Secure Gateway for Windows Administrator's Guide

Secure Gateway 3.1 for Windows®

Copyright and Trademark Notice

Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement. A printable copy of the End User License Agreement is included on your product media.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

© 2001-2008 Citrix Systems, Inc. All rights reserved.

Citrix, ICA (Independent Computing Architecture), and Program Neighborhood are registered trademarks, and Citrix Presentation Server, Citrix XenApp, Citrix Password Manager, Citrix Developer Network, Citrix Application Gateway, Citrix Application Firewall, and SpeedScreen are trademarks of Citrix Systems, Inc. in the United States and other countries.

RSA Encryption © 1996-1997 RSA Security Inc., All Rights Reserved.

This product includes software developed by The Apache Software Foundation (http://www.apache.org/)

This product includes software developed by Salamander Software Ltd. © 2002 Salamander Software Ltd. Parts © 2003 Citrix Systems, Inc. All rights reserved.

Licensing: Portions of this documentation that relate to FLEXnet Operations and FLEXnet Publisher are trademarks and/or registered trademarks of Acresso Software Inc. and/or InstallShield Co. Inc.

Portions created by gSOAP are Copyright © 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

The software in this product was in part provided by Genivia, Inc., and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Trademark Acknowledgements

Java, Sun, and SunOS are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Solaris is a registered trademark of Sun Microsystems, Inc. Sun Microsystems, Inc has not tested or approved this product.

Portions of this software contain imaging code owned and copyrighted by Pegasus Imaging Corporation, Tampa, FL. All rights reserved.

Microsoft, MS-DOS, Windows, Windows Media, Windows Server, Windows NT, Win32, Outlook, ActiveX, Active Directory, and DirectShow are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corp. in the U.S. and other countries.

Oracle, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates.

Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Licensing: FLEXnet Operations and FLEXnet Publisher are trademarks and/or registered trademarks of Acresso Software Inc. and/or InstallShield Co. Inc.

SAP is the registered trademark of SAP AG in Germany and in several other countries.

All other trademarks and registered trademarks are the property of their respective owners.

Document Code: August 1, 2008 (BC)

Contents

1 Getting Started with the Secure Gateway 9

2 Introducing the Secure Gateway 11

About the Secure Gateway and Secure Gateway Proxy 12
Secure Gateway Support for Citrix XenApp 12
Secure Gateway Features 13

3 Planning a Secure Gateway Deployment 17

Securing Citrix XenApp with the Secure Gateway 18
Establishing a Secure Connection to a Server Farm 20
The Secure Gateway in a Double-Hop Demilitarized Zone 21
Establishing a Secure Connection in a Double-Hop DMZ 22

4 System Requirements 25

System Software Requirements 26
System Hardware Requirements 26
Client Device System Requirements 27
Software System Requirements 27
Citrix Components and Client Compatibility 28
Certificate Requirements 28
Certificate Requirements for a Single-Hop Demilitarized Zone Deployment 29
Certificate Requirements for a Double-Hop Demilitarized Zone Deployment 29

5 Deploying the Secure Gateway with Citrix XenApp 31

Deploying the Secure Gateway in a Single-Hop Demilitarized Zone 31
Running the Web Interface behind the Secure Gateway in the Demilitarized Zone 31
Locking Down Internet Information Services 32
Running the Web Interface Parallel with the Secure Gateway 33
Deploying the Secure Gateway in a Double-Hop Demilitarized Zone 33
Setting Up and Testing a Server Farm 34

Installing the Secure Ticket Authority 34
Configuring the Web Interface to Support the Secure Gateway 34
Deployment Scenario A: Secure Gateway in a Single-Hop Demilitarized Zone 35
Setting Up the Web Interface and Secure Gateway in a Single-Hop Demilitarized Zone . 36
Deployment Scenario B: Double-Hop Demilitarized Zone 36
Setting Up the Secure Gateway and the Secure Gateway Proxy in a Double-Hop Demilitarized Zone 38
Setting Up and Testing the Web Interface in a Double-Hop Demilitarized Zone 38
Publishing the Web Address for the Secure Gateway in a Double-Hop Demilitarized Zone 38
Testing Your Deployment. 39
To test your deployment 39

6 Installing and Configuring the Secure Gateway and Secure Gateway Proxy 41

Upgrading Secure Gateway or Secure Gateway Proxy 41
Using Firewall Software with the Secure Gateway or Secure Gateway Proxy. 42
Preparing for Installation. 42
Certificate Requirements for a Single-Hop Demilitarized Zone Deployment. 42
Certificate Requirements for a Double-Hop Demilitarized Zone Deployment 43
Installing the Secure Gateway or Secure Gateway Proxy 43
To install the Secure Gateway or Secure Gateway Proxy 44
Configuring the Secure Gateway or Secure Gateway Proxy. 45
To start the configuration wizard manually 45
To select a configuration level (Secure Gateway) 46
To select a configuration level (Secure Gateway Proxy) 46
Task Summary for Secure Gateway, Advanced or Standard Configuration 47
Task Summary for Secure Gateway Proxy, Advanced or Standard Configuration. 48
To select a server certificate 48
To configure secure protocol settings 49
To configure inbound client connections 50
To configure outbound connections 51
To configure an access control list for outbound connections 51
To configure servers running the Secure Gateway Proxy. 53
To add the Secure Ticket Authority details. 54
To configure connection parameters. 54
To configure logging exclusions. 55
To add the Web Interface server details 57
To configure the logging parameters. 58
To complete the configuration. 58

To stop the Secure Gateway/Secure Gateway Proxy service 59
To uninstall the Secure Gateway 59

7 Managing the Secure Gateway 61

Viewing Session and Connection Information with the Secure Gateway Console. 62
To view session connection properties 62
To disconnect an active session. 63
To freeze (pause) and resume the display of session information 63
Viewing Secure Gateway Performance Statistics 63
Performance Counters Available for the Secure Gateway 64
To view the Secure Gateway performance statistics 67
Generating and Viewing the Secure Gateway Diagnostics Report 68
To generate a diagnostics report 68
Global Settings 69
Interfaces. 69
The Secure Gateway Proxy 70
Authority Servers 70
Certificate Check 71
Viewing the Secure Gateway Events and Logs 71
Logging Events with the Secure Gateway Event Viewer. 71
To view Secure Gateway events 72
Access Logs for the Secure Gateway and Secure Gateway Proxy. 72
HTTP Access Log 72
CGP Access Log 72
SOCKS Access Log 73
To view Secure Gateway access logs 73
Secure Gateway Configuration Wizard 73

8 Secure Gateway Optimization and Security Guidelines 75

Configuring Firewalls for the Secure Gateway 75
Planning for High Availability of the Secure Gateway 76
Load Balancing Multiple Secure Gateway Servers 77
Load Balancing an Array of the Secure Gateway Proxy 78
Certificate Requirements for Load Balancing Secure Gateway Servers 78
Using Load Balancers and SSL Accelerator Cards with Secure Gateway Servers 79
Secure Gateway Keep-Alive Values and Citrix XenApp 79
Connection Keep-Alive Values and the Secure Gateway 79

Recommendations for Improving Security of the Secure Gateway 81
Deploying the Secure Gateway in the DMZ 81
Changing or Restricting Ciphersuites 81
To change or restrict the ciphersuites 82
Restricting Ciphersuite Use to Secure Communication 82
Using Secure Protocols 83
Removing Unnecessary User Accounts 83
Removing Sample Code Installed with Internet Information Services 83
Secure Components that Run on Internet Information Services 83
Stopping and Disabling Unused Services 84
Installing Service Packs and Hotfixes 84
Following Microsoft Security Guidelines 84
Preventing Indexing by Search Engines 85

9 Troubleshooting the Secure Gateway 87

The Secure Gateway Fails with a CSG0188 Error 88
To check your certificates 88
Client Connections Launched from IP Addresses in the Logging Exclusions List Fail 88
Load Balancers Do Not Report Active Client Sessions if They Are Idle 89
Performance Issues with Transferring Files Between a Client Device and a Citrix XenApp Server 89
Gateway Client Connections Fail When Using Windows XP Service Pack 2 90
Failed Client Connections to the Secure Gateway Result in Duplicate Entries in the Secure Gateway Log 90
Placing the Secure Gateway Behind a Reverse Web Proxy Causes an SSL Error 4 90
Run the Secure Gateway Parallel to the Reverse Web Proxy 91
Use a Network Address Translator Instead of a Reverse Web Proxy 93
If You Cannot Resolve the Problem 93

10 Digital Certificates and the Secure Gateway 95

Understanding SSL and TLS 95
Understanding Cryptography 96
Types of Cryptography 96
Combining Public Key and Secret Key Cryptography 97
Understanding Digital Certificates and Certificate Authorities 98
Certificate Chains 99
Certificate Revocation Lists 101
Certificate Expiration and Renewal 101

Getting Certificates 102
If Your Organization Is its Own Certificate Authority 102
If Your Organization Is Not its Own Certificate Authority 102
Obtaining and Installing Server Certificates 103
Certificate Considerations 103
Obtaining and Installing Root Certificates 104
Obtaining a Root Certificate from a CA 104
Support for Wildcard Certificates with the Secure Gateway 105

11 Using the Secure Gateway Proxy in Relay Mode 107

Modes of Operation for the Secure Gateway Proxy 107
Normal Mode 107
Relay Mode 107
When to Use Relay Mode 108
How Relay Mode Works 108
Installing the Secure Gateway Proxy in Relay Mode 110
To install the Secure Gateway Proxy in Relay Mode 110
To configure the Secure Gateway in relay mode 112
To start or stop the Secure Gateway Proxy Service manually 114
To run the Secure Gateway Proxy Configuration wizard 114
Configuring Client Devices 114
To configure client connections to the Secure Gateway Proxy 114
To configure all application sets for the client to connect to the Secure Gateway Proxy . . 115
To modify an ICA file to enable a connection to the Secure Gateway Proxy 116
To test relay mode operation 117

Index 119

Getting Started with the Secure Gateway

The *Secure Gateway for Windows Administrator's Guide* is designed to help anyone who plans, designs, pilots, or deploys the Secure Gateway for Citrix XenApp for Microsoft Windows Server 2003 and Windows Server 2008. (XenApp is the new name for Citrix Presentation Server). It provides information to administrators about features, installation and setup, implementation, and deployment of the Secure Gateway.

The audience for this information is experienced administrators responsible for installing, configuring, and maintaining Citrix environments, and assumes knowledge of the following:

- System administration
- Networking and security technologies
- Microsoft Windows Server 2003 and Windows Server 2008
- Microsoft Internet Information Services (IIS)
- Internet and network protocols
- Citrix XenApp

Use this information with:

- *Citrix XenApp Administrator's Guide*
- *Web Interface Administrator's Guide*
- Appropriate Citrix XenApp plugin or client administrator guides

The following table highlights references to typical administrative tasks and conceptual information:

Task	See This Topic
Using the Secure Gateway with computers running XenApp	"Deploying the Secure Gateway with Citrix XenApp" on page 31
Installing and configuring the Secure Gateway	"Installing and Configuring the Secure Gateway and Secure Gateway Proxy" on page 41
Learning more about the Secure Gateway's performance counters and error logs	"Managing the Secure Gateway" on page 61
Getting general recommendations about using network components such as load balancers, SSL accelerator cards, and firewalls	"Secure Gateway Optimization and Security Guidelines" on page 75
Learning more about troubleshooting a Secure Gateway deployment	"Troubleshooting the Secure Gateway" on page 87
Learning about digital certificates and certificate installation	"Digital Certificates and the Secure Gateway" on page 95

Introducing the Secure Gateway

The Secure Gateway helps you to secure access to computers running Citrix XenApp.The Secure Gateway transparently encrypts and authenticates all user connections to help protect against data tampering and theft.

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 XenApp 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 Citrix XenApp.

About the Secure Gateway and Secure Gateway Proxy

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.

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.

Secure Gateway Support for Citrix XenApp

Your enterprise network can contain one or more servers running Citrix XenApp. A server farm is used for hosting published resources that users can access over the network.

The Secure Gateway works with the following components of Citrix XenApp for logon and authentication:

Citrix 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.

Secure Ticket Authority (STA). The STA is responsible for issuing session tickets in response to connection requests for published resources on Citrix XenApp. These session tickets form the basis of authentication and authorization for access to published resources. During installation of Citrix XenApp, the STA is installed automatically. 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.

Citrix XenApp Web Plugin.

Note: The Secure Gateway and Secure Gateway Proxy are not supported in environments using Advanced Access Control.

Secure Gateway Features

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

Network protocol support. The Secure Gateway supports the TCP/IP protocols, such as FTP, HTTP, and Telnet.

IPv4 and IPv6 protocol support. The Secure Gateway can be configured to accept inbound connections from clients using IPv4 and IPv6 addresses.

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

Simple deployment. Citrix XenApp includes the Secure Ticket Authority (STA) and is merged into a single Windows Installer package resulting in a more efficient deployment. The STA is deployed automatically on the same computer as Citrix XenApp, 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 XenApp.

Certificate management. The Secure Gateway Configuration wizard prevents the selection of a certificate that does not have a private key and verifies that the appropriate certificate is installed in the local computer certificate store. Wildcard certificate support. Wildcard certificates can be deployed on the Secure Gateway, the Secure Gateway Proxy, and on the computer where Citrix XenApp is 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.

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.

Instrumentation. The Secure Gateway includes a new set of performance counters to analyze the usage and load on the Secure Gateway server. See "Viewing Secure Gateway Performance Statistics" on page 63

Based on Apache Technology. The software code based on Apache technology is used as a foundation for building the Secure Gateway.

Section 508 compliance. Secure Gateway is compliant with Section 508 of the United States Workforce Rehabilitation Act of 1973.

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 remain visible while reconnection is attempted automatically in the background.

Relay mode. 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. See "Using the Secure Gateway Proxy in Relay Mode" on page 107.

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 XenApp" on page 31.

Supports secure communication between the Secure Gateway components. The Secure Gateway components support the use of digital certificates and the task of securing links by using SSL/TLS between components

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. The Secure Gateway Diagnostics tool, available from the Secure Gateway Management Console, reports configuration values, certificate details, and the state of each configured component.

Minimal client configuration. 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. 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 and authorization. The Secure Gateway works with the Web Interface to facilitate authentication of users attempting to establish connections to a server farm. Authorization occurs 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 Citrix XenApp server is eliminated and server certificate management is simplified. The Secure Gateway allows a single point of encryption and access to computers running Citrix XenApp

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 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 special hardware devices or network equipment upgrades.

Event and audit logging. Critical and fatal system events are logged to the Secure Gateway application log, enabling administrators to help diagnose 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.

Planning a Secure Gateway Deployment

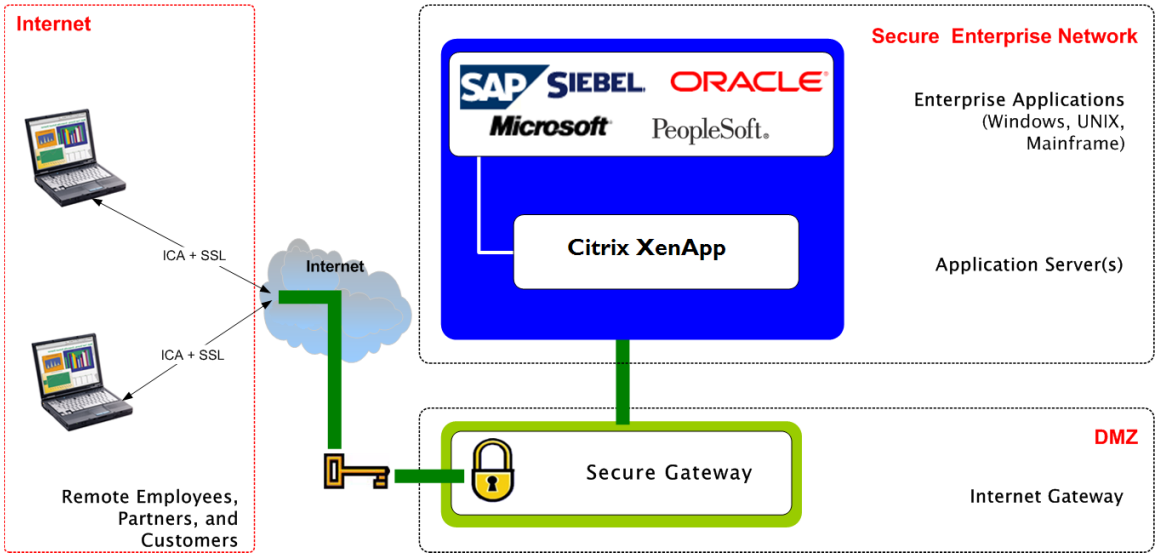
The Secure Gateway provides secure Internet access to computers running Citrix XenApp in an enterprise network.

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 XenApp.

If you have a server farm using Citrix XenApp, 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.

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. All data between the Internet and secure enterprise network segments use SSL and pass through the DMZ segment containing the Secure Gateway.



Securing a server farm and applications with the Secure Gateway.

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

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

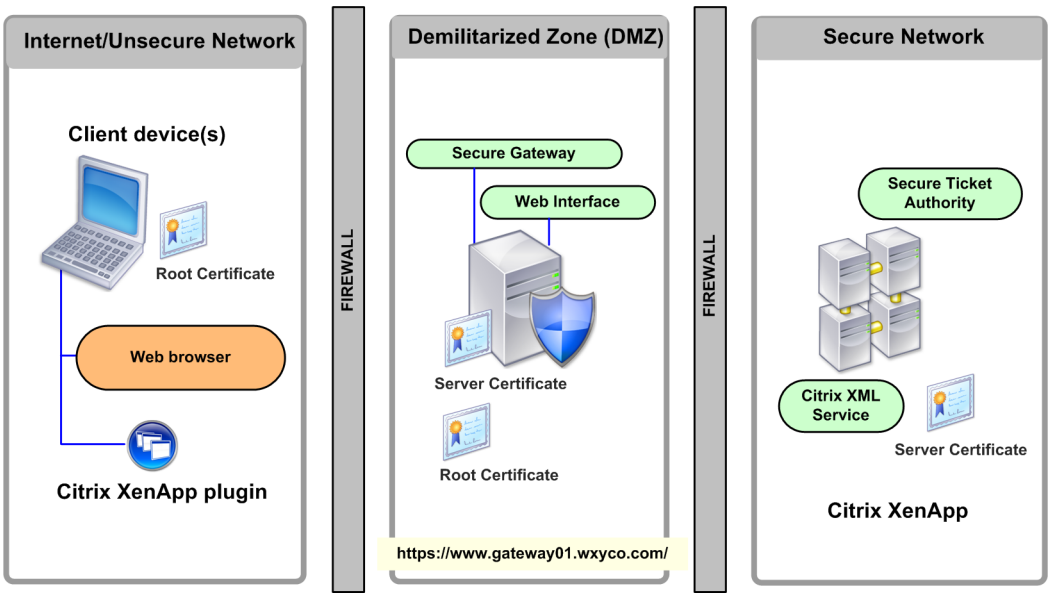
Users must log on to the secure network with valid user credentials; the Secure Gateway is completely transparent to users.

Note: The Secure Gateway and Secure Gateway Proxy are not supported in environments using Advanced Access Control.

Securing Citrix XenApp with the Secure Gateway

One or more computers running Citrix XenApp 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 Citrix XenApp servers in the secure network.

In this configuration, the Secure Gateway is deployed to provide secure Internet access directly to computers running Citrix XenApp 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.



A Secure Gateway deployment securing Citrix XenApp.

The 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 XenApp plugin. 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 XenApp 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 XenApp with Citrix XML Service and STA enabled on one or more computers (these are enabled by default as part of the installation process)

- Web Interface

Establishing a Secure Connection to a Server Farm

The Secure Gateway works with the Web Interface to provide secure access to published resources available on a secure enterprise network.

- 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.
- The Secure Gateway receives the request and relays the request to the Web Interface.
- The Web Interface responds by sending a logon page to the client browser.
- 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.
- The Web Interface populates the Web page with the list of published resources that the user is authorized to access.
- When the user clicks a published application link, the Web Interface sends the IP address and port for the requested Citrix XenApp 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.
- 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 XenApp is never revealed to the Citrix XenApp plugin.

- The client Web browser uses the ICA file to launch the Citrix XenApp plugin. The plugin 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.
- The Secure Gateway receives the session ticket from the client and contacts the STA for ticket validation.

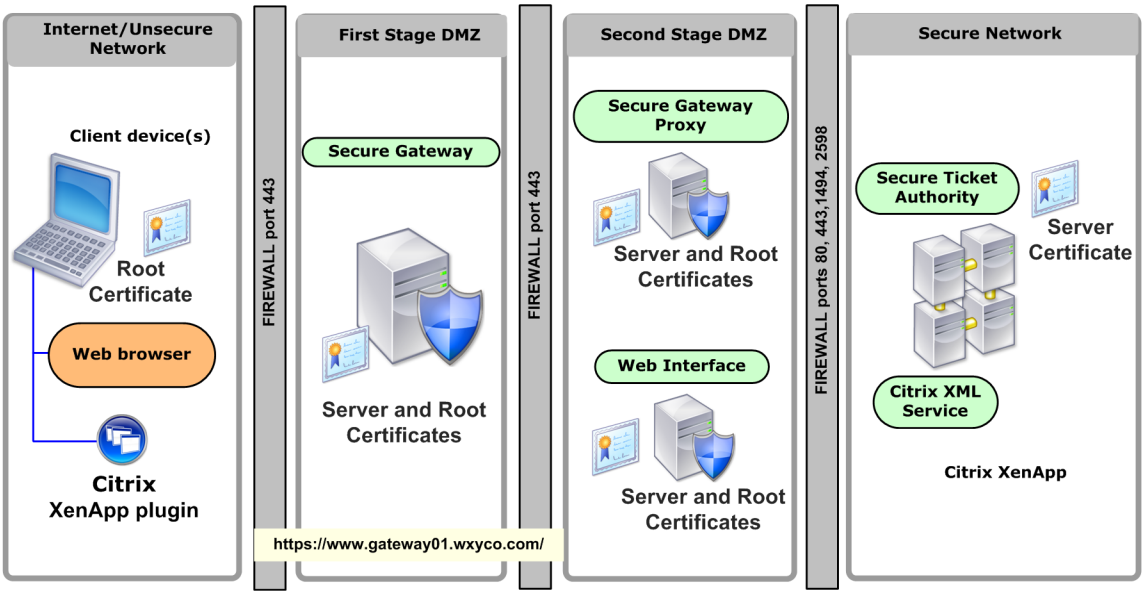
- If the ticket is valid, the STA returns the IP address of the Citrix XenApp server on which the requested application resides. If the session ticket is invalid or has expired, the STA informs the Secure Gateway and an error message appears on the client device.
- On receipt of the IP address for the Citrix XenApp 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 XenApp" on page 31 for detailed instructions about deploying the Secure Gateway in this scenario.

The Secure Gateway in a Double-Hop Demilitarized Zone

Depending on the security and network policies practiced by your organization, you may want to secure your network by using a demilitarized zone (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.



The Secure Gateway deployed in a double-hop DMZ.

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 a Citrix XenApp plugin. 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 XenApp and internal Web servers. A server within the 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 in a Double-Hop DMZ

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 XenApp” on page 31.

System Requirements

This topic describes the minimum requirements for hardware and software for deploying the Secure Gateway and the Secure Gateway Proxy, including the following:

- "System Software Requirements" on page 26
- "System Hardware Requirements" on page 26
- "Client Device System Requirements" on page 27
- "Citrix Components and Client Compatibility" on page 28
- "Certificate Requirements" on page 28

Note: Upgrading from earlier versions of Secure Gateway or Secure Gateway Proxy on the Windows Server 2003 platform is supported. Upgrading on the Windows Server 2008 platform is not supported; you must perform a fresh installation of Secure Gateway or Secure Gateway Proxy in this case.

Note: The Secure Gateway and Secure Gateway Proxy are not supported in environments using Advanced Access Control.

System Software Requirements

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

- Windows Server 2008 Family, except Web Server
- Windows Server 2003

Important: Secure Gateway runs as a 32-bit application on 64-bit versions of the Windows Server 2008 operating system.

System Hardware Requirements

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

The Secure Gateway requires the minimum hardware requirements for Windows Server 2003 and Windows Server 2008, as specified by Microsoft:

Windows Server 2003	
Processor	266Mhz or higher Pentium-compatible CPU
Memory	512MB RAM
Hard drive	4GB with 2GB of free space. Reserve 150MB for Secure Gateway installation.
Networking	One network adapter
Display	VGA or higher resolution monitor
Keyboard	Required
Pointing device	Required

Windows Server 2008	
Processor	1 GHz (32-bit) or higher Pentium-compatible CPU, 1.4 GHz (64-bit) or higher Itanium CPU
Memory	512MB RAM
Hard drive	10GB with 4GB of free space. Reserve 150MB for Secure Gateway installation.

Networking	One network adapter
Display	Super VGA or higher resolution monitor
Keyboard	Required
Pointing device	Required

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 2000 Professional
- Windows XP Home Edition
- Windows XP Professional
- Windows Vista
- Windows Server 2003
- Windows Server 2008

Citrix Components and Client Compatibility

The Secure Gateway is compatible with the following Citrix products:

- Citrix XenApp for Windows Server 2008
- Citrix XenApp for Windows Server 2003
- Web Interface

You can use Secure Gateway installed on a computer running Windows Server 2003 in the same environment as a Citrix XenApp server for Windows Server 2008. You can also use Secure Gateway installed on a computer running Windows Server 2008 in the same environment as a Citrix XenApp server for Windows Server 2003.

The Secure Gateway is compatible with the following Citrix XenApp Plugin for Hosted Apps software:

- Citrix XenApp (the new name for Program Neighborhood Agent and related clients)
- Citrix XenApp Web Plugin (the new name for Web Client)
- Program Neighborhood

Note: Secure Gateway and Secure Gateway Proxy do not support the Citrix XenApp Plugin for Streamed Apps, formerly known as the Citrix Streaming Client.

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. See "Digital Certificates and the Secure Gateway" on page 95.

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 Demilitarized Zone Deployment

If your secure network contains Citrix XenApp 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 XenApp.

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.

Certificate Requirements for a Double-Hop Demilitarized Zone Deployment

If your secure network contains Citrix XenApp 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 Citrix XenApp 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 XenApp

Citrix XenApp is the world's most widely deployed software for centrally managing multiple applications and delivering their functionality as a service to employees, wherever they may be.

One or more computers running Citrix XenApp 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 Citrix XenApp server.

Deploying the Secure Gateway in a Single-Hop Demilitarized Zone

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 log on 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 Demilitarized Zone

In a single-hop DMZ deployment 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.

Advantages	A single server certificate is required on the server running the Secure Gateway and the Web Interface.
	A single port, 443, must be opened on the firewall facing the Internet.
	The Web Interface cannot be contacted directly from the Internet and is more secure.
Disadvantages	Deploying the Secure Gateway in this configuration affects Web Interface functionality. When you deploy the Secure Gateway in this configuration, you lose some of the features available with the Web Interface, including the following:
	Smart Card Authentication. The Secure Gateway negotiates the SSL handshake and terminates the SSL connection before forwarding the client connection request to the Web Interface. Smart card authentication integrated with the Web Interface is unavailable because the Secure Gateway terminates the SSL connection before it reaches the Web Interface.
	.**Firewall and Proxy Settings Requiring Knowledge of the Client IP Address Are Ineffective**. All communication from the client device to the Web Interface is proxied through the Secure Gateway. As a result, all client communications to the Web Interface originate from the IP address of the server running the Secure Gateway. Though you can still configure firewall and proxy settings on the Web Interface for specific client address prefixes, these settings must allow all client communications through the Secure Gateway to have the Web Interface IP address. You will not be able to distinguish between different client devices connecting through the Secure Gateway.

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 33.

Locking Down Internet Information Services

All traffic to the server running the Web Interface is proxied through the server running the Secure Gateway. You need to lockdown Internet Information Services (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 your version of Microsoft Windows Server.

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/AccessPlatform or https://*Web Interface FQDN*/citrix/XenApp, 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.

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.

Deploying the Secure Gateway in a Double-Hop Demilitarized Zone

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.

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.

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.

- Install and configure a server farm in the enterprise network.
- Install, configure, and publish applications on the server farm.
- 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 XenApp Administrator's Guide*.

Installing the Secure Ticket Authority

When Citrix XenApp is installed, the Secure Ticket Authority (STA) is installed and configured automatically.

The 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.

During installation of the Secure Gateway, enter the FQDN of the server running Citrix XenApp. 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

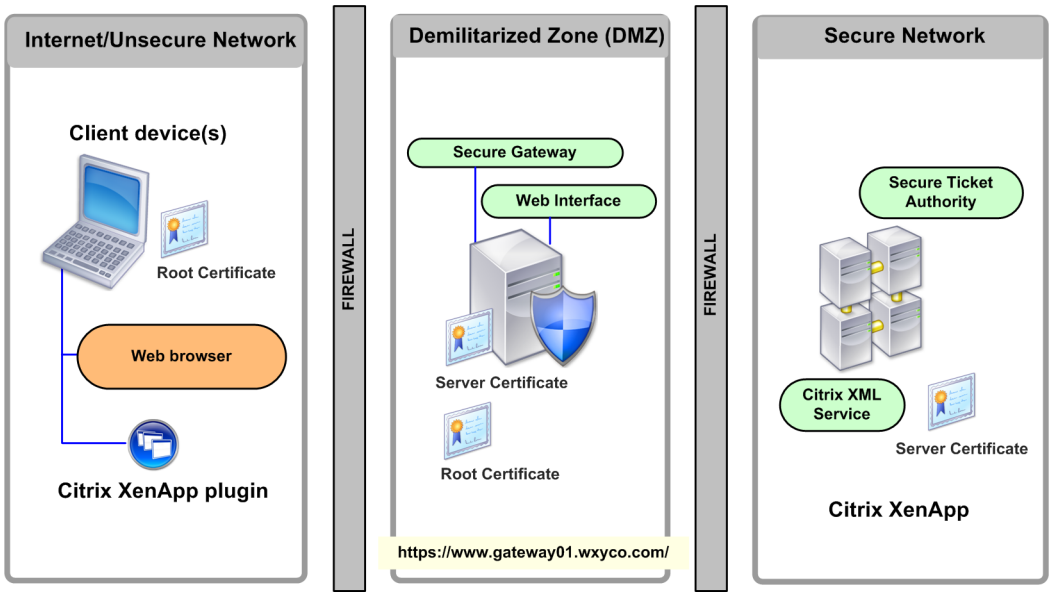
You need to configure the Web Interface to interact with the Secure Gateway components to provide authentication and authorization functionality. Ensure that the configuration settings on the server running the Web Interface correctly reflect the details of the STA and the Secure Gateway.

Deployment Scenario A: Secure Gateway in a Single-Hop Demilitarized Zone

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

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 XenApp. 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 reduce remote access costs dramatically.



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 XenApp 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 XenApp plugin 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 XenApp has a server certificate installed. For more information about certificates, see "Digital Certificates and the Secure Gateway" on page 95.

Setting Up the Web Interface and Secure Gateway in a Single-Hop Demilitarized Zone

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.

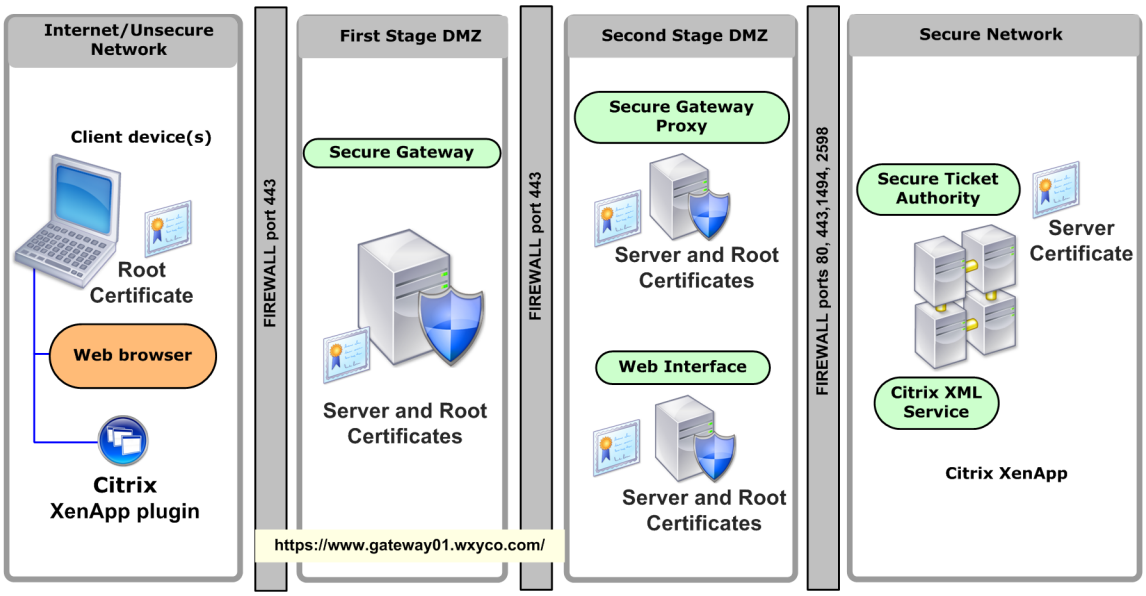
The Secure Gateway is installed on the same server as the Web Interface in the DMZ. To install and configure the Secure Gateway, see "Installing and Configuring the Secure Gateway and Secure Gateway Proxy" on page 41.

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in "Client Device System Requirements" on page 27.

Deployment Scenario B: Double-Hop Demilitarized Zone

WXYCo, Inc. deployed the Web Interface for access to published resources hosted on Citrix XenApp servers. 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.



A Secure Gateway deployment in a double-hop DMZ environment with a server farm

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 XenApp 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 XenApp plugin for 32-bit Windows.

Setting Up the Secure Gateway and the Secure Gateway Proxy in a Double-Hop Demilitarized Zone

The Secure Gateway is installed on a standalone server in the first DMZ. To install and configure the Secure Gateway, see "Installing and Configuring the Secure Gateway and Secure Gateway Proxy" on page 41.

The Secure Gateway Proxy is installed on a stand-alone server in the second DMZ. To install and configure the Secure Gateway Proxy, see "Installing and Configuring the Secure Gateway and Secure Gateway Proxy" on page 41.

Setting Up and Testing the Web Interface in a Double-Hop Demilitarized Zone

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.

Publishing the Web Address for the Secure Gateway in a Double-Hop Demilitarized Zone

Because all traffic to the Web Interface is proxied through the Secure Gateway, users need to type one of the following default Web address to access the logon page or XenApp Web site:

https://*Secure Gateway FQDN*/Citrix/AccessPlatform

https://*Secure Gateway FQDN*/Citrix/XenApp

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

In the case of WXYCo, the default Web address for the logon page or Web site is one of the following:

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

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

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 or Web site by connecting directly to the root Web address; that is, https://*Secure Gateway FQDN*/.

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

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

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 “Generating and Viewing the Secure Gateway Diagnostics Report” on page 68.

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/AccessPlatform/ or https://*Web Interface FQDN*/Citrix/XenApp.
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 and Configuring the Secure Gateway and Secure Gateway Proxy

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 have access to administrative privileges to install and configure the Secure Gateway and use the management tools.

Upgrading Secure Gateway or Secure Gateway Proxy

Upgrading from earlier versions of Secure Gateway or Secure Gateway Proxy on the Windows Server 2003 platform is supported. You must perform the following steps:

1. Remove any installed Secure Gateway hotfix software packages.
2. Remove the Secure Gateway or Secure Gateway Proxy software.
3. Perform a fresh installation of Secure Gateway or Secure Gateway Proxy.

Upgrading from earlier versions of Secure Gateway or Secure Gateway Proxy on the Windows Server 2008 platform is not supported. You must perform a fresh installation of Secure Gateway or Secure Gateway Proxy in this case.

Using Firewall Software with the Secure Gateway or Secure Gateway Proxy

The firewall software included in your Microsoft Windows server operating system (such as Windows Firewall with Advanced Security) where the Secure Gateway or Secure Gateway Proxy is used might not automatically allow access to required ports. Non-Microsoft firewall software might also disallow port access by default.

Also, the Secure Gateway or Secure Gateway Proxy does not automatically create an exception to allow access to the default SSL port 443, the default Secure Gateway Proxy port 1080, or any port number you select when configuring the software.

You must manually add or allow access to these ports to any firewall software you are using in your environment. Otherwise, the firewall software might block access to the functionality provided by the Secure Gateway or Secure Gateway Proxy.

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 25.

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.

Certificate Requirements for a Single-Hop Demilitarized Zone 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 XenApp.

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.

Certificate Requirements for a Double-Hop Demilitarized Zone Deployment

If the Secure Gateway is in the first DMZ, the Secure Gateway Proxy is 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 XenApp.
- 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. Although not a requirement, Citrix recommends that the communication links between the Secure Gateway and other servers in the DMZ or secure network be encrypted.

Installing the Secure Gateway or Secure Gateway Proxy

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.

Note: Install the Secure Gateway Proxy on a stand-alone 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.

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

- Install Citrix XenApp.
- Install root and server certificates on the appropriate computers. For more information, see "Digital Certificates and the Secure Gateway" on page 95.
- If using a double-hop DMZ, install the Secure Gateway Proxy in the second DMZ.
- 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 Web Interface and the Secure Ticket Authority (STA), if used, are functional. If a required component is not found, the Secure Gateway may fail to start. Ensure that you 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.

To install the Secure Gateway or Secure Gateway Proxy

1. Insert the installation media in the media drive.
2. From the Autorun screen, click **Platinum**, **Enterprise**, or **Advanced** and then click **Common Components**.
3. Click **Secure Gateway**.
4. On the **Welcome** screen, click **Next**.
5. Read and accept the license agreement, and then click **Next**.
6. In Installation Mode, select **Secure Gateway** or **Secure Gateway Proxy**.
7. To install the Secure Gateway components 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.
8. In **Service Account**, select the user account to determine credentials and privileges. Citrix recommends that you select an account that restricts privileges.

9. Click **Next** and follow the instructions in the wizard to complete installation.
10. After installing the Secure Gateway, configure it as described in "Configuring the Secure Gateway or Secure Gateway Proxy" on page 45.

Configuring the Secure Gateway or Secure Gateway Proxy

The Secure Gateway Configuration or Secure Gateway Proxy 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.

Configuring the Secure Gateway for use with Citrix XenApp requires 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 start the wizard manually, see "To start the configuration wizard manually" on page 45. See also "Using Firewall Software with the Secure Gateway or Secure Gateway Proxy" on page 42.

To start the configuration wizard manually

If you need to start the configuration wizard manually (for instance, to change the configuration at any time after initial installation and configuration), perform the following steps.

1. Log on as an administrator to the computer running the Secure Gateway.
2. Open the wizard by clicking **Start** and locating the **Secure Gateway Management Console**.
3. In the **Secure Gateway Management Console** menu, click **Action** > **All Tasks** and select **Stop** to stop the Secure Gateway Service.
4. From the Start button, locate and click **Secure Gateway Configuration Wizard** or **Secure Gateway Proxy Configuration Wizard**.
5. Click **OK**.

To select a configuration level (Secure Gateway)

"Task Summary for Secure Gateway, Advanced or Standard Configuration" on page 47 describes the task summary depending on the configuration level you select.

Select one of the following to access the parameters available for modification during the configuration process:

- **Standard**

  Includes only the minimum set of parameters required to configure the Secure Gateway. The Secure Gateway Configuration wizard sets all remaining parameters to their default values, respectively.

- **Advanced**

  Includes all of the Secure Gateway's configurable parameters, for example, supported secure protocols and logging exclusions.

To select a configuration level (Secure Gateway Proxy)

"Task Summary for Secure Gateway Proxy, Advanced or Standard Configuration" on page 48 describes the task summary depending on the configuration level you select.

1. Select one of the following to access the parameters available for modification during the configuration process:

   - **Standard**

     Includes only the minimum set of parameters required to configure the Secure Gateway Proxy. The Secure Gateway Proxy Configuration wizard sets all remaining parameters to their default values, respectively.

   - **Advanced**

     Includes all of the Secure Gateway Proxy's configurable parameters, for example, supported secure protocols and logging exclusions.

2. Select the **Secure traffic between the Secure Gateway and Secure Gateway Proxy** option to secure communications between the Secure Gateway and the Secure Gateway Proxy servers using SSL or TLS.

   When this option is not selected, the connection between the Secure Gateway and Secure Gateway Proxy is not secured. To secure traffic between the Secure Gateway and Secure Gateway Proxy you must also:

- Install a server certificate on the server running the Secure Gateway Proxy
- Install a client certificate on the Secure Gateway

Task Summary for Secure Gateway, Advanced or Standard Configuration

The task summary when selecting the advanced or standard configuration type is as follows:

Tasks	Advanced Configuration Selected	Standard Configuration Selected
"To select a server certificate" on page 48	X	X
"To configure secure protocol settings" on page 49	X	Not available
"To configure inbound client connections" on page 50	X	X
"To configure outbound connections" on page 51	X	X
"To add the Secure Ticket Authority details" on page 54	X	X
"To configure connection parameters" on page 54	X	Not available
"To configure logging exclusions" on page 55	X	Not available
"To add the Web Interface server details" on page 57	X	X
"To configure the logging parameters" on page 58	X	X

Task Summary for Secure Gateway Proxy, Advanced or Standard Configuration

The task summary when selecting the advanced or standard configuration type is as follows:

Tasks	Advanced Configuration Selected	Standard Configuration Selected
"To select a server certificate" on page 48	X	X
"To configure secure protocol settings" on page 49	X	Not available
"To configure inbound client connections" on page 50	X	X
"To configure outbound connections" on page 51	X	X
"To add the Secure Ticket Authority details" on page 54	Not available	Not available
"To configure connection parameters" on page 54	X	Not available
"To configure logging exclusions" on page 55	X	Not available
"To configure the logging parameters" on page 58	X	X

To select a server certificate

Server certificates enable client devices to verify the identity of the server running the Secure Gateway.

Note: This option is not displayed when you are installing the Secure Gateway Proxy and you select the **Secure traffic between the Secure Gateway and Secure Gateway Proxy** option as described in "To select a configuration level (Secure Gateway Proxy)" on page 46

.

1. Select a valid server certificate installed on the computer running Secure Gateway or Secure Gateway Proxy from the **Certificates Found** menu.
2. Click **View** to display the details of the selected certificate.

To configure secure protocol settings

This configuration dialog appears if you selected **Advanced** for the Secure Gateway's configuration level. Select the secure protocol and cipher suite used to secure the data transmitted between the Secure Gateway and the client device or Secure Gateway Proxy.

Note: When deployed in proxy mode, the Secure Gateway Proxy's client is the Secure Gateway. However, when deployed in relay mode, the Secure Gateway Proxy's client is the Citrix XenApp plugin (formerly known as Program Neighborhood Agent).

---

1. Select a secure protocol:

   - **Transport Layer Security (TLSv1)**

     Configure the Secure Gateway to use only TLS as its secure protocol. If you select this option, verify that all client devices support and are configured to use TLS as well.

   - **Secure Sockets Layer (SSLv3) and TLSv1**

     Configure the Secure Gateway and Secure Gateway Proxy to use SSL and TLS as its secure protocols. This option is useful when deploying the Secure Gateway or Secure Gateway Proxy in an environment in which some clients support only SSL.

     Note: If a client device supports both the SSL and TLS protocols, TLS is used to secure the data transmitted between the Secure Gateway/Secure Gateway Proxy and the client.

     ---

2. Select a cipher suite:

   - **GOV**

     You can configure the Secure Gateway/Secure Gateway Proxy to use the following government strength cipher suite:
     RSA_WITH_3DES_EDE_CBC_SHA or {0x00,0x0A}

   - **COM**

     You can configure the Secure Gateway/Secure Gateway Proxy to use the following commercial strength cipher suites:
     RSA_WITH_RC4_128_MD5 or {0x00,0x04},
     RSA_WITH_RC4_128_SHA or {0x00,0x05}

   - **ALL**

You can configure the Secure Gateway/Secure Gateway Proxy to use both the commercial and government strength cipher suites. This option is useful when deploying the Secure Gateway/Secure Gateway Proxy in an environment where some client devices support only COM while others support only GOV.

Note: When the Secure Gateway and a client device support both COM and GOV cipher suites, the Secure Gateway uses the COM cipher suite.

---

3. Click **Next** to proceed.

To configure inbound client connections

Specify the IP addresses and TCP ports that you want the Secure Gateway/Secure Gateway Proxy to monitor for incoming connections. See also "Using Firewall Software with the Secure Gateway or Secure Gateway Proxy" on page 42.

1. Select each **Monitor all IP addresses** check box to configure the Secure Gateway to listen for connections on all available IPv4 or IPv6 addresses.

   This option is useful when configuring the Secure Gateway/Secure Gateway Proxy on a server using multiple network interface cards (NICs). When configured in proxy mode, the Secure Gateway Proxy listens on all available IP addresses for Secure Gateway connections. When configured for relay mode, the Secure Gateway Proxy listens on all available IP addresses for client connections.

2. Type a listener TCP port number in the **TCP Port** field.

   This option is available only when the **Monitor all IP addresses** option is selected. The Secure Gateway/Secure Gateway Proxy listens for Secure Gateway or client connections on all available IP addresses using the port specified on the server. The default TCP port is 443.

3. Clear the **Monitor all IP addresses** check boxes to configure the Secure Gateway/Secure Gateway Proxy to listen on one or more specific IP addresses. Then click **Add** to add one or more IP addresses and related TCP port address.

Typically, you would exclude dynamic IP addresses. When a dynamic IP address changes, new connections are not accepted on that address and the service can fail to start when the server is restarted.

To configure outbound connections

Select the servers to which the Secure Gateway can connect:

Options	Description
No outbound traffic restrictions	Select this option to enable the Secure Gateway/ Secure Gateway Proxy to establish connections to any server within the DMZ or secure network. Click **Next** to continue.
Use the Secure Gateway Proxy	This option is not available when configuring the Secure Gateway Proxy. Select this option when configuring the Secure Gateway in a double-hop environment. See "To configure servers running the Secure Gateway Proxy" on page 53. Select the **Secure traffic between the Secure Gateway and the Secure Gateway Proxy** check box to use HTTPS to secure communications between them.
Use an Access Control List (ACL)	Select this option to create an access control list for the Secure Gateway/Secure Gateway Proxy. An access control list restricts the Secure Gateway/Secure Gateway Proxy to establishing connections to servers specified in the list. Click **Configure** to specify the start and end IP address range for allowed connections. See "To configure an access control list for outbound connections" on page 51.

Note: In a double-hop DMZ, configure outbound access control lists on the Secure Gateway Proxy server only.

To configure an access control list for outbound connections

You do not need to include servers running the Secure Ticket Authority because these are configured elsewhere in the wizard.

1. Select the **Use an Access Control List (ACL)** button, click **Configure**, and then click **Add**.

2. If you select the **IP Address Range** option, type or select the following information:

Options	Description
Start address	Enter the IP address of a server that you want to add to the outbound access control list. When specifying an IP address range, enter the range's start IP address. If you use an IP address range for multiple servers running XenApp, be sure that the servers you specify offer the full range of applications that you want to be available.
End address	Leave this field blank if you are creating an entry for a single server. Otherwise, enter the end address of the range.
TCP port	Enter the TCP port used by the server(s). To allow connections to any port on a server you can use the wild card asterisk character (*) in the TCP port field. You can use this wild card to allow one ACL entry for a range of IP addresses to permit connections using the ICA and Common Gateway Protocol (CGP) protocols.
Use default port	Select this option to use the default port used by the server for the protocol selected.
ICA	Select this option to allow ICA/SOCKS connections to the selected servers. Typically, you would use ICA for servers running Citrix XenApp that accept ICA/SOCKS connections. This option is not available to the Secure Gateway Proxy.
CGP	Select this option to allow CGP connections to the selected servers. Typically, you would use CGP for servers running Citrix XenApp that accept CGP connections. CGP can provide session reliability if you enable session reliability on the selected servers. To allow CGP as well as ICA/SOCKS connections to the same servers, add a separate entry for each protocol. This option is not available to the Secure Gateway Proxy.

3. If you select the **Server FQDN** option, type or select the following information:

Options	Description
FQDN	Enter the fully qualified domain name of the server to which the Secure Gateway Proxy allows access.

Options	Description
TCP port	Enter the TCP port used by the server. To allow connections to any port on a server, you can use the wild card asterisk character (*) in the TCP port field.
Secure traffic between the server and the Secure Gateway Proxy	Select this option to secure communications between the server and the Secure Gateway Proxy servers using SSL or TLS. When this option is not selected, the connection is not secured.

4. Click **OK**, then click **Add** to add another connection, or click **OK** to close the dialog box.

To configure servers running the Secure Gateway Proxy

1. From the **Configure outbound connections** dialog window, select **Use the Secure Gateway Proxy** radio button and click **Configure**.
2. Click **Add**.
3. Type the fully qualified domain name (FQDN) or IP addresses and TCP port of the Secure Gateway Proxy servers to which you want the Secure Gateway server to connect.

   The default TCP port for unsecured communications between the Secure Gateway and the Secure Gateway Proxy is 1080. The default TCP port for secure communications between the Secure Gateway and Secure Gateway Proxy is 443.
4. Click **OK**.
5. Select the **Secure traffic between the Secure Gateway and Secure Gateway Proxy** option to secure communications between the Secure Gateway and the Secure Gateway Proxy servers using SSL or TLS.

   When this option is not selected, the connection between the Secure Gateway and Secure Gateway Proxy is not secured. To secure traffic between the Secure Gateway and Secure Gateway Proxy you must also:

   - Install a server certificate on the server running the Secure Gateway Proxy
   - Install a client certificate on the Secure Gateway
6. Click **OK**.

To add the Secure Ticket Authority details

You can configure the Secure Gateway to contact multiple STAs for failover protection. If you specify multiple STAs, be sure that this list matches the list of STAs that the Web Interface is configured to contact.

Type or select the following information:

Option	Description
FQDN	Enter the fully qualified domain name of the server running the STA.
Path	This field is populated automatically with the default virtual directory path, /Scripts/CtxSTA.dll or CitrixAuthService/AuthService.asmx. If you changed the default path when you configured the Citrix XML Service to share a port with Internet Information Services on the server running Citrix XenApp, enter the correct path.
ID	This field is populated automatically by the Secure Gateway when it resolves the specified FQDN and reads the ID string from the server running the STA. If the Secure Gateway is unable to resolve the address specified you are prompted to enter the ID for the STA. The ID for the STA is a randomly generated string. You can view STA IDs by running the Secure Gateway diagnostic tool.
Secure traffic between the STA and the Secure Gateway	Select this option to secure communications between the Secure Gateway and the STA by using SSL or TLS. To enable this security feature, the FQDN of the STA must match the FQDN specified by its server certificate.
TCP port	Enter a network port number used by the Secure Gateway to contact the STA.
Use default	Select this option to use the default port assignment for the STA. The default TCP port for unsecured communications between the Secure Gateway and the STA is 80. The default TCP port for secure communications between the Secure Gateway and STA is 443.

To configure connection parameters

You can configure how connection requests time out. Preventing requests from timing out may be useful if your network has periods of high latency. However, uncompleted connection requests that do not time out, or time out slowly, can preempt additional connections through the Secure Gateway. The number of connections the Secure Gateway server can support depends on the server processor, usage, and limits set in the **Concurrent Connection Limits** section.

Select one of the following options:

Option	Description
No connection timeout	Select this option if you do not want to limit the time in which Secure Gateway must complete a connection request. Do not select this option if typical usage behavior can result in so many uncompleted connection requests that the server stops accepting connection requests.
Connection timeout (seconds)	Set the interval of time in which the Secure Gateway can complete a connection request. If the connection is not established by the time the specified value elapses, then the connection times out. By default, the connection timeout value is configured for 100 seconds.
Concurrent Connection Limits	This option is not available for the Secure Gateway Proxy. Set the following values using numbers suitable to your environment. Consider processor type and processor speed as well as typical usage behavior. Failure to do so may overload the processor and result in a poor quality of service for your end users. • **Unlimited**. Select this option to configure the Secure Gateway to support up to 1,920 concurrent client connections (250 connections are allocated to HTTP/S by default, leaving 1,670 ICA/CGP connections, including MAPI over CGP connections). The Secure Gateway stops accepting new connection requests if the number of concurrent client connections reaches 1,920. This setting overrides the value entered in Maximum connections. • **Maximum Connections**. Specify the maximum number of concurrent ICA/CGP connections supported by the Secure Gateway. The Secure Gateway stops accepting new ICA/CGP connection requests when the number of concurrent connections equals the value entered in this field.

To configure logging exclusions

Typically, third-party network devices such as load balancers generate extraneous Secure Gateway log information. For example, load balancers might poll the Secure Gateway repeatedly to ensure that the server is active. Each poll is recorded by the Secure Gateway as a connection, resulting in the event log containing several unnecessary entries.

The Secure Gateway and the Secure Gateway Proxy generate their own log files. Therefore, if you deployed the Secure Gateway in proxy mode, you must configure each component's logging exclusions separately.

1. Click **Add** to enter the IP address of a network device that you want the Secure Gateway to exclude from its logging operations.

2. After typing the IP address, click **OK**.

To add the Web Interface server details

The Web Interface works with the Secure Gateway to provide a logon interface, and facilitates the authentication and authorization of connection requests to server farms.

Running the Secure Gateway and the Web Interface on a single server is supported only in a single-hop DMZ environment.

1. Select one of the following access options:

   - **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 the **Installed on this computer** check box (this option is not available in a double-hop environment).

     If you configure your firewall to permit connections to the Secure Gateway only, the Web Interface is not exposed to the Internet, which is preferable in some enterprises. Configuring indirect access can be economical if you deploy the Web Interface on the Secure Gateway server. In that case, all that is required is one SSL certificate, one public IP address, and one server.

   - **Direct**

     If you configure your firewall to permit connections to the Secure Gateway only, the Web Interface is not exposed to the Internet, which is preferable in some enterprises. Configuring indirect access can be economical if you deploy the Web Interface on the Secure Gateway server. In that case, all that is required is one SSL certificate, one public IP address, and one server.

2. If you do not select the **Installed on this computer** check box, type or select the following information in the **Details** area:

   - **FQDN**

     Enter the fully qualified domain name of the server running the Web Interface. If you selected **Installed on this computer**, this field is automatically populated with the value localhost.

   - **TCP port**

     Enter the port number the Secure Gateway should use when communicating with the Web Interface.

3. Select the **Secure traffic between the Web Interface** check box to configure the Secure Gateway to use HTTPS when communicating with the Web Interface.

To configure the logging parameters

1. Specify the type of errors and events that the Secure Gateway/Secure Gateway Proxy writes to the event log and Event Viewer. The logging levels available include the following:

   - **Fatal Events Only**

     Fatal error messages are logged when an operational failure prevents the Secure Gateway Proxy from starting. Select this option to log only fatal events.

   - **Error and Fatal Events**

     Error messages are logged when a partial failure, such as the Secure Gateway Proxy being out of memory, occurs. Select this option to log errors and fatal events.

   - **Warning, error, and fatal events**

     Warning messages are logged when tickets time out, data packets are corrupted, and similar events occur. Select this option to log warnings, errors, and fatal events.

   - **All events including informational**

     All events are logged, including informational messages resulting from client connections. Select this option to log all events and errors. Selecting this option will result in the Event Viewer window and event log filling up rapidly.

2. Click **Next**.

To complete the configuration

You must start or restart the Secure Gateway/Secure Gateway Proxy to use the new configuration settings. If the Secure Gateway/Secure Gateway Proxy is already running, restarting it disconnects all active sessions. To avoid disconnecting active user sessions, you can clear the **Restart Secure Gateway Proxy** check box.

Select **Start the Secure Gateway** or **Start the Secure Gateway Proxy** and click **Finish**.

Note: If a client is connected to the Secure Gateway and the Secure Gateway is restarted, the Secure Gateway does not generate service stop and service start event log messages. If a client is not connected and the Secure Gateway is restarted, Secure Gateway does generate these messages.

See also "Using Firewall Software with the Secure Gateway or Secure Gateway Proxy" on page 42.

To stop the Secure Gateway/Secure Gateway Proxy service

1. Log on as an administrator to the Secure Gateway.
2. From the **Start** button, locate and click **Secure Gateway Management Console**.
3. In the Secure Gateway Management Console, on the **Action** menu, click **All Tasks** and click **Stop**.

To uninstall the Secure Gateway

1. Exit any applications running on the server.
2. Open the **Control Panel** and click **Programs and Features**.
3. Select **Secure Gateway** and click **Uninstall**.

Managing the Secure Gateway

The Secure Gateway Management Console is an MMC snap-in that 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. 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, expand the **Secure Gateway Management Console** node, right-click **Session Information**, 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 “Viewing Session and Connection Information with the Secure Gateway Console” on page 62.

  The sessions for the Web Interface have 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 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.

Note: Running the Secure Gateway Configuration Wizard requires administrative privileges.

Viewing Session and Connection Information with the Secure Gateway Console

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

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:

- **Protocol**. The network protocol with which the client is connecting.
- **Resource**. The published application.
- **Server**. The IP address and port of the computer in the server farm to which the client is connecting.
- **Secure Gateway Proxy**. The IP address and port of the Secure Gateway Proxy. If your network is using a single-hop DMZ that does not have the Secure Gateway Proxy, this column displays N/A.

You can refresh the connection information, disconnect one connection, or disconnect all of the connections in the **Connection Information** dialog box.

To view session connection properties

1. From the **Session Information** pane, select a session.
2. Right-click and select **Properties**. Alternatively, double-click a session.

The following statistics are available for all active sessions running through the Secure Gateway:

Statistic	Description
Client IP	The IP address and port of the remote client.
User	The current user associated with the session, if any.
Domain	The network domain from which the current user is logged on.
Time Established	The time that this connection was established.

Statistic	Description
Time Elapsed	The amount of time, in seconds, that elapsed since this connection was established.

To disconnect an active session

1. From the **Session Information** pane, right-click the active session you want to disconnect and select **All Tasks > Disconnect**.
2. Right-click and select **All Tasks - Disconnect**.

To freeze (pause) and resume the display of session information

The information in the session information pane refreshes every five seconds. If you want to view details of a particular session, you may find it useful to turn off the automatic screen refresh feature.

1. From the **Session Information** pane, right-click any session entry and select **All Tasks > Freeze Display**.
2. From the **Session Information** pane, right-click any session entry and select **All Tasks > Resume Display**.

Viewing Secure Gateway Performance Statistics

The Secure Gateway includes a customized Windows System Monitor containing real-time performance statistics, or counters, for the Secure Gateway. You can use this monitor to evaluate and troubleshoot connections running through the Secure Gateway.

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

Performance statistics include the data throughput rate in bytes per second across CGP, HTTP/S, SOCKS, and total client connections through Secure Gateway. The "Successful" counters indicate the number of users' connections that have successfully completed since the Secure Gateway service was last started. Users can have multiple connections within each session. The "Active" counters indicate the number of active connections going through the Secure Gateway.

You can use these statistics to troubleshoot connections to the Secure Gateway. For example:

- The Secure Gateway processor load might be too high because too many users are connected to the Secure Gateway server. You can look at the total active connections to check how many users are connected.
- Users might not be able to launch their published applications because the Secure Gateway cannot connect to the XenApp servers. The failed "Backend" connections counter is high if this is the problem.

The Secure Gateway System Monitor takes advantage of several of the features included in the Windows System Monitor, including customizing the display of counter information and saving counter data. You can use the System Monitor icons at the top of the pane or shortcut keys to customize the display. For a list of the shortcut keys, see the Windows System Monitor help.You can display the Windows Performance monitor from the Secure Gateway Management Console.

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

Performance Counters Available for the Secure Gateway

The following performance counters are available for the Secure Gateway:

Counter name	Description
Bytes/Sec from Client	The data throughput rate (bytes per second) from all connected clients to the Secure Gateway.
Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients.
CGP Active Connections	The total number of CGP client connections currently active.
CGP Bytes/Sec from Client	The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the CGP protocol.
CGP Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the CGP protocol.

Counter name	Description
CGP Kilobytes from Client	The total number of kilobytes sent from all clients connected to the Secure Gateway using the CGP protocol.
CGP Kilobytes to Client	The total number of kilobytes sent from the Secure Gateway to all clients connected using the CGP protocol.
CGP Peak Bytes/Sec from Client	The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the CGP protocol.
CGP Peak Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the CGP protocol.
CGP Successful Connections	The total number of successful CGP connections.
Client Connect Time: Average (in ms)	The average amount of time (in milliseconds) for a client connection request to complete the connection process.
Client Connect Time: Longest (in ms)	The longest amount of time (in milliseconds) for a client connection request to complete successfully.
Connections/Second	The number of successful client connection requests per second.
Connections/Second: Peak	The highest number of successful client connection requests per second.
Connections: Peak Active	The highest number of concurrent connections through the Secure Gateway.
Connections: Total Active	The total number of client connections currently active.
Connections: Total Successful	The total number of successful client connections. It is the sum of all successful connections for all protocols: CGP, HTTP/S, and SOCKS.
Connections:Pending	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.
Failed Backend Connections	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.
Failed Connections: Client Timed Out	The total number of client connection requests that were accepted but timed out before completing the protocol handshake.

Counter name	Description
Failed Connections: General Client Error	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.
Failed Connections: SSL Client Handshake Error	The total number of client connection requests that were accepted but did not successfully complete the SSL handshake.
Failed Connections: Total Client	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.
HTTP/S Active Connections	The total number of HTTP/S connections currently active.
HTTP/S Bytes/Sec from Client	The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the HTTP/S protocol.
HTTP/S Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the HTTP/S protocol.
HTTP/S Kilobytes from Client	The total number of kilobytes sent from all clients connected to the Secure Gateway using the HTTP/S protocol.
HTTP/S Kilobytes to Client	The total number of kilobytes sent from all connected clients to the Secure Gateway using the HTTPS protocol.
HTTP/S Peak Bytes/Sec from Client	The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the HTTP/S protocol.
HTTP/S Peak Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the HTTP/S protocol.
HTTP/S Successful Connections	The total number of successful HTTP/S connections.
Kilobytes from Client	The total number of kilobytes sent from all connected clients to the Secure Gateway.
Kilobytes to Client	The total number of kilobytes sent from the Secure Gateway to all connected clients.
Peak Bytes/Sec from Client	The highest data throughput rate (bytes per second) from all connected clients to the Secure Gateway.
Peak Bytes/Sec to Client	The highest data throughput rate (bytes per second) from the Secure Gateway to all connected clients.
SOCKS Active Connections	The total number of SOCKS client connections currently active.

Counter name	Description
SOCKS Bytes/Sec from Client	The data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the SOCKS protocol.
SOCKS Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the SOCKS protocol.
SOCKS Kilobytes from Client	The total number of kilobytes sent from all clients connected to the Secure Gateway using the SOCKS protocol.
SOCKS Kilobytes to Client	The total number of kilobytes sent from all connected clients to the Secure Gateway using the SOCKS protocol.
SOCKS Peak Bytes/Sec from Client	The highest data throughput rate (bytes per second) from all clients connected to the Secure Gateway using the SOCKS protocol.
SOCKS Peak Bytes/Sec to Client	The data throughput rate (bytes per second) from the Secure Gateway to all connected clients using the SOCKS protocol.
SOCKS Successful Connections	The total number of successful SOCKS connections.
SSL Handshake Time: Average	Average length of time (in milliseconds) for an SSL handshake to complete.
SSL Handshake Time: Longest	Length of time (in milliseconds) for the longest SSL handshake to complete.
SSL Handshakes/Sec	Number of successful SSL handshakes per second.
SSL Handshakes/Sec: Peak	Highest number of successful SSL handshakes per second.
SSL Handshakes: Pending	Number of SSL handshakes currently in progress between a client and the Secure Gateway.
SSL Handshakes: Total	Total number of SSL handshakes that completed successfully between a client and the Secure Gateway.

To view the Secure Gateway performance statistics

1. Open the Secure Gateway Management Console.
2. In the tree view, select **Secure Gateway Performance Statistics**. Performance statistics for the Secure Gateway appear in the right pane.
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.

Generating and 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:

Information icon	A registry or configuration value is present.
Warning icon	A registry or configuration value is missing.
Passed check icon	A communication check for the component passed.
Failed check icon	A communication check for the component failed.

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

To generate a diagnostics report

Locate **Secure Gateway Diagnostics** from the Administration Tools found in the Citrix program group or from the Secure Gateway Management Console on the Start menu.

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 3.1.1


Computer NetBIOS Name: GATEWAY01
Configuration captured on: 2/27/2005 9:44:55 AM
-----------------------------------------------


Secure Gateway Global Settings
-----------------------------------------------
Version = 3.1.1
 Products Secured = Citrix XenApp
 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.

```
Secure Gateway Proxy - All output is directed to a Secure Gateway Proxy
------------------------------------------------------------------------
 FQDN = gwyproxy.company.com
 Port = 1080
Secured = No
 Tested OK
```

Authority Servers

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

```
Authority Servers
-----------------


ID = STAFE565EE5A52E
 --------------------
  FQDN = sta01.company.com
  Port = 443
  Path = /Scripts/CtxSTA.dll
  Type = STA
  Secured = Yes
  Protocol = BOTH
  Ciphersuites = ALL
  Tested OK
```

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.

```
Certificate Check
-----------------
 FQDN = gateway01.company.com
This certificate is currently valid.
```

Viewing the Secure Gateway Events and 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.

Logging Events with the Secure Gateway Event Viewer

The Secure Gateway Event Viewer is a customized Windows Event Viewer that displays errors and events generated by the Secure Gateway. 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.

If a client is connected to the Secure Gateway and the Secure Gateway is restarted, the Secure Gateway does not generate service stop and service start event log messages. If a client is not connected and the Secure Gateway is restarted, Secure Gateway does generate these messages.

To view Secure Gateway events

1. Open the Control Panel and double-click **Administrative Tools**.
2. Double-click **Event Viewer**.
3. Expand the **Applications and Services Logs** node and select **Secure Gateway**.

   All errors and events generated by the Secure Gateway appear in the right pane.
4. To view additional information, double-click an entry in the right pane.

   The **General** tab contains the event ID and a brief description of the Secure Gateway error.

Access Logs for the Secure Gateway and Secure Gateway Proxy

The access logs generated by the Secure Gateway service 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

To view Secure Gateway access logs

1. Open Windows Explorer.
2. Navigate to the following path:

   The default path for the error logs is the installation path for the Secure Gateway or the Secure Gateway Proxy, typically %systemroot%\Program Files\Citrix\Secure Gateway\logs.
3. Open the log file with an ASCII text editor such as Notepad.

Secure Gateway Configuration Wizard

The Secure Gateway Configuration wizard guides you through the process of specifying configuration parameters for the Secure Gateway. Each dialog box includes context-sensitive Help so that you can obtain additional information specific to the parameters you are configuring. Click **Help** within any dialog box to access the context-sensitive Help.

You can access the Secure Gateway Configuration wizard from the **Secure Gateway Management Console** node in this console. You can also access the Secure Gateway Configuration wizard or the Secure Gateway Proxy Configuration wizard from **All Programs** in the **Start** menu of the server running the service or proxy. Running the Secure Gateway Configuration Wizard requires administrative privileges.

Secure Gateway Optimization and Security Guidelines

This topic 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 topic contains the following:

- "Configuring Firewalls for the Secure Gateway" on page 75
- "Planning for High Availability of the Secure Gateway" on page 76
- "Secure Gateway Keep-Alive Values and Citrix XenApp" on page 79
- "Recommendations for Improving Security of the Secure Gateway" on page 81
- "Preventing Indexing by Search Engines" on page 85

Configuring Firewalls for the Secure Gateway

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 XenApp. 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 XenApp are less affected than ICA connections to computers running Citrix XenApp.

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 of the Secure Gateway

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 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 server 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 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 log on 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 this case, it might 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 for Load Balancing Secure Gateway Servers

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 XenApp.

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.

Using Load Balancers and SSL Accelerator Cards with Secure Gateway Servers

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 Citrix XenApp server. The Secure Gateway does not expect non–SSL traffic and drops the connection.

Secure Gateway Keep-Alive Values and Citrix XenApp

If you enable TCP/IP keep-alive parameters on computers running Citrix XenApp, 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 Citrix XenApp 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 Citrix XenApp server. Setting the keep-alive values on the server running the Secure Gateway to match the values set on the Citrix XenApp 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.

For more information about the use of ICA and TCP/IP keep-alives on computers running Citrix XenApp, see the Citrix Knowledgebase Article CTX708444, available from the Support page of http://www.citrix.com.

Connection Keep-Alive Values and the Secure Gateway

The Secure Gateway establishes connections over the Internet between remote clients and Citrix XenApp servers. 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\

For more information about making changes to these parameters, 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". Under normal circumstances, it is not necessary to change these settings.

Recommendations for Improving Security of the Secure Gateway

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 XenApp, 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.

Important: 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 Secure Gateway 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 Internet Information Services

An important security step is to disable or remove all sample Web applications installed by the Internet Information Services (IIS). 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 Internet Information Services

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.

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 *Threats and Countermeasures Guide* on the Microsoft Web site. Note that 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.

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

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

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 determine whether configuration settings are incorrect or if the required components or services are unavailable.

For instructions about using the Secure Gateway Diagnostics tool, see “Generating and Viewing the Secure Gateway Diagnostics Report” on page 68.

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 incorrect certificate store. In general, information in the event log helps you trace a record of activity leading up to the event of failure.

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. Open the **Secure Gateway Configuration Wizard**.
3. Select the products you want to secure and then click **OK**.
4. On the **Secure Gateway configuration level** screen, select **Advanced**.
5. In the **Select server certificate** dialog box, select the certificate the Secure Gateway is configured to use and click **View**.
6. Check that the value in the **Issued To** field matches the FQDN of this server.
7. 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.
8. 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.

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 load balance 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 "Secure Gateway Keep-Alive Values and Citrix XenApp" on page 79.

Performance Issues with Transferring Files Between a Client Device and a Citrix XenApp Server

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.

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/.

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

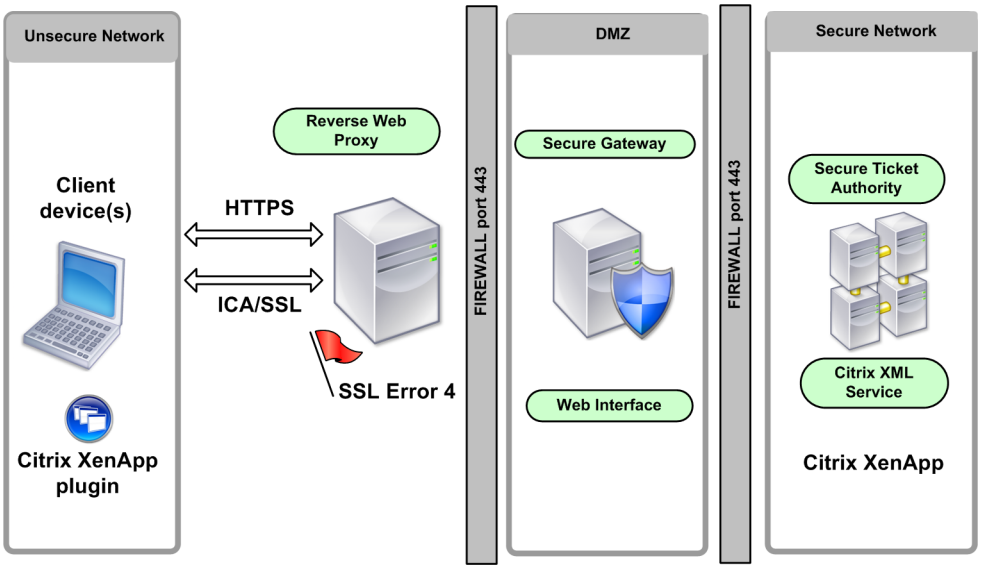
You may find duplicate entries for client connection attempts in the Secure Gateway application and performance logs. Duplicate entries can occur in the following situations:

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

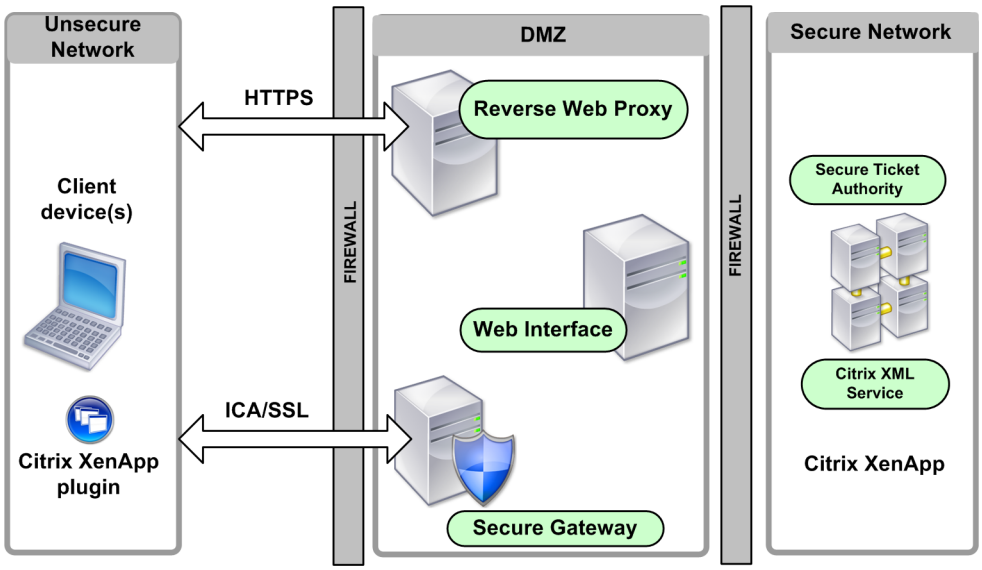
The Secure Gateway views the reverse Web proxy as a "man in the middle" that compromises the integrity of the ICA/SSL network stream. This causes the SSL handshake between the client and the Secure Gateway to fail.

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.

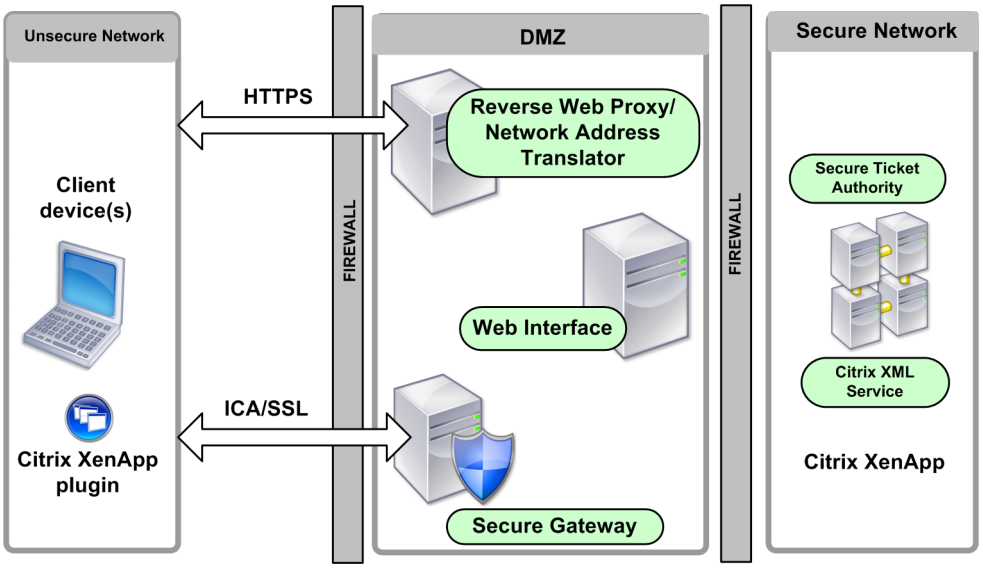


Correct placement of the Secure Gateway, which is parallel to the reverse Web proxy.

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 Secure Gateway users. To cross the Secure Gateway, users must first satisfy the reverse Web proxy and log on to 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 from 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://support.citrix.com/ for available technical support options.

Digital Certificates and the Secure Gateway

SSL and TLS are leading Internet protocols providing security for e-commerce, Web services, and many other network functions. The SSL/TLS protocol uses cryptography to secure communications. Cryptography provides the ability to encode messages to ensure confidentiality. To establish an SSL/TLS connection, you need a digital certificate.

For more information about obtaining, exporting, and installing security certificates for your operating system, consult the Microsoft TechNet library available at http://technet.microsoft.com.

Understanding SSL and TLS

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 U.S. 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.

Understanding Cryptography

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.

Understanding 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 International Telecommunication Union (ITU) standards. The certificate contains information that includes the:

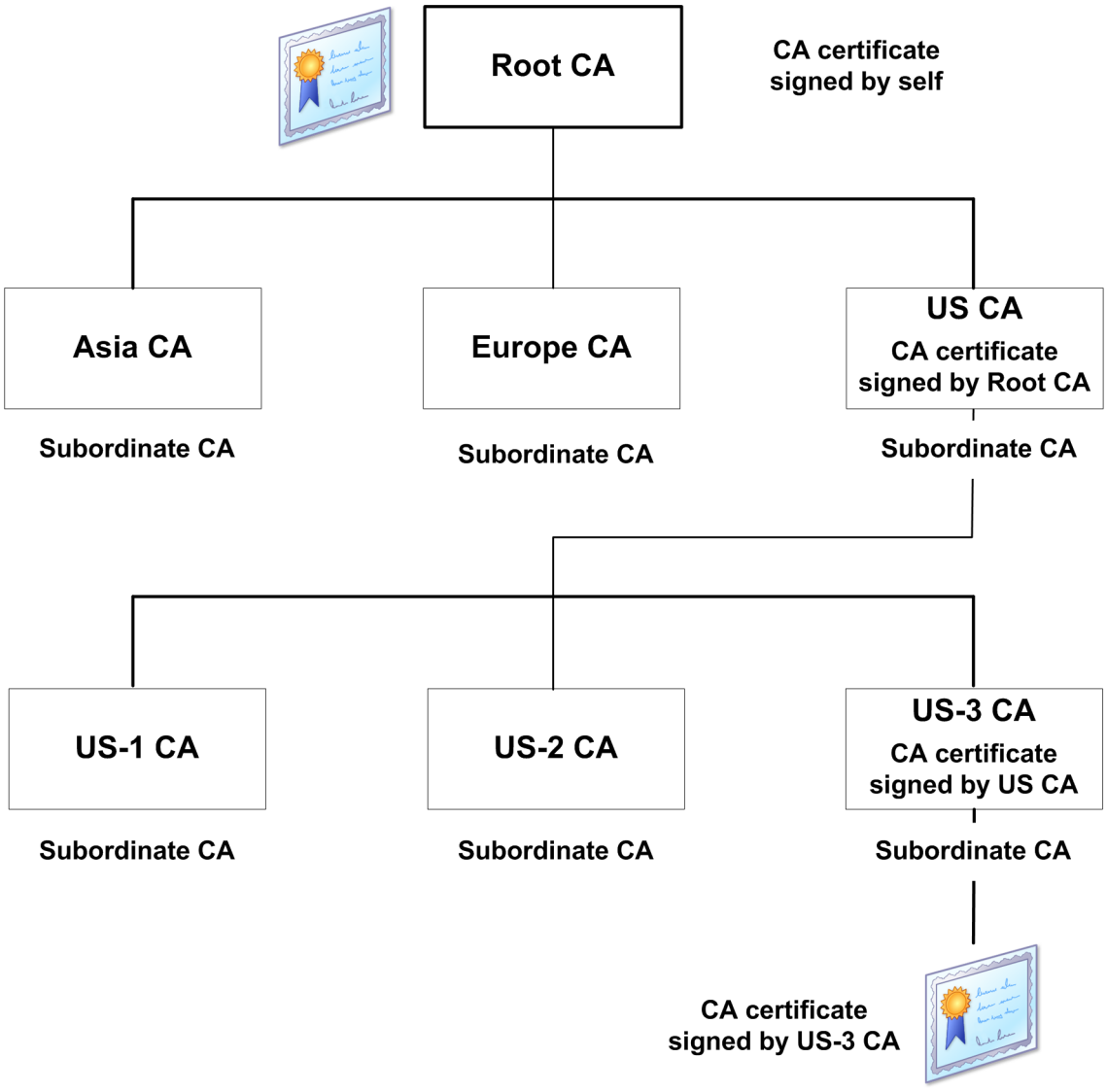
- **Issuer**. The organization that issues the certificates.
- **Subject**. The party that is identified by the certificate.
- **Period of validity**. The certificate's start date and expiration date.
- **Public key**. The subject's public key used to encrypt data.
- **Issuer's signature**. The CA's 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.



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.

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 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 or the reputation of a particular public CA

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 whom they can call if there are queries.

Obtaining and Installing 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.

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.

Certificate Considerations

Consider the following before obtaining and installing certificates:

- When requesting a certificate, 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.
- 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.

- Typically, the procedure for generating a key pair requires you to specify a password to encrypt the pair. The password prevents any person with access to the keypair data from extracting the private key and using it to decrypt SSL/TLS traffic to and from your server. Ensure that you store the password in a secure location.
- 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. Use the proper procedures or wizard as specified by your operating system to place certificates in the correct store on local computers. Do not attempt to import the server certificate 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.

Obtaining and Installing 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.

Support for Wildcard Certificates with the Secure Gateway

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

Relay mode, a feature of Citrix XenApp, 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.

Modes of Operation for the Secure Gateway Proxy

You can use the Secure Gateway Proxy in either normal mode or relay mode. Normal mode provides strong security and is the recommended mode of operation. Relay mode provides more flexibility in the way the Secure Gateway is used at the expense of ticketing support.

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 XenApp.

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

The Secure Gateway Proxy is installed on a stand-alone 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 XenApp.

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

When to Use Relay Mode

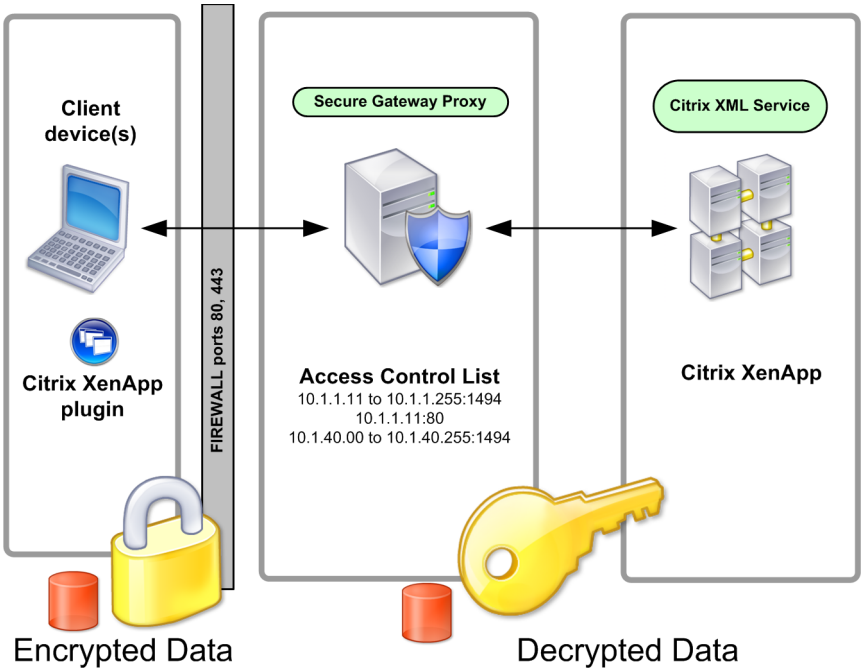
Use the Secure Gateway in relay mode only when:

- 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 Relay Mode Works

To use the Secure Gateway Proxy in relay mode, install the Secure Gateway Proxy on a stand-alone server. The figure below illustrates the communications that take place between the client, the Secure Gateway Proxy, and a server farm in relay mode.



Relay mode communications with the Secure Gateway Proxy and a server farm.

- A remote user connects to the Secure Gateway Proxy server on port 443 and requests access to a published application or a Citrix XenApp 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 XenApp 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.

Installing the Secure Gateway Proxy in Relay Mode

Before installing the Secure Gateway Proxy, compile all of the required information to correctly configure the Secure Gateway Proxy.

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

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.

Print and fill out the Secure Gateway Pre-Installation Checklist. Keep the completed checklist near when you install the Secure Gateway Proxy.

A server certificate must be installed on the Secure Gateway Proxy and a root certificate on the client device. For instructions about obtaining and installing certificates, see "Digital Certificates and the Secure Gateway" on page 95.

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.

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 from port 443. If both IIS and the Secure Gateway Proxy use port 443, client connections fail.

2. Install the server certificate.

See “Getting Certificates” on page 102 for information about how to install certificates.

3. Install the Secure Gateway Proxy as described in “Installing the Secure Gateway or Secure Gateway Proxy” on page 43.
4. Follow the instructions in the configuration wizard to complete the installation.

Immediately after installation, the Secure Gateway Proxy Configuration wizard starts.

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 XenApp. 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. In the **Configure allowed outbound connections** dialog box, click **Add** 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 XenApp server. To secure the traffic between the Secure Gateway Proxy and Citrix XenApp, click **Secure traffic between the server and the Secure Gateway Proxy**. Click **OK** and then click **Next**.

    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.

To start or stop the Secure Gateway Proxy Service manually

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**

To run the Secure Gateway Proxy Configuration wizard

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.

1. Click **Start** and locate the **Secure Gateway Proxy Configuration** wizard.
2. Make the necessary changes. When the wizard completes, click **Finish** to restart the Secure Gateway Proxy.

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 Program Neighborhood 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. On the **Start** menu, locate **Program Neighborhood**.
2. Double-click **Application Set Manager**.
3. Double-click **Custom ICA Connections** and then double-click **Add ICA Connection** to start the **Add New ICA Connection** wizard.

4. Select the type of connection to use.
5. 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.
6. 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.
7. Follow the rest of the steps in the wizard to complete configuring the ICA connection.

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. On the **Start** menu, locate **Program Neighborhood**.
2. On the **File** menu, click **Application Set Settings**.
3. In the **Network Protocol** drop-down list, select **SSL/TLS+HTTPS**.
4. Click **Add**, type the name of the server and port, and then click **OK**.
5. 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.
6. Click the **Default Options** tab. Clear the **Enable session reliability** check box.

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

7. 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

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

1. Open the .ica file using a text editor such as Notepad.
2. Create or modify the following entries:

[Application Name]	Section containing published application settings
SSLProxyHost=	Value specifying the Secure Gateway relay server and port to which you can connect; for example, csgwy.company.com:443
SSLEnable=	Default value is On; do not change.

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.

3. Save and close the .ica file.

To test relay mode operation

1. Ensure that the client device is configured to connect through Secure Gateway. See “Configuring Client Devices” on page 114 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.

If you have trouble launching an ICA connection or a connection fails, see “Troubleshooting the Secure Gateway” on page 87 for information about known problems and typical troubleshooting procedures.

Index

A

accelerators cards, SSL 79
access control list 112
access logs 71–72
    CGP 72
    description 13
    HTTP 72
    SOCKS 73
asymmetric encryption 97
audit logging 15
authentication 11, 98
    description 15
authorization
    description 15

C

CAs. See certificate authorities
certificate authorities 98–99
    public 102
    subordinate 99
certificate revocation lists 101
certificates 98
    certificate chains 99
    chain 99
    content 99
    double-hop DMZ 43
    expiration 101
    hierarchy 99
    intermediate 100
    management 13
    obtaining 102
    private 102
    renewal 101
    requirements 28
    revocation lists 101
    root 98
    server 98
    single-hop DMZ 42
    subordinate 100
    trial period 103
    verification process 102
    wildcard 13, 105
    X.509 103
    .cer format 103
    .pfx format 103
CGP access log 72
chain certificates 99
cipher
    description 96
ciphersuites 81–82
    COM 81
    GOV 81
    restricting 82
Citrix XML Service
    description 12
client connections
    disconnect 61
    double-hop DMZ 22
    relay mode 114
    to XenApp 20
client operating system requirements 27

communications links, securing 14
compatibility
    Citrix products 28
components
    for Presentation Server 19
configuring
    Secure Gateway 45
connecting with
    Presentation Server 17
connection information 13, 72
    CGP 72
    HTTP 72
    SOCKS 73
connection keep-alive settings 79
connections 61
cryptography 95–96
    asymmetric encryption 97
    public key 96
    secret key 96
    symmetric key 96

D

demilitarized zone 11, 81
deployment
    improvements 13
    Presentation Server 31
    testing 39
diagnostic tools 14, 68
Digital certificates. See certificates
DMZ. See demilitarized zone
DNS. See Domain Name Server
Domain Name Server 20
double-hop DMZ
    client connections 22
    planning 21
    Presentation Server 33, 36
    Web Interface 23

E

encryption 11, 15, 81
    asymmetric 97
    public key 98
error messages 71

F

fault tolerance 15, 76
Federal Information Processing Standard 95
FIPS 140. see Federal Information Processing Standard
firewalls
    forwarding mode 75
    ICA traffic 75
    ICA traffic, supporting 75–76
    traversal 15, 75
FQDN. See Fully Qualified Domain Name
Fully Qualified Domain Name 20

H

high availability 76
HTTP access log 72

I

ICA
    file 20
IETF. see Internet Engineering Taskforce
indexing
    preventing 85
information
    connections 61
    sessions 61
installing
    configuration 45
    pre-installation checklist 42
    preparation 42
    procedure 43
    Secure Gateway Proxy 43
    sequence 43
    Web Interface 31, 33
Internet Engineering Taskforce 95
Internet Information Services 34
    access 32
    lock down 84
    relay mode 110
Internet security protocols 95
ISO X.509 protocol 98

K

keep-alive parameters 79
    registry keys 80

L

load balancing 76–77
    benefits 77
    certificate requirements 78
    Secure Gateway array 77
    SSL accelerator cards 79

M

management and report tools 14
Management Console 61

P

performance monitoring 63
    counters 64
    description 13
Personal Information Exchange format 103
PKCS #12. see Personal Information Exchange format
PKI. see Public Key Infrastructure
pre-installation checklist 42
preventing
    indexing 85
private certificate authority 102
public certificate authority 102
public key encryption 98
Public Key Infrastructure 18, 95

R

redundancy 76
relay mode
    benefits 107
    certificates required 110
    configuration 111
    configure client devices 114
    default encryption level 115
    description 14
    how it works 108
    installing 110
    modify configuration 114
    port 110
    understanding 107
requirements
    client software 27
    server hardware 26
    server software 26
reverse Web proxy
    SSL Error 4 90
root certificate 98–99, 104

S

search engines
    preventing indexing 85
Section 508 compliance
    description 14
Secure Gateway
    components 12
    configuration guidelines 41
    description 12
    double-hop DMZ 21
    installation guidelines 41
    Management Console 61
    planning 17
    planning with Presentation Server 18
    pre-installation checklist 42
    use with Presentation Server 12, 17
Secure Gateway Proxy
    description 12
    installation 43
    load balancing 78
    modes of operation 107
    normal mode 107
    planning 21
    relay mode 107
Secure Sockets Layer. See SSL
Secure Ticket Authority
    changes 13
    Internet Information Services requirements 34
    session tickets 20
security recommendations 81
server certificate 98
    installing 103
server farm
    description 18, 31
    setting up 34
server hardware requirements 26
server requirements 26
session information 61
session reliability
    description 14
session tickets 20
sessions 61
Single point of entry 15
single-hop DMZ
    Presentation Server 31
    Web Interface 31, 33
SOCKS access log 73
SSL 18, 83, 95
    accelerator cards 79
    support 13
SSL error 4 90
system requirements 26

T

TCP/IP keep-alives 80

test certificates 103
TLS 18, 83, 95
Transport Layer Security. See TLS
troubleshooting
    application log 87
    CSG0188 error 88
    diagnostics 87
    network address translator 93
    SSL error 4 90
    support 93
    Windows XP Service Pack 2 90

W

Web Interface
    connecting 38
    connecting with 17
    double-hop DMZ 23
    firewall 32
    installing 31, 33
    proxy settings 32
    setting up 36, 38
    Smart Card authentication 32
wildcard certificates 13, 105
Windows operating system
    server 26
Windows registry
    keep-alive parameters 80
Windows XP Service Pack 2 90

X

X.509 standard 99

Z

.cer format certificate 103
.pfx format certificate 103