Installation Guide Supplement

for use with

Integrated Citrix® Servers

Websense® Web Security
Websense Web Filter

v7

©1996 -2008, Websense, Inc.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
All rights reserved.

Published 2008
Printed in the United States of America and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense, Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense and Websense Enterprise are registered trademarks of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Citrix, Citrix Presentation Server, and MetaFrame are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds in the United States and other countries.

Novell, Novell Directory Services, eDirectory, and ZENworks are trademarks or registered trademarks of Novell, Inc., in the United States and other countries.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

This product includes software developed by the Apache Software Foundation (www.apache.org).
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

WinPcap

Copyright (c) 1999 - 2008 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2008 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Politecnico di Torino, CACE Technologies nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" 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 COPYRIGHT OWNER OR CONTRIBUTORS 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.

Contents

Chapter 1 **Citrix Integration 5**

Supported Citrix versions 5
Client computers 6
Filtering Citrix server users 6
Filtering both Citrix and Non-Citrix Server Users 8
Installation 8
Installing Websense software to integrate with Citrix 8
Installing the Citrix Integration Service on a Citrix Server 9
Configuring user access on Citrix servers 9
Initial Setup 10
Blocking Internet access when Filtering Service is unavailable 11
Configuring for Citrix Virtual IP Addresses 11

Chapter 2 **Combining Citrix with Another Integration 13**

Combined integrations overview 13
Deployment scenarios 13
Deploying with Network Agent 14
Configuration 14
Installing the non-Citrix integration 14
Configuring the non-Citrix integration 15

Index **19**

1 Citrix Integration

This supplement provides additional information for installing and setting up Websense® Web Security™ or Websense Web Filter™ with the Citrix® MetaFrame® Presentation Server or Citrix Presentation Server™. Installing Websense software integrated with a Citrix server allows you to apply user-based Web filtering policies to users who access the Internet through a Citrix server.

See the Websense *Installation Guide* for basic instructions.

- **Websense Citrix Integration Service**: The Integration Service must be installed on each Citrix server to allow that server to communicate with Websense Filtering Service.
- **Network Agent**: Manages Internet protocols that are not managed by your Citrix server integration. It can also detect HTTP network activity and instruct Filtering Service to log this information.

> **Note**
> If your Citrix server runs applications that use protocols other than HTTP, FTP, or SSL, Network Agent can apply protocol filtering to those applications based on a computer or network policy, or the Default policy. It cannot apply user and group based policies to protocol filtering of applications running on the Citrix server.

Supported Citrix versions

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

Client computers

- To be filtered by Websense software, a Citrix client computers must access the Internet through a Citrix server.
- Non-Citrix clients in the network also may be filtered by the same installation of Websense software. This instance can be either Websense Stand-Alone Edition, or integrated with another product. See *Chapter 2: Combining Citrix with Another Integration* for more information.

Filtering Citrix server users

Websense software integrated with a Citrix server can monitor individual Citrix users for HTTP, HTTPS, FTP, and SSL. Network Agent can be used to filter other protocols, based on policies set for the server.

The machines running as Citrix servers communicate with Websense Filtering Service using a Websense component called the Citrix Integration Service, which is installed on the Citrix server machine.

When Websense software is integrated with Citrix:

- A recommended maximum of 10 Citrix servers can be connected to one Filtering Service. This number can be configured and depends on the user load.

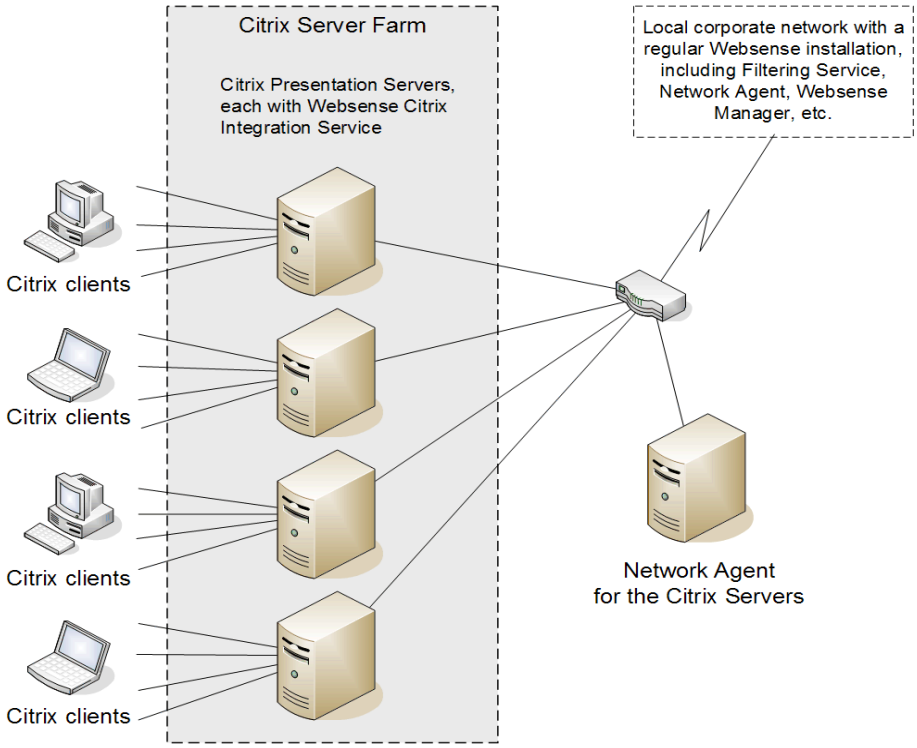
  Multiple Filtering Services are needed if more than 15 Citrix servers are used, with each Citrix server handling about 20 to 30 Citrix users.
- The Filtering Service and Network Agent monitoring Citrix traffic should be installed on a dedicated machine, and not on a machine running as a Citrix server.
- The Filtering Service and Network Agent monitoring Citrix traffic use the same Policy Broker, Policy Server, User Service, and other Websense components that are used to monitor non-Citrix traffic.
- Separate Network Agents must be used to monitor non-Citrix traffic.
- Do not configure a separate Websense integration to filter HTTP, HTTPS, FTP, or SSL requests from Citrix servers.
- If you want to use Network Agent to filter protocol traffic from the Citrix Servers:
  - Network Agent must be located where it can see all of the traffic between the Citrix servers and the Filtering Services. For example, the machine running Network Agent could be located on a span port on the same switch as the machines running Filtering Service.
  - If the Citrix server is configured to use virtual IP addresses, configure Network Agent to monitor the entire range of the IP addresses. Also, a single policy should be set for this range. See the Network Configuration topic in Websense Manager Help for instructions on configuring IP ranges for Network Agent.

- If you are running Websense Stand-Alone Edition, a separate instance of Network Agent must be installed to monitor users of the Citrix servers. Do not monitor non-Citrix traffic with this Network Agent.

  While Network Agent can be used to filter protocols for Citrix, user-based and group-based policies cannot be applied. Policies can be applied to individual computers and network ranges, identified by IP addresses or IP address ranges. Otherwise, the Default policy is applied to all users.

  Also, Network Agents monitoring non-Citrix traffic (users who access the Internet without going through a Citrix server) must not be used to monitor Citrix traffic.

This diagram shows a typical deployment to filter users who access the Internet through a Citrix server. To simplify the diagram, not all individual Websense components are shown.



Typical Citrix Integration

The main Websense filtering components are installed on a separate, dedicated machine that can communicate with all of the Citrix server machines, and the non-Citrix users, if applicable. The Websense Citrix Integration Service must be installed on each Citrix server to allow it to communicate with Filtering Service. No other Websense components can be installed on the Citrix server machines.

Filtering both Citrix and Non-Citrix Server Users

If your network includes some users who access the Internet via a Citrix server, and others who access the Internet through another gateway (firewall, caching appliance, or proxy server), the integrations can be configured to work together.

- To install the Citrix Integration Service on a Citrix Server, see page 9.
- If you have Citrix users and non-Citrix users in your network, the same Websense components, except for Network Agent, can be used for both sets of users. A separate installation of Network Agent is needed for the Citrix users. See *Installing Websense software to integrate with Citrix*, page 8, for instructions.
- To install Websense software for non-Citrix users, refer to the *Installation Guide* and the supplement for the integration product, if applicable.
- To configure the Websense components installed with the non-Citrix integration to communicate with Citrix, refer to the section pertaining to your integration in *Chapter 2: Combining Citrix with Another Integration*.

Installation

Most Websense components must be installed on a separate machine from the Citrix server. Only the Citrix Integration Service is installed on each Citrix server machine.

If Websense will be filtering both Citrix and non-Citrix users, refer to *Chapter 2: Combining Citrix with Another Integration* after installing the Websense Citrix Integration Service.

Installing Websense software to integrate with Citrix

If you are installing the Websense Stand-Alone Edition (no non-Citrix integration), the Websense software must be installed before the Websense Citrix Integration Service is installed on the Citrix servers. Network Agent must be installed on a separate machine.

1. Start the Websense installer, and follow the prompts. See the *Installation Guide* for basic instructions.
2. Select a **Custom** installation.
3. Select **Policy Broker**, **Policy Server**, **Filtering Service**, and **User Service**, and any other Websense components you want to install. Do **not** select Network Agent.
4. Select **Integrated** as the integration option, and select the **Citrix** integration.
5. Follow the onscreen instructions to complete the installation.
6. On a separate machine, start the Websense installer.
7. Select a **Custom** installation.
8. Select **Network Agent** as the component to install.
9. Follow the onscreen instructions to complete the installation.

Installing the Citrix Integration Service on a Citrix Server

After the Filtering Service is installed on a separate machine, the Citrix Integration Service must be installed on every Citrix server machine in your network that will be integrated with Websense software. The Citrix Integration Service can be installed only on Windows-based Presentation Servers.

1. Log on with **local** administrator privileges to the machine running Citrix Presentation Server or Citrix MetaFrame Presentation Server.
2. Close all applications and stop any anti-virus software.
3. Run the Websense installer.
4. Select a **Custom** installation.
5. From the components list, select **Filtering Plug-in** to install the Citrix Integration Service.
6. Enter the IP address of the Filtering Service machine, and the port is communicates over.

> **Note**
> The default port number (15868) is displayed. If you installed Filtering Service with a different port number, enter that port number here.

7. Follow the onscreen instructions to complete the installation.
8. If you stopped your anti-virus software, be sure to start it again.

Repeat this procedure for each Citrix server in your server farm.

Configuring user access on Citrix servers

To allow Websense software to apply policies to individual users and groups defined in a directory service, you must configure user access for your published applications in Citrix. The procedure varies according to the Citrix version.

Citrix Presentation Server v4.0

User access is configured in the Citrix Publish Application wizard. See the Citrix documentation for more information on this wizard.

1. Log on to the Citrix server as an administrator.
2. Open the Publish Application wizard.
3. Go to the Specify Users screen.

4. Specify all users who can access the application so that they must log on with **domain** credentials.

Important

- Do **not** allow users to log on with local or administrative credentials.
- Do **not** allow anonymous connections.

Citrix Presentation Server v4.5

Following is an overview of the procedure for configuring user access in Citrix Presentation Server v4.5. See the Citrix documentation for more information on this wizard.

1. Log on to the Citrix server Access Management Console as an administrator.
2. Select **Applications** in the left navigation pane, or select a particular application you have published.
3. Under **Other Tasks**, select **Permissions**.
4. Click **Add** in the Permissions for folder “Applications” dialog box.
5. Click **Add** in the Add access to folder dialog box.
6. Select the computer or domain for adding users, and mark the **Show users** check box.
7. Select a user, and click **Add** to move that user into the Configured Accounts list.
8. Repeat step 7 to add other users to the Configured Accounts list.
9. Click **OK** twice to save the newly added users.

If you need to change the permissions for a user, use the Edit button in the Permissions for folder “Applications” dialog box.

Important

- Do **not** allow users to log on with local or administrative credentials.
- Do **not** allow anonymous connections.

Initial Setup

- You can configure how Internet requests from Citrix clients are handled when Filtering Service is unavailable. See *Blocking Internet access when Filtering Service is unavailable*, page 11, for instructions.
- If the integrated Citrix server is configured to use virtual IP addresses, additional Websense configuration is required. See *Configuring for Citrix Virtual IP Addresses*, page 11, for instructions.

Blocking Internet access when Filtering Service is unavailable

If the Citrix Integration Service is unable to connect with Filtering Service, the Integration Service fails open by default. All Internet requests from users on Citrix client machines are permitted.

You can change this default setting so that all traffic is blocked when connectivity with Filtering Service is lost. To make this change, perform the following steps on each Citrix server machine running the Citrix Integration Service:

1. On the Citrix server machine, go to the `\bin` folder in the Websense installation directory (by default, `\Websense\bin`).
2. Open the `wscitrix.ini` file in a text editor.
3. Change the value of the `FailClose` parameter to `true`.

   If the Citrix Integration Service loses connectivity with the Filtering Service, all Internet requests are blocked.
4. Save your changes.
5. Restart the Citrix Integration Service in the Windows Services dialog box.

Configuring for Citrix Virtual IP Addresses

If an integrated Citrix server is configured to use virtual IP addresses, you must configure Network Agent to monitor the entire range of the IP addresses.

You should also set a single Websense filtering policy for this range of virtual IP addresses.

See the Network Configuration topic in Websense Manager Help for instructions on adding and editing IP address ranges for Network Agent, and configuring policies for specific IP address ranges.

2 Combining Citrix with Another Integration

Websense software can be set up to filter both Citrix and non-Citrix users. This chapter provides the instructions for configuring the Stand-Alone Edition or a Websense integration to work with the Citrix integration.

Combined integrations overview

Some configurations allow a single installation of Websense software in the same network to filter both Citrix users and non-Citrix users. Citrix users may be working from remote locations, while non-Citrix users may be located in the office where Websense software is installed.

Deployment scenarios

The corporate network (non-Citrix users) can access the Internet through an integration, such as Cisco® PIX®, Check Point®, Microsoft® Internet Security and Acceleration (ISA) Server 2006, or Network Agent (Websense Stand-Alone Edition). That integration sends Internet requests to Websense software for filtering.

Citrix clients access the network through a Citrix Presentation Server or Citrix MetaFrame Presentation Server. Depending on the number of Citrix users, the access may be through one server, or through a server farm consisting of multiple Citrix servers. For more information on deploying Websense software with Citrix, see *Filtering Citrix server users*, page 6.

Websense filtering is accomplished by installing the Websense Citrix Integration Service on each Citrix server. See *Installing the Citrix Integration Service on a Citrix Server*, page 9, for instructions.

In lower volume networks, each Integration Service communicates with the same Filtering Service. The non-Citrix users can be pointed to the same instance of Filtering Service as the Integration Services.

Deploying with Network Agent

If Websense Stand-Alone Edition is installed using Network Agent for filtering, separate instances of Network Agent are needed for the Citrix and non-Citrix users. See *Stand-Alone Edition configuration*, page 17, for configuration information.

Configuration

If Websense software is used to filter both Citrix users and users accessing the Internet through another integration, the non-Citrix Websense integration must be running before the Citrix Integration Service is installed.

1. Install Websense software with the non-Citrix integration first. See the *Websense Installation Guide Supplement* for your integration product for instructions.
2. Next, install the Citrix Integration Service on each Citrix server. See *Installing the Citrix Integration Service on a Citrix Server*, page 9, for instructions.

   This component sends requests from Citrix clients to Filtering Service for filtering. Up to 10 Integration Services can be pointed to the same Filtering Service. If more than 10 Citrix servers are deployed, then additional Filtering Services can be used.
3. Configure the non-Citrix integration, as described in this chapter, to ensure that requests coming from the Citrix clients are not filtered twice.

Installing the non-Citrix integration

Before the Citrix environment can be integrated, Websense software must be installed with the non-Citrix integration. If an older version of Websense software is already installed, upgrade to v7.0.

The Stand-Alone Edition is installed in a non-integrated environment where Network Agent is used for filtering. See the Websense *Installation Guide* and *Upgrade Guide* for more information.

Installation and upgrade instructions for integrated editions are found in the *Installation Guide* supplement for each integration.

Websense, Inc., supports the following integrations with the Citrix Integration Service. This chapter provides the configuration steps needed to enable the non-Citrix and Citrix integrations to work together in the same network:

- Cisco PIX v6.3. See *Cisco PIX configuration*, page 15.
- Check Point FireWall-1 NGX. See *Check Point FireWall-1 configuration*, page 16.
- Microsoft Internet Security and Acceleration (ISA) Server 2006. See *Microsoft ISA configuration*, page 16.
- Stand-Alone Edition (Network Agent). See *Stand-Alone Edition configuration*, page 17.

Configuring the non-Citrix integration

Before the integrations can be used together, the non-Citrix integration must be set up to prevent Internet requests sent via the Citrix servers from being filtered twice.

A request from a Citrix client is passed to the Citrix server. The Citrix Integration Service sends the request to Filtering Service for filtering. The request is either blocked or permitted by Websense software. Simultaneously, the Citrix server sends the same request to the non-Citrix integration, which must be configured to allow the request pass to the Internet without sending it to Websense software for filtering.

Cisco PIX configuration

Use a console or TELNET session to configure your Cisco PIX Firewall (security appliance). This configuration has been tested for Cisco PIX version 6.3 and later.

1. Access the security appliance.
2. Enter your login password.
3. Put the security appliance into privilege EXEC mode by entering **`enable`**, followed by your enable password.
4. Activate the configure mode by entering: **`configure terminal`**.

> **Note**
> For help with individual commands, enter **`help`** followed by the command. For example, **`help filter`** shows the complete syntax for the **`filter`** command, and explains each of the options.

5. Use the **`filter url except`** command with the IP address or addresses for the Citrix servers to disable the second filtering by Websense software of requests from Citrix users.
   - For a group of Citrix servers in a server farm, you can enter a range:

     `filter url except` *<IP address range>*
   - For one or two Citrix servers, you can add the commands individually:

     `filter url except` *<internal IP address> <internal subnet mask> <external IP address> <external subnet mask>*

     where the *internal IP address* and *subnet mask* refer to the Citrix server, and the *external IP address* and *subnet mask* are for a secondary machine, other than the PIX firewall, that is used for Internet access. The external settings are generally set to zero:
     `0.0.0.0 0.0.0.0`.
6. Type **`exit`** to exit the configure mode.

See the Cisco PIX documentation and the *Websense Installation Guide Supplement for use with Integrated Cisco® Products* for more information on this integration.

Check Point FireWall-1 configuration

To configure Check Point FireWall-1 to work properly with a Citrix integration, you must define a rule on FireWall-1 to allow requests from the Citrix server to pass to the Internet without sending those requests to Websense software for filtering.

- Using the Firewall-1 SmartDashboard™ (or Policy Editor in older versions) add the Citrix Presentation Servers to the Allow Rule. Do **not** add the Presentation Servers to the Block rule.

See the CheckPoint FireWall-1 documentation and the Websense *Installation Guide Supplement for use with Integrated Check Point Products* for more information.

Microsoft ISA configuration

The Websense ISAPI plug-in must be set to ignore traffic from the Citrix servers. This configuration is done by adding the host name of each Citrix server to the `isa_ignore.txt` file on the Microsoft ISA Server machine.

Also, ensure that none of the Citrix servers are set to use the Microsoft ISA Server machine as a proxy server.

1. On the Microsoft ISA Server machine, open the `isa_ignore.txt` file in a text editor. This file is located in the following folder: `WINDOWS\system32`.

   Note

   The default `isa_ignore.txt` file installed with Websense software contains the following URL: `url=http://ms_proxy_intra_array_auth_query/`

   Do not delete this URL. It is used by ISA Servers in a CARP array for communication. This URL must be ignored by Websense software to allow filtering and logging to work properly when multiple ISA Servers are deployed in an array.

2. Enter the host name for each Citrix server on its own line in the `isa_ignore.txt` file.

   Important

   You must enter each host name in the exact same format that the ISA Server passes it to Filtering Service.

   Use the following format: **`hostname=`**<*host_name*>

   where <*host_name*> is replaced by the name of the machine hosting Citrix server.

3. Restart the ISA Server machine.

See the Microsoft ISAPI documentation and the *Websense Installation Guide Supplement for use with Integrated Microsoft® Products* for more information.

Stand-Alone Edition configuration

If Websense Stand-Alone Edition is running, separate instances of Network Agent must be installed to filter Citrix and non-Citrix users. The Network Agent monitoring non-Citrix users must be set to ignore the Citrix servers. This configuration allows protocol filtering of both Citrix and non-Citrix requests.

1. Open Websense Manager, and go to **Settings** > **Network Agent**.
2. In the left navigation pane, select the IP address of the NIC used for monitoring Internet requests to open its Local Settings page.
3. Under **Monitor List Exceptions**, add each Citrix server that Network Agent should exclude from monitoring.
   a. To identify a machine, click **Add**, and then enter the Citrix server's IP address, or a range of IP addresses for a group of Citrix servers in a server farm. Then, click **OK**.
   b. Repeat this process until all Citrix servers have been added, either individually or as part of a range.
4. Click **OK** to cache your changes and return to the NIC Settings page. Changes are not implemented until you click **Save All**.

See the Network Agent section under the Network Configuration topic in Websense Manager Help for instructions on configuring NIC settings.

Index

C

Citrix
  filtering fail closed parameter, 11
  server configuration, 9
  user access, 9
  virtual IP addresses, 11
Citrix Integration Service
  installation of, 9
Citrix Plug-in
  deployment of, 5

D

deployment
  filtering Citrix and non-Citrix server users, 8
  filtering Citrix server users, 6

F

FailClose parameter
  Citrix Integration Service, 11
filtering
  Citrix and non-Citrix server users, 8
Filtering Plug-in
  deployment of, 5

I

installation
  Citrix Integration Service, 9

N

Network Agent
  defined, 5

V

Virtual IP addresses in Citrix, 11

W

Websense Filtering Plug-in, 5
wscitrix.ini file, 11