websense®

Deployment Guide

Websense® Web Security
Websense® Web Filter

v7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

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 6,606,659 and 6,947,985 and other patents pending.

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.

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

Sun, Sun Java System, Sun ONE, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

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

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

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.

Citrix, Citrix Presentation Server, and MetaFrame are trademarks or registered 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.

Cisco, Cisco Systems, Cisco PIX Firewall, Cisco IOS, Cisco Routers, and Cisco Content Engine are registered trademarks or trademarks of Cisco Systems, Inc., in the United States and certain other countries.

Check Point, OPSEC, FireWall-1, VPN-1, SmartDashboard, and SmartCenter are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Inktomi, the Inktomi logo, and Inktomi Traffic Server are registered trademarks of Inktomi Corporation.

Network Appliance is a trademark and NetCache is a registered trademark of Network Appliance, Inc., in the U.S. and other countries.

This product includes software distributed by the Apache Software Foundation (**http://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.

Contents

List of Figures

List of Tables

1 Introduction

Use this guide to plan your Websense software deployment before installation. The guide provides an overview of how Websense software can be deployed in a network, as well as operating system and hardware requirements.

This guide applies to Websense Web Security and Websense Web Filter, Version 7. References to *Websense software* or *Websense Web Security* include both products, unless otherwise indicated.

✓ **Note**

The technical papers and other documents mentioned in this guide are available from the Documentation > Planning, Installation, and Upgrade folder in the Websense Knowledge Base (www.websense.com/docs).

Websense software consists of components which work together to monitor Internet requests, log activity, apply Internet usage filters, and report on activity. Websense components can be installed together on one machine, or distributed across multiple machines. The appropriate deployment is determined by the network size and configuration, Internet request volume, hardware available, and filtering needs.

This manual provides system recommendations to optimize Websense component performance. Performance can also be improved by using more powerful machines for resource-intensive components.

This chapter introduces the Websense filtering and reporting components. See also:

- *Chapter 2: General Deployment Recommendations*—operating system requirements for running Websense components, component limits, tips for maximizing performance, plus recommendations for deploying transparent identification agents, Remote Filtering, and the Stand-Alone Edition. Version requirements are also included for various integrations.
- *Chapter 3: Deploying Network Agent*—information for deploying across single and multiple segment networks. Also provides Network Agent placement details, settings, and relationship to hubs, switches and gateways.
- *Chapter 4: Integration Deployment*—overview of deploying Websense software with firewalls, proxy servers, caching applications, network appliances, or other integration products or devices.

A series of supplements to this document provide deployment and hardware recommendations based on network size:

- Small network: 1-500 users, or 1-25 requests per second
- Medium network: 500 - 2,500 users, or 25-125 requests/sec
- Large network: 2,500 - 10,000 users, or 125 - 500 requests/sec
- Enterprise network: 10,000 - 25,000 users, or 500 - 1250 requests/sec
- Very large enterprise network: 25,000+ users, or more than 1250 requests/sec

Requests per second estimates are based on average usage with “medium”—neither light nor heavy—Internet access needs.

✓ **Note**

Deployment recommendations allow for some network growth and an increase in Internet requests.

As your network reaches the upper limits of its size classification (small, medium, and so on), review the deployment documents to ensure an optimal system configuration.

A deployment supplement is also included for Websense Content Gateway. The gateway provides Web and proxy caching, dynamic classification of Web sites, Web 2.0 categorization, and an optional SSL manager. See the Websense Content Gateway documentation for more information on this product.

✓ **Note**

Please contact Websense Sales Engineering for assistance in designing your Websense software deployment. A Sales Engineer can help you optimize Websense component deployment and understand the associated hardware needs.

Websense Components

- Table 1 provides a brief description of the Websense filtering components. This table groups the components into *core* (included in a standard deployment) and *optional*.
- Table 2, on page 14, provides a brief description of the Websense reporting components.

Review these descriptions to better understand the interaction between components. See Table 3, on page 18, and Table 4, on page 23, for information on the operating system versions needed to run these components.

✓ **NOTE**

Certain integrations include Websense plug-ins. These are discussed in Table 9, on page 44.

Table 1 Websense Components

Component	Definition
Core Components	
Policy Database	Stores global Websense software settings (configured in Websense Manager) and policy information (including clients, filters, and filter components). • Is installed in the background with Policy Broker. • Settings specific to a single Policy Server instance are stored separately. In multiple Policy Server environments, a single Policy Database holds policy and general configuration data for multiple Policy Servers.
Policy Broker	Manages requests from Websense components for policy and general configuration information stored in the Policy Database.
Policy Server	• Identifies and tracks the location and status of other Websense components. • Logs event messages for Websense components. • Stores configuration information specific to a single Policy Server instance. • Communicates configuration data to Filtering Service for use in filtering Internet requests. Policy and most configuration settings are shared between Policy Servers that share a Policy Database. Policy Server is typically installed on the same machine as Filtering Service. Large or distributed environments can include multiple Policy Servers.

Table 1 Websense Components

Component	Definition
Filtering Service	Works with Network Agent or an integration product to provide Internet filtering. When a user requests a site, Filtering Service receives the request and determines which policy applies. ◆ Filtering Service must be running for Internet requests to be filtered and logged. ◆ Each Filtering Service instance downloads its own copy of the Websense Master Database. Filtering Service is typically installed on the same machine as Policy Server. Large or distributed environments may include multiple Filtering Service instances.
Network Agent	Enables protocol management, bandwidth-based filtering, and reporting on bytes transferred. ◆ In a stand-alone deployment, enables HTTP and non-HTTP filtering ◆ In an integrated deployment, enables filtering for protocols not managed by your integration product and provides enhanced logging information
Master Database	◆ Includes millions of Web sites, sorted into more than 90 categories and subcategories ◆ Contains more than 100 protocol definitions for use in filtering protocols Download the Websense Master Database to activate Internet filtering, and make sure that the database is kept up to date. If the Master Database is more than 2 weeks old, no filtering can occur. A copy of the Master Database is downloaded by each Filtering Service instance.
Websense Manager	Serves as the configuration and management interface to Websense software. Use Websense Manager to define and customize Internet access policies, add or remove filtering clients, configure Websense software components, and more. In a Windows installation, Websense Manager also provides reporting functionality.
Usage Monitor	Enables alerting based on Internet usage. Usage Monitor tracks URL category and protocol access, and generates alert messages according to the alerting behavior you have configured. Alerts can be sent via email or on-screen display, or an SNMP alert can be sent to an SNMP Trap Server.
User Service	Communicates with an LDAP or NTLM-based directory service to apply filtering policies based on users, groups, domains and organizational units. The directory service is not a Websense product or component.

Table 1 Websense Components

Component	Definition
Optional Components	
DC Agent[1]	- Offers transparent user identification for users in a Windows-based directory service. - Polls domain controllers in the network to transparently identify users. - Communicates with User Service to provide up-to-date user logon session information to Websense software for use in filtering.
eDirectory Agent [1, 2]	- Works with Novell® eDirectory™ to transparently identify users. - Gathers user logon session information from Novell eDirectory, which authenticates users logging on to the network. - Associates each authenticated user with an IP address, and then works with User Service to supply the information to Filtering Service.
Logon Agent[1]	- Provides unsurpassed accuracy in transparent user identification in Linux and Windows networks. - Does not rely on a directory service or other intermediary when capturing user logon sessions. - Detects user logon sessions as they occur. Logon Agent communicates with the logon application on client machines to ensure that individual user logon sessions are captured and processed directly by Websense software.
Logon Application	Runs from a logon script on a domain controller to capture logon sessions as users log on to, or log off of, Windows domains in the network. The application, `LogonApp.exe`, identifies the user and sends the information to the Logon Agent.
RADIUS Agent[1]	Enables transparent identification of users who use a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection to access the network.
Remote Filtering Client	- Resides on client machines outside the network firewall. - Identifies the machines as clients to be filtered. - Communicates with Remote Filtering Server, installed inside the organization’s firewall.
Remote Filtering Server	- Allows filtering of clients outside a network firewall. - Acts as a proxy that accepts requests from Remote Filtering Client and submits them for filtering. - Communicates with Filtering Service to provide Internet access management of remote machines.

[1] Websense, Inc. supports certain combinations of transparent identification agents within the same network, or on the same machine. For more information, see *Deploying transparent identification agents*, page 31.

[2] Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

Reporting Components

All reporting components rely on the Websense filtering components. Install reporting components after installing the filtering components.

The filtering components (including Filtering Service, Policy Server, and User Service) must be running in order for complete log records to be generated.

Installation instructions for Websense reporting components can be found in the *Installation Guide*. Consult the Websense Manager Help for information about using Websense reporting tools.

Table 2 Reporting Components

Component	Definition
Database Components	
Log Database (*requires a supported database engine*)	Stores Internet request data collected by Log Server for use by Websense reporting tools. The database is created when Log Server is installed. ◆ In a Windows environments, reporting components require either Microsoft® SQL Server or MSDE. (MSDE can be installed from the Websense Web site.) ◆ MySQL is required for Websense Explorer for Linux.
Log Server, *or* Linux Log Server	Required for Websense reporting. Logs Internet request data, including: ◆ The request source ◆ The category or protocol associated with the request ◆ Whether the request was permitted or blocked ◆ Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied Log Server can log to only one Log Database at a time, and only one Log Server can be installed for each Policy Server. Log Server must be installed on a Windows machine to enable investigative and presentation reports, and Today and History page charts, in Websense Manager. Environments with a high volume of Internet activity should place Log Server on a separate machine. Log Server processing can consume considerable system resources.
Reporting applications	
Websense Manager	When Websense Manager and Log Server are installed on Windows machines, Websense Manager includes multiple, graphical reporting options: ◆ Charts on the Today and History pages show current and recent Internet activity. ◆ Investigative reports provide an interactive way to view information in the Log Database. ◆ Presentation reports include a series of templates that you can use to generate graphical reports.

Table 2 Reporting Components

Component	Definition
Explorer for Linux	Generates a variety of easy-to-understand detail and summary reports using data from the Log Database. Explorer for Linux requires: ◆ Apache 2.0.50 (Web server; included in the installation package) ◆ Firefox 2.x. or later (Web browser)

2 General Deployment Recommendations

Before deploying Websense software, ensure that your hardware and network configuration meet the recommendations provided in this document. This chapter focuses on:

- *Operating system requirements*
- *VMWare support*
- *Component limits*
- *Component suggestions*
- *Required external resources*
- *Deploying transparent identification agents*
- *Maximizing system performance*
- *Stand-Alone Edition*
- *Remote Filtering*
- *Supported integrations*

See *Websense Components*, page 11, for descriptions of the Websense filtering and reporting components. Note that Websense filtering is based on protocols (like HTTP and FTP), not on the operating system of the computer being filtered.

Supplements to this document provide recommendations for deploying Websense filtering and reporting software in networks of different sizes, and also for deploying Websense Content Gateway.

✓ **Note**

Websense software supports only TCP/IP-based networks. If your network uses both TCP/IP and non-IP based network protocols, only users in the TCP/IP portion of the network are filtered.

Operating system requirements

The tables in this section list supported operating systems and required applications for the Websense components.

✓ **Note**

Websense components have been successfully tested on the operating systems listed below. The components may also run on subsequent versions of these operating systems, but testing was not completed before publication.

Table 3 lists each component and its supported operating systems, along with other software required to run the component. Table 4, on page 23, organizes the requirements by operating system.

Table 9, on page 44, lists the supported integration versions.

Table 3 Components and Required Software

Component	Supported Operating Systems	Other Required Software
DC Agent	• Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	One of these directory services: • Windows Active Directory® • Windows NT Directory
eDirectory Agent	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	• Novell eDirectory 8.51 or later • NMAS authentication is supported. • Recommend Novell Client v4.83 or v4.9 (v4.81 and later are supported)
Explorer for Linux (Web server)	• Red Hat Enterprise Linux 5 base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS	• Firefox 2 • Apache HTTP Server 2.0.50 (Included with the Websense software installation.)

Table 3 Components and Required Software

Component	Supported Operating Systems	Other Required Software
Filtering Service	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	If Network Agent is used for protocol filtering *and* User Service is installed on a Linux machine, Samba client (v2.2.8a or later) is required on the User Service machine to allow Windows clients to display protocol block messages.
Log Database (Windows)	• The Log Database is dependent on the database engine (Microsoft SQL Server or MSDE), and not the operating system version.	One of these must be installed: • Microsoft SQL Server 2005 SP2 (Workgroup, Standard, Enterprise, or 64-bit edition) (recommended) • Microsoft SQL Server 2000 SP4 • MSDE 2000 SP4
Log Database (Linux)	• When running Explorer for Linux, the Log Database requires MySQL.	• MySQL 5.0
Log Server (Windows)	• Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	• Internet Explorer 7 One of these databases: • Microsoft SQL Server 2005 SP2 (Workgroup, Standard or Enterprise, or 64-bit edition) (recommended) • Microsoft SQL Server 2000 SP4 • MSDE 2000 SP4
Log Server (Linux)	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS	• MySQL 5.0
Logon Agent	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	Can be used with: • Windows NT Directory (NTLM) • Windows Active Directory (native or mixed mode) • Other LDAP-based directory services

Table 3 Components and Required Software

Component	Supported Operating Systems	Other Required Software
Logon Application	• Windows XP Professional, SP1 or SP2 • Windows Vista Ultimate • Windows Vista Business • Windows Vista Enterprise • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows 2000, SP3 or later (Professional or Server) • Windows NT 4.0 SP 6a (Workstation or Server)	
Network Agent	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise)(32 bit only) • Windows Server 2003, SP1 (Standard or Enterprise)(32 bit only) • Windows Server 2003 (Standard or Enterprise)(32 bit only)	Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows clients to display protocol block messages, if Network Agent is used for protocol filtering and User Service is installed on a Linux machine.
Policy Broker	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	
Policy Server	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	

Table 3 Components and Required Software

Component	Supported Operating Systems	Other Required Software
RADIUS Agent	◆ Red Hat Enterprise Linux 5: base server ◆ Red Hat Enterprise Linux 3 or 4: AS, ES, and WS ◆ Windows Server 2003, R2 (Standard or Enterprise) ◆ Windows Server 2003 SP1 or SP2 (Standard or Enterprise)	Most standard RADIUS servers are supported. The following servers have been tested: ◆ Livingston (Lucent) 2.x ◆ Cistron RADIUS server ◆ Merit AAA ◆ Microsoft IAS
Remote Filtering Client	◆ Windows XP Professional with SP1 or SP2 ◆ Windows Vista Ultimate ◆ Windows Vista Business ◆ Windows Vista Enterprise ◆ Windows Server 2003, R2 (Standard or Enterprise) ◆ Windows Server 2003, SP1 (Standard or Enterprise) ◆ Windows Server 2003 (Standard or Enterprise) ◆ Windows 2000 with SP3 or later (Professional, Server, Advanced Server)	
Remote Filtering Server	◆ Red Hat Enterprise Linux 5: base server ◆ Red Hat Enterprise Linux 3 or 4: AS, ES, and WS ◆ Windows Server 2003, R2 (Standard or Enterprise) ◆ Windows Server 2003, SP1 (Standard or Enterprise)	
Usage Monitor	◆ Red Hat Enterprise Linux 5: base server ◆ Red Hat Enterprise Linux 3 or 4: AS, ES, and WS ◆ Windows Server 2003, R2 (Standard or Enterprise) ◆ Windows Server 2003, SP1 (Standard or Enterprise) ◆ Windows Server 2003 (Standard or Enterprise)	

Table 3 Components and Required Software

Component	Supported Operating Systems	Other Required Software
User Service	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	Supports: • NTLM-based directory services • Active Directory • Sun Java™ System Directory Server, 4.2 and 5.2 • Novell Directory Services®/eDirectory, 8.51 and later Samba client (v2.2.8a or later) is required to enable Windows clients to display protocol block messages, if Network Agent is used for protocol filtering and User Service is installed on a Linux machine.
Websense Manager	• Red Hat Enterprise Linux 5: base server • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Windows Server 2003, R2 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003 (Standard or Enterprise)	• Internet Explorer 7 or Firefox 2 • Common Desktop Environment (CDE) • Apache Tomcat 6.0.13 (installed automatically with Websense Manager)

Table 4 lists the operating systems on which the Websense components run.

Table 4 Operating Systems

Operating System	Component
Microsoft Windows	
Windows Server 2003, R2 Standard or Enterprise Editions Windows Server 2003, SP1 Standard and Enterprise Editions (SP1 is required for Remote Filtering Server) Windows Server 2003 Standard and Enterprise Editions	All Websense components: ◆ Log Database (Microsoft SQL Server or MSDE database engine) ◆ DC Agent ◆ eDirectory Agent ◆ Explorer ◆ Filtering Service ◆ Log Server ◆ Logon Agent ◆ Logon Application ◆ Network Agent ◆ Policy Server ◆ RADIUS Agent ◆ Remote Filtering Client ◆ Remote Filtering Server ◆ Reporter ◆ Usage Monitor ◆ User Service ◆ Websense Manager
Windows Vista Ultimate (32-bit only) Windows Vista Business (32-bit only) Windows Vista Enterprise (32-bit only)	◆ Logon Application ◆ Remote Filtering Client
Windows XP Professional	◆ Logon Application
Windows 2000 Professional, SP3 or later	◆ Logon Application
Windows NT Server or Workstation, 4.0 SP 6a	◆ Logon Application

Table 4 Operating Systems

Operating System	Component
Linux	
Red Hat Enterprise Linux 5: base server Red Hat Enterprise Linux 3 or 4 AS (Advanced Server) Red Hat Enterprise Linux 3 or 4 ES (Enterprise Server) Red Hat Enterprise Linux 3 or 4 WS (Workstation)	• Log Database (MySQL database engine) • eDirectory Agent • Explorer for Linux • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent • Remote Filtering Server • Unix Log Server • Usage Monitor • User Service • Websense Manager

VMWare support

Websense Web Security and Websense Web Filter are supported on VMWare ESX Server. Installation, filtering, and reporting (but not logging) have been tested in a Windows 2003 Server environment, running on ESX Server versions 2.5.x and 3.x.

This section discusses:

- *Network considerations*
- *System recommendations*, page 25
- *Deployment configurations*, page 25

Network considerations

Websense Network Agent requires that the network card (NIC) it uses for monitoring be set to promiscuous mode to see network traffic. The VMWare virtual NIC must be configured for use by Network Agent.

To use bridged networking, each virtual machine must have its own IP address. In addition, VMWare requires that if a virtual machine is configured to include multiple operating systems, each OS must have a unique network address, even if only one OS runs at a time.

Consult your VMWare documentation for more configuration information.

System recommendations

The *Deployment Guide* supplements provide hard disk space and RAM recommendations for Websense components in specific environments. The VMWare documentation provides recommendations for running VMWare.

General recommendations for running Websense software on VMWare include:

- RAID for fault tolerance
- Quad-Core Intel® Xeon® processor, 3.0 GHz or greater
- 8 GB of RAM
- 3 - 1 GB NICs are required; 4 - 1 GB NICs are recommended:
  - One NIC dedicated to the VMWare management console.
  - One NIC allocated for a virtual switch used to monitor traffic (stealth mode, without an IP address).
  - One NIC allocated for a virtual switch used for communication between Websense components.
  - One NIC used by the VMWare host system for other communication.

These recommendations can vary with a higher volume of Internet requests.

No specific operating system is specified on which to run VMWare, although testing with Websense software was done on Windows Server 2003, SP2.

Deployment configurations

In VMWare environments, Websense components can be installed on separate virtual machines.

The following tables provide possible deployments for Websense software in a distributed environment.

The recommendations in these tables are for small networks, with up to approximately 2000 users. Hardware needs and component location may vary depending on the volume of Internet requests. For larger networks, more system resources or more distribution of Websense components may be needed. For specific component deployment recommendations, see the *Deployment Guide* supplements.

IMPORTANT

Microsoft does not support running SQL Server or MSDE on VMWare.

To install Websense reporting components on a Windows operating system, the database engine must be installed and running on a separate machine.

To install Websense reporting components on a Linux operating system, refer to the *Websense Explorer for Linux Administrator's Guide* for system requirements.

Table 5 Distributed Layout

Virtual Machine	Allocated Hardware	Websense Components
#1	• 2 GB RAM • 20 GB free disk space • 2 NICs	• Policy Broker • Policy Server • Filtering Service – Master Database • Network Agent • User Service • Transparent identification agent
#2	• 2 GB RAM • 20 GB free disk space	• Remote Filtering Server
#3	• 4 GB RAM • 100 GB free disk space	• Websense Manager

Component limits

When deploying Websense software, these component limits must be considered:

- 1 Policy Broker per deployment
- 1 User Service per Policy Server
- 1 Usage Monitor per Policy Server
- 1 Master Database for each Filtering Service
- 1 primary Remote Filtering Server per Filtering Service
- Each Filtering Service can communicate with only 1 Log Server

Component suggestions

This section includes suggested component deployment ratios. The optimum deployment may vary based on network configuration and Internet traffic volume.

Larger systems (more than 1000 users) may require a more distributed deployment for load balancing and support of multiple languages.

- Multiple Network Agent instances may be required, for example, to detect outbound traffic on individual network segments.
- It may be appropriate to install multiple Filtering Service instances for load balancing. Some load balancing configurations allow the same user to be filtered by different Filtering Service installations, depending on the current load.

This section includes:

- *Network Agent suggestions*, page 28
- *Number of Filtering Services allowed per Policy Server*, page 28

For limits on transparent identification agents, see *Deploying transparent identification agents*, page 31.

For more information about the interaction of Websense components, see the *Installation Guide Supplement* for the integration used with your Websense software, and the Websense Manager Help.

Network considerations

To ensure effective filtering, Websense software must be installed so that:

- Filtering Service can receive HTTP requests from an integrated firewall, proxy server, or caching application, or Network Agent.

  In a multi-segmented network, Filtering Service must be installed in a location where it can both receive and manage Internet requests from the integration product and communicate with Network Agent.
- Network Agent:
  - Must be deployed where it can see all internal Internet traffic for the machines that it is assigned to monitor.
  - Can be installed on a dedicated machine to increase overall throughput.
  - Must have bidirectional visibility into Internet traffic to filter non-HTTP requests (such as instant messaging, chat, streaming media, and other Internet applications and protocols).
  - Multiple instances of Network Agent may be required in larger or distributed networks. Each Network Agent monitors a specific IP address range or network segment.

    Using multiple Network Agents ensures that all network traffic is monitored, and prevents server overload. The required number of Network Agents depends on network size and Internet request volume.

For more information, see *Chapter 3: Deploying Network Agent*.

- As a network grows and the number of Internet requests increases, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
    - You can deploy multiple Filtering Service instances, connected to one Policy Server. This is useful for remote or isolated sub-networks. For more information, see *Number of Filtering Services allowed per Policy Server*.
    - Since a maximum of 5000 connections per Policy Server is recommended, multiple Policy Servers may be needed.
- *IMPORTANT*: To ensure the integrity of the firewall, **do not** install Websense components on the firewall machine.

> ✓ **Note**
>
> Network Agent can be deployed with the filtering components or on a separate machine. Network Agent should **not** be deployed on the same machine as response-critical components. For more information, see *Chapter 3: Deploying Network Agent*.

Network Agent suggestions

- Up to four Network Agents per Filtering Service

One Filtering Service may be able to handle more than four Network Agents.

Network Agent can typically monitor 50 Mbits of traffic per second, or about 800 requests per second. The number of users that Network Agent can monitor depends on the volume of Internet requests from each user, the configuration of the network, and the location of Network Agent in relation to the computers it is assigned to monitor. Network Agent functions best when it is close to those computers.

If a component’s capacity is exceeded, filtering and logging inconsistencies may occur.

Contact your Websense software provider for technical assistance with specific Network Agent sizing guidelines.

Number of Filtering Services allowed per Policy Server

- Up to 10 Filtering Services per Policy Server is recommended. A Policy Server may be able to handle more, depending on the load.

Multiple Filtering Service instances are useful to manage remote or isolated sub-networks.

The appropriate number of Filtering Service instances for a Policy Server depends on:

- The number of users per Filtering Service

- The configuration of the Policy Server and Filtering Service machines
- The volume of Internet requests
- The quality of the network connection between the components

  If a ping command sent from one machine to another receives a response in fewer than **30 milliseconds (ms)**, the connection is considered high quality. See the *Testing the connection*, page 29 for more information.

A Policy Server may be able to handle more than 10 Filtering Service instances. If the number of Filtering Service instances exceeds the Policy Server’s capacity, however, responses to Internet requests may be slow.

If the connection between Filtering Service and Policy Server breaks, all Internet requests are either blocked or permitted, depending on which option you have chosen in Websense Manager. For more information, see the *Getting Started* topic in the Websense Manager Help.

Filtering Service machines running behind firewalls or remotely (at a great physical distance communicating through a series of routers) may need their own Policy Server instance. In a multiple Policy Server environment, a single Websense Policy Database holds the policy settings for all Policy Server instances. See the Websense Manager Help for more information.

Testing the connection

Run a **ping** test to check the response time and connection between the Policy Server and Filtering Service machines. A response time of fewer than 30 milliseconds is recommended.

1. Open a command prompt (Windows) or terminal session (Linux) on the Policy Server machine.
2. Enter the following command:

   ```
   ping <IP address or hostname>
   ```

   Here, *<IP address or hostname>* identifies the Filtering Service machine.

Interpreting your results

When you run the **ping** command on a Windows machines, the results resemble the following:

```
C:\>ping 11.22.33.254
Pinging 11.22.33.254 with 32 bytes of data:
Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63
Reply from 11.22.33.254: bytes=32 time=14ms TTL=63
Reply from 11.22.33.254: bytes=32 time=15ms TTL=63
Ping statistics for 11.22.33.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

In a Linux environment, the results look like this:

```
[root@localhost root]# ping 11.22.33.254
PING 11.22.33.254 (11.22.33.254) 56(84) bytes of data.
64 bytes from 11.22.33.254: icmp_seq=2 ttl=127 time=0.417 ms
64 bytes from 11.22.33.254: icmp_seq=3 ttl=127 time=0.465 ms
64 bytes from 11.22.33.254: icmp_seq=4 ttl=127 time=0.447 ms
64 bytes from 11.22.33.254: icmp_seq=1 ttl=127 time=0.854 ms
```

Ensure that **Maximum** round trip time or the value of **time=x.xxx ms** is fewer than 30 ms. If the time is greater than 30 ms, move one of the components to a different network location and run the ping test again. If the result is still greater than 30 ms, locate and eliminate the source of the slow response.

Required external resources

Websense software relies on certain external resources to function properly in your network.

- **TCP/IP**: Websense software provides filtering in TCP/IP-based networks only. If your network uses both TCP/IP and non-TCP protocols, only those users in the TCP/IP portion of your network are filtered.
- **DNS server**: A DNS server is used to resolve requested URLs to an IP address. Websense software or your integration product requires efficient DNS performance. DNS servers should be fast enough to support Websense filtering without becoming overloaded.
- **Directory services**: If Websense software is configured to apply user- and group-based policies, User Service queries the directory service for user information. Although these users and group relationships are cached by Websense software, directory service machines must have the resources to rebuild the cache rapidly Websense software requests user information. See *Supported directory services*.
- **Network efficiency**: The ability to connect to resources such as the DNS server and directory services is critical to Websense software. Network latency must be minimized if Filtering Service is to perform efficiently. Excessive delays under high load circumstances can impact the performance of Filtering Service and may cause lapses in filtering. See the *Deploying in a Distributed Enterprise* supplement to this guide for tips on improving network communication.

Supported directory services

If your environment includes a directory service, you can configure Websense software to filter Internet requests based on policies assigned to users, groups, and domains (organizational units).

Websense software can work with the following directory services:

- Windows NT Directory and Windows Active Directory (Mixed Mode)
- Windows Active Directory (Native Mode)

- Sun Java System Directory Server
- Novell Directory Services/Novell eDirectory

For information on configuring Websense software to communicate with a supported directory service, see the Websense Manager Help. Websense software does not need to run on the same operating system as the directory service.

Deploying transparent identification agents

If you are using Websense software in stand-alone mode, or if your integration product does not send user information to Websense software, use Websense transparent identification agents to identify users without prompting them for a user name and password.

There are 4 optional transparent identification agents:

- DC Agent
- eDirectory Agent
- Logon Agent
- RADIUS Agent

> ✓ **Note**
> DC Agent must have domain administrator privileges to retrieve user logon information from the domain controller.

If you have deployed Websense software in a single network location, a single transparent identification agent instance is recommended.

In deployments that cover multiple locations, you can install an agent instance in multiple domains.

For example:

- One **DC Agent** instance can handle multiple trusted domains. Add additional instances based on:
  - The load placed on DC Agent
  - Whether a DC Agent instance can see all the domains on the network, including remote offices

  Load results from the number of user logon requests. If the network is large (10,000+ users, 30+ domains), having multiple DC Agent instances allows for faster identification of users.

  If multiple Filtering Services are installed, each Filtering Service instance must be able to communicate with all DC Agent instances.
- One **eDirectory Agent** is required for each eDirectory Server.

- One **Logon Agent** is required for each Filtering Service instance.
- One **RADIUS Agent** instance is required for each RADIUS server.

  Websense, Inc. recommends installing and running RADIUS Agent and the RADIUS server on separate machines. (The agent and server cannot have the same IP address, and must use different ports.)

In some environments, a combination of transparent identification agents may be appropriate within the same network, or on the same machine. See *Combining transparent identification agents*.

Refer to the *Installation Guide* for transparent identification agent installation instructions. See the Websense Manager Help for detailed configuration information. More information is also available in the *Transparent Identification of Users* technical white paper.

Combining transparent identification agents

Websense software can be work with multiple transparent identification agents. If your environment requires multiple agents, it is best to install them on separate machines.

- eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate server on the same network.
- Running eDirectory Agent and DC Agent in the same deployment is not supported.

Table 6 lists supported combinations.

Table 6 Deploying Multiple Transparent ID Agents

Combination	Same machine?	Same network?	Configuration required
Multiple DC Agents	No	Yes	Ensure that all instances of DC Agent can communicate with Filtering Service, and that the individual DC Agents are not monitoring the same domain controllers.
Multiple RADIUS Agents	No	Yes	Configure each agent to communicate with Filtering Service. Multiple instances of the RADIUS Agent cannot be installed on the same machine.
Multiple eDirectory Agents	No	Yes	Configure each instance to communicate with Filtering Service.
Multiple Logon Agents	No	Yes	Configure each instance to communicate with Filtering Service.

Table 6 Deploying Multiple Transparent ID Agents

Combination	Same machine?	Same network?	Configuration required
DC Agent + RADIUS Agent	Yes	Yes	Install these agents in separate directories. Use a different port for communication between DC Agent and Filtering Service than you use for communication between RADIUS Agent and Filtering Service. See the Websense Knowledge Base for more details.
DC Agent + eDirectory Agent	No	No	Websense does not support communication with both Windows and Novell Directory Services in the same deployment. However, both agents can be installed, with only one active agent.
DC Agent + Logon Agent	Yes	Yes	Configure both agents to communicate with Filtering Service. By default, each agent uses a unique port, so port conflicts are not an issue unless these ports are changed.
RADIUS Agent + Logon Agent	Yes	Yes	Configure all agents to communicate with Filtering Service.
eDirectory Agent + Logon Agent	No	No	Websense does not support communication with both Novell Directory Services and a Windows or LDAP-based directory service in the same deployment. However, both agents can be installed, with only one active agent.
RADIUS Agent + eDirectory Agent	Yes	Yes	Configure all agents to communicate with Filtering Service. When adding agents to Websense Manager, use an IP address to identify one, and a machine name to identify the other. See the *Transparent Identification of Users* white paper for details.
DC Agent + Logon Agent + RADIUS Agent	Yes	Yes	This combination is rarely required. Install each agent in a separate directory. Configure all agents to communicate with Filtering Service. Use separate ports for this communication.

Maximizing system performance

Adjust Websense components to improve filtering and logging response time, system throughput, and CPU performance. Websense software can be optimized for:

- Network Agent
- Logging of bytes transferred
- Database engine (Microsoft SQL Server 2005/2000, MSDE 2000, MySQL 5.0). SQL Server 2005 is recommended.

For enterprise networks, see *Deploying in a Distributed Enterprise* supplement to this guide for more information.

Network Agent

Network Agent can be installed on the same machine as other Websense components, or on a separate machine.

When a small or medium network, for example, exceeds 1000 users, or when Network Agent misses Internet requests, place Network Agent on a different machine than Filtering Service and Policy Server.

If Websense software is running in a high load environment, or with a high capacity (T3) Internet connection, you can increase throughput and implement load sharing by installing multiple Network Agent instances. Install each agent on a different machine, and configure each agent to monitor a different portion of the network.

Important

Network Agent must have bidirectional visibility into the network or network segment that it monitors.

If multiple Network Agents are installed, each agent must monitor a different network segment (IP address range).

If a Network Agent machine connects to a switch, the monitor NIC must plug into a port that mirrors, monitors, or spans the traffic of all other ports. *Multiple segment network*, page 51, and *Network Agent location*, page 49, discuss locating Network Agent in more detail.

HTTP reporting

You can use Network Agent or an integration product to track HTTP requests and pass the information to Websense software, which uses the data to filter and log requests.

Network Agent and some integration products also track bandwidth activity (bytes sent and received), and the duration of each permitted Internet request. This data is also passed to Websense software for logging.

When both Network Agent and the integration partner provide logging data, the amount of processor time required by Filtering Service doubles.

If you are using both Network Agent and an integration product, you can avoid extra processing by configuring Websense software to use Network Agent to log HTTP requests (enhanced logging). When this feature is enabled:

- Websense software does not log HTTP request data sent by the integration product. Only the log data provided by Network Agent is recorded.
- As a best practice, Network Agent and Filtering Service should not run on the same machine.

Consult the Websense Manager Help for configuration instructions.

Database Engine

In Microsoft Windows environments, the Websense Log Database can be created using any of the following database engines:

- Microsoft SQL Server 2005 (*recommended*)
- Microsoft SQL Server 2000
- Microsoft Database Engine (MSDE) 2000

Websense Explorer for Linux and the Linux version of Log Server use MySQL 5.0.

Log Server logs Internet activity information to only one Log Database at a time.

Microsoft SQL Server

Microsoft SQL Server works best for larger networks, or networks with a high volume of Internet activity, because of its capacity for storing large amounts of data over longer periods of time (several weeks or months). Microsoft SQL Server 2005 is recommended.

Under high load, Microsoft SQL Server operations are resource intensive, and can be a performance bottleneck for Websense software reporting. You can tune the database to improve performance, and maximize the hardware on which the database runs:

- Improve CPU performance to alleviate resource conflicts between Log Server and Microsoft SQL Server:
  - Increase the CPU speed, the number of CPUs, or both.
  - Consider providing a dedicated machine for Log Server.
- Provide adequate disk space to accommodate the growth of the Log Database. Microsoft SQL Client Tools can be used to check database size.
- Use a disk array controller with multiple drives to increase I/O bandwidth.

- Increase the RAM on the Microsoft SQL Server machine to reduce time-consuming disk I/O operations.

> ✓ **Note**
> Consult the Microsoft Web site for detailed information about optimizing Microsoft SQL Server performance.

MSDE

Microsoft Database Engine (MSDE) is a free database engine best suited to smaller networks, organizations with a low volume of Internet activity, or organizations plan to generate reports on only short periods of time (for example, daily or weekly archived reports, rather than historical reports over longer time periods). MSDE cannot be optimized.

With MSDE, the maximum size of the Log Database is about 1.5 GB. When the existing database reaches this limit, it is saved (rolled over), and a new Log Database is created. Use the ODBC Data Source Administrator (accessed via the Windows Control Panel) to see information about database that have been saved.

If the is rolling over frequently, consider upgrading to Microsoft SQL Server 2005, SP2.

> ✓ **Note**
> Consult the *Installation Guide* for detailed information about selecting the appropriate database engine for the deployment.

When using MSDE, make sure that the latest service packs have been applied. Microsoft SQL Server service packs can be applied to MSDE 2000. The service pack updates only those files relevant to MSDE.

MySQL

Websense Explorer for Linux requires MySQL 5.0. Although MySQL is available for free, a licensed version must be purchased for commercial use.

For more information on MySQL, visit the MySQL Web site: www.mysql.com.

Log Database disk space recommendations

Log Database requirements vary, based on the size of the network and the volume of Internet activity. This guide uses the following baseline information to provide general recommendations:

- An average user requests 100 URLs (*visits*) per day.
- The Log Database creates a record for each visit.

- Each record is approximately 500 bytes.
- Each URL requires roughly 5 to 10 HTTP GETS (*hits*).

  If the Log Database is configured to write a record for each hit, the size of the database may increase by a factor of five.

During installation, you are provided options for minimizing the size of the Log Database.

After installation, additional configuration options, including selective category logging, are available to help manage the size of the Log Database. Consult the Websense Manager Help for details.

Logging visits (default settings)

If the Log Database is configured to record **visits** (the default), you can calculate the disk space required for the database as follows:

(# of URLs) x (# of bytes) x (# of users)

If an average user generates 50 KB per day (100 visits x 500 bytes), and is logged on for 20 work days per month, that user consumes 1 MB in the Log Database each month (20 days x 50 KB/day). Extrapolating to 500 users, the database would use 500 MB per month to record visits.

Logging hits

If the Log Database is configured to record each **hit**, you can calculate the disk space required for the database as follows:

[(avg. # of URLs) x (avg. # of hits) x (# of bytes)] x (# of users)

If an average user generates 250 KB per day (100 URLs x 5 gets per URL x 500 bytes), and is logged on for 20 work days per month, that user consumes 5 MB in the Log Database each month (20 days x 250 KB/day). Extrapolating to 500 users, the database would use 2.5 GB per month.

In this example, the Log Database would requires 30 GB of disk space for one year's worth of data (500 users at 500 hits per day).

Due to the large amount of disk space required, and due to the performance impact on reporting, Websense, Inc., does not recommend keeping live data from large networks for a year. When you break the database into smaller pieces, you can generate reports much more quickly.

Logging full URLs

If the Log Database is configured to log the full URLs, each URL recorded can be up to 1000 characters, or 2000 bytes (2 KB) in length. When full URL logging is turned off, a log entry requires only 500 bytes per URL.

If the Log Database is growing too quickly, you can turn off full logging to decrease the size of each entry and slow growth by a factor of 4.

Configure URL logging options in Websense Manager. Consult the Websense Manager Help for details.

Consolidation

Consolidation helps to reduce the size of the database by recording a single entry for multiple visits to the same URL by the same user. Instead of recording each hit or visit by a user, the information is stored in a temporary file. At a specified interval, the file is processed and the duplicate records are not written to the database.

For example, the user visits *www.cnn.com* and receives multiple pop-ups during the session. The visit is logged as a record.

- If consolidation is turned off (the default), and the user returns to the site later, a second visit is logged.
- If consolidation is turned on, additional visits to the site within a specified period are logged as a single record.

Protocol logging

In addition to logging HTTP and HTTPS traffic, if your deployment includes Network Agent, you have the option to log non-HTTP protocol traffic (for example, instant messaging or streaming media traffic).

The more protocols you choose to log, the greater the impact on the size of the Log Database. See the Websense Manager Help for information about filtering and logging non-HTTP protocols.

Log Database strategy

Using the hits and visits calculations provided under *Logging hits*, page 37, even without logging full URLs, storing data for 1 year could require:

- 600 GB for hits
- 120 GB for visits

Generating reports against such large amounts of data can significantly slow report processing.

Use **database partitions** to limit the scope of the data use to generate reports.

- A database rollover is triggered by a time or size limit.
- New data is collected in a new partition.
- Older data is preserved in other partitions.
- You configure which partition you want to use to generate reports.

Adjust the partition or rollover limits to maximize reporting performance and ease the management of the data. Consult the Websense Manager Help for details.

Stand-Alone Edition

The Stand-Alone Edition of Websense Web Security or Websense Web Filter uses Network Agent (rather than an integration product or device) to provide HTTP, HTTPS, FTP, and other protocol filtering. Network Agent:

- Detects all Internet requests (HTTP and non-HTTP)
- Communicates with Filtering Service to see if each request should be blocked
- Calculates the number of bytes transferred
- Sends a request to Filtering Service to log request information

For more information, see the *Installation Guide* or the Websense Manager Help.

The Stand-Alone Edition runs on the operating systems listed earlier in this chapter (see Table 3, on page 18, and Table 4, on page 23).

Reporting is runs under Websense Manager in the Stand-Alone Edition on Windows. Websense Explorer for Linux must be installed for reporting in a Linux installation. As in any deployment, reporting components, including Log Server, should run on a separate machine from the filtering components.

✓ **Note**

If you are using Logon Agent in a Linux deployment, the Logon Application must be installed on Windows.

The Stand-Alone Edition can be deployed in small, medium, and large networks. Components may need to be distributed over multiple machines for load balancing and improved performance in larger networks. For example, you could deploy multiple Network Agents (on Windows or Linux) to accommodate a high Internet traffic load.

Table 7, on page 40, provides system recommendations for deploying the Stand-Alone Edition, based on network size. System needs vary, depending on the volume of Internet traffic.

The following baseline is used to create the recommendations:

- 1 - 500 users = 1 - 100 requests per second
- 500 - 2,500 users = 100 - 500 requests/sec
- 2,500 - 10,000 users = 500 - 2,250 requests/sec

If your network traffic exceeds these estimates, more powerful systems or greater distribution of components may be required.

Important

- To ensure the integrity of a firewall, do not install Websense components on a firewall machine.
- Each Network Agent machine must be positioned to see all Internet requests for the machines that it is assigned to monitor.
- eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service, or on a separate machine in the same network, but not on the same machine as Log Server.

Table 7 Stand-Alone System Recommendations

Network Size	Filtering Components	Reporting (Windows) —or—	Reporting (Linux)
1 - 500 users	**Windows** or **Linux** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 2 GB RAM • 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 4 GB RAM • 100 GB free disk space • Microsoft SQL Server 2005 SP2, Microsoft SQL Server 2000 SP4, or MSDE 2000	**Linux** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 2 GB RAM • 80 GB free disk space • MySQL 5.0
500 - 2,500 users	**Windows** or **Linux** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 2 GB RAM • 10 GB free disk space (Free space must equal at least 20% of total disk space.)	**Windows** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 4 GB RAM • 100 GB free disk space • Microsoft SQL Server 2000 SP4, Microsoft SQL Server 2005 SP2, or MSDE 2000	**Linux** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 2 GB RAM • 100 GB free disk space • MySQL 5.0

Table 7 Stand-Alone System Recommendations

Network Size	Filtering Components	Reporting (Windows) —or—	Reporting (Linux)
2,500 - 10,000 users	**Windows** or **Linux** • Load balancing required • Quad Xeon, 3.0 GHz, or greater • 2 GB RAM • 10 GB free disk space (Free space must equal at least 20% of total disk space.) • See the Important note below.	**Windows** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 4 GB RAM • 200 GB free disk space with a disk array (The Log Database requires a disk array to increase I/O reliability and performance.) • High-speed disk access • Microsoft SQL Server 2005 SP2, or Microsoft SQL Server 2000 SP4	**Linux** • Quad Xeon, 2.5 GHz or greater • 2 GB RAM • 200 GB free disk space, with a disk array, RAID level 10 • High speed disk access • MySQL 5.0

Important

Two Network Agent instances run on separate machines are required for 2500-10000 user networks. The machines should have:

- Quad-Core Intel Xeon processor, 2.5 GHz or greater
- At least 1 GB of RAM

Multiple Filtering Service machines may also be needed. Machine requirements depend on the number of users being monitored and filtered.

To run both filtering and reporting on the same machine in the two smaller network sizes, increase the RAM to 6 GB, and consider using a faster processor and hard drive to compensate for the increased load.

Remote Filtering

The Remote Filtering feature allows Websense software to monitor computers outside the corporate network. A **Remote Filtering Client** must be installed on each remote machine.

The remote clients communicate with a **Remote Filtering Server**, which acts as a proxy to Filtering Service. This communication is authenticated and encrypted.

When installing Remote Filtering:

- The Remote Filtering Server should be installed on a dedicated machine that can communicate with the Filtering Service machine. See Table 8, on page 42.
- Do **not** install Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
- Each Filtering Service instance has one Remote Filtering Server.
- As a best practice, the Remote Filtering Server should be installed inside the outermost firewall, in the DMZ outside the firewall protecting the rest of the corporate network. This is highly recommended.
- See Table 3, on page 18, for operating system requirements for the Remote Filtering Server.

Remote Filtering Client system recommendations:

- Pentium 4 or greater
- Free disk space: 25 MB for installation; 15 MB to run the application
- 512 MB RAM

Table 8 Remote Filtering Server System Recommendations

Network Size	Hardware Recommendations
1-500 clients	**Windows** or **Linux** • Quad-Core Intel Xeon processor, 2.5 GHz or greater • 1 GB RAM • 20 GB free disk space
500-2000 clients	**Windows** or **Linux** • Quad-Core Intel Xeon processor, 3.2 GHz or greater • 2 GB RAM • 20 GB free disk space
2000-5000 clients	**Windows** or **Linux** • Quad-Core Intel Xeon processor, 3.2 GHz or greater • 2 GB RAM • 20 GB free disk space

Table 8 Remote Filtering Server System Recommendations

Network Size	Hardware Recommendations
5000-10000 clients	**Windows** or **Linux** • Quad Xeon, 3.2 GHz or greater *- or -* Static load balancing with Dual Xeon, 3.2 GHz or greater • 2 GB RAM • 20 GB free disk space
10000+ clients	**Windows** or **Linux** • Static load balancing with Quad Xeon, 3.2 GHz or greater • 2 GB RAM • 20 GB free disk space

Figure 1 provides an example of a Remote Filtering deployment. The illustration does not include all Websense components.

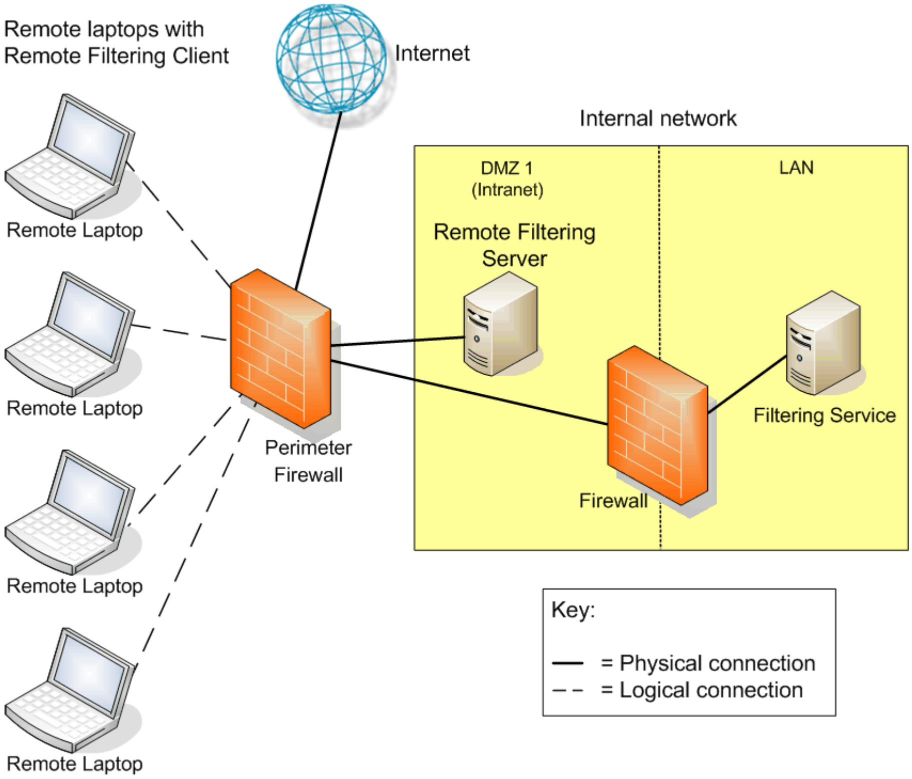


Figure 1 Example of Remote Filtering Deployment

Supported integrations

Websense software can be integrated with the following firewalls, proxy servers, and caching applications (collectively referred to as **integration products**) to provide Internet filtering.

Table 9 Supported Integrations

Integration	Version Supported	Comments
Cisco®	◆ Cisco PIX Firewall Software v5.0 or greater ◆ Cisco Adaptive Security Appliances (ASA) Software v7.0 or greater ◆ Cisco Content Engine ACNS v5.4 or greater ◆ Cisco Routers with Cisco IOS Software Release 12.3 or greater	
Check Point®	◆ FireWall-1 FP1 or greater ◆ FireWall-1 NG AI ◆ FireWall-1 NGX ◆ CheckPoint Edge ◆ CheckPoint R61 ◆ Check Point R65	Contact Check Point for assistance is determining which FireWall-1 version is running. Network Agent can run on same machine **only** if it and the integration each has its own processor.
Citrix® – Citrix Presentation Server™ – MetaFrame® Presentation Server	◆ MetaFrame Presentation Server 3.0 ◆ Citrix Presentation Server 4.0 ◆ Citrix Presentation Server 4.5	**Websense Plug-in**: The Citrix plug-in is only supported on Windows. Requires either: ◆ Microsoft Windows Server 2003 (32 bit) ◆ Microsoft Windows 2000 Server (32 bit)
Microsoft® Internet Security and Acceleration (ISA) Server	Integrations: ◆ Microsoft ISA Server 2004, Standard Edition and Enterprise Edition ◆ Microsoft ISA Server 2006, Standard Edition and Enterprise Edition Clients: ◆ ISA Firewall Clients ◆ Secure NAT Clients	**Websense Plug-in**: The ISAPI Plug-in for the Microsoft ISA Server is supported only on Windows.
Network Appliance™ NetCache®	◆ NetCache OS v5.2.1 R1D4 or greater.	Websense protocol management requires NetCache v5.5 or later.

Table 9 Supported Integrations

Integration	Version Supported	Comments
Squid Web Proxy Cache	- Squid STABLE v2.5 - Squid STABLE v2.6	**Websense Plug-in**: The Squid Plug-in for the Squid Web Proxy Cache is supported only on Linux.

3 Deploying Network Agent

When your Websense software deployment includes Network Agent, the positioning of the agent and other Websense filter components depends on the composition of your network.

For the most part, Ethernet networks are built of **segments**. (Very simple networks are the exception.) A segment is a sort of neighborhood for a group of machines, which are connected to the rest of the network via a central connection point (router, bridge, switch, or smart hub). Most of these devices keep local traffic within a segment, while passing traffic intended for machines on other segments. This architecture reduces network congestion by keeping unnecessary traffic from passing to the whole network.

A very simple network may require only a single Network Agent. A segmented network may require (or benefit from) a separate Network Agent instance for each segment. Network Agent functions best when it is closest to the computers that it is assigned to monitor.

This chapter provides configuration information and sample deployment diagrams to help you position Network Agent in your deployment.

Network Agent

Network Agent manages Internet protocols (including HTTP, HTTPS, and FTP), by examining network packets and identifying the protocol.

As with third-party integration products (like firewalls, routers, proxies, or network appliances), Network Agent can be configured to route HTTP requests to Filtering Service for filtering. In addition, when Network Agent detects a non-HTTP request, it queries Filtering Service to determine whether the protocol should be blocked, and then logs the results of the query.

Network Agent must be installed on the **internal** side of the corporate firewall, in a location where can it see all Internet requests for the machines it is assigned to monitor. The agent then monitors HTTP and non-HTTP requests from those machines, and the response that they receive.

Network Agent only monitors and manages traffic that passes through the network device (switch, hub, or gateway) to which it is attached. Multiple Network Agent instances may be needed, depending on the size, volume of Internet requests and the network configuration.

The Network Agent machine can connect to the network via a switch or a hub. See *Hub configuration*, page 54, and *Switched networks with a single Network Agent*, page 55.

Network Agent can be installed on the same machine as an integration product. See *Gateway configuration*, page 59.

> ⚠ **Warning**
>
> Do **not** install Network Agent on a machine running a firewall or Remote Filtering Server. On a firewall, Network Agent's packet-capturing that may conflict with the firewall software. On a Remote Filtering Server, machine resources may be too heavily taxed.
>
> **There is one exception:** A blade server or appliance with separate processors or virtual processors may be able to support both Network Agent and firewall software or Remote Filtering Server.

Network Agent settings

Configure Network Agent global (applying to all agent instances) and local (specific to a single agent instance) settings in Websense Manager. These settings tell Network Agent which machines to monitor and which to ignore.

- Global settings:
    - Specify which machines are part of your network.
    - Identify any machines in your network that Network Agent should monitor for **incoming** requests (for example, internal Web servers).
    - Specify bandwidth calculation and protocol logging behavior.
- Local settings:
    - Specify which Filtering Service is associated with each Network Agent.
    - Identify proxies and caches used by the machines that this Network Agent monitors.
    - Determine which network card (NIC) the Network Agent instance uses to monitor requests and which it uses to send block pages.

      Configuration settings for the NIC used to monitor requests determine which segment of the network the agent instance monitors.

Network Agent location

Network Agent must be able to see all outgoing and incoming Internet traffic on the network segment that it is assigned to monitor. Multiple instances of Network Agent may be needed to monitor an entire network.

- Multiple Network Agents may be needed for larger or high-traffic organizations.
- A Network Agent instance can be placed in each internal network segment.

The Network Agent machine may be:

- Connected to a **switch** or **router**.
    - Configure the device to use a mirror or span port, and connect Network Agent to this port, to allow the agent to see Internet requests from all monitored machines. (On most switches, you can change a port mode to spanning, mirroring, or monitoring mode. The term varies by manufacturer; the function is the same.)

      ✓ **Note**

      Not all switches support port spanning or mirroring. Contact the switch vendor to verify that spanning or mirroring is available, and for configuration instructions.

    - Websense, Inc., strongly recommends using a switch that supports bidirectional spanning. This allows Network Agent to use a single network card (NIC) to both monitor traffic and send block pages.

      If the switch does not support bidirectional spanning, the Network Agent machine must have at least 2 NICs: one for monitoring and one for blocking. See *Using multiple NICs*, page 61.
- On a dedicated machine, connected to an **unmanaged, unswitched hub** located between an external router and the network.

To ensure that Network Agent is able to monitor the expected traffic, you must both position the Network Agent machine appropriately, and configure Network Agent settings in Websense Manager. Consult the Websense Manager Help for instructions.

The following sections illustrate possible single and multiple Network Agent configurations.

Single segment network

A single segment network is a series of logically connected nodes (computers, printers, and so on) operating in the same portion of the network. In a single segment network, Filtering Service and Network Agent must be positioned to monitor Internet traffic across the entire network.

Figure 2 shows the filtering components of the Websense software Stand-Alone Edition installed in a central location to see both HTTP and non-HTTP traffic.

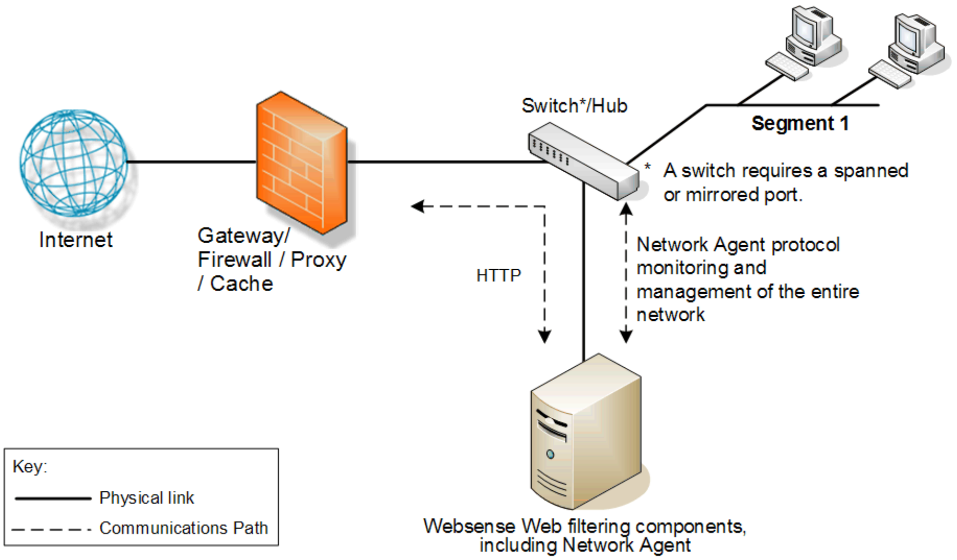

Switch*/Hub
Segment 1
Internet
Gateway/ Firewall / Proxy / Cache
* A switch requires a spanned or mirrored port.
HTTP
Network Agent protocol monitoring and management of the entire network
Key:
Physical link
Communications Path
Websense Web filtering components, including Network Agent

Figure 2 Websense software in a single-segment network

To learn more about installing Network Agent in a network:

- With a hub, see *Hub configuration*, page 54.
- With a switch, see *Switched networks with a single Network Agent*, page 55.
- With a gateway, see *Gateway configuration*, page 59.

Multiple segment network

Depending on the device used to connect network segments, some traffic may not be sent to all segments. A router, bridge or smart hub serves as traffic control, preventing unneeded traffic from being sent to a segment. In this environment, the Websense filtering components must be deployed to see all network traffic.

- Filtering Service must be installed where it can receive and manage Internet requests from the integration product, if any, and communicate with Network Agent.
- Each Network Agent instance must be able to see all Internet requests on the segment or segments that it is configured to monitor.

Deploying multiple Network Agents

Multiple Network Agent instances may be needed in a multiple segment network to capture all Internet requests. A Network Agent can be installed on each segment to monitor the Internet requests from that segment.

✓ **Note**

A limit of 4 Network Agents is suggested for each Filtering Service. It may be possible to use more agent instances, depending on system and network configuration and the volume of Internet requests.

If multiple Network Agent instances are installed:

- Ensure that the instances are deployed to monitor the entire network. Partial deployment results in incomplete filtering and loss of log data in network segments not watched by the Network Agent.
- Network Agent instance must not be configured to monitor overlapping IP address ranges. An overlap can result in inaccurate logging and network bandwidth measurements, and improper bandwidth-based filtering.

  The network segment or IP address range monitored by each Network Agent is determined by the NIC settings for the agent configured in Websense Manager. See the Websense Manager Help for instructions.
- Avoid deploying Network Agent across different LANs. If you install Network Agent on a machine in the 10.22.x.x network, and configure it to communicate with a Filtering Service machine in the 10.30.x.x network, communication may be slow enough to prevent Network Agent from blocking an Internet request before the site is returned to the user.

For examples of central and distributed Network Agent placement, see:

- *Hub configuration*, page 54
- *Switched networks with a single Network Agent*, page 55.
- *Gateway configuration*, page 59

Central Network Agent placement

A network with multiple segments can be filtered from a single location. Install Filtering Service where it can receive Internet requests from both the integration product, if any, and each Network Agent.

If the network contains multiple switches, Network Agent instances are inserted into the network at the last switch in the series. This switch must be connected to the gateway that goes out to the Internet.

In Figure 3:

- One Network Agent instance is installed with Filtering Service on Machine A. This machine is connected to the network via a switch that is configured to mirror or span the traffic of network Segment 1.
- A second Network Agent is installed on Machine B, which is connected to the same switch as Machine A. Machine B is connected to a different port that is configured to mirror the traffic of Segments 2 and 3.
- Both Network Agents are positioned to see all traffic for the network segments they monitor, and to communicate with other Websense components.
- The switch is connected to the gateway, allowing the Network Agent instances to monitor network traffic for all network segments.

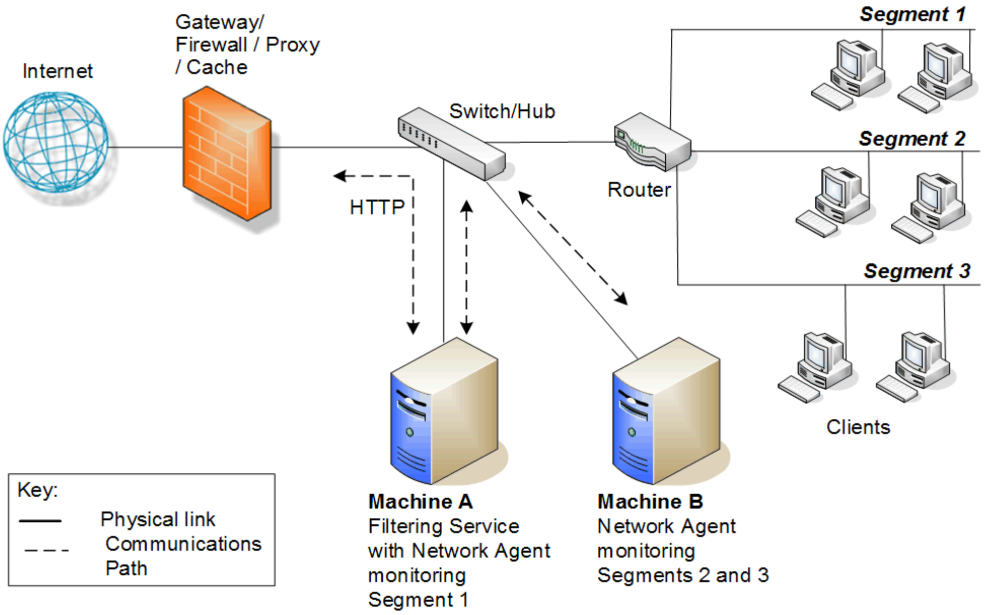


Figure 3 Websense software in a multiple-segment network

Distributed Network Agent placement

The network diagram below shows a single Filtering Service with 3 Network Agents, one for each network segment. A deployment like this might be useful in organizations with satellite offices, for example.

- Filtering Service (Machine C) must be installed where it is able to receive and manage Internet requests from both the integration product (if any) and each of the Network Agent instances in all network segments.
- Each Network Agent (machines A, B and C) is connected to the network segment it monitors via the span or mirror port of a switch.

See *Deploying multiple Network Agents*, page 51, for more information.

In Figure 4, the switches are not connected in a series. However, each switch is connected to the router, which is connected to the gateway.

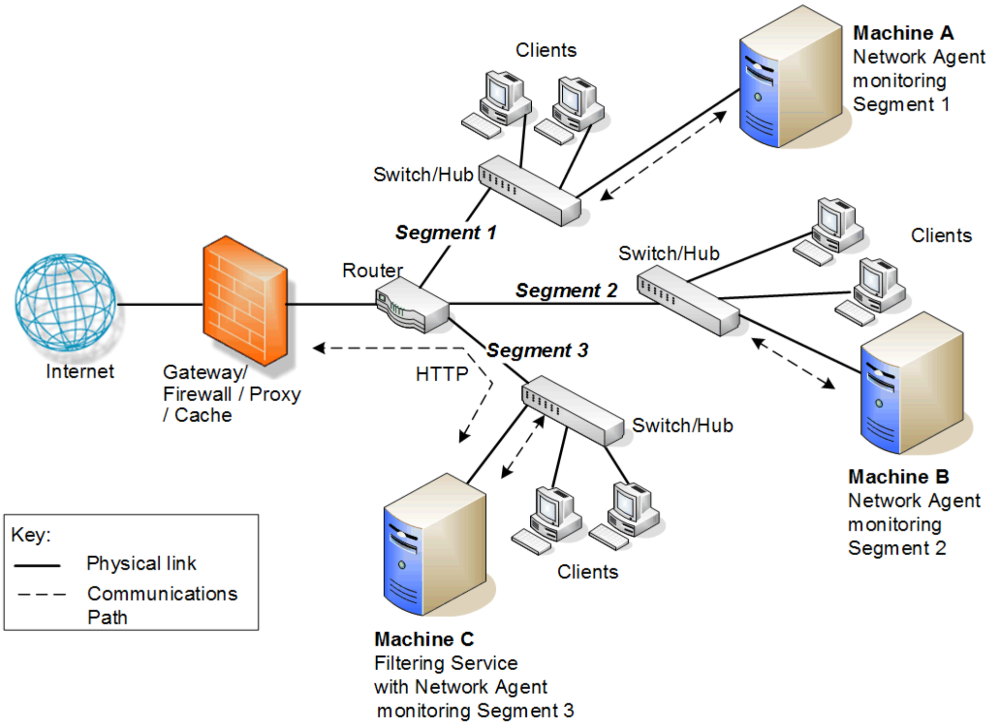
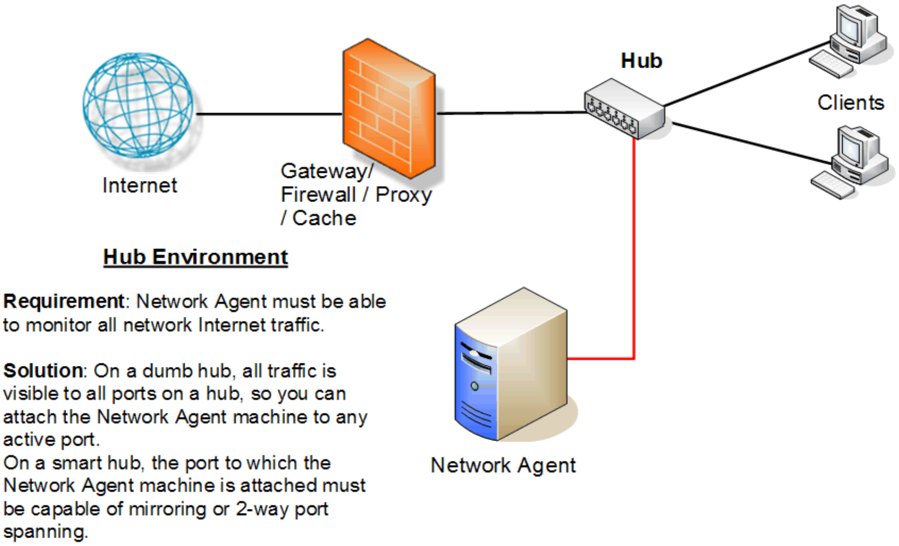


Figure 4 Multiple Network Agents in a multiple-segment network

Hub configuration

At the simplest level, a network hub provides a central connection point for the segments in a network and the devices in those segments. The port to which the Network Agent machine connects is dependent on the type of hub. Some hubs broadcast traffic to all of their ports, while others do not.

Network Agent must be able to see the traffic for the network segments it is assigned to monitor.



Hub Environment

Requirement: Network Agent must be able to monitor all network Internet traffic.

Solution: On a dumb hub, all traffic is visible to all ports on a hub, so you can attach the Network Agent machine to any active port.
On a smart hub, the port to which the Network Agent machine is attached must be capable of mirroring or 2-way port spanning.

Figure 5 Network Agent connected to a hub

Switched networks with a single Network Agent

A switch is a bridge that routes traffic between network segments. It prevents all traffic from going to all segments, reducing network congestion. Since not all traffic going through a switch is visible to all devices on the network, the machine running Network Agent must be connected at a point where it can monitor all Internet traffic for the network.

Connect the Network Agent machine to the port on the switch that mirrors, monitors, or spans the traffic on the gateway or firewall port. The span or mirror port sees all the traffic that leaves each network segment.

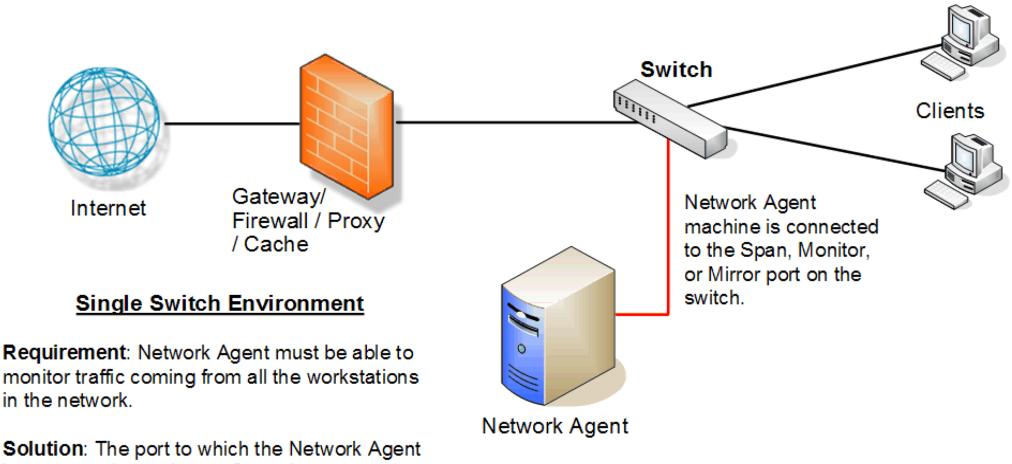
✓ **Note**

Not all switches support bidirectional port spanning or mirroring. Contact the switch vendor to verify that spanning or mirroring is available, and for configuration instructions.

If bidirectional communication is not available, at least 2 network cards (NICs) are needed to monitor traffic and communicate with other Websense components.

If port spanning is not available, Network Agent cannot properly monitor the network.

Figure 6 shows a network with a single switch. The Network Agent machine is attached to the port that mirrors all traffic from connected clients. Subsequent illustrations show multiple switch and multiple subnetwork configurations.


Internet
Gateway/ Firewall / Proxy / Cache
Switch
Clients
Network Agent machine is connected to the Span, Monitor, or Mirror port on the switch.
Network Agent

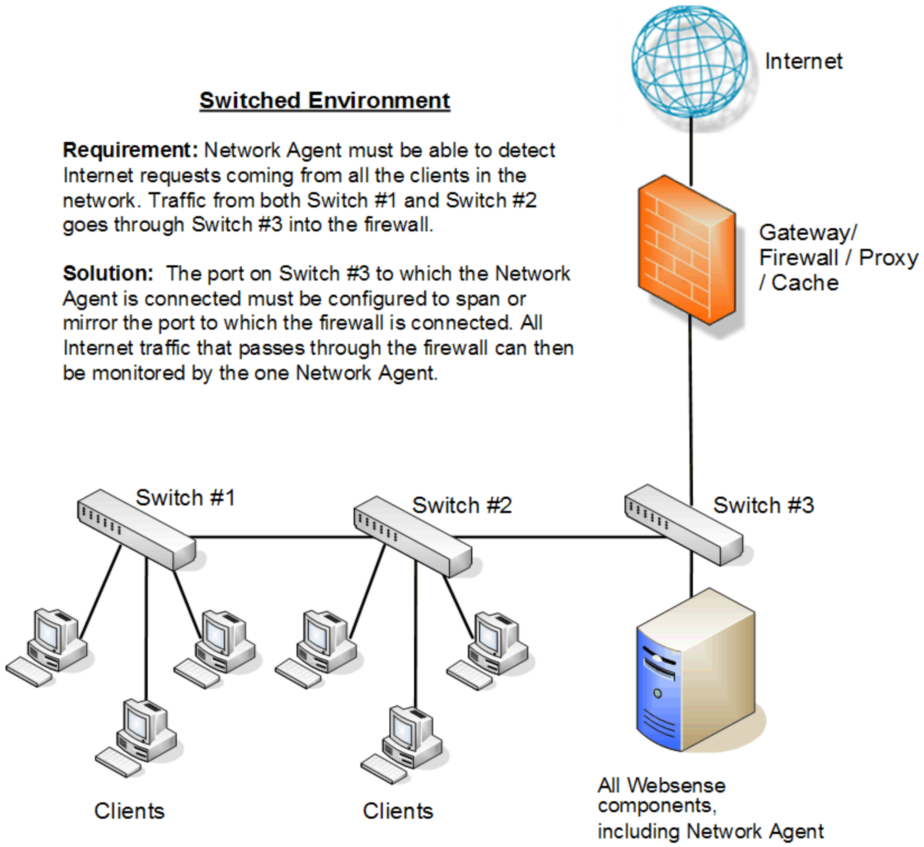
Single Switch Environment

Requirement: Network Agent must be able to monitor traffic coming from all the workstations in the network.

Solution: The port to which the Network Agent is connected must be configured to span or mirror the port to which the firewall is connected. All Internet traffic that passes through the firewall can then be monitored by the Network Agent.

Figure 6 Simple deployment in a switched environment

Figure 7 shows the use of additional switches to create 2 network segments. All Internet traffic from these network segments must pass through Switch #3, to which Network Agent is attached. In a multiple switch environment, failure to enable port spanning or mirroring could result in missed filtering and inaccurate reports.



Switched Environment

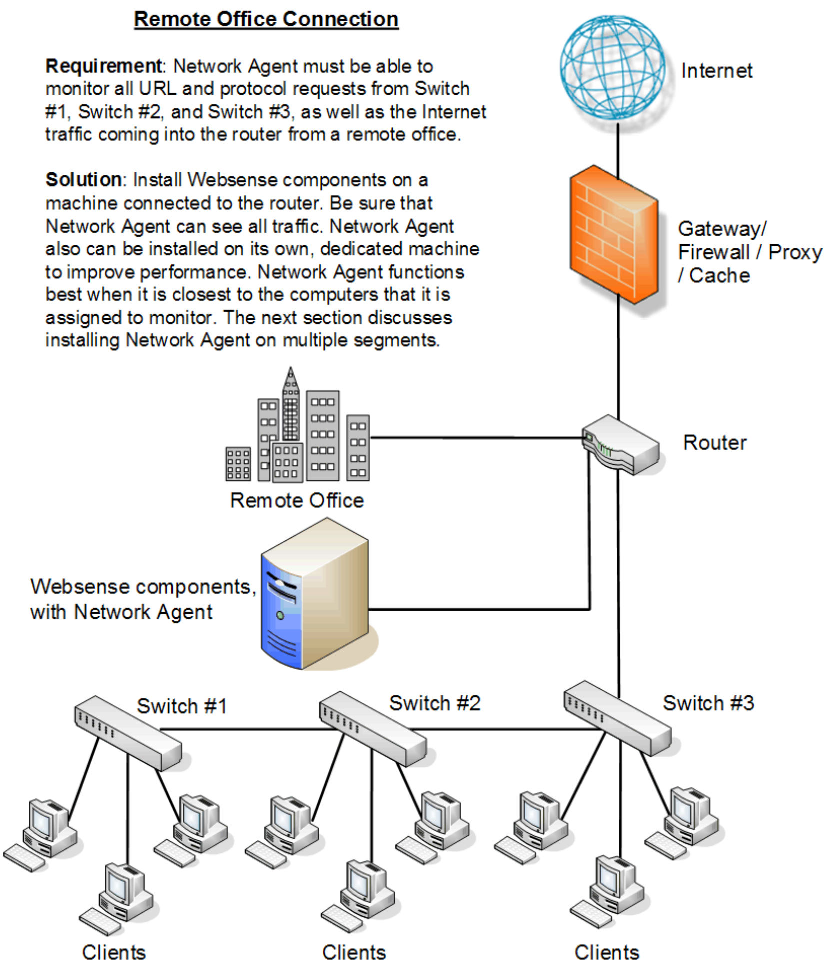
Requirement: Network Agent must be able to detect Internet requests coming from all the clients in the network. Traffic from both Switch #1 and Switch #2 goes through Switch #3 into the firewall.

Solution: The port on Switch #3 to which the Network Agent is connected must be configured to span or mirror the port to which the firewall is connected. All Internet traffic that passes through the firewall can then be monitored by the one Network Agent.

Internet
Gateway/ Firewall / Proxy / Cache
Switch #1
Switch #2
Switch #3
Clients
Clients
All Websense components, including Network Agent

Figure 7 Multiple subnets in a switched environment

Figure 8 also contains multiple network segments. This network adds a router for communication with a remote office. The machine running Network Agent is connected to an additional switch.



Remote Office Connection
Requirement: Network Agent must be able to monitor all URL and protocol requests from Switch #1, Switch #2, and Switch #3, as well as the Internet traffic coming into the router from a remote office.
Solution: Install Websense components on a machine connected to the router. Be sure that Network Agent can see all traffic. Network Agent also can be installed on its own, dedicated machine to improve performance. Network Agent functions best when it is closest to the computers that it is assigned to monitor. The next section discusses installing Network Agent on multiple segments.
Internet
Gateway/ Firewall / Proxy / Cache
Router
Remote Office
Websense components, with Network Agent
Switch #1
Switch #2
Switch #3
Clients
Clients
Clients

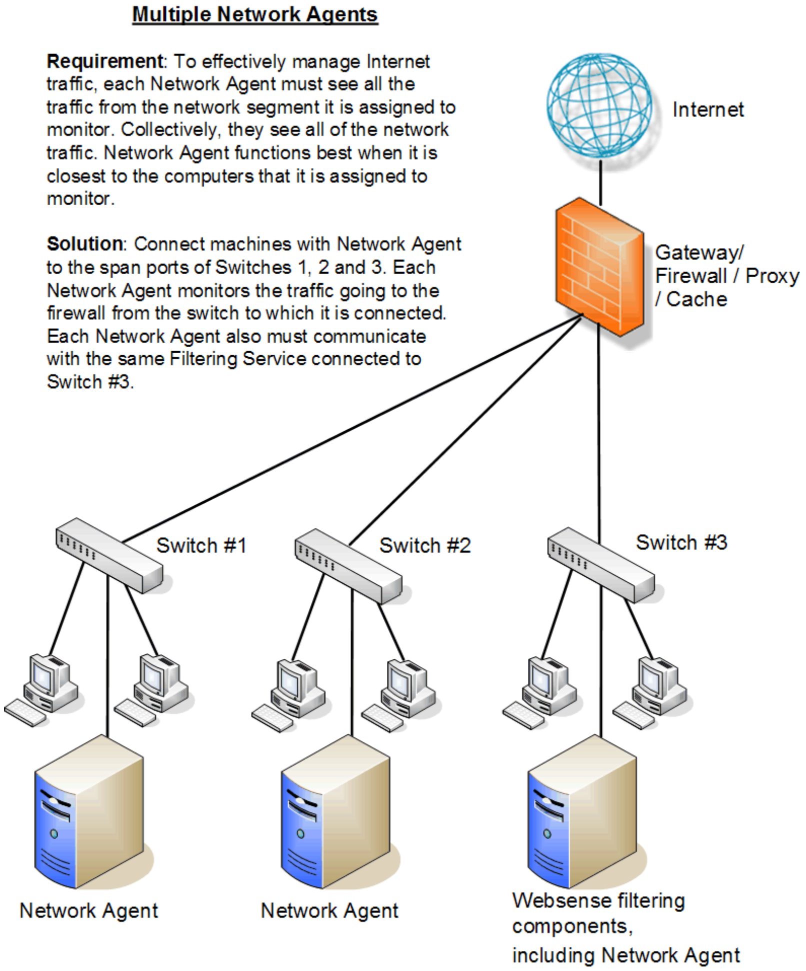
Figure 8 Switched environment with a remote office connection

Network Agent can also be positioned closer to the clients, as shown in Figure 9, page 58.

Switched networks with multiple Network Agents

A busy network may need multiple Network Agents to monitor different network segments or IP address ranges. Network Agent operates best when it is closer to the computers it is assigned to monitor. Figure 9 shows a network in which multiple Network Agent instances monitor separate network segments.

See *Deploying multiple Network Agents*, page 51, for more information.



Multiple Network Agents

Requirement: To effectively manage Internet traffic, each Network Agent must see all the traffic from the network segment it is assigned to monitor. Collectively, they see all of the network traffic. Network Agent functions best when it is closest to the computers that it is assigned to monitor.

Solution: Connect machines with Network Agent to the span ports of Switches 1, 2 and 3. Each Network Agent monitors the traffic going to the firewall from the switch to which it is connected. Each Network Agent also must communicate with the same Filtering Service connected to Switch #3.

Internet
Gateway/ Firewall / Proxy / Cache
Switch #1
Switch #2
Switch #3
Network Agent
Network Agent
Websense filtering components, including Network Agent

Figure 9 Multiple Network Agents in a switched environment

Gateway configuration

A gateway provides a connection between two networks. The networks do not need to use the same network communication protocol. The gateway can also connect a network to the Internet.

Network Agent can be installed on the gateway machine, allowing Network Agent to manage and monitor all Internet traffic. The gateway can either be a third-party proxy server or a network appliance. Do **not** install Network Agent on a firewall.

Important

The gateway configuration shown here is best used in small to medium networks.

In larger networks, performance can suffer as a result of resource competition between the gateway software and Network Agent.

Figure 10 shows Network Agent monitoring the Internet traffic at the proxy gateway or caching appliance directly attached to the firewall.

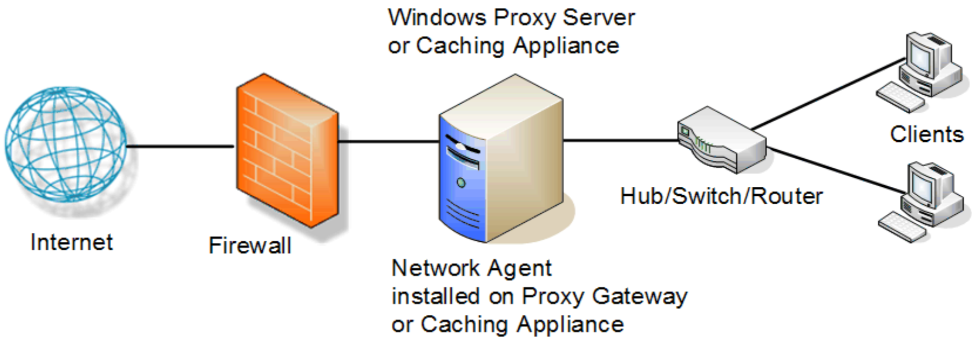


Figure 10 Network Agent installed on the gateway

Figure 11 shows Network Agent deployed in a network that includes Websense Content Gateway. Do not install Network Agent on the Websense Content Gateway machine.

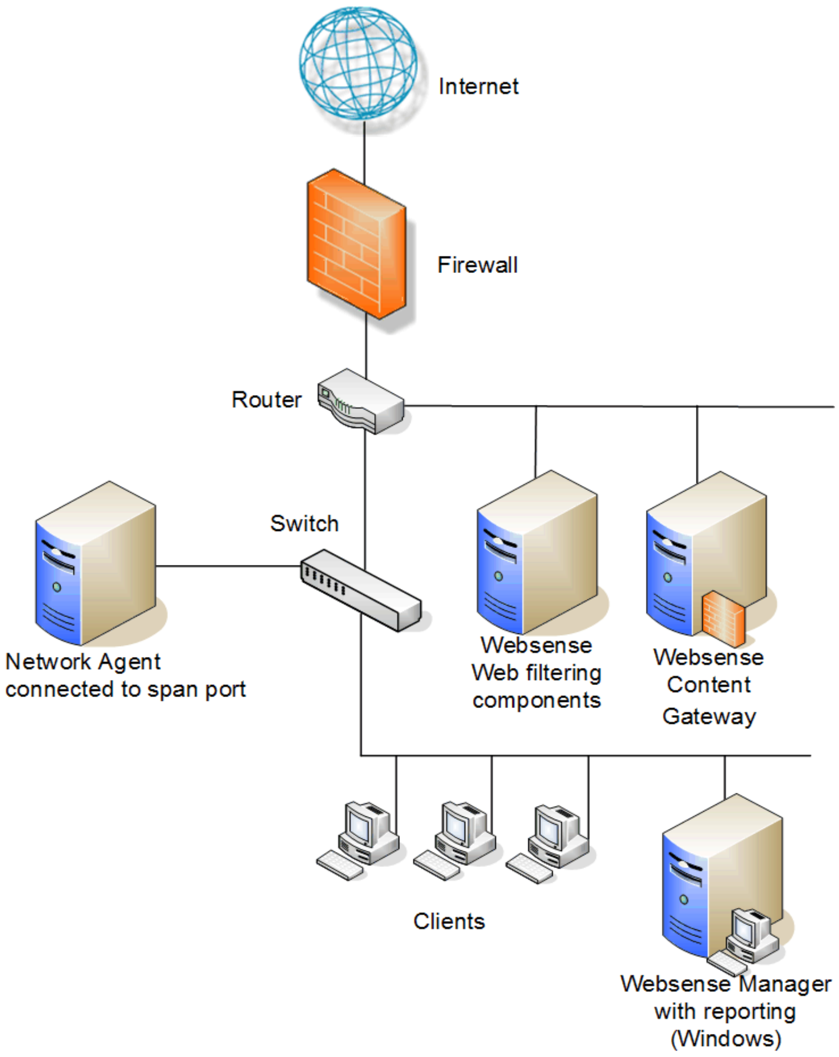

Internet
Firewall
Router
Switch
Network Agent connected to span port
Websense Web filtering components
Websense Content Gateway
Clients
Websense Manager with reporting (Windows)

Figure 11 Network Agent deployed with Websense Content Gateway

Using multiple NICs

Network Agent is capable of using more than one network card (NIC).

- Best practices suggest a maximum of 5 NICs
- The NICs can be connected to ports on the same network device (switch or router), or to different network devices.

If the machine running Network Agent has multiple NICs:

- Only one instance of Network Agent can be installed on the machine.
- The blocking or inject NIC (used to serve block pages) must have an IP address.
- Each NIC can be configured to monitor or block Internet requests, or both.
- Each NIC can be configured to monitor a different network segment.
- At least one NIC must be configured for blocking.

When you configure separate network cards to monitor traffic and send block messages (shown in Figure 12, page 62):

- The monitoring and blocking NIC do not have to be assigned to the same network segment.
- The monitoring NIC must be able to see all Internet traffic in the network segment that it is assigned to monitor.
- Multiple monitoring NICs can use the same blocking NIC.
- The blocking NIC must be able to send block messages to all machines assigned to the monitoring NICs, even if the machines are on another network segment.
- A monitoring NIC can be set for **stealth mode** (no IP address). For information on configuring stealth mode, see the Websense Web Security and Websense Web Filter *Installation Guide*.
- The blocking NIC **must** have an IP address (cannot be set to stealth mode).

The installer requests the IP addresses for the NICs that Websense software uses for communication, and for the NICs that Network Agent uses to monitor traffic. For more information, see the Websense Web Security and Websense Web Filter *Installation Guide*.

For information on configuring multiple NICs, consult the Websense Manager Help.

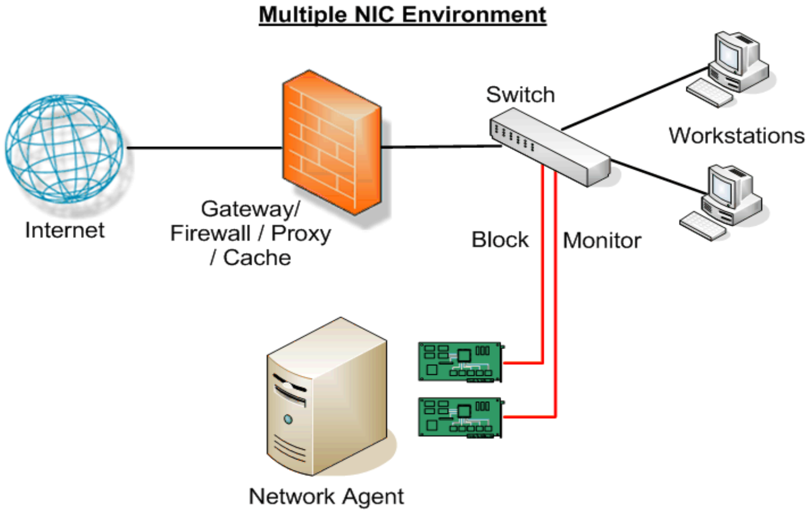


Figure 12 Dual NIC configuration

NAT and Network Agent deployment

If you use Network Address Translation (NAT) on internal routers, Network Agent may be unable to identify the source IP address of client machines. When Network Agent detects traffic after being passed through such a router, the agent sees the IP address of the router’s external interface as the source of the request, rather than the IP address of the client machine.

To address this issue, either disable NAT, or install Network Agent on a machine located **between** the NAT router and the monitored clients.

4 Integration Deployment

This chapter addresses considerations for deploying Websense components with an integration product (such as a firewall, proxy, or caching application).

Most of the network diagrams included in this chapter show a typical small network installation (500 users or fewer). The diagrams show the recommended location of your integration product relative to Websense components.

- The diagrams are intended to provide a general overview, and do not show all Websense components.
- Larger networks require that Websense components be distributed across several dedicated machines. See the *Deployment Guide Supplements* for more information.

> ✓ **Note**
> DC Agent is listed as the transparent identification agent in many of the diagrams in this chapter. Logon Agent can also be used.

Websense Content Gateway

Websense Content Gateway™ is a central gateway for controlling Web content that offers:

- The advantages of a proxy cache, improving bandwidth usage and network performance by storing requested Web pages and, if the page is still considered "fresh," serving the Web page to the requesting client.
- Real-time content categorization. This feature examines the content of uncategorized sites and sites that include rapidly changing content, and then returns a recommended category to Filtering Service.

Websense Content Gateway can run in explicit or transparent proxy mode.

- In explicit proxy mode, client browsers must be configured to point to the proxy.
- In transparent proxy mode, the client request is intercepted and redirected to the proxy. Traffic is redirected through a router or a Layer 4 switch and the ARM (Adaptive Redirection Module) feature of the proxy.

Websense Content Gateway can participate in flexible cache hierarchies, where Internet requests not fulfilled in one cache can be routed to other regional caches. The gateway also scales from a single node into multiple nodes that form a cluster, to improve system performance and reliability.

Websense Content Gateway is installed on a Linux machine, separate from other Websense components. See the Websense Content Gateway *Installation Guide* for more information.

Figure 13 shows Websense Content Gateway and Websense Data Security Suite deployed with Websense Web filtering components (including Policy Broker, Policy Server, Filtering Service, User Service, and a transparent identification agent).

- The Websense Data Security Suite, Websense Content Gateway, and Websense filtering component machines access network traffic through a router.
- Network Agent is installed on a separate machine, attached to the span port on a switch.

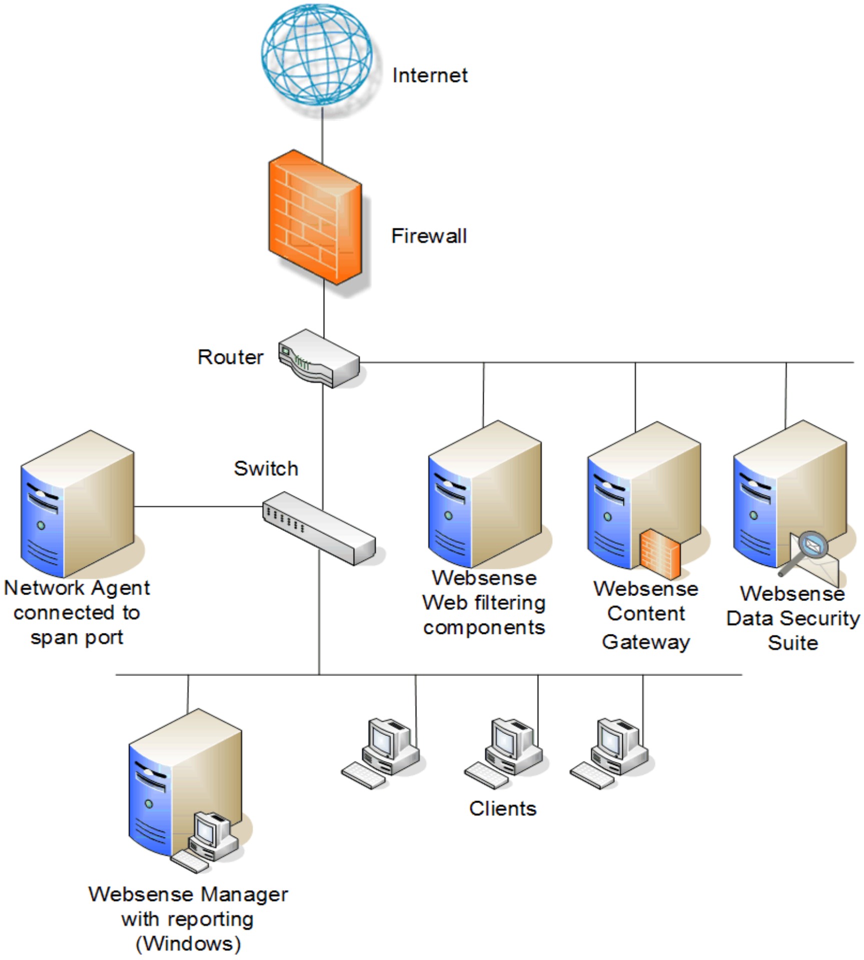

Internet
Firewall
Router
Switch
Network Agent connected to span port
Websense Web filtering components
Websense Content Gateway
Websense Data Security Suite
Clients
Websense Manager with reporting (Windows)

Figure 13 Integration with Websense Content Gateway

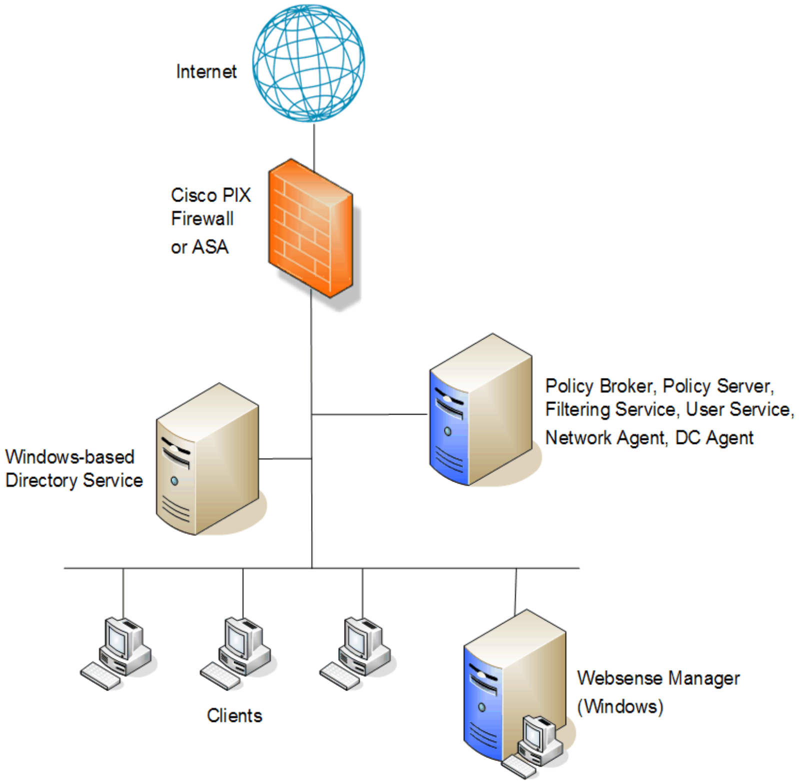
Cisco deployment

A simple and common network topology places Websense filtering components on a single machine, or group of dedicated machines, communicating with the Cisco PIX Firewall or Cisco Adaptive Security Appliance (ASA) via TCP/IP.

- Websense reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

See the *Installation Guide Supplement for use with Cisco Integrated Products* for configuration instructions.

Figure 14 Common Windows Network Configuration for Cisco PIX Firewall or ASA



Other configurations are possible. Consult your Cisco PIX Firewall or ASA documentation and the information in this section to determine the best configuration for your network.

Cisco Content Engine

In this common configuration, Websense filtering components are installed on a single machine, communicating with the Cisco Content Engine through TCP/IP.

- Websense reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

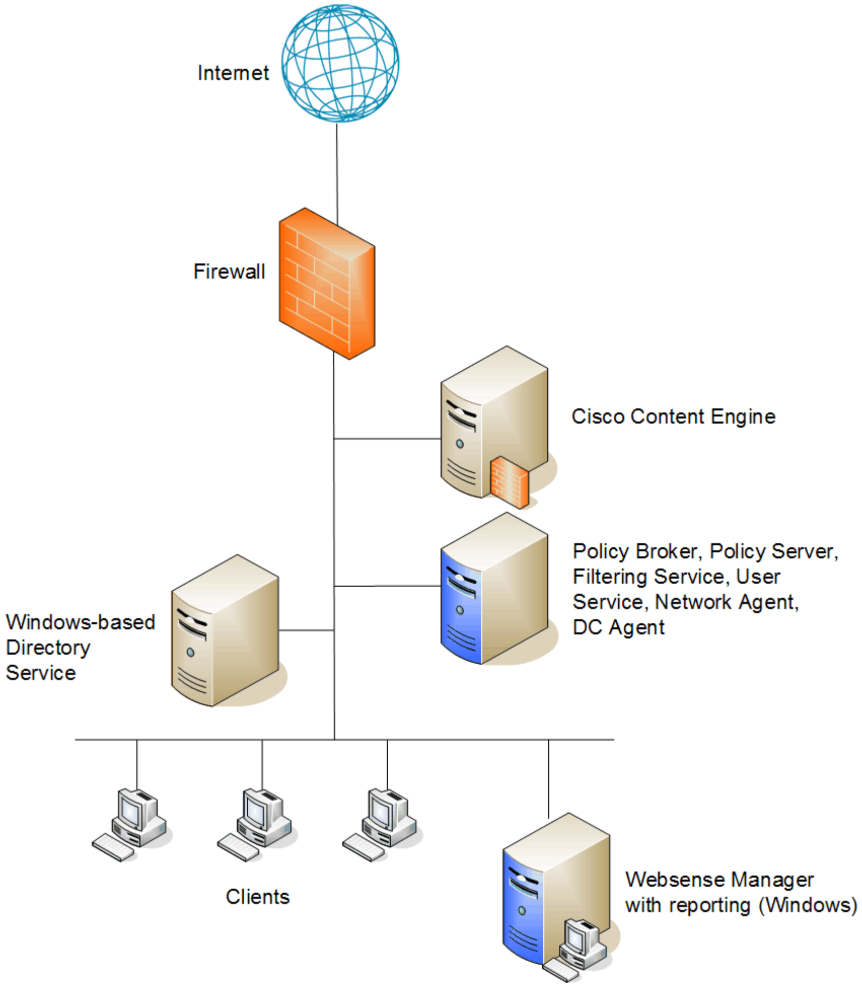

Internet
Firewall
Cisco Content Engine
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent, DC Agent
Windows-based Directory Service
Clients
Websense Manager with reporting (Windows)

Figure 15 Common Windows network configuration for Cisco Content Engine

Other configurations are possible. Consult your Content Engine documentation and the information in this chapter to determine the best configuration for your network.

Cisco IOS Routers

In this common configuration, Websense filtering components are installed on a single machine, communicating with the Cisco IOS Router.

- Websense reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

The router has firewall functionality and can be used with or without an accompanying firewall.

If the Cisco IOS Router is used with a separate firewall, ensure that all Internet traffic is configured to pass through the router and is not set to bypass the router and go directly to the firewall. Traffic filtered through the separate firewall cannot be filtered by the Websense software.

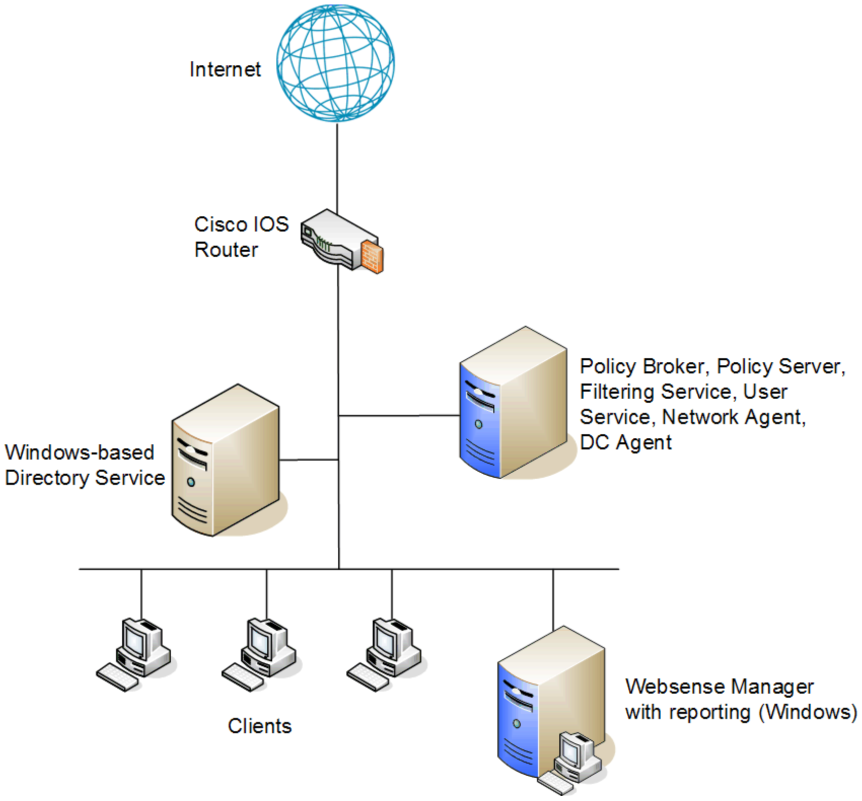

Internet
Cisco IOS Router
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent, DC Agent
Windows-based Directory Service
Clients
Websense Manager with reporting (Windows)

Figure 16 Common Windows network configuration for Cisco IOS Routers

Other configurations are possible. Consult your Cisco Router documentation and the information in this chapter to determine the best configuration for your network.

Check Point

This section includes a general discussion of 2 common Check Point integration deployment options: simple deployment with unified components, and distributed deployment. See the *Installation Guide Supplement for use with Check Point Integrated Products* for configuration instructions.

Simple

In the simplest and most common network topology, an organization has one firewall that resides on a dedicated server. All Websense filtering components are installed on a separate machine on the internal network.

- Websense reporting components are installed on a separate machine.
- If you install Network Agent, it must be positioned to see all traffic on the internal network.

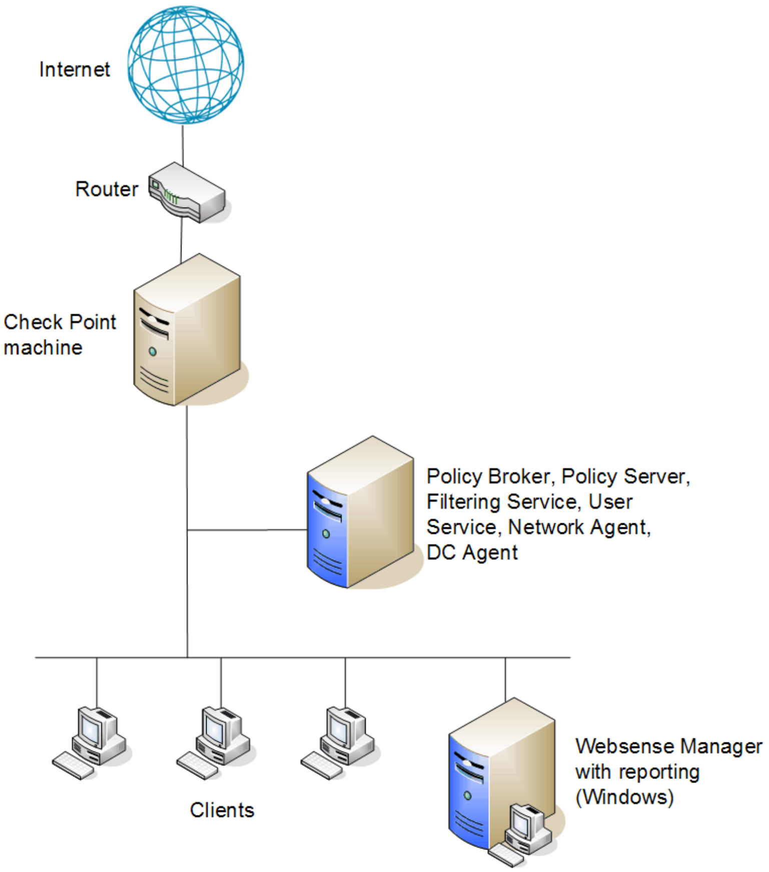

Internet
Router
Check Point machine
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent, DC Agent
Clients
Websense Manager with reporting (Windows)

Figure 17 Simple network configuration

Distributed

In Figure 18, Websense filtering software is installed on a single machine in a central location where it can manage both protocol and HTTP traffic. HTTP requests are handled by the Check Point appliance, and the non-HTTP traffic is managed by Network Agent, which is positioned to detect all outbound traffic.

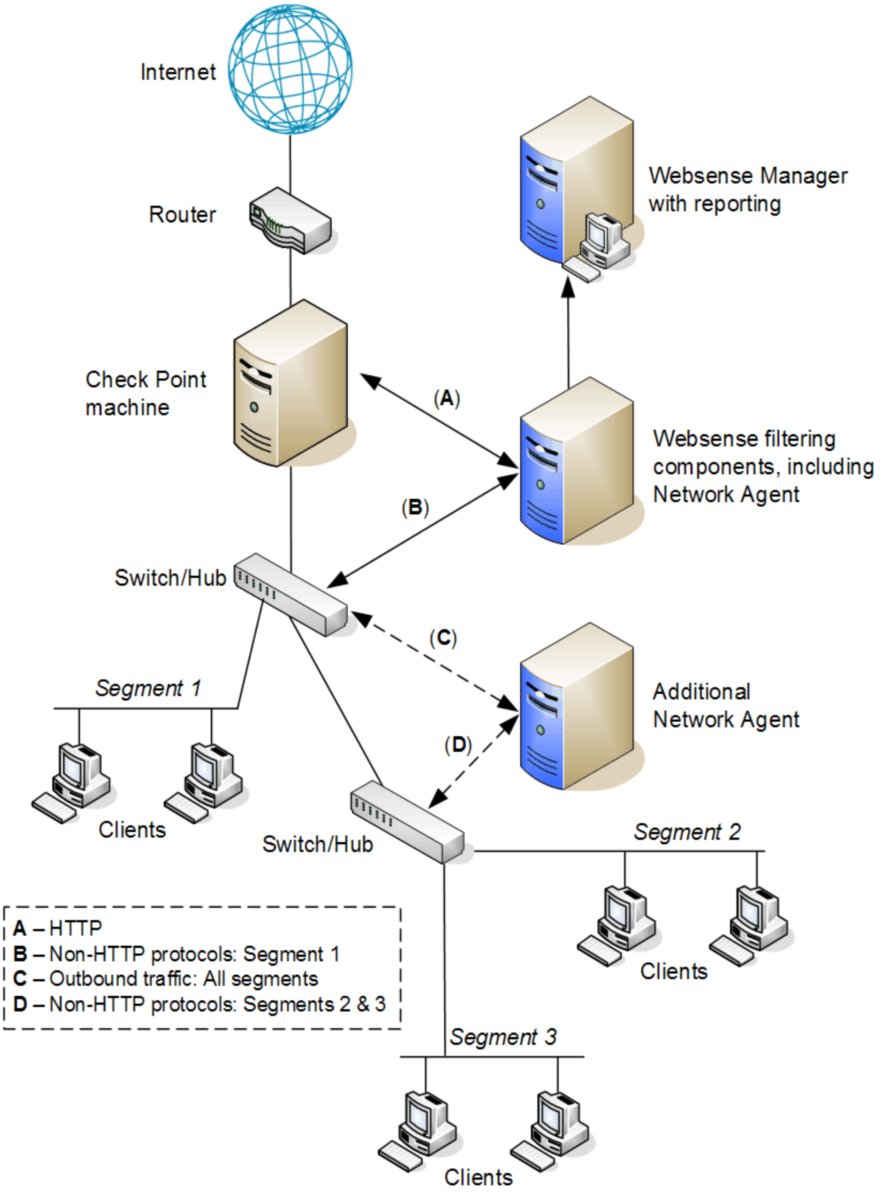

Internet
Router
Websense Manager with reporting
Check Point machine
(A)
Websense filtering components, including Network Agent
(B)
Switch/Hub
(C)
Segment 1
Additional Network Agent
(D)
Clients
Switch/Hub
Segment 2
A – HTTP
B – Non-HTTP protocols: Segment 1
C – Outbound traffic: All segments
D – Non-HTTP protocols: Segments 2 & 3
Clients
Segment 3
Clients

Figure 18 Multi-Segmented network configuration

To avoid performance and security issues, do **not** install Websense components on a machine running Check Point software, unless the machine is a blade server that has separate processors to accommodate each product. Network Agent will not function correctly if installed on the Check Point machine.

Warning

Websense, Inc., and Check Point do not recommend installing Websense software and Check Point on the same machine. Do **not** install Network Agent on the same machine as Check Point software.

Microsoft ISA Server

When you integrate Websense software with Microsoft ISA Server, the Websense ISAPI plug-in must be installed on the ISA Server machine. The plug-in allows Microsoft ISA Server to communicate with Filtering Service, and must be installed on every ISA Server machine that communicates with Websense software.

- You can install Policy Broker, Policy Server, Filtering Service, and User Service on the same machine as Microsoft ISA Server.
- When Websense filtering software is installed on the same machine as Microsoft ISA Server, the Websense ISAPI Filtering plug-in must be installed at the same time.

If your environment includes an array of Microsoft ISA Server machines, install Websense software on a machine outside the array.

See the *Websense Installation Guide Supplement for use with Microsoft ISA Server* for instructions and more information.

Single Microsoft ISA Server configuration

Figure 19 shows all Websense components, including the Websense ISAPI Filter, running on the same machine as Microsoft ISA Server. Unless the Internet traffic volume is light, this configuration requires a powerful machine.

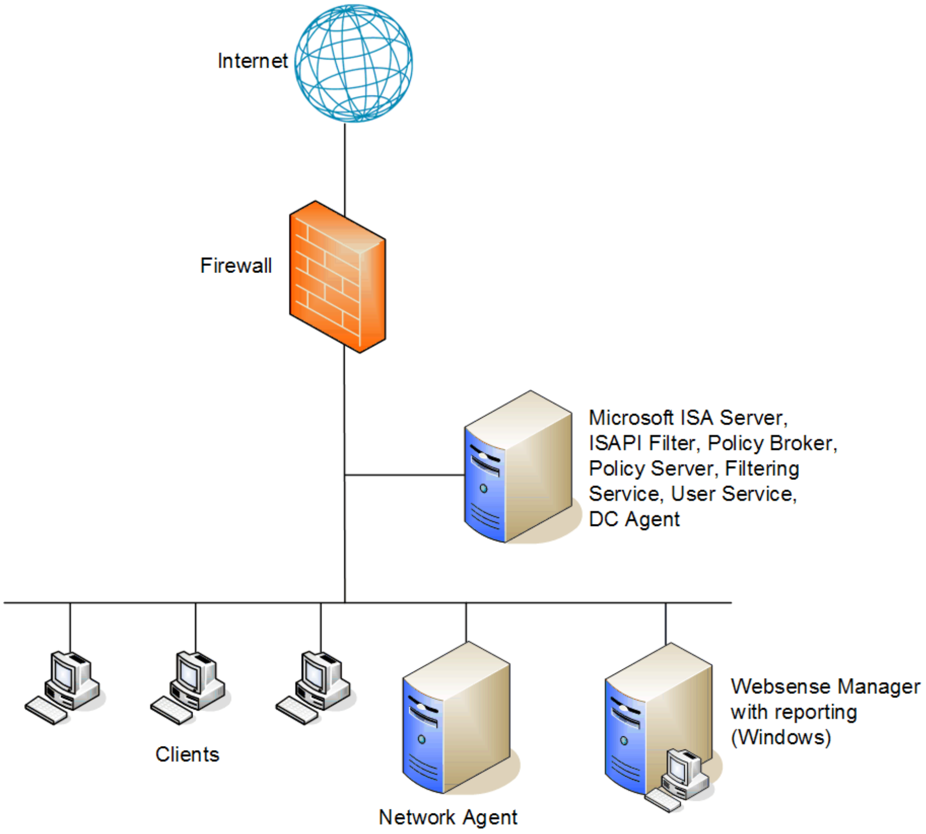


Figure 19 Filtering components installed with Microsoft ISA Server

An alternate setup, Figure 20, places Websense filtering components on a Windows machine separate from the Microsoft ISA Server machine. This configuration eases the load on the Microsoft ISA Server machine.

- The ISAPI Filter must be installed on the Microsoft ISA Server machine so that Internet activity information can be communicated to Filtering Service.
- The Filtering Service and Microsoft ISA Server machines must be able to communicate over the network.

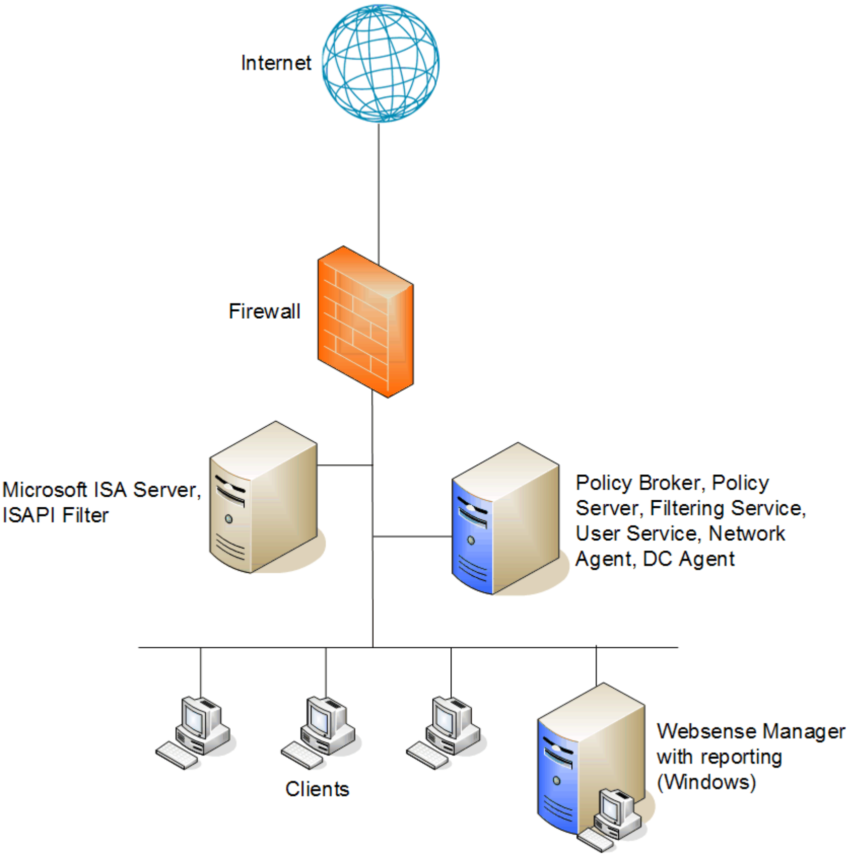

Internet
Firewall
Microsoft ISA Server, ISAPI Filter
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent, DC Agent
Clients
Websense Manager with reporting (Windows)

Figure 20 Filtering components installed separately from Microsoft ISA Server

Array configuration

Websense software is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. If the Microsoft ISA Server machines in the array can run Websense software without a performance impact, installing the Websense components on one of the array machines is recommended. In this configuration, the two applications do not have to communicate over the network.

Install the Websense ISAPI Filter on each Microsoft ISA Server machine in the array.

Figure 21 shows Websense filtering components running on a Microsoft ISA Server machine, with Websense Manager and Log Server installed on a computer that has network access to the Websense filtering machine.

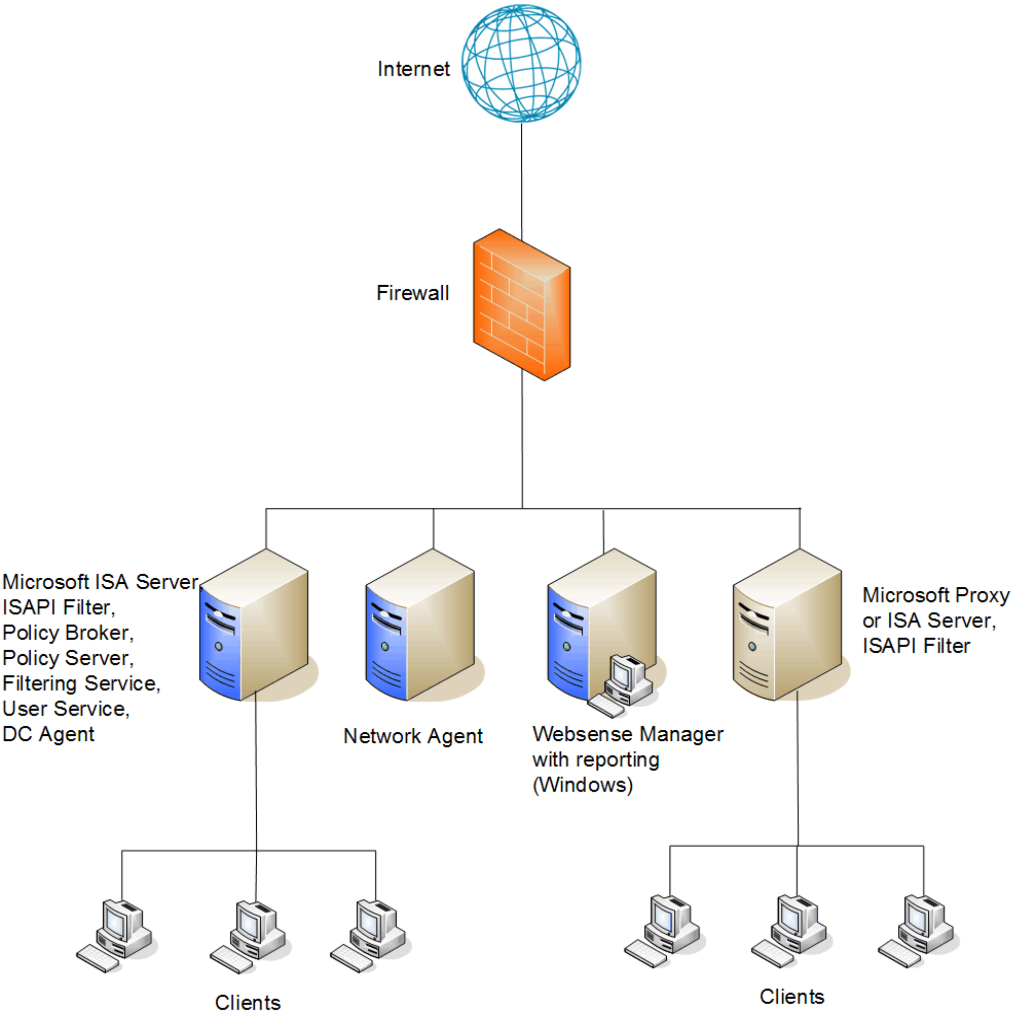


Figure 21 Microsoft ISA Server array configuration #1

If installing Websense filtering components on a Microsoft ISA Server machine is likely to have a performance impact, install Websense software outside the array. Install the Websense ISAPI Filter on each member of the array. See Figure 22.

When Websense software is deployed in this configuration, all array members send Internet requests to Filtering Service outside the array.

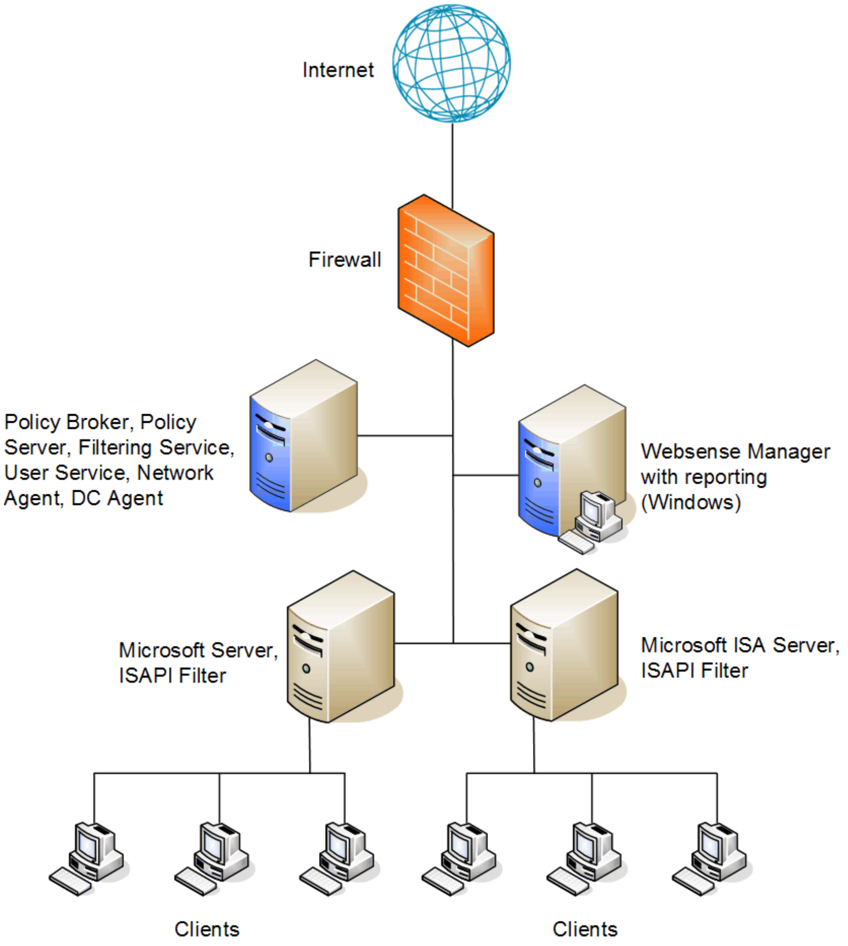

Internet
Firewall
Policy Broker, Policy Server, Filtering Service, User Service, Network Agent, DC Agent
Websense Manager with reporting (Windows)
Microsoft Server, ISAPI Filter
Microsoft ISA Server, ISAPI Filter
Clients
Clients

Figure 22 Microsoft ISA Server array configuration #2

Other configurations are possible. Consult your Microsoft ISA Server documentation for information about Microsoft ISA Server configurations.

Squid Web Proxy Cache deployment

Websense filtering components can be installed on the same machine as Squid Web Proxy Cache, on a separate machine, or on multiple machines.

Squid Web Proxy Cache machines may be deployed in an array to share the load in a larger network.

A Websense Squid plug-in must be installed on each machine running Squid Web Proxy Cache.

The diagrams in this section assume a Linux installation.

- If Websense filtering components are installed on a Windows machine, move Websense Manager to another machine.
- If you are running Websense Manager on Windows, do not install a second instance of Websense Manager on a Linux machine.

Single Squid Web Proxy Cache configuration

Figure 23 shows the Websense filtering components, the Squid plug-in, and the Squid Web Proxy Cache running on the same machine. In this configuration, the Websense filtering and components are installed on the Squid Web Proxy Cache machine. You can also install a Websense transparent identification agent on the same machine, or on a separate machine.

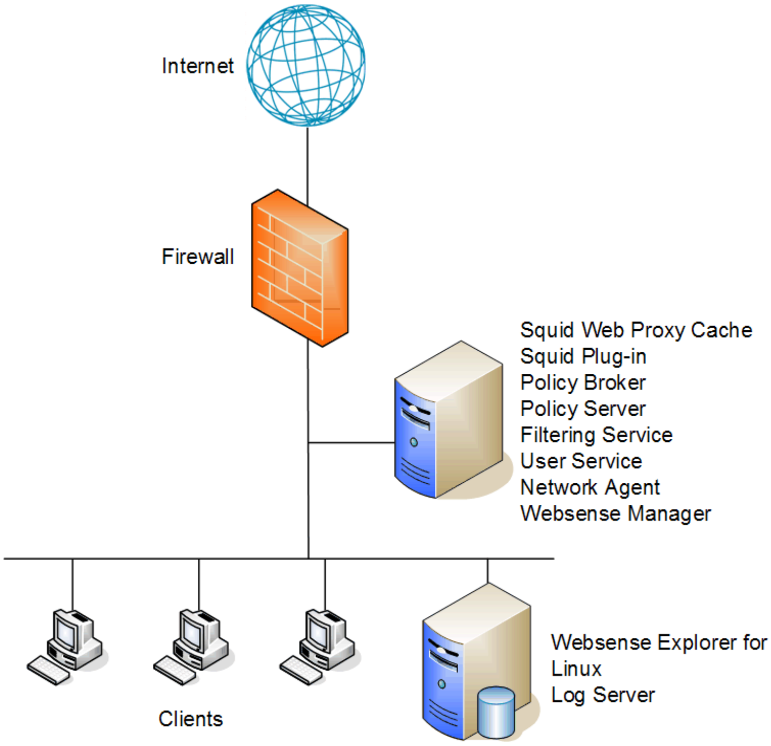


Figure 23 Filtering components installed with Squid Web Proxy Cache

An alternate deployment places all Websense filtering components on a separate machine from the Squid Web Proxy Cache. This configuration eases the load on the Squid Web Proxy machine.

- The Websense Squid Plug-in must be installed on the Squid Web Proxy machine to enable communication with Filtering Service.
- The Filtering Service and Squid Web Proxy machines must be able to communicate over the network.

Figure 24 Filtering components and Squid Web Proxy Cache on separate machines

Array configuration

Websense software is compatible with most array configurations, including Cache Array Routing Protocol (CARP) arrays. If the Squid Web Proxy Cache machines in an array can run Websense software without a performance impact, install the main Websense filtering components on one of the array machines. In this configuration, the two applications do not have to communicate over the network.

Figure 25 shows the Websense filtering components running on a Squid Web Proxy Cache machine, with Websense reporting components on a separate machine.

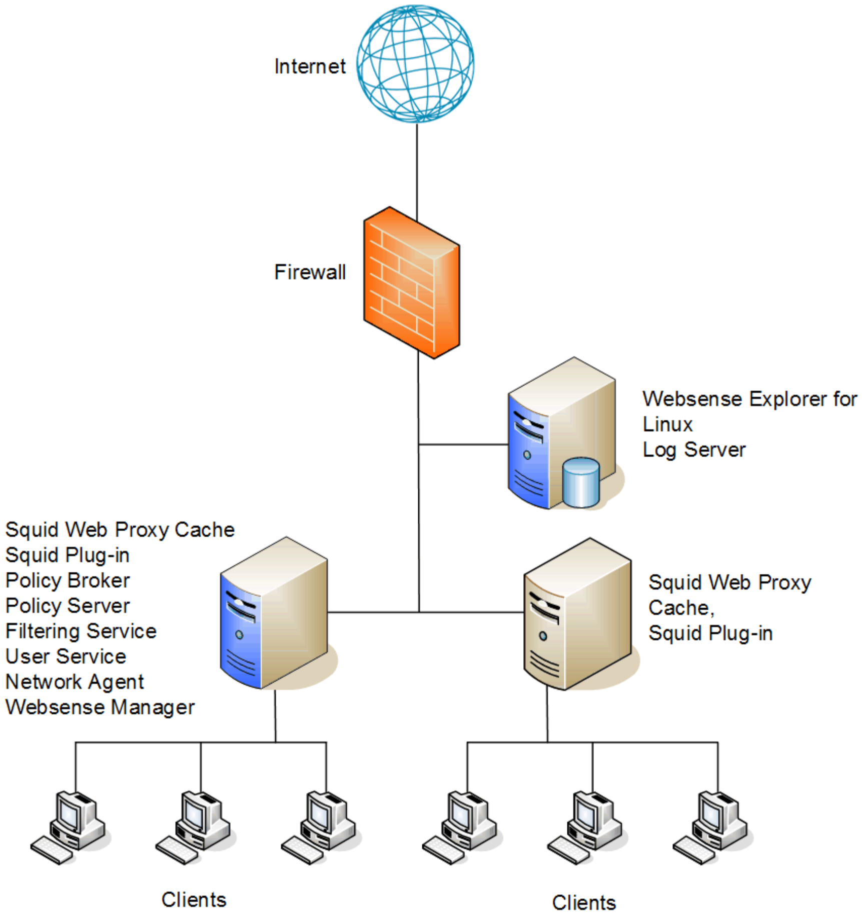


Figure 25 Squid Web Proxy Cache array configuration #1

If installing the Websense filtering components on the Squid Web Proxy Cache machine is likely to have a performance impact, install Websense software on a separate machine outside the array, and then install the Squid plug-in on each member of the array. See Figure 26.

When Websense software is installed in this configuration, all array members send Internet requests to Filtering Service outside the array.

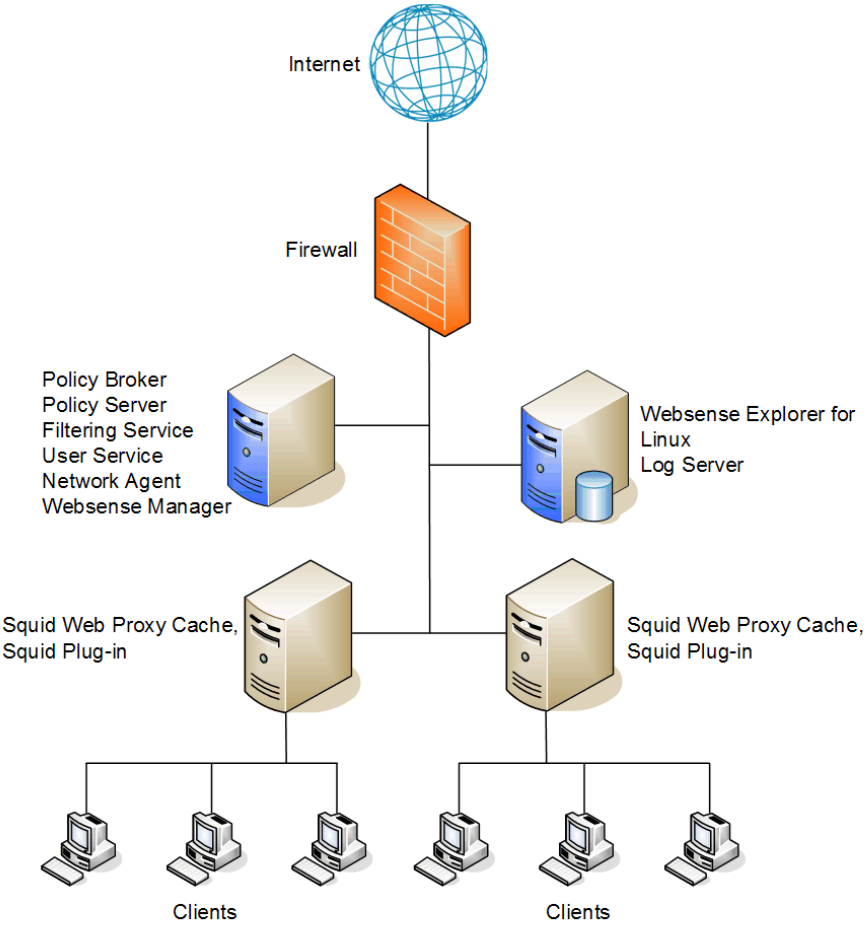


Figure 26 Squid Web Proxy Cache array configuration #2

Other configurations are possible. Consult your Squid Web Proxy Cache documentation for information about array configurations. See the *Installation Guide Supplement for use with Squid Web Proxy Cache* for Websense software configuration instructions.

NetCache integration

NetCache has been specifically enhanced to integrate with Websense software. When NetCache receives a client's Internet request, it queries Filtering Service to find out whether or not the site should be blocked. If the site is assigned to a permitted category, Filtering Service notifies NetCache that the site is not blocked, and the site is returned to the user.

Figure 29 shows Websense filtering components installed together on a single machine. Remember that Network Agent must be able to monitor all Internet traffic.

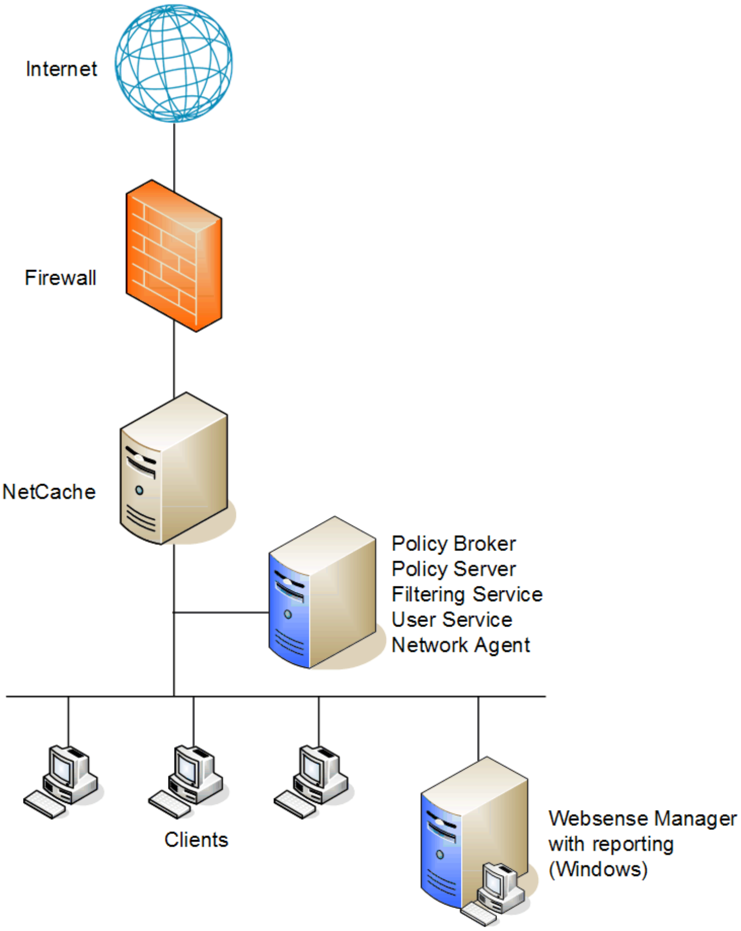


Figure 27 Common network configuration

Other configurations are possible. Consult your NetCache documentation for information about array configurations. See the *Installation Guide Supplement for use with NetCache* for Websense software configuration instructions.

Universal integration

If your firewall, proxy server, caching application, or network appliance is not one of the products listed in this chapter, you may still be able to integrate it with Websense software. Check the list of Websense Technology Partners at www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/ to see if Websense software can be integrated with the product. If your integration product is listed, that product has been specifically enhanced to integrate with Websense software.

Typical configurations include networks with a single firewall, proxy server, or caching application, and networks with an array of firewalls, proxy servers, or caching appliances. A Websense transparent identification agent (DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent) can be installed on the Filtering Service machine or on a separate machine.

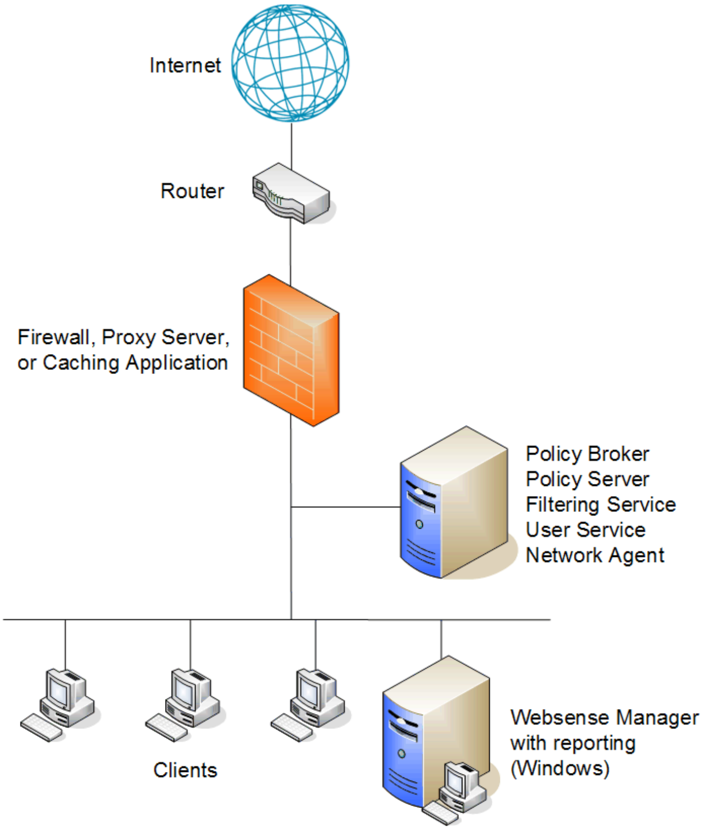


Figure 28 Common network configuration

Other configurations are possible. Consult your integration product’s documentation for other recommendations. See the *Installation Guide Supplement for use with Universal Integrations* for Websense software configuration instructions.

Citrix

Websense software integrated with a Citrix server can monitor HTTP, FTP, and SSL requests from individual Citrix users. Network Agent can be used to filter other protocols, if needed.

Figure 29 shows a typical deployment used to filter both users who access the Internet through a Citrix server and users who access the Internet locally.

- The Websense filtering components are installed on a dedicated machine that can filter both the Citrix server clients and the non-Citrix clients.
- 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.

Separate Network Agent instances are needed for the Citrix and non-Citrix users.

To simplify the diagram, not all individual Websense components are shown.

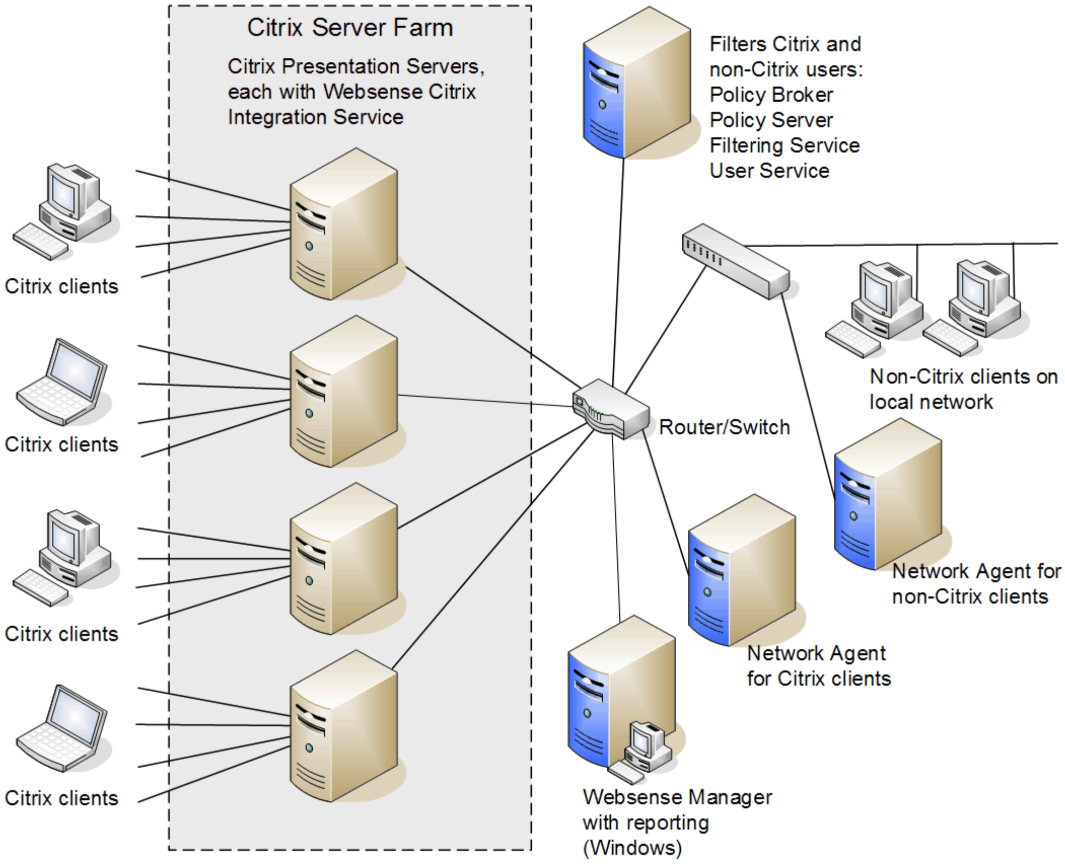

Citrix Server Farm
Citrix Presentation Servers, each with Websense Citrix Integration Service
Filters Citrix and non-Citrix users:
Policy Broker
Policy Server
Filtering Service
User Service
Citrix clients
Citrix clients
Citrix clients
Citrix clients
Non-Citrix clients on local network
Router/Switch
Network Agent for non-Citrix clients
Network Agent for Citrix clients
Websense Manager with reporting (Windows)

Figure 29 Citrix integration

Other integrations also can be used in the non-Citrix portion of the network. See the *Installation Guide Supplement for use with Integrated Citrix Servers* for Websense software configuration instructions.

Index