Secure Gateway Pre-Installation Checklist

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)

Secure Gateway Pre-Installation Checklist

This checklist helps you compile the tasks and planning information you need before you install the Secure Gateway.

Space is provided so that you can check off each task as you complete it. Note the configuration values needed during the installation and configuration of the Secure Gateway. General steps are also provided for the tasks you need to perform to ensure Citrix XenApp, the Web Interface, Citrix XenApp plugins, and other clients are configured and functioning correctly.

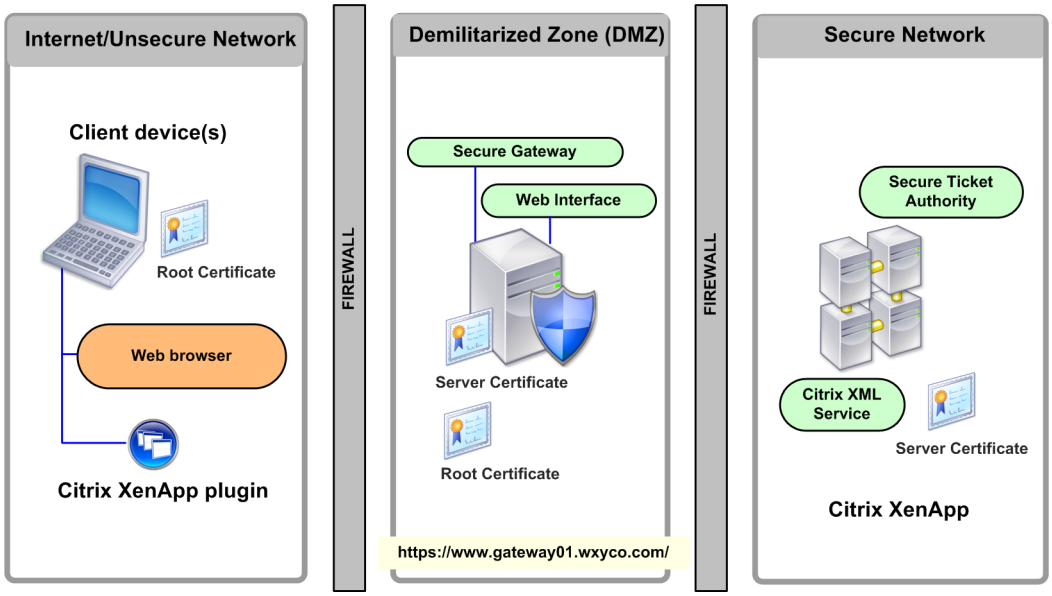
Citrix recommends that you print and complete this checklist before proceeding with the installation. See the *Secure Gateway for Windows Administrator's Guide* for instructions about installing and configuring the Secure Gateway.

Choose the Option that Represents Your Secure Gateway Deployment

Pre-installation tasks required to set up and evaluate the Secure Gateway in a Secure Access to Citrix XenApp scenario are described in this document. In this scenario, you deploy the Secure Gateway for Windows to provide secure access to published resources within a server farm. Print and complete information as you follow the instructions in this checklist.

For information about advanced deployment scenarios supported by the Secure Gateway for Windows, including double-hop DMZ deployment and securing all communication links, see the *Secure Gateway for Windows Administrator's Guide*.

Secure Access to Citrix XenApp



This illustration shows a typical Secure Gateway deployment used to secure a server farm. The network is divided into three segments. The unsecured network contains a user device running a Web browser and Citrix XenApp plugin such as the Citrix XenApp Plugin for Hosted Apps. The demilitarized zone contains the Secure Gateway and Web Interface components, and the secure network contains a server farm running the Citrix XML Service and the Secure Ticket Authority. A firewall separates the unsecured network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed to enable secure communications.

End-User (Client) Devices

☐ 1. Ensure end-user devices meet the installation prerequisites described in the *Secure Gateway for Windows Administrator's Guide.*

☐ 2. Ensure end-user devices have root certificates that correspond to the server certificate on the destination server in the DMZ.

On the Firewall between the Unsecured Network and the DMZ

☐ Ensure port 443 (default SSL port) on the firewall is open between the Internet and the server running the Secure Gateway.

Server Reserved for the Secure Gateway for Windows

☐ 1. Ensure this server meets the installation prerequisites described in the *Secure Gateway for Windows Administrator's Guide.*

☐ 2. Enter the IP address for this server.

☐ 3. Ensure a server certificate with a key bit length of 1024 or higher is installed on the server running the Secure Gateway.

☐ 4. Enter the Fully Qualified Domain Name (FQDN) of this server.

Important: Ensure the FQDN entered matches the FQDN that appears in the **CN** (Common Name) field on the **Subject** line of the server certificate installed on this machine.

☐ 5. **Optional:** If this server communicates with a secure server in the DMZ or the secure network, install a root certificate (that corresponds to the server certificate on the destination server) on this server.

☐ 6. Restart the server on which you installed Secure Gateway.

Server Running the Web Interface

☐ 1. Do you intend to run the Web Interface and the Secure Gateway on a single server (Yes/No)?

If you answered **Yes**, skip to Step 6 of this procedure.

☐ 2. If you are running the Web Interface on a separate server, enter its IP address.

☐ 3. Do you plan to secure communications between the Web Interface and the Secure Gateway (Yes/No)?

If you answered **No**, skip to Step 6 of this procedure.

☐ 4. Ensure a server certificate is installed on the server running the Web Interface.

☐ 5. Enter the FQDN of this server.

Important: Ensure the FQDN entered matches the FQDN that appears in the **CN** (Common Name) field on the **Subject** line of the server certificate installed on this machine.

☐ 6. **Optional**. If this server communicates with a secure server in the DMZ or the secure network, install a root certificate (that corresponds to the server certificate on the destination server) on this server.

☐ 7. Ensure the Web Interface is configured to provide access to published applications within a server farm.

On the Firewall between the DMZ and the Secure Network

☐ 1. Ensure port 443 (default SSL port) is open if the Secure Gateway connects to any secure servers in the secure network.

-or-

Ensure port 80 (default HTTP port) is open.

☐ 2. Ensure port 443 is open if the Web Interface connects to any secure servers in the secure network.

-or-

Ensure port 80 (default HTTP port) is open.

☐ 3. Ensure port 1494 is open on the firewall between the Secure Gateway and the server(s) running Citrix XenApp.

☐ 4. If session reliability is enabled, ensure port 2598 is open.

Server Farm

☐ 1. Ensure your server farm is set up and configured for access to published applications.

For help with configuring computers running Citrix XenApp, see the *Citrix XenApp Administrator's Guide*.

☐ 2. Enter the the default virtual directory path /Scripts/CtxSTA.dll. 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.

☐ 3. Enter the port used to communicate with the Secure Ticket Authority (STA).

This is the same port used by the Citrix XML Service.

☐ 4. Do you plan to secure communications between servers in the DMZ and the server(s) running the STA?

If you answered No, enter the FQDN of any server running the STA and skip to Step 8 of this procedure.

☐ 5. Ensure a server certificate is installed on each server running the STA with which the servers in the DMZ will communicate.

☐ 6. Enter the FQDN(s) of the secured server(s) running the STA.

Important: Ensure the FQDN entered matches the FQDN that appears in the **CN** (Common Name) field on the **Subject** line of the server certificate installed on this machine.

☐ 7. Enter the IP address(es) of the server(s) running the STA.

☐ 8. Do you plan to configure an outbound access control list in the Secure Gateway?

If you answered **Yes**, enter the IP address range or IP addresses of the servers to include in the access control list. This list must include all servers with which the servers in the DMZ must communicate.

☐ 9. Is there a firewall separating the Secure Gateway and the computer(s) running Citrix XenApp? (Yes/No)

If you answered **No**, skip the remaining question.

☐ 10. Is the firewall using NAT (Network Address Translation)? (Yes/No)
If you answered **Yes**, do the following:

☐ A. Ensure that **altaddr** is enabled on the computer(s) running Citrix XenApp. The altaddr command is used to query and set the alternate (external) IP address that a computer running Citrix XenApp returns to clients requesting this information. The alternate address is an external address used by clients outside a firewall.

☐ B. Enable alternate addressing on the server running the Web Interface. See the *Web Interface Administrator's Guide* for instructions about configuring alternate addressing.