certificate.
4. Choose the Place all certificates in the following store option and then click Browse.
5. On the Select Certificate Store screen, select Show physical stores.
6. Expand the Trusted Root Certification Authorities store and then select Local Computer. Click OK.
7. Click Next and then click Finish.

The root certificate is installed in the store you select.

For information about root certificate availability and installation on platforms other than 32-bit Windows, refer to product documentation appropriate for the operating system you are using.
Wildcard Certificates

The Secure Gateway supports wildcard certificates that can be used if you have a load-balanced domain. The wildcard certificate has an asterisk (*) in the certificate name. Clients can choose different Web addresses, such as http://www1.citrix.com or http://www2.citrix.com. The use of a wildcard certificate allows several Web sites to be covered by a single certificate.
Using the Secure Gateway Proxy in Relay Mode

This appendix describes the relay mode operation of the Secure Gateway Proxy and provides instructions for installing and configuring the Secure Gateway Proxy in relay mode.

This appendix contains the following topics:

• “Understanding Relay Mode” on page 120
• “Before Installation” on page 123
• “Installing the Secure Gateway Proxy in Relay Mode” on page 124
• “Configuring Client Devices” on page 128
• “Testing Relay Mode Operation” on page 130
Understanding Relay Mode

Relay mode is designed to provide flexibility in the way the Secure Gateway is used. It is a simpler solution and requires fewer hardware resources. The benefits of this mode of operation are:

- Compatibility with client deployments that do not include the Web Interface or ticketing support. Relay mode can be used in secure corporate environments such as intranets, LANs, and WANs.
- Fully secures data but provides relatively weaker authentication.
- Enables use of Program Neighborhood to browse for applications.

**Important:** Relay mode is a feature of Citrix Presentation Server. It is not supported for Access Gateway 4.0.

Modes of Operation

You can use the Secure Gateway Proxy in either normal mode or relay mode.

**Normal Mode**

The recommended mode of operation for the Secure Gateway Proxy is normal mode. In normal mode, the Secure Gateway server functions as an Internet gateway with authentication and authorization support provided by the Web Interface and the Secure Ticket Authority that is used with Citrix Presentation Server. Normal mode provides strong security and is the recommended mode of operation.

**Relay Mode**

The Secure Gateway Proxy can also be used in relay mode. The biggest difference in this mode is the absence of ticketing support provided by the STA. This mode of operation was implemented to provide more flexibility in the way the Secure Gateway is used.

**Caution:** Installing the Secure Gateway Proxy in relay mode does not provide secure connections.

The Secure Gateway Proxy is installed on a standalone server. In relay mode, a client connects to a server farm through the Secure Gateway Proxy server, which acts as a server-side proxy. User authentication is performed by Citrix Presentation Server.
In this mode, the Secure Gateway Proxy supports client attempts to locate the Citrix XML Service, ICA browsing, and ICA connections to a server farm.

**Important:** When the Secure Gateway Proxy is installed in relay mode, session reliability is not supported.

### When to Use Relay Mode

Use the Secure Gateway in relay mode only when:

- You want to use the Secure Gateway but do not want to use the ticketing support available through the STA.
- You want to use the Secure Gateway but are not using the Web Interface and do not intend to.
- You want to use the Secure Gateway to secure your corporate intranet, LAN, or WAN, and your clients are connecting from a secure network. Do not use relay mode for clients that are connecting from an external network or the Internet.

**Caution:** Relay mode is not the recommended mode in which to use the Secure Gateway. In this mode, the Secure Gateway is essentially an encrypted tunnel through your firewall. IP addresses of your servers are visible from the client. Be aware that you are opening up a well-known port on your firewall and of the associated risks in doing so.
How it Works
To use the Secure Gateway Proxy in relay mode, install the Secure Gateway Proxy on a standalone server. The figure below illustrates the communications that take place between the client, the Secure Gateway Proxy, and a server farm in relay mode.

A remote user connects to the Secure Gateway Proxy server on port 443 and requests access to a published application or a Citrix Presentation Server resource. The Secure Gateway Proxy checks that the server address and port for the requested resource exists in its Access Control List. If the server address and port are found, the connection is made. The Citrix Presentation Server prompts the user to log on using valid user credentials. When authenticated, the ICA connection is established and the published application or application list is made available to the user. When the connection is established, the Secure Gateway Proxy decrypts data from the client before sending the data to the server, and encrypts data from the server before forwarding it to the client. The IP addresses in the Access Control List (ACL) should be static; if the servers get a different IP address from the DHCP server, the ACLs have to be updated.
Before Installation

Before installing the Secure Gateway Proxy, compile all of the required information to correctly configure the Secure Gateway Proxy. Print and fill out the Secure Gateway Pre-Installation Checklist. Keep the completed checklist near when you install the Secure Gateway Proxy.

Compile the Following Information

Compile the following information before you begin installation of the Secure Gateway Proxy in Relay mode.

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN of the server running the Citrix XML Service.</td>
<td>mfserver01.company.com</td>
</tr>
<tr>
<td>IP addresses, or IP address ranges, and port numbers</td>
<td>10.1.1.11 to 10.1.1.255:1494</td>
</tr>
<tr>
<td>of the server(s) that the Secure Gateway is allowed</td>
<td>10.1.1.11:80</td>
</tr>
<tr>
<td>to access. This list should also include separate</td>
<td>10.1.40.11 to 10.1.40.255:1494</td>
</tr>
<tr>
<td>entries for the Citrix Presentation Server running</td>
<td></td>
</tr>
<tr>
<td>the Citrix XML Service used for HTTP browsing. The</td>
<td></td>
</tr>
<tr>
<td>port number used by Citrix Presentation Server for</td>
<td></td>
</tr>
<tr>
<td>ICA traffic is 1494, and for the Citrix XML Service</td>
<td></td>
</tr>
<tr>
<td>it is 80.</td>
<td></td>
</tr>
<tr>
<td>FQDN of the Secure Gateway server.</td>
<td>csgwy.company.com</td>
</tr>
<tr>
<td>IP address of the Secure Gateway server.</td>
<td>10.42.1.17</td>
</tr>
<tr>
<td>Listener port number for SSL/TLS connections on the</td>
<td>443</td>
</tr>
<tr>
<td>Secure Gateway server.</td>
<td></td>
</tr>
</tbody>
</table>

You can specify these values during installation. The values in this listing are for illustration purposes only; replace them with specifics of your network environment.

Install Certificates

A server certificate must be installed on the Secure Gateway Proxy and a root certificate on the Citrix Presentation Server client device. For instructions about obtaining and installing certificates, see “Certificate Requirements” on page 57 and “About Digital Certificates” on page 101.

Note: When configuring the client device to connect to the Secure Gateway Proxy, use the FQDN of the server certificate that is installed on the Secure Gateway Proxy.
Installing the Secure Gateway Proxy in Relay Mode

To install the Secure Gateway Proxy in relay mode, follow the steps below:

To install the Secure Gateway Proxy in Relay Mode

1. Ensure port 443 on this server is not being used by any Windows service.

   The Secure Gateway Proxy uses port 443. This is the default setting. Internet Information Services (IIS) also uses port 443. If IIS and the Secure Gateway Proxy are installed on the same server, change the IIS port to something different than port 443. If both IIS and the Secure Gateway Proxy used port 443, client connections fail.

2. Install the server certificate.

   See “Getting Certificates” on page 109 for information about how to install certificates.

3. Insert the Citrix Presentation Server Components CD-ROM.


5. Click Install Secure Gateway and then click Next.

6. Read and accept the license agreement, and click Next.

7. In Installation Mode, click Secure Gateway Proxy and click Next.

8. Select the destination folder and click Next.

9. In Service Account, select the user account to determine credentials and privileges. Select an account that restricts privileges.

10. Click Next and follow the instructions in the wizard to complete the installation.
Configuring the Secure Gateway Proxy

Immediately after installation, the Secure Gateway Proxy Configuration wizard starts. To run the Secure Gateway Proxy in relay mode, you need the following settings.

To configure the Secure Gateway in relay mode

1. On the **Secure Gateway configuration level** screen, select one of the following:
   - Click **Standard** to specify the minimum set of configuration values required to run the Secure Gateway
   - Click **Advanced** if you are an expert user and prefer to specify all the configuration values required for Secure Gateway operation

2. Check **Secure traffic between the Secure Gateway and Secure Gateway Proxy** and click **Next**.

   **Note:** For the Secure Gateway Proxy to run in relay mode, a certificate must be used, otherwise the Secure Gateway Proxy runs in normal mode. Checking **Secure traffic between the Secure Gateway and Secure Gateway Proxy** ensures that a certificate is used.

3. Select the server certificate that is required by the Secure Gateway.
   If you have more than one certificate installed, click **View** to examine details of a certificate.

4. Click **Next**.

5. Select the network protocols and the ciphersuites you want to use.

6. Click **Next** to accept the default to monitor all IP addresses.
   The Secure Gateway listens on port 443 for inbound connections. To monitor for specific IP addresses, clear the **Monitor all IP addresses** check box, click **Add**, and then type the IP address and TCP port of the network interface you want to monitor.

7. Click **OK** and then click **Next**.

8. In **Configure outbound connections**, click **Use an Access Control List (ACL)** to define the IP addresses for the ACL and then click **Configure**.
   To use the Secure Gateway in relay mode, an access control list (ACL) must be defined. The ACL lists the IP addresses and the TCP port numbers (1494) for allowed access to Citrix Presentation Server. The ACL also contains IP addresses and the TCP port number (80) of servers running the
Citrix XML Service. You can enter a range of IP addresses and ports to include IP addresses of all servers in a given range. The listener port for ICA traffic is 1494.

9. Click **Add** in the **Configure allowed outbound connections** dialog box to add an entry to this list.

   The **Enter IP address range** dialog box appears.

10. Enter the range of IP addresses that the Secure Gateway Proxy will use.

11. To specify a single IP address, leave the **End** address field blank.

    The default TCP port is 1494.

12. After the IP addresses are configured, click **OK**.

    The IP addresses appear in the **Configure allowed outbound connections** dialog box.

13. Click **Add** and then click **Server FQDN**. Enter the FQDN of the Citrix Presentation Server. To secure the traffic between the Secure Gateway Proxy and the Citrix Presentation Server, click **Secure traffic between the server and the Secure Gateway Proxy**. Click **OK** and then click **Next**.

    **Note:** The port for secure traffic between the server and the Secure Gateway Proxy is 443.

14. Specify the connection time limits and then click **Next**.

15. To specify the IP addresses to exclude from logging, click Add and then type the address of the device to exclude.

16. Click **OK** and then click **Next**.

17. Specify the error logging level you want to use. The value you enter specifies the type of events to be logged in the Windows system event log. Click **Next**.

18. Click **Finish** to complete configuration of the Secure Gateway Proxy in relay mode. The Secure Gateway Proxy automatically restarts when the configuration is complete.

**Important:** You must also define the IP address and port of any server on which the Citrix XML Service is running. The port listener for the Citrix XML Service is port 80.
Starting the Secure Gateway Proxy
The Secure Gateway Proxy runs automatically when the computer starts.

To start or stop the Secure Gateway Proxy Service
1. Log on as an administrator to the Secure Gateway Proxy.
2. On the desktop of the Secure Gateway Proxy, right-click My Computer and select Manage.
3. In the Computer Management Console, double-click Services and Applications, and then click Services. A list of all services registered for this computer is shown in the right hand pane.
4. Select Secure Gateway Proxy and do one of the following:
   • To start the Secure Gateway Proxy, on the Action menu, click Start.
   • To stop the Secure Gateway Proxy, on the Action menu, click Stop.

Changing Secure Gateway Proxy Configuration Settings
To change configuration settings entered during the install process, run the Secure Gateway Proxy Configuration wizard. Stop the Secure Gateway Proxy before changing its configuration settings.

To run the Secure Gateway Proxy Configuration wizard
1. Click Start > Programs.
2. Click Citrix > Administration Tools > Secure Gateway Proxy Configuration wizard.
3. Make the necessary changes. When the wizard completes, the Secure Gateway Proxy is restarts.
Configuring Client Devices

In relay mode, clients connect directly to the Secure Gateway Proxy’s external DNS name. You must configure settings on the client device to enable connections to the Secure Gateway Proxy.

Configuration of the Program Neighborhood Client is described here to illustrate client-side settings required for connections to a Secure Gateway Proxy relay server.

To configure client connections to the Secure Gateway Proxy

1. Click Start > Programs.
2. Click Citrix > Citrix Access Clients > Program Neighborhood.
3. Double-click Application Set Manager.
4. Double-click Custom ICA Connections and then double-click Add ICA Connection to start the Add New ICA Connection wizard.
5. Select the type of connection to use.
6. Type a description for the connection. In Select the network protocol that your computer will use to communicate with the server farm select SSL/TLS + HTTPS, type either the name of the server or the location of the published application, and then click Next.
   The default encryption level for the SSL/TLS + HTTPS network protocol is SSL and Basic.
7. In Session reliability, clear the Enable check box.
   
   **Important:** When the Secure Gateway Proxy is installed in relay mode, disable session reliability. If session reliability is enabled, client connections are refused.

8. Follow the rest of the steps in the wizard to complete configuring the ICA connection.

All custom connections defined in the Custom ICA Connections window inherit these settings.

**Important:** The address specified must be the same FQDN to which clients connect from an external network. Clients must be able to resolve the DNS name to the external IP address of the Secure Gateway Proxy.
To configure all application sets for the client to connect to the Secure Gateway Proxy

1. Click Start > Programs.
2. Click Citrix > Citrix Access Clients > Program Neighborhood.
3. On the File menu, click Application Set Settings. The Connection Settings dialog box for the selected application set appears.
4. In the Network Protocol drop-down list, select SSL/TLS+HTTPS.
5. Click Add, type the name of the server and port, and then click OK.
6. Click Firewalls. In the Firewall Settings dialog box, specify the Secure Gateway address and the Port.

**Important:** For SSL network connections, the address specified must be the same server certificate FQDN to which clients connect from an external network. Clients must be able to resolve the DNS name to the external IP address of the Secure Gateway Proxy.

7. Click the Default Options tab. Clear the Enable session reliability checkbox.

**Important:** When the Secure Gateway Proxy is installed in relay mode, disable session reliability. If session reliability is enabled, client connections are broken.

8. Click OK to exit the Connection Settings dialog box.

Note that all applications defined within the application set inherit these settings.
To modify an ICA file to enable a connection to the Secure Gateway Proxy

1. To use an ICA file to connect to the Secure Gateway Proxy, modify the .ica file as follows:

2. Open the .ica file using a text editor such as Notepad.

3. Create or modify the following entries:

<table>
<thead>
<tr>
<th>[Application Name]</th>
<th>Section containing published application settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLProxyHost=</td>
<td>Value specifying the Secure Gateway relay server and port to which you can connect. For example, csgwy.company.com:443</td>
</tr>
<tr>
<td>SSLEnable=</td>
<td>Default value is On; do not change.</td>
</tr>
</tbody>
</table>

4. Save and close the .ica file.

**Important:** If the line CGP=*:2598 appears in the .ica file, session reliability is enabled. Remove this line when installing the Secure Gateway Proxy in relay mode. If session reliability is enabled, client connections are refused.

---

**Testing Relay Mode Operation**

When installation is complete, test your Secure Gateway deployment to ensure that it is functioning correctly.

**To test relay mode operation**

1. Ensure that the client device is configured to connect through Secure Gateway. See “Configuring Client Devices” on page 128 for instructions about configuring client devices.

2. In Program Neighborhood, double-click an ICA connection to launch it. If you did not enter your user credentials for this application set or custom ICA connection, a logon dialog box appears. Enter a valid user name, domain, and password. After a brief interval, the application window appears.

3. Open the ICA Connection Center and check the entry for the published application you have open. You will see the string “\Remote, 128-bit SSL/TLS” appended to the application name as shown below.
If you have trouble launching an ICA connection or a connection fails, see “Troubleshooting” on page 93 for information about known problems and typical troubleshooting procedures.
Glossary

This appendix provides a glossary of terms and acronyms used throughout the Secure Gateway documentation.

**access center.** A Web site you can use to aggregate information, applications, and services for users.

**access control list (ACL).** In the context of Secure Gateway, an access control list is a mechanism that restricts access to resources. The ACL is a data structure containing the IP addresses, ports, and domain name servers of computers running on the secure network to which the Secure Gateway components has access.

**authentication.** The process of identifying a user, usually based on a user name and password. In security systems, authentication is distinct from authorization, which is the process of giving users access to system objects based on their identity. Authentication confirms the identity of the user, but does not impact the access rights of the user.

**authorization.** The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which confirms the identity of the user. The second stage is authorization, which allows the user access to various resources based on the user's identity.

**certificate.** An attachment to electronic data used for security purposes. The most common use of a digital certificate is to verify the identity of the user sending the data, and to provide the receiver with the means to encode a reply.

**ciphersuites.** An encryption/decryption algorithm. When establishing an SSL/TLS connection, the client and server determine a common set of supported ciphersuites and then use the most secure one to encrypt the communications. These algorithms have differing advantages in terms of speed, encryption strength, exportability, and so on.

**Citrix Presentation Server Client.** Citrix software that enables users to connect to computers running Citrix Presentation Server from a variety of client devices.

**Citrix Presentation Server.** Computer on which Citrix Presentation Server software is running. You can publish applications, content, and desktops for remote access by clients on these servers.

**Citrix XML Service.** A Windows service that provides an HTTP interface to the client's browser. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80.
**common gateway protocol.** A general-purpose tunneling protocol to be used for secure tunneling of payload connections as well as for tunneling payload connections with no security layer.

**demilitarized zone (DMZ).** A network isolated from the trusted or secure network using firewalls. Network administrators often isolate public resources, such as Web or email servers in the DMZ to prevent an intruder from attacking the internal network.

**ICA.** Independent Computing Architecture. The architecture that Citrix Presentation Server uses to separate an application’s logic from its user interface. With ICA, only the keystrokes, mouse clicks, and screen updates pass between the client and server on the network, while 100% of the application’s logic executes on the server.

**ICA file (.ica).** A text file (with the extension ica) containing information about a published application. ICA files are written in Windows Ini file format and organize published application information in a standard way that Citrix Presentation Server Clients can interpret. When a client receives an ICA file, it initializes a session running the specified application on the server specified in the file.

**ICA protocol.** The protocol that Citrix Presentation Server Clients use to format user input (keystrokes, mouse clicks, and so forth) and address it to servers for processing. Servers use the ICA protocol to format application output (display, audio, and so forth) and return it to the client device.

**ICA session.** A connection between a client and a computer running Citrix Presentation Server, identified by a specific user ID and ICA connection. The session consists of the status of the connection, the server resources allocated to the user for the duration of the session, and any applications executing during the session. An ICA session normally terminates when the user logs off from the server.

**normal mode.** A computer that is running the Secure Gateway Proxy, typically in the second segment of a double-hop DMZ. When the Secure Gateway Proxy is running in normal mode, it provides full functionality and security for the enterprise network.

**Program Neighborhood.** The user interface for Citrix Presentation Server Client for 32-bit Windows that lets users view the published resources they are authorized to use in the server farm. Program Neighborhood contains application sets and custom ICA connections.

**published application.** An application installed on a computer running Citrix Presentation Server that is configured for multuser access from clients.

**relay mode.** In this mode, the Secure Gateway Proxy functions without ticketing support from the STA and the Web Interface. It is a less secure mode, in which Secure Gateway functions as a server-side proxy server and provides a single point of entry into a server farm.
Secure Gateway. A Citrix component that provides a secure, encrypted channel for network traffic over the Internet, using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) between client devices and the Secure Gateway. The Secure Gateway provides a single point of encryption and access to servers running Citrix Presentation Server.

Secure Gateway Proxy. A component of the Secure Gateway that functions as a proxy server between the Secure Gateway and the secure network.

Secure Ticket Authority (STA). The STA is a ticketing mechanism that issues session tickets for clients. These tickets form the basis of authentication and authorization for connections to a server farm.

server farm. A group of computers running Citrix Presentation Server managed as a single entity with some form of physical connection between servers and a database used for the farm’s data store.

session ID. A unique identifier for a specific client session on a specific computer running Citrix Presentation Server.

session reliability. Session reliability keeps ICA sessions active and on the user’s screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

Web Interface. A component that provides users with access to Citrix Presentation Server applications and content through a standard Web browser.
Index

A
accelerators cards, SSL 85
access control list 125
access logs 77
  CGP 78
description 17
HTTP 78
SOCKS 78
accessibility. See Section 508 compliance
asymmetric encryption 103
audit logging 20
authentication 13, 105
description 19
authorization
description 19

C
CAs. See certificate authorities
certificate authorities 105–106
  public 110
  subordinate 106
certificate requirements 57
certificate revocation lists 108
certificates 101, 105
certificate chains 106
  chain 106
content 105
creating a certificate request 111
detection 17
do double-hop DMZ 58
expiration 108
hierarchy 106
importing X.509 certificate 113
intermediate 107
management 16
obtaining 109
private 109
renewal 108
requirements 34
response file 112
revocation lists 108
root 34, 105
selection 17
server 105
single-hop DMZ 57
subordinate 107
trial period 110
verification process 110
wildcard 17, 117
X.509 111
X.509 format file 112
.cer format 111
.pfx format 111
CGP access log 78
chain certificates 106
cipher
description 103
ciphersuites 88–89
  COM 88
  GOV 88
  restricting 89
Citrix XML Service 49
description 15
client connections
disconnect 69
do double-hop DMZ 27
relay mode 128
to Presentation Server 24
client operating system requirements 33
communications links, securing 18
compatibility
Citrix products 33
Presentation Server 33
Web Interface 33
components
for Presentation Server 24
configuration values, requiring restart 68
configuration wizard 68
configuring
Secure Gateway 60
Secure Gateway Proxy 63
connecting with
Presentation Server 21
connection information 17, 77
CGP 78
HTTP 78
SOCKS 78
connection keep-alive settings 86
connections 69
cryptography 102–103
asymmetric encryption 103
public key 104
secret key 103
symmetric key 103

demilitarized zone 14, 88
deployment
improvements 16
Presentation Server 38
testing 53
diagnostic tools 18, 68, 74
Digital certificates. See certificates
DMZ. See demilitarized zone
DNS. See Domain Name Server
documentation
accessing 10
Domain Name Server 25
double-hop DMZ
client connections 27
planning 26
Presentation Server 40, 45
Web Interface 27

E
encryption 13, 19, 88
asymmetric 103
bit length 112
public key 104
error messages 77
exporting server certificates 114

F
fault tolerance 20, 83
Federal Information Processing Standard 102
FIPS 140. see Federal Information Processing Standard
firewalls
forwarding mode 82
ICA traffic 82
ICA traffic, supporting 82
traversal 20, 82
FQDN. See Fully Qualified Domain Name
Fully Qualified Domain Name 25

H
high availability 83
HTTP access log 78

I
ICA
file 25
IETF. see Internet Engineering Taskforce
indexing
preventing 92
information
connections 69
sessions 69
installing
cancelling 59
components 58
configuration 60
pre-installation checklist 56
preparation 56
procedure 58
removing Secure Gateway 65
Secure Gateway Proxy 62
sequence 56
upgrading 64
Web Interface 38, 40
Internet Engineering Taskforce 102
Internet Information Services 41
  access 39
  lock down 91
  relay mode 124
Internet security protocols 102
ISO X.509 protocol 105

K
keep-alive parameters 86
  registry keys 87

L
load balancing 83–84
  benefits 84
  certificate requirements 85
  description 17
  Secure Gateway array 84
  SSL accelerator cards 85

M
management and report tools 18
Management Console 68
Microsoft Windows Update 33

P
performance monitoring 70
  counters 71
  description 17
Personal Information Exchange format 111
PKCS #12. see Personal Information Exchange format
PKI. see Public Key Infrastructure
pre-installation checklist 56
preventing
  indexing 92
private certificate authority 109
public certificate authority 110
public key encryption 104
Public Key Infrastructure 22, 102

R
redundancy 83
relay mode 119
  benefits 120
  certificates required 123
  configuration 125
  configuration information 123
  configure client devices 128
  default encryption level 128
  description 18
  how it works 122
  installation tasks 123
  installing 124
  modify configuration 127
  port 124
  understanding 120
requirements
  client software 33
  Section 508 compliance 32
  server hardware 32
  server software 32
reverse Web proxy
  SSL Error 4 97
root certificate 105, 116
  multiple 34

S
search engines
  preventing indexing 92
Section 508 compliance 32, 69
  description 17
Secure Gateway
  components 14
  configuration guidelines 56
  configuration wizard 68
  diagnostics 68
  double-hop DMZ 26
  installation guidelines 56
  Management Console 68
  managing 68
  planning 21
  planning with Presentation Server 23
  pre-installation checklist 56
  requirements 28
  upgrade requirements 28
  upgrading 28, 64
  use with Presentation Server 15, 21
Secure Gateway Proxy
configuration 63
description 14
installation 62
load balancing 84
modes of operation 120
normal mode 120
planning 26
relay mode 119–120
Secure Sockets Layer. See SSL
Secure Ticket Authority
changes 16
description 15
Internet Information Services requirements 41
requirements 24
session tickets 25
upgrading 49
security concepts 101
security recommendations 88
server certificate 105
applying for 112
installing 111
server farm
description 23, 38
setting up 41
upgrading 49
server hardware requirements 32
server requirements 32
session information 69
session reliability
description 18
requirements 28
session tickets 25
sessions 69
Single point of entry 19
single-hop DMZ
Presentation Server 38
Web Interface 38, 40
SOCKS access log 78
SSL 22, 90, 102
accelerator cards 85
support 17
SSL error 4 97
system requirements 32

T
TCP/IP keep-alives 86
test certificates 110
TLS 22, 90, 102
Transport Layer Security. See TLS
troubleshooting
application log 94
certificates 94
connection problems 95
CSG0188 error 94
diagnostics 93
general procedures 93
network address translator 100
SSL error 4 97
support 100
Windows XP Service Pack 2 96

U
uninstalling
procedure 65
upgrading
procedure 64
upgrading Secure Gateway 28, 64
installation order 29
with Presentation Server 28

W
Web Interface
connecting 47, 52
connecting with 21
described 15
double-hop DMZ 27
firewall 39
installing 38, 40
proxy settings 39
setting up 44, 46
Smart Card authentication 39
upgrading 51
wildcard certificates 17, 117
Windows 2000 32
Windows 2003 32
Windows operating system
server 32
Windows registry
keep-alive parameters 87
Windows XP Service Pack 2 96

X
X.509 certificate
importing 113
X.509 standard 106
Z
.cer format certificate 111
.pfx format certificate 111