DEPLOYMENT GUIDE

Websense Enterprise®
Websense® Web Security Suite™

v6.3.2

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

Published January 26, 2008
Printed in the United States of America and Ireland

Trademarks

Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

The *Websense® Deployment Guide* provides an overview of how Websense software can be deployed in a network, plus operating system and hardware requirements. The information in this document is especially useful for planning the deployment before installing the product.

This guide applies to:

- Websense Enterprise®
- Websense Web Security Suite™

Any references mentioning *Websense Enterprise* apply to both editions.

Websense software consists of components which work together to monitor internet requests, log activity, and apply filters. Websense components can be installed together on 1 machine, or distributed across multiple machines. 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 Websense components. The remaining chapters in this document include:

- *Chapter 2: General Deployment Recommendations*—provides 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 in Networks up to 10,000 Users*—provides hardware and deployment recommendations for networks with fewer than 10,000 users.
- *Chapter 4: Deploying in Networks with Over 10,000 Users*—provides hardware and deployment recommendations for networks with more than

10,000 users. Deployment of Websense software over a distributed enterprise network with remote offices is also discussed.

- *Chapter 5: Deploying Network Agent*—discusses deployment across single and multiple segment networks. Network Agent location is also discussed, along with settings, and configurations in relation to hubs, switches and gateways.

> **Note**
> Please contact Websense Sales Engineering for assistance in designing a deployment. A Field System Engineer can help determine hardware needs and the Websense component deployment.

Websense Components

Table 1, on page 13 provides a brief description of the Websense components that are discussed in this guide. This table groups the components into *core* (required) and *optional*.

Table 2, on page 16, provides a brief description of the Websense Reporting components that are discussed in this guide. Reviewing these component descriptions helps to clarify the interaction of the components. See Table 3, on page 20 and Table 4, on page 27 for information on the operating system versions needed to run these components.

> **NOTE**
> Certain integrations include Websense plug-in components. These plug-ins are discussed in Table 9, on page 56.

Table 1 Websense Components

Component	Definition
Core Components	
Bandwidth Optimizer™	Allows limits to be set on Internet access based on bandwidth availability. Network Agent enables this threshold filtering, or filtering of particular types of internet content based on available network bandwidth.
Filtering Service (formerly EIM Server)	Receives internet requests, determines the appropriate filtering policy, and either permits the request or sends the appropriate block message. Filtering Service is typically installed on the same machine as Policy Server.
Network Agent	Detects network activity to support the Protocol Management, Bandwidth Optimizer, IM attachments, and reporting on bytes transferred of a session. In the Stand-Alone edition, Network Agent also provides filtering for HTTP and HTTPS, plus non-HTTP protocols, such as instant messaging, streaming media, FTP, and others.
Policy Server	Stores Websense software configuration information and communicates this information to the other Websense components. Policy Server also logs event messages for Websense components. Policy Server is typically installed on the same machine as Filtering Service.
User Service	Communicates with the directory service to apply filtering policies based on users, groups, domains and organizational units. The directory service is not an element of Websense, but can be either Windows®-based, or LDAP-based directory service.
Websense Manager	An administrative interface that communicates with Policy Server to configure and manage the Websense software functionality. Websense Manager can be installed on the same machine as Policy Server, and also on one or more different machines on the network. A minimum monitor screen resolution of 1024 x 768 is required.

Table 1 Websense Components

Component	Definition
Websense Master Database	A downloadable list of internet sites, each categorized by content. Network protocols are also contained in this database.
Optional Components	
DC Agent[1]	An optional component that polls the identified domain controllers in the network, to transparently identify users. The DC Agent can also query the workstations at a preset interval to ensure the same user is associated with an IP address.
eDirectory Agent [1, 2]	An optional component that works with a Novell® eDirectory™ server to transparently identify users so Websense software can filter them according to particular policies assigned to users or groups.
Logon Agent[1]	Provides user information to Websense components when a user logs onto the network via a Windows workstation.
Logon Application	Deployed to Window-based workstations to capture logon sessions as users log on to Windows domains in the network. Identifies the user, and sends the information to the Logon Agent.
RADIUS Agent[1, 3]	An optional component that enables Websense software to transparently identify users who access the network using a dial-up, virtual private network (VPN), Digital Subscriber Line (DSL), or other remote connection (depending on the network configuration).
Remote Filtering Client	Allows filtering of remote users outside of the corporate firewall. For example, an employee who is traveling and is using a laptop to access the internet outside the corporate network.
Remote Filtering Server	Acts as a proxy that accepts requests from Remote Filtering Clients and submits them for filtering.

Table 1 Websense Components

Component	Definition
Usage Monitor	Tracks the users' internet activity and sends alerts when the activity for particular URL categories or network protocols reaches configurable threshold limits. The alerts are sent to designated people via email or an on-screen display. An SNMP alert also can be sent to an SNMP Trap Server for delivery to a network management system.

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 37.
2. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.
3. Multiple instances of the RADIUS Agent cannot be installed on the same machine. 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.) For more information, see the *Transparent Identification of Users in Websense Enterprise* technical white paper. See the Websense Product Documentation site—www.websense.com/global/en/SupportAndKB/ProductDocumentation/.

Reporting Components

All reporting modules and their components rely on the other Websense software. The reporting components are always installed after the other Websense software.

The filtering components, such as Filtering Service, Policy Server, User Service, etc., must be running in order for logging to work.

For more information on how Reporter and Websense software work together, see the *Websense Enterprise Reporter Administrator's Guide*.

For more information on installing Websense Reporter and Explorer products, see the *Websense Enterprise Reporting Installation Guide*.

Table 2 Reporting Components

Component	Definition
Database Components	
Database Engine	In a Windows environments, reporting components require either Microsoft® SQL Server or MSDE. MySQL is required for Explorer for Unix. MSDE is not included with the Websense installation, but a link to install MSDE is included with the Reporting installation.
Log Database	Required storage for data about internet activity. This database contains the activity records of Filtering Service, as gathered by the Log Server, and used by Reporter and Explorer to create reports. This database is created when Log Server is installed.
Log Server/Unix Log Server	Records and stores internet activity on the network in the Log Database. Log Server can log to only 1 Log Database at a time. Also, only 1 Log Server can be installed for each Policy Server.
Database Administration (replaced Database Manager)	Allows management of the Log Database with scheduled rollovers and automatic creation of database partitions. When a partition's threshold is exceeded, a new partition is created. If incoming records are outside the date and time range for a partition, the data is written to the appropriate partition.
Reporting applications	
Explorer/Explorer for Unix	A web-based application that generates a variety of easy-to-understand detailed and summary reports from data stored in the Log Database as well as archived data. Explorer utilizes a: • Web server—either Microsoft IIS (Windows-only) or Apache 2.0.50 (Apache is included in the installation package). • Web browser—Microsoft Internet Explorer® 5.5 or later (not included in installation).

Table 2 Reporting Components

Component	Definition
Real-Time Analyzer (RTA)	A web-based application that displays the real-time status of the traffic filtered by Websense software, using Internet Explorer 5.5 or later. RTA graphically displays bandwidth information and shows requests by category or protocol. RTA can run on either Apache 2.0.50 or Microsoft IIS web servers. (Apache is included in the installation package). A minimum screen resolution of 1024 x 768 is required.
Reporter	Displays reports based on specific templates. Over 80 report formats are available, and are grouped by type into Trend, Management, Detail, and Summary. Select a report type and filter criteria; then generate a report. From a single window, a report type can be selected, and the report can be viewed, sent via email or printed. A minimum screen resolution of 1024 x 768 is required.

Log Server, Log Database and the Database Engine are required to run Reporter, Explorer and Database Administration.

CHAPTER 2

General Deployment Recommendations

Operating system requirements for running Websense components are listed in this chapter, along with component limits, and tips for maximizing performance. See Chapter 1 for definitions of these components. Note that Websense filtering is based on protocols, not on the operating system of the user workstation being filtered.

Recommendations are also provided for deploying the transparent identification agents, Remote Filtering and the Stand-Alone Edition. Version requirements for various integrations is also included. Later chapters provide recommendations for deploying Websense software in different size networks.

System Software Requirements

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

Note

The Websense components have been successfully tested on the operating systems listed in these tables. The components may run on subsequent versions of these operating systems, but had not been tested as of this writing.

Table 3 lists each component and its required operating systems, along with other software required to run the component. Table 4, on page 27 organizes the requirements by operating system.

Table 9, on page 56 lists the supported integration versions.

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
Database Administration	• Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	• Installed with Enterprise Explorer • Internet Explorer v5.5 or later One of these web servers must be installed on the same machine: • Microsoft IIS v5.0 or 6.0. IIS is available from Microsoft. • Apache HTTP Server 2.0.50 (Included with the Websense software installation. This version also can be downloaded from the Apache website, www.apache.org/.)
DC Agent	• Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	One of these services must be installed on the network: • Windows Active Directory® • Windows NTLM
eDirectory Agent	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	• Novell eDirectory 8.51 and later. • NMAS authentication is supported. • Recommend Novell Client v4.83 or v4.9 (v4.81 and later are supported)

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
Explorer (Web server)	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 • Windows Server 2003 (Standard, Enterprise, or Web) • Windows Server 2003, SP1 (Standard, Enterprise, or Web) • Windows Server 2003, R2 (Standard or Enterprise)	• Internet Explorer 5.5 or later One of these web servers must be installed on the same machine: • Microsoft IIS v5.0 or 6.0. IIS is available from Microsoft. • Apache HTTP Server 2.0.50 (Included with the Websense software installation. This version also can be downloaded from the Apache website, www.apache.org/.)
Filtering Service	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block messages, if Network Agent is used for protocol filtering and User Service is installed on a Linux or Solaris machine.
Log Database (Windows)	• The Log Database is dependent upon the database engine, MSDE or Microsoft SQL Server, and not the operating system.	One of these must be installed: • MSDE 2000 • Microsoft SQL Server 2000 • Microsoft SQL Server 2005 (Workgroup, Standard, Enterprise, or 64-bit edition)
Log Database (Solaris and Linux)	• When running Explorer for Unix, the Log Database depends on MySQL.	• MySQL 5.0

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
Log Server (Windows)	• Windows 2000 Server SP3 or later, or Advanced Server SP1 • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	• Internet Explorer 5.5 or later One of these databases: • MSDE 2000 • Microsoft SQL Server 2000 • Microsoft SQL Server 2005 (Workgroup, Standard or Enterprise)
Unix Log Server	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1]	• MySQL 5.0
Logon Agent	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	Can be used with a Windows-based directory service (Active Directory or NTLM), or an LDAP-based directory service.

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
Logon Application	• Windows NT 4.0 SP 6a (Workstation or Server) • Windows XP Professional, SP1 or SP2 • Windows Vista Ultimate • Windows Vista Enterprise • Windows Vista Business • Windows 2000, SP3 or later (Professional or Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	
Network Agent	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block messages, if Network Agent is used for protocol filtering and User Service is installed on a Linux or Solaris machine.
Policy Server	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
RADIUS Agent	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 SP1 or SP2 (Standard or Enterprise) • Windows Server 2003, R2 (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
Real-Time Analyzer (RTA)	• Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	• Internet Explorer v5.5 or later. • One of the following web servers must be installed on the same machine: – Microsoft IIS v5.0 or 6.0. IIS is available from Microsoft. – Apache HTTP Server 2.0.50 (Included with the Websense software installation. This version also can be downloaded from the Apache website, www.apache.org/.)
Remote Filtering Client	• Windows XP Professional with SP1 or SP2 • Windows Vista Ultimate • Windows Vista Enterprise • Windows Vista Business • Windows 2000 with SP3 or later (Professional, Server, Advanced Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
Remote Filtering Server	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server with SP3 or later • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	
Reporter	• Windows 2000, SP3 or later (Professional or Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise) • Windows XP Professional	• A web browser to view the help files.
Usage Monitor	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 with SP3 or later (Professional, Server, Advanced Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise)	

Table 3 Components and Required Software

Component	Operating System Requirements	Other Required Software
User Service	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows 2000 Server SP3 or later • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (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 workstations to display protocol block messages, if Network Agent is used for protocol filtering and User Service is installed on a Linux or Solaris machine.
Websense Manager	• Red Hat Linux 9 • Red Hat Enterprise Linux 3 or 4: AS, ES, and WS • Solaris 9 or 10, with current patches[1] • Windows XP Professional, SP1 or SP2 • Windows 2000, SP3 or later (Professional or Server) • Windows Server 2003 (Standard or Enterprise) • Windows Server 2003, SP1 (Standard or Enterprise) • Windows Server 2003, R2 (Standard or Enterprise) • Windows Vista (32-bit only) (Ultimate, Enterprise or Business)	• A web browser to view the help files. • Common Desktop Environment (CDE) • Java Virtual Machine (JVM) to run on Solaris.

1. Install the most current Solaris patch cluster before running the Websense installer. See the Sun website, www.sun.com, to download the latest patch cluster.

Table 4, on page 27 lists the operating systems on which the Websense components run.

Table 4 Operating Systems

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

Table 4 Operating Systems

Operating System	Component
Windows XP Professional	• Logon application • Websense Manager
Linux environment	
Red Hat Linux 9 Red Hat Enterprise 3 or 4 AS (Advanced Server) Red Hat Enterprise 3 or 4 ES (Enterprise Server) Red Hat Enterprise 3 or 4 WS (Workstation)	• Database Engine with Log Database (MySQL) • eDirectory Agent • Explorer for Unix • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent • Remote Filtering Server • Unix Log Server • Usage Monitor • User Service • Websense Manager
Solaris environment	
Solaris 9 or 10, with current patches[1]	• Database Engine with Log Database (MySQL) • eDirectory Agent • Explorer for Unix • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent • Remote Filtering Server • Unix Log Server • Usage Monitor • User Service • Websense Manager

1. Install the most current Solaris patch cluster before running the Websense installer. See the Sun website, www.sun.com, to download the latest patch cluster.

VMWare Support

Websense software supports running on VMWare ESX Server. Websense software installation and functionality (but not logging) was tested for Windows 2003 Server, running on ESX Server versions 2.5.x and 3.x. The VMWare support includes Websense Enterprise, Websense Security Suite and CPM.

This section discusses:

- Network Considerations
- System Recommendations
- Deployment Configurations

Network Considerations

Websense Network Agent requires that the monitoring NIC be set to promiscuous mode to see the traffic on the network. The Virtual NIC on VMWare must be configured to be used by Network Agent.

To use bridged networking, each virtual machine must have its own network identity. On a TCP/IP network, the virtual machine must have its own IP address. VMWare requires that if a virtual machine is set up to boot multiple operating systems, each OS must have a unique network address, even if only one OS will be running at one time.

More information on configuring VMWare can be found on the VMWare support and publications websites.

System Recommendations

The following chapters provide the 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.
- Dual or Quad Xeon processor.

- 8 GB of RAM
- 3 GB NICs are required, 4 GB NICs are recommended:
  - One NIC dedicated to VMWare management console.
  - One NIC allocated for a virtual switch used to monitor traffic (Stealth Mode without IP).
  - One NIC allocated for a virtual switch used for Websense components' communication.
  - One NIC to be used by VMWare host system for other communication.

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

Deployment Configurations

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

The following table provides possible deployments for Websense software in a distributed environment.

These recommendations are for small networks, with up to approximately 1000-2000 users. Hardware needs and component location may vary, depending on the volume of internet requests. For larger networks, more system resources or distribution of Websense components may be needed. For specific component deployment recommendations, see the remaining chapters in this guide.

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 Unix Administrator's Guide* for system requirements.

Table 5 Distributed Layout

Virtual Machine	Allocated Hardware	Websense Components
#1	• 512 MB RAM	• Policy Server • User Service • Transparent ID Agent
#2	• 1 GB RAM • 20 GB free disk space	• Websense Manager • Filtering Service • Master Database
#3	• 1 GB RAM • Dual-NIC	• Network Agent
#4	• 2 GB RAM • 20GB free disk space	• Remote Filtering Server
#5	• 2 GB RAM	• Websense Explorer • RTA • Reporting Client
	Logging is not supported on VMware	

Component Limits

When deploying Websense software, dependencies must be considered:

- 1 Log Server per Log Database
- 1 Log Server per Policy Server
- 1 User Service per Policy Server
- 1 Real-Time Analyzer (RTA) per Policy Server
- 1 Usage Monitor per Policy Server
- 1 primary Remote Filtering Server per Filtering Service

Component Suggestions

The ratios in this section are suggestions for deploying these components. These limits may be exceeded, depending on network configuration and internet traffic volume.

This section includes:

- *Network Agent Suggestions*
- *Number of Filtering Services Allowed per Policy Server*, page 32

For limits on transparent identification agents, see *Deploying Transparent Identification Agents*, page 37.

For more information on the interaction of Websense components, see the *Websense Enterprise Installation Guide* for the integration, and the *Websense Enterprise Administrator's Guide*.

Network Agent Suggestions

- Up to 4 Network Agents per Filtering Service.
- 1000 users per Network Agent.

A Filtering Service may be able to handle more than 4 Network Agents, and a Network Agent may be able to handle more than 1000 users. However, if the components' capacity is exceeded for what they can handle in a deployment, filtering and logging inconsistencies may occur.

Number of Filtering Services Allowed per Policy Server

- Up to 10 Filtering Services per Policy Server.

A Policy Server may be able to handle more than 10 Filtering Services. However, if the number of Filtering Services exceeds the capacity that the Policy Server can handle in the deployment, responses to internet request may be slow, and the connection between Filtering Service and Policy Server breaks, causing inconsistent filtering. Depending on the setting in Websense Manager (**Block users when subscription expires or is exceeded**), all internet requests are either blocked or permitted. For more information on this setting. For more information, see the *Websense Enterprise Administrator's Guide*.

While 10 Filtering Services per Policy Server is suggested, the actual number of Filtering Services that work with a Policy Server depends on:

- The number of users to a Filtering Service.
- The configuration of the machines on which the components are running.
- The volume of internet requests.
- The quality of the network connection between the components.

  If a ping command sent from 1 machine to another receives a response in fewer than *30 milliseconds* (*ms*), the connection is considered high quality. See the *Testing the connection* section, below.

Filtering Service machines running remotely (those at a great physical distance communicating through a series of routers), or those behind firewalls, may need their own Policy Servers. If additional Policy Servers must be deployed, the *Central Policy Distribution* feature can be used to push policies out to the remote Policy Server machines. For more information, see the *Websense Enterprise Administrator's Guide*.

Testing the connection

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

1. Open a command prompt (Windows) or terminal session (Linux and Solaris).
2. At the prompt, enter: `ping <IP address or hostname>` where *<IP address or hostname>* identifies the machine to which this machine is trying to connect.

Linux or Solaris Results

In a Linux or Solaris environment, the results look similar to these:

```
[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 `time=x.xxx ms` is fewer than 30.000 ms. If the time is greater than 30 ms, then move 1 of the components different location on the network, and run the ping test again. If the result is still greater than 30 ms, locate and eliminate the source of the slow response.

Windows Results

In Windows, the results look similar to these:

```
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
```

Ensure that *Maximum* round trip time is fewer than 30 ms. If the time is greater than 30 ms, then move 1 of the components different location on the network, and run the ping test again. If the result is still greater than 30 ms, locate and eliminate the source of the slow response.

External Resources

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

- **TCP/IP**: Websense filtering software supports TCP/IP-based networks only. If your network uses both TCP/IP and non-TCP protocols, only those users on the TCP/IP portion of your network are filtered by Websense software.
- **DNS server**: If IP addresses are not sent to the Websense Filtering Service together with a URL request, a DNS server can be used to resolve the URL into an IP address. Websense software or your integration product (where applicable) require efficient DNS performance. Make sure your DNS servers are fast enough to support Websense filtering without becoming overloaded.

- **Directory services**: Websense Filtering Service can be configured with policies based on user and group names. The Filtering Service queries the directory service to identify users and their associated groups as specified in a policy. Although these users and group relationships are cached by Websense, directory service machines must have the resources to rebuild the cache rapidly when the Websense Filtering Service requests user information. See *Supported Directory Services*.
- **Network efficiency**: Connectivity to resources such as DNS and directory services is critical to the Websense Filtering Service. Network latency must be minimized if the Filtering Service is to perform efficiently. Excessive delays under high load circumstances can affect the performance of the Filtering Service and may cause lapses in filtering. See *Optimizing Network Performance*, page 129 for tips on improving network communication.

Supported Directory Services

If your environment includes a directory service, Websense allows you to filter internet requests based on individual policies assigned to directory objects. Directory objects identified in a directory service can be added to Websense and assigned specific policies, using Websense Manager.

Websense can communicate with the following directory services:

- Windows NTLM-based directories
- Windows Active Directory
- Sun Java System Directory Server
- Novell Directory Services/Novell eDirectory

For information about configuring directory service access, see the *Administrator's Guide* for Websense Enterprise and Web Security Suite.

Note

Websense software can communicate with your directory service whether it runs on the same operating system as the Websense components, or on a different system.

Filtering can be based on individual user, group, and domain/organizational unit policies, providing that Websense is able to identify the user making an internet request. The authentication method you configure must allow

Filtering Service to obtain directory object information from a Windows or LDAP directory. For information about accessing LDAP and Windows directories, see the *Administrator's Guide for Websense Enterprise and Web Security Suite*.

Deploying Transparent Identification Agents

The Websense transparent identification feature allows Websense to filter internet requests from users in the directory service, without prompting users to manually authenticate when using Stand-Alone Edition, or when the integration product does not send user information to Websense software.

Websense currently provides 4 optional components for identifying users transparently in various environments:

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

Note

DC Agent must have administrator privileges on the network to retrieve user logon information from the domain controller.

When using 1 of these agents in a network in a single location, Websense, Inc., recommends only 1 instance of an agent be installed on the network.

However, in deployments that cover multiple locations or remote offices, an agent may be installed in multiple domains.

For example:

- DC Agent—1 instance can handle multiple trusted domains. The need for additional DC Agent instances is dependent on the load placed on the DC Agent, and the ability of the DC Agent to see all the domains on the network, such as remote offices.

  The load results from the number of logon requests generated by users. If the network is large (10,000+ users, 30+ domains), installing DC Agent on multiple machines allows DC Agent to react more quickly by sharing the load.

  If multiple Filtering Services are installed, each Filtering Service must be able to communicate with all DC Agents.

- eDirectory Agent—1 instance per each eDirectory Server.
- Logon Agent—1 instance for each Filtering Service that is installed.
- RADIUS Agent—1 instance for each RADIUS server.

  The RADIUS server authenticates users: The RADIUS server checks the user name and password entered against the corresponding account in the directory service; then sends a response to RADIUS Agent indicating the status of the authentication request.

In some environments, some combinations of transparent identification agents may be appropriate within the same network, or on the same machine. See *Combining Transparent Identification Agents*.

For installation instructions for the transparent identification agents, see the *Websense Enterprise Installation Guide*. For more information on configuring these agents, see the *Websense Enterprise Administrator's Guide*. For more information on transparent identification agents, see the *Transparent Identification of Users in Websense Enterprise* white paper.

Go to the Websense Product Documentation site to see these documents—www.websense.com/global/en/SupportAndKB/ProductDocumentation/

Combining Transparent Identification Agents

Websense software can be configured to work with multiple agents. If the network configuration 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 installed on a separate server on the same network.
- Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

Table 6, on page 39 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 individual domain controllers.
Multiple RADIUS Agents	No	Yes	Configure each agent to communicate with Filtering Service.
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.
DC Agent + RADIUS Agent	Yes	Yes	See Websense Knowledge Base article #1115.
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 1 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. See Websense Knowledge Base article #1115.
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 1 active agent.

Table 6 Deploying Multiple Transparent ID Agents

Combination	Same machine?	Same network?	Configuration required
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 1, and a machine name to identify the other. See the *Transparent Identification of Users in Websense Enterprise* white paper for details.
DC Agent + Logon Agent + RADIUS Agent	Yes	Yes	Though this combination is rarely required, it is functionally supported. Configure all agents to communicate with Filtering Service. See Websense Knowledge Base article #1115.

Maximizing System Performance

By adjusting Websense components, filtering and logging response times can be improved, along with system throughput and the CPU performance of the machine running the components. Websense software can be optimized for:

- Network Agent
- Real-Time Analyzer (RTA)
- Logging of bytes transferred
- Database engine (MSDE 2000, Microsoft SQL Server 2000/2005, MySQL 5.0)

For enterprise networks, see *Optimizing Network Performance*, page 129.

Network Agent

Network Agent may be installed on either the same machine as other Websense components, or separately from the rest of the components, depending on the machine configuration and network size.

For example, in a small or medium size network, Network Agent can be moved to a separate machine from Filtering Service and Policy Server as the

network exceeds 1000 users, or if response times slow down for internet requests.

If Websense software is running in a high load environment, or with a high capacity connection to the internet such as a T3 connection, or both, consider installing Network Agent on multiple machines, with each agent designated to monitor a specific portion of the network. This deployment increases throughput and divides the load.

IMPORTANT

Network Agent must be installed so that it can have bi-directional visibility of the internal network or segment that it is to monitor.

If multiple Network Agents are installed, each network segment must be monitored by 1 Network Agent. An IP address range monitored by 1 Network Agent must not overlap the range monitored by another Network Agent.

If the machine with Network Agent is connected to a switch, plug the machine into a port that mirrors, monitors or spans the traffic of all other ports. *Multiple Segment Network*, page 139 and *Network Agent Location*, page 137 discuss locating Network Agent in more detail.

Real-Time Analyzer (RTA)

Real Time Analyzer (RTA) can be memory and CPU demanding, depending on the system settings and network load conditions. RTA should be moved off of real-time critical machines.

- Memory consumption can be managed via the Real-Time Analyzer system settings. For more information, see the *Websense Enterprise Reporting Administrator's Guide*.
- If RTA must be installed on the same machine with Filtering Service or Network Agent, system performance gains can be made by increasing the CPU speed or number of CPUs, and the amount of RAM.
- If CPU spikes continue, consider moving RTA to another machine, separate from Filtering Service and Network Agent. This change provides maximum system performance.

If additional throughput is needed in Websense software, disable or stop the RTA service if it is running on the same server as Filtering Service and Network Agent.

HTTP Reporting

Network Agent and integration products both track HTTP requests and pass that information to Websense software, which uses this data create logs to track the HTTP traffic and filter.

Network Agent and some integrations also track bandwidth activity (bytes sent and received), and the duration for each permitted internet request. Network Agent or the integration prompt Websense software to log this data.

If both Network Agent and the integration partner are providing logging data, Filtering Service uses twice as much CPU.

To avoid additional processing, enable Network Agent to log HTTP requests (enhanced logging) in the Websense Manager. Enabling this feature prevents Websense software from logging the HTTP requests coming from the integration partner. Instead, Websense software relies on Network Agent to log that traffic. See the Network Agent chapter in the *Websense Enterprise Administrator's Guide* for more information on configuring Network Agent.

If enhanced logging is used, consider installing Network Agent on a separate machine from Filtering Service. See the *Websense Enterprise Installation Guide* for details.

Database Engine

Log Database can reside in either Microsoft Database Engine (MSDE) 2000 or Microsoft SQL Server 2000/2005. Explorer for Unix and Unix Log Server use MySQL 5.0. Log Server logs to 1 Log Database at a time.

MSDE

Microsoft Database Engine is a freely distributed database engine. MSDE works best for smaller networks and organizations that either have a low volume of internet access, or plan to generate reports that are archived on a daily or weekly basis. MSDE allows the Log Databases to grow to about 1.5 GB. Upon reaching this maximum size, MSDE dates and saves the Log Database (called rollover), and creates a new Log Database. To see the names

of the databases that have been saved, access the ODBC Data Source Administrator through the Windows Control Panel.

If the database is frequently rolling over, consider purchasing Microsoft SQL Server 2000 Standard Edition or Microsoft SQL Server 2005 to upgrade the database to a more scalable platform. Also, MSDE cannot be optimized.

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

- Ensure the latest service packs are applied. Microsoft SQL Server service packs can be applied to MSDE 2000 SQL. If MSDE is installed, Microsoft SQL Server service packs recognize the database and update only the MSDE files.

Microsoft SQL Server

Microsoft SQL Server works best for larger networks and those deployments with a high volume of internet usage. Microsoft SQL Server has a larger capacity than the Microsoft Database Engine (MSDE) for reporting over long periods of time, such as several weeks or months.

Microsoft SQL Server operations under high loads are resource intensive and can be a performance bottleneck for the Websense software reporting system. The Microsoft SQL Server database can be tuned to improve performance. Some hardware improvements can also be made:

- Improve CPU performance to alleviate CPU contention between Log Server and the Microsoft SQL Server:
  - Increase the CPU speed, or the number of the system's CPUs, or both.
  - Consider providing a dedicated machine for the reporting components, such as Log Server.
- Consider disk space usage and requirements, and ensure adequate space is available to accommodate the growth of the Log Database. Microsoft SQL Client Tools can be used to check the size of a database created in either MSDE or Microsoft SQL.

- 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 website for more detailed information on Microsoft SQL Server performance optimization.

MySQL

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

For more information on MySQL, see the MySQL website: www.mysql.com.

Log Database Disk Space Recommendations

While this guide provides some disk space recommendations for the machine running the Log Database, requirements may vary, depending on the size of the network and the usage of the internet.

As an approximate calculation:

- An average user surfs to 100 URLs (*visits*) per day.
- By default, the Log Database creates a record for each visit.
- Each record is approximately 500 bytes.
- Each URL requires roughly 5-10 HTTP GETS or *hits*. The Log Database can be configured to write a record for each hit. This configuration can increase the size of database by a factor of 5.

Selective Category Logging can also be used to reduce the size of the Log Database. Selective Category Logging is used to set which URL categories are or are not logged. Categories not logged are not reported. Selective Category Logging is configured in the Websense Manager. For more information, see the *Websense Enterprise Administrator's Guide*.

Logging Visits (default settings)

If the default setting of recording visits is used, calculate the disk space required in the Log Database as follows:

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

Therefore, an average user generates 50 KB per day (100 visits x 500 bytes). If the user is logged in for 20 workdays per month, each user consumes 1 MB in the Log Database each month (20 days x 50 KB/day). Extrapolating to a 500 user deployment, the database could use 500 MB per month to record visits. This amount can vary greatly, depending on internet usage.

Logging Hits

If the Log Database is configured to record each hit, calculate the disk space required for each user in the Log Database as follows:

(# of URLs) x (# of hits) x (# of bytes)

Therefore, an average user generates 250 KB per day
(100 URLs x 5 gets/URL x 500 bytes).

To get the disk space required for all users, multiply the space for one user by the number of users:

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

If the user is logged in for 20 workdays per month, each user consumes in 5 MB in the Log Database each month (20 days x 250 KB/day).

Extrapolating to 500 users, the Log Database could use 2.5 GB per month.

In this example, the Log Database requires 30 GB of disk space for 1 year's worth of data in a 500 user network with 500 hits per day.

Due to the large amount of disk space required, Websense, Inc., does not recommend keeping live data from large networks for a year.

That amount of data also significantly slows down reporting. By breaking the database into smaller pieces, reports can be run much quicker.

Logging Full URLs

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

If the Log Database is growing too quickly, turning off full logging decreases the size of each entry and the database by a factor of 4, thus saving disk space.

If logging full URLs is desired, you must turn on Full URL Logging in Database Administration. See the *Websense Reporting Administration Guide* for instructions on using Database Administration.

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* with multiple pop-ups during a session. The visit is logged as a record. If consolidation is turned off and the user revisits the site later, another visit is logged. With consolidation on, multiple visits to the same site within a specified period are logged as a single record. Consolidation is turned *off* by default.

Protocol Logging

The smaller the database, the faster reports can be run. Also, Network Agent can log protocol filtering. The more protocols that are filtered, the greater the impact on the size of the Log Database.

Log Database Strategy

Using the hits and visits calculations provided under *Logging Hits*, page 45, even without logging full URLs, the data for 1 year could require:

- 600 GB for hits
- 120 GB for visits

Such large amounts of data can significantly slow down reporting functions.

Auto-archiving can be used to limit the size of the current Log Database, while preserving the older data. The auto-archive can be triggered by a size or time limit. When the trigger point is reached, then Explorer or Reporter start writing to a new Log Database. The old records are preserved, and reports can be run against it as well.

For instructions on the Database Administration, see the *Websense Enterprise Reporting Administrator's Guide*.

Stand-Alone Edition

The Stand-Alone Edition allows Websense software to use Network Agent to provide HTTP, HTTPS, FTP and other protocol information instead of relying on a third party firewall, network appliance or proxy server. Network Agent detects all internet requests, both URL and protocol requests, and checks with Filtering Service to see if the internet request should be blocked. Network Agent also calculates the number of bytes transferred and sends a request to Filtering Service to log this information.

For more information, see the *Websense Enterprise Installation Guide for the Stand-Alone Edition*.

The Stand-Alone Edition runs on the same operating systems listed earlier in this chapter for Websense components. See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

The optional Reporter or Explorer can run along with the Stand-Alone Edition. As with the integrations, reporting components should be run on a separate machine, due to the amount of processing related to reporting.

Note

In a Linux environment, the Logon application must be installed on a Windows machine, if it is used.

While the Stand-Alone Edition can be deployed in small, medium, and large networks, multiple machines may be required in the larger networks to distribute the processing evenly. Multiple machines ensure that a single machine does not become overwhelmed. This distribution can include deploying multiple Network Agents to accommodate and balance the heavier internet traffic flow. Network Agent can be installed on a Linux, Solaris or Windows machine.

Table 7, on page 49, provides system recommendations for deploying the Stand-Alone edition, according to network size. System needs can vary, depending on the volume of internet traffic.

On average, requests per second are approximately as follows:

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

Larger systems may be needed in networks where traffic exceeds the average for the specified number of users.

IMPORTANT

- To ensure the integrity of a firewall, do not install Websense components on the firewall machine.
- Whether Network Agent is installed on the same machine as the other Websense components, or is installed on a separate machine, it must be able to see all internet requests for the machines that it is assigned to monitor.
- If eDirectory or RADIUS Agent are used, they can be installed on the same machine as Filtering Service or installed on a separate server on the same network, but not on the same machine as the Reporting components.

Table 7 Stand-Alone System Recommendations

Network Size	Filtering Deployment	Reporter/Explorer Deployment (Windows Only)	Explorer for Unix Deployment
1 - 500 users	**Windows** or **Linux** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IIIi • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.	**Windows** • Pentium 4, 2.4 GHz, or greater • 1 GB RAM • 80 GB of free disk space • Microsoft SQL Server 2000, Microsoft SQL Server 2005, or MSDE 2000	**Linux** • Pentium 4, 2.4 GHz or greater • 1 GB RAM • 80 GB of free disk space • MySQL 5.0 **Solaris** • UltraSPARC IIIi • 1 GB RAM • 80 GB of free disk space. • MySQL 5.0

Table 7 Stand-Alone System Recommendations

Network Size	Filtering Deployment	Reporter/Explorer Deployment (Windows Only)	Explorer for Unix Deployment
500 - 2,500 users	**Windows** or **Linux** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IIIi • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 100 GB of free disk space • Microsoft SQL Server 2000, Microsoft SQL Server 2005, or MSDE 2000	**Linux** • Pentium 4, 2.0 GHz or greater • 2 GB RAM • 100 GB of free disk space • MySQL 5.0 **Solaris** • UltraSPARC IIIi • 2 GB RAM • 100 GB of free disk space • MySQL 5.0

Table 7 Stand-Alone System Recommendations

Network Size	Filtering Deployment	Reporter/Explorer Deployment (Windows Only)	Explorer for Unix Deployment
2,500 - 10,000 users	**Windows** or **Linux** • Load Balancing Required • Dual Xeon, 3.0 GHz, or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. • See the Important note below. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.	**Windows** • Dual Xeon, 2.0 GHz or greater • 2 GB RAM • 200 GB of free disk space utilizing a disk array[1] • High speed disk access • Microsoft SQL Server 2000, or Microsoft SQL Server 2005	**Linux** • Dual Xeon, 2.0 GHz or greater • 2 GB RAM • 200 GB of free disk space, with a disk array, RAID level 10 • High speed disk access • MySQL 5.0 **Solaris** • UltraSPARC IV • 1 GB RAM • 200 GB of free disk space, with a disk array, RAID level 10 • High speed disk access • MySQL 5.0

1. The Log Database needs a disk array, running, to increase I/O reliability and performance.

IMPORTANT

Network Agents running on 2 separate machines are required for a network of this size. A Pentium 4 with a 3.0 GHz or greater processor and at least 1 GB of RAM is recommended for running Network Agent. The amount of RAM needed may vary, depending on the number of users being monitored. Multiple Filtering Services may also be needed. These machine requirements also depend on the number of users being monitored.

Remote Filtering

The Remote Filtering feature allows Websense software to monitor computers outside the corporate network. A *Remote Filtering Client* must be installed on the 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, which can communicate with Filtering Service. See Table 8, on page 53 for recommendations.
- Do not install Remote Filtering Server on the same machine as the Filtering Service or Network Agent.
- Each Filtering Service has 1 primary Remote Filtering Server.
- The Remote Filtering Server must be installed inside the outermost firewall, but in the DMZ outside the firewall protecting the rest of the corporate network. This configuration is highly recommended.
- See Table 3, on page 20 for operating system requirements for the Remote Filtering Server and Client.

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

See Table 8, on page 53 for Remote Filtering Server recommendations.

Table 8 Remote Filtering Server System Recommendations

Network Size	Hardware Recommendations
1-500 clients	**Windows** or **Linux** • Pentium 4, 2.0 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
500-2000 clients	**Windows** or **Linux** • Xeon, 3.2 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
2000-5000 clients	**Windows** or **Linux** • Dual Xeon, 3.2 GHz or greater • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, dual CPUs, 1.593 GHz • 1 GB RAM • 20 GB of 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 • 1 GB RAM • 20 GB of free disk space **Solaris** • Sun V440s, quad CPUs, 1.593 GHz • 1 GB RAM • 20 GB of free disk space
10000+ clients	**Windows** or **Linux** • Static load balancing with Quad Xeon, 3.2 GHz or greater • 2 GB RAM • 20 GB of free disk space **Solaris** • Sun V490s, with 4 hyper-threaded CPUs, 1.593 GHz • 2 GB RAM • 20 GB of free disk space

Figure 1, page 55 provides an example of Remote Filtering deployment. To simplify the drawing, this example does not include all Websense components.

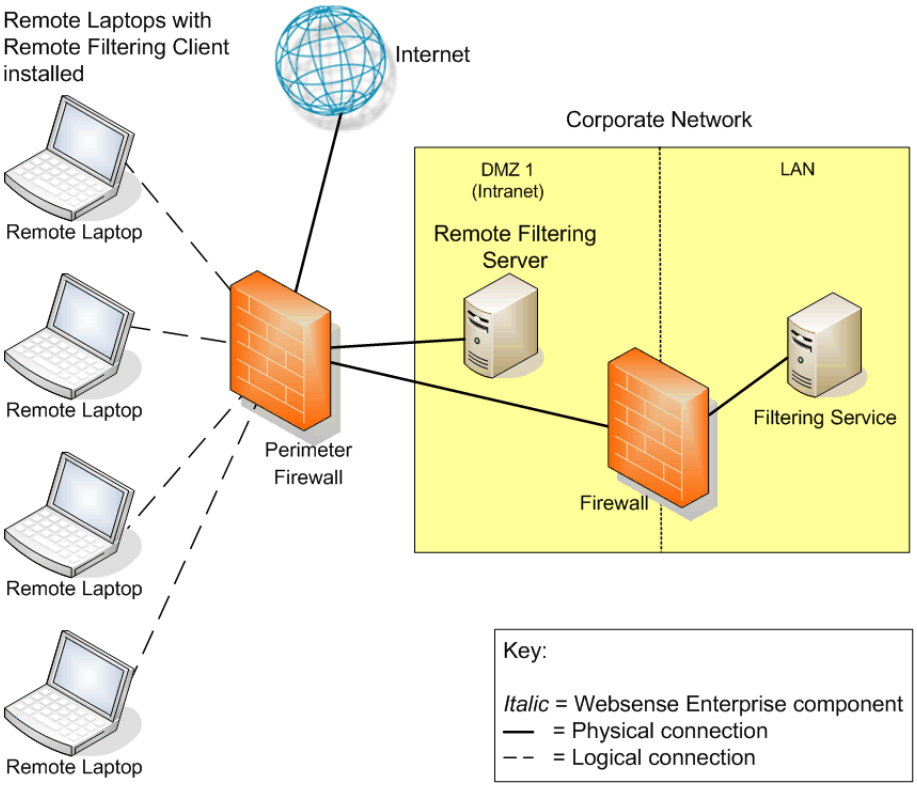

Figure 1 Example of Remote Filtering Deployment

Integrations

Websense software integrates with the following firewalls, proxy servers, or caching applications (integration product) to provide internet filtering.

The deployment recommendations in this guide apply only to the Websense Stand-Alone Edition, and the integrations listed in Table 9.

Table 9 Supported Integrations

Integration	Version Supported	Comments
Cisco®	• Cisco PIX Firewall Software v5.3 and higher • Cisco Adaptive Security Appliances (ASA) Software v7.0 and higher • Cisco Content Engine ACNS v4.1 and higher • Cisco Routers with Cisco IOS Software Release 12.3 and higher	
Check Point® FireWall-1®	• FireWall-1 NG, Feature Pack 1 to Feature Pack 3 • FireWall-1 NG with Application Intelligence (AI) • FireWall-1 NGX	Contact Check Point for assistance is determining which FireWall-1 version is running. Network Agent can run on same box with Firewall-1 *only* if each product has its own processor.
Citrix® – Citrix Presentation Server™ – MetaFrame® Presentation Server	• MetaFrame Presentation Server 3.0 • Citrix Presentation Server 4.0	**Websense Plug-in**: The Citrix plug-in is only supported on Windows. Requires either: • Microsoft Windows 2000 Server (32 bit) • Microsoft Windows Server 2003 (32 bit)

Table 9 Supported Integrations

Integration	Version Supported	Comments
Inktomi® Traffic Server®	• Inktomi Traffic Server version 4.0.18 or later.	**Websense Plug-in**: The Inktomi Filter for the Inktomi Traffic Server is supported only on Solaris.
Microsoft® Internet Security and Acceleration (ISA) Server and Microsoft Proxy Server	Integrations: • Microsoft ISA Server 2004, Standard Edition and Enterprise Edition • Microsoft ISA Server 2006, Standard Edition and Enterprise Edition • Microsoft ISA Server 2000 with Feature Pack 1 • Microsoft Proxy Server 2.0 Clients: • ISA Firewall Clients • Secure NAT Clients	**Websense Plug-in**: The ISAPI Plug-in for the Microsoft ISA Server and Microsoft Proxy Server is supported only on Windows.
Network Appliance™ NetCache®	• Network Appliance NetCache v5.2.1 R1D4 and later.	The use of Websense protocol management requires NetCache v5.5 or later.
Squid Web Proxy Cache	• Squid v2.5.	**Websense Plug-in**: The Squid Plug-in for the Squid Web Proxy Cache is supported only on Solaris and Linux.
Sun Java System Web Proxy Server	• Sun Java System Web Proxy Server 3.6 and 4.0 • Sun ONE™ Web Proxy Server 3.6 • iPlanet™ Web Proxy Server 3.6 • Netscape® Proxy Server 3.5	**Websense Plug-in**: The Sun Web Proxy Plug-in for the Sun Java System Web Proxy Server is supported only on Solaris.

CHAPTER 3

Deploying in Networks up to 10,000 Users

Websense software can be deployed in different configurations, depending on the size and characteristics of the network and filtering needs. Websense components can be installed together on 1 machine, or distributed across multiple machines. Deployment depends on the operating systems, the network size, and volume of internet requests.

Most components can be installed on separate machines using the Websense installation program.

Table 1 and Table 2 in Chapter 1 describe Websense components.

This chapter provides system and deployment recommendations for these ranges:

- Small (1–500 users)
- Medium (500–2,500 users)
- Large (2,500–10,000 users)

Networks with over 10,000 users are discussed in *Chapter 4: Deploying in Networks with Over 10,000 Users*.

These network ranges are intended as general guidelines only. Deployment designs vary between networks, depending on the configuration of the network, operating systems installed, and the volume of internet activity.

Depending on the size and configuration of the network, the deployment may need multiple instances of certain components, such as Network Agent, the Reporter client application, Websense Manager, the transparent identification agents, or Filtering Service.

This manual provides system recommendations to optimize Websense component performance. Performance also can be improved by using more powerful machines for resource intensive components, such as the Log Server and database engine (Microsoft SQL, MSDE, MySQL).

Note

- These recommendations allow for some network growth and an increase in internet requests. As the network reaches the upper limits for a particular network size, revisit these recommendations to ensure the system is configured to optimize each component's performance.
- If the network grows to over 10,000 users, see *Chapter 4: Deploying in Networks with Over 10,000 Users*.
- Websense software supports TCP/IP-based networks only. If the network uses both TCP/IP and non-IP based network protocols, only those users on the TCP/IP portion of the network are filtered by Websense software.

Small Networks: 1–500 Users

Websense filtering components can be installed on a single Windows machine for a small network. If a Linux or Solaris machine is used, separate Windows machines are required to run Windows-only components. The deployment recommendations cover each of these operating systems.

Reporting components may require a separate machine, depending on the configuration of the machine running the components.

Additional machines may be needed to run certain components as the network grows and internet requests increase. On average, a small network has 1 to 100 requests per second. More powerful machines may be needed in a higher traffic, small network.

Note

Dedicated machines are recommended for running some Websense components. The tables in this section list possible configurations for these dedicated machines. Only Websense components and applications related to running those components are installed the dedicated machine.

Network Considerations

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

- Filtering Service can receive HTTP requests from the gateway or integration device (if any) or Network Agent.
- Network Agent must be deployed where it can see all internal internet traffic for the machines that it is assigned to monitor. For more information, see *Chapter 5: Deploying Network Agent*.
- Network Agent must have bidirectional visibility of internet traffic to filter non-HTTP traffic, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and other network protocols.
- If User Service is installed on a Linux or Solaris machine and Network Agent is used for protocol filtering, then Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block pages.
- As a network grows and the number of internet requests increase, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
- *IMPORTANT*: *do not* install Websense components on the firewall machine to ensure the integrity of the firewall.

Windows Deployment Recommendations

In a Windows environment, filtering and reporting components can be installed on a single, dedicated machine with a Pentium 4, 3.0 GHz processor. As an alternative, a dedicated machine can run Websense filtering components, and a second dedicated machine can run Reporting components.

Table 10, on page 62 provides deployment recommendations. Figure 2, page 65 provides an overview of a small Windows network deployment.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 10 Windows Deployment in a Small Network

Machine	Software	Hardware Recommendations
Single Dedicated machine	• All components. See the components listed below for both dedicated machines 1 and 2.	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 85 GB free disk space
—or—		

Table 10 Windows Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later • Transparent ID agent:[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent • Usage Monitor • User Service • Websense Manager	**Windows** • Pentium 4, 2.4 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2	• Database Administration • Explorer – Requires Apache or IIS web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005, MSDE 2000 • Reporter client application	**Windows** • Pentium 4, 2.4 GHz or greater • 1 GB RAM • 80 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		

Table 10 Windows Deployment in a Small Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Network Agent	**Windows** • Pentium 4, 2.5 GHz or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent	**Windows** • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Windows** • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Windows** • Pentium 4, or greater • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.

Figure 2, page 65 illustrates the distribution of the Websense components in a small Windows network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments. For example, filtering and reporting components can be installed on the same machine in a small Windows network.

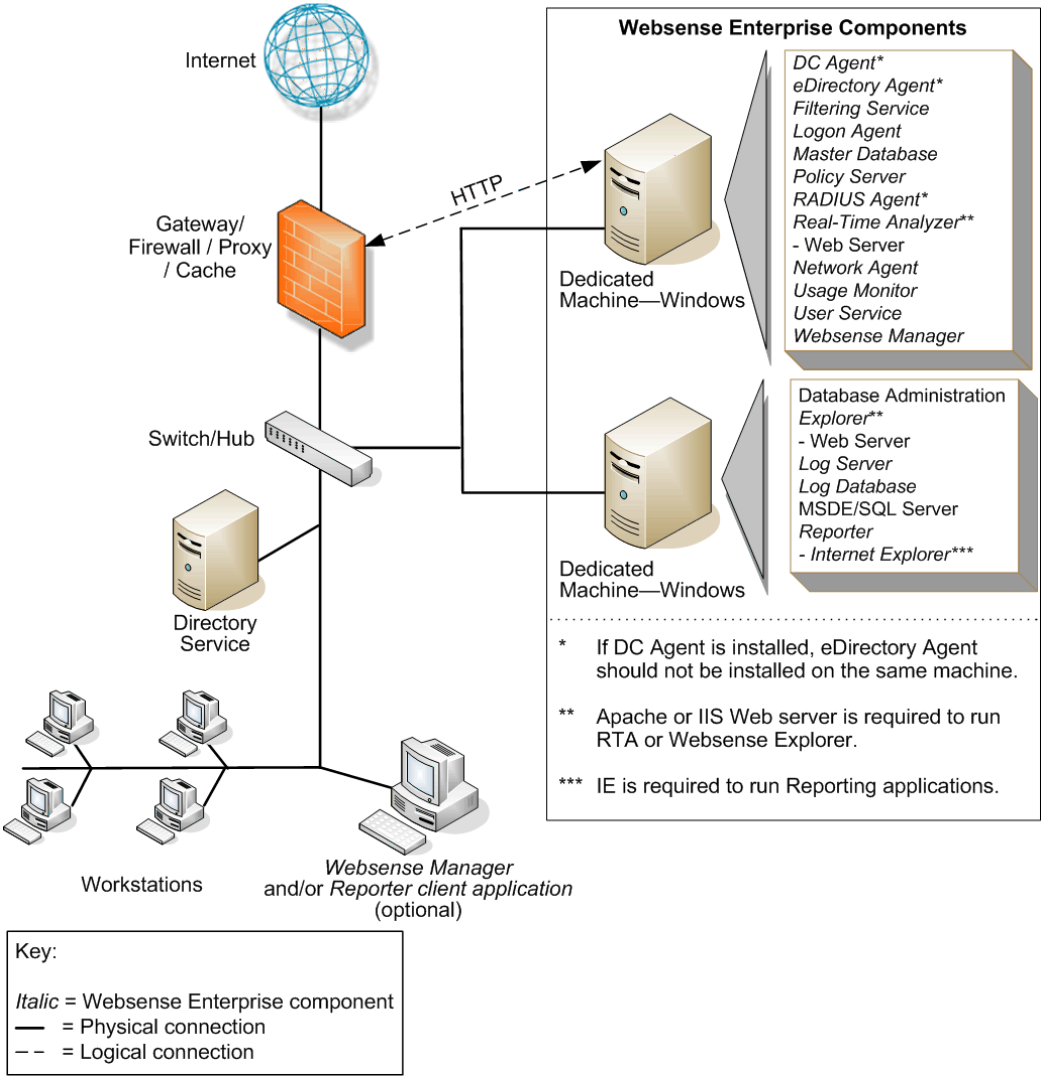

Figure 2 Concept of Windows Deployment—Small Network

Linux/Solaris Deployment Recommendations

To run Websense software in a small network on a Linux or Solaris machine, at least 1 Windows machine is needed to run some components. Table 11 provides deployment recommendations. Figure 3, page 69 provides an overview of a Linux or Solaris deployment in a small network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 11 Linux or Solaris Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Transparent ID agent:[1] – Logon Agent – eDirectory Agent – RADIUS Agent • Usage Monitor • User Service • Websense Manager	**Linux** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IIIi • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.

Table 11 Linux or Solaris Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #2	• Database Administration • Explorer – Requires IIS or Apache web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005, or MSDE 2000 • Reporter client application	**Windows** • Pentium 4 • 1 GB RAM • 80 GB of free disk space
Dedicated Machine #2[2]	• Explorer for Unix – Requires Apache web server • Log Database • Unix Log Server • MySQL 5.0	**Linux** • Pentium 4, or greater • 512 MB RAM • 80 GB of free disk space **Solaris** • UltraSPARC IIIi • 1 GB RAM • 40 GB of free disk space.
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer – Requires Apache, or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 1 GB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		

Table 11 Linux or Solaris Deployment in a Small Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Network Agent	**Linux** or **Windows** • Pentium 4, 2.5 GHz or greater • 1 GB RAM **Solaris** • UltraSPARC IIIi • 1 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4 or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent (Windows only) – eDirectory Agent – Logon Agent – RADIUS Agent	**Linux** or **Windows** • Pentium 4, or greater • 256 MB RAM **Solaris** • UltraSPARC IIIi • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.

2. A separate installation of Explorer for Unix is also available. This Explorer only runs with Unix Log Server, and utilizes a MySQL database (a licensed install of v4.0x or v4.1). The Unix and Windows Reporting products are not cross-platform compatible.

Figure 3, page 69 illustrates the distribution of the Websense components in a small Linux or Solaris network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

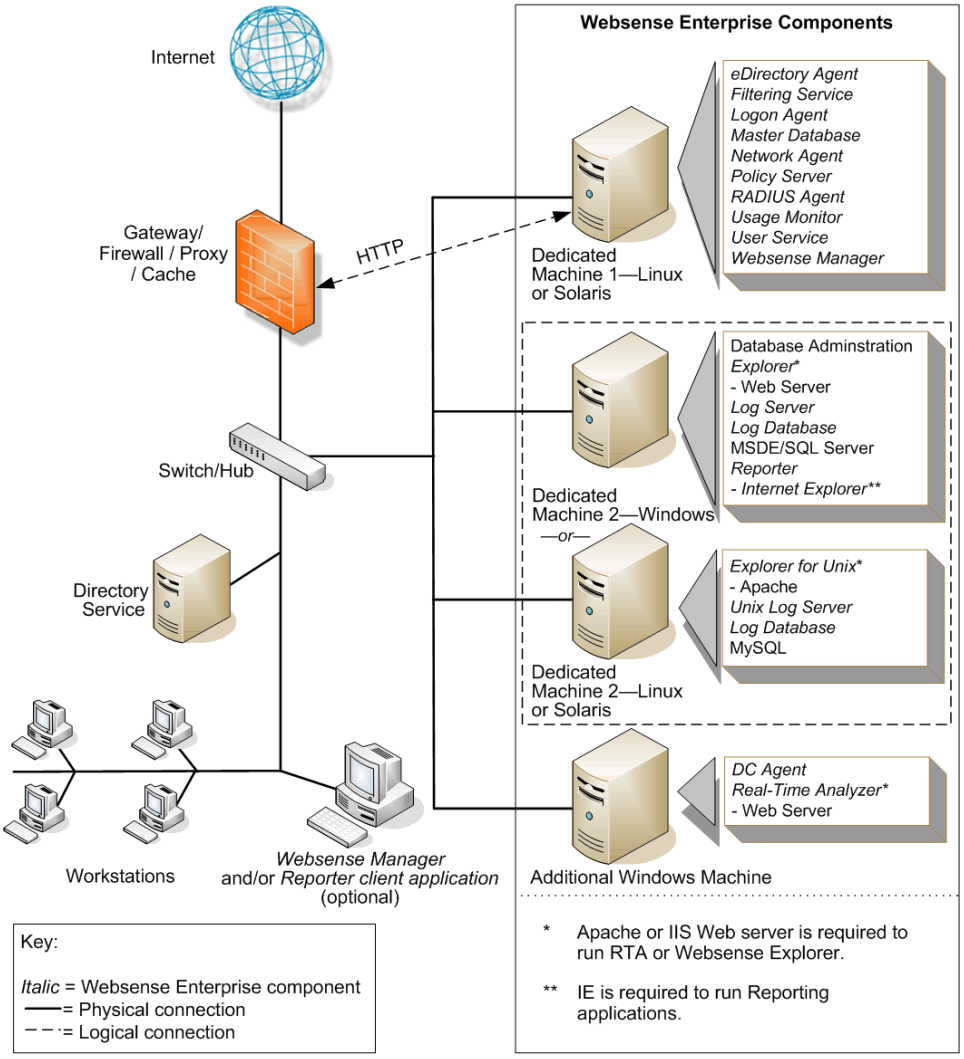

Figure 3 Concept of Linux or Solaris Deployment—Small Network

Medium Networks: 500–2,500 Users

In a medium network, Websense components should be distributed on 2 or more dedicated machines, depending on the operating environment. One machine is responsible for filtering, while a second machine is set up as a web server and runs the reporting components. The filtering machine can be running a Windows Server, Linux or Solaris operating system. Linux and Solaris systems may require an additional dedicated Windows machine to run Websense components that only run in a Windows environment. The deployment recommendations cover each of these operating systems.

Note

Dedicated machines are recommended for running some Websense components. The tables in this section list possible configurations for these dedicated machines. Only Websense components and applications related to running those components are installed the dedicated machine.

More powerful machines are recommended to run the components in a medium network as compared to the machines in a small network. These machines also need more RAM.

On average, a medium network has 100 to 500 requests per second. More powerful machines than the recommendations may be needed in a higher traffic, medium network.

Network Considerations

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

- Filtering Service can receive HTTP requests from the gateway or integration device (if any) or Network Agent.
- Network Agent must be deployed where it can see all internal internet traffic for the machines that it is assigned to monitor. For more information, see *Chapter 5: Deploying Network Agent*.
- Network Agent must have bidirectional visibility of internet traffic to filter non-HTTP traffic, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and other network protocols.
- Multiple instances of Network Agent may be needed, with each Network Agent monitoring a specific IP address range or network segment. For more information, see *Chapter 5: Deploying Network Agent*.
- If User Service is installed on a Linux or Solaris machine and Network Agent is used for protocol filtering, then Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block pages.
- Multiple Filtering Services can be deployed, connected to 1 Policy Server. This deployment is useful for remote or isolated sub-networks. For more information, see *Network Agent Suggestions*, page 32.
- As a network grows and the number of internet requests increase, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
- *IMPORTANT*: To ensure the integrity of the firewall, *do not* install Websense components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, 2 dedicated machines are recommended to run Websense software in a medium network. Table 12, on page 72 provides a breakdown of the recommended deployment. Figure 4, page 75 provides an overview of a medium Windows network deployment.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 12 Windows Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Transparent ID agent:[1] – DC Agent – Directory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2[2]	• Database Administration • Explorer – Requires Apache or IIS web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005, MSDE 2000 • Reporter client application	**Windows** • Pentium 4,2.0 GHz or greater • 2 GB RAM • 100 GB of free disk space

Table 12 Windows Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (not dedicated)	• Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 2 GB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Filtering Service – Websense Master Database	An additional machine or machines running Filtering Service may be needed, depending on the volume of internet requests. **Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (optional)	• Network Agent	**Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent	**Windows** • Pentium 4, or greater • 256 MB RAM

Table 12 Windows Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Usage Monitor	**Windows** • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Windows** • Pentium 4, or greater • 512 MB RAM • 80 MB free disk space

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Depending on the configuration of the machine, Microsoft SQL Server and the Log Database may need to run on a separate machine than Log Server and the Reporting applications.

Figure 4, page 75 illustrates the distribution of the Websense components in a medium Windows network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

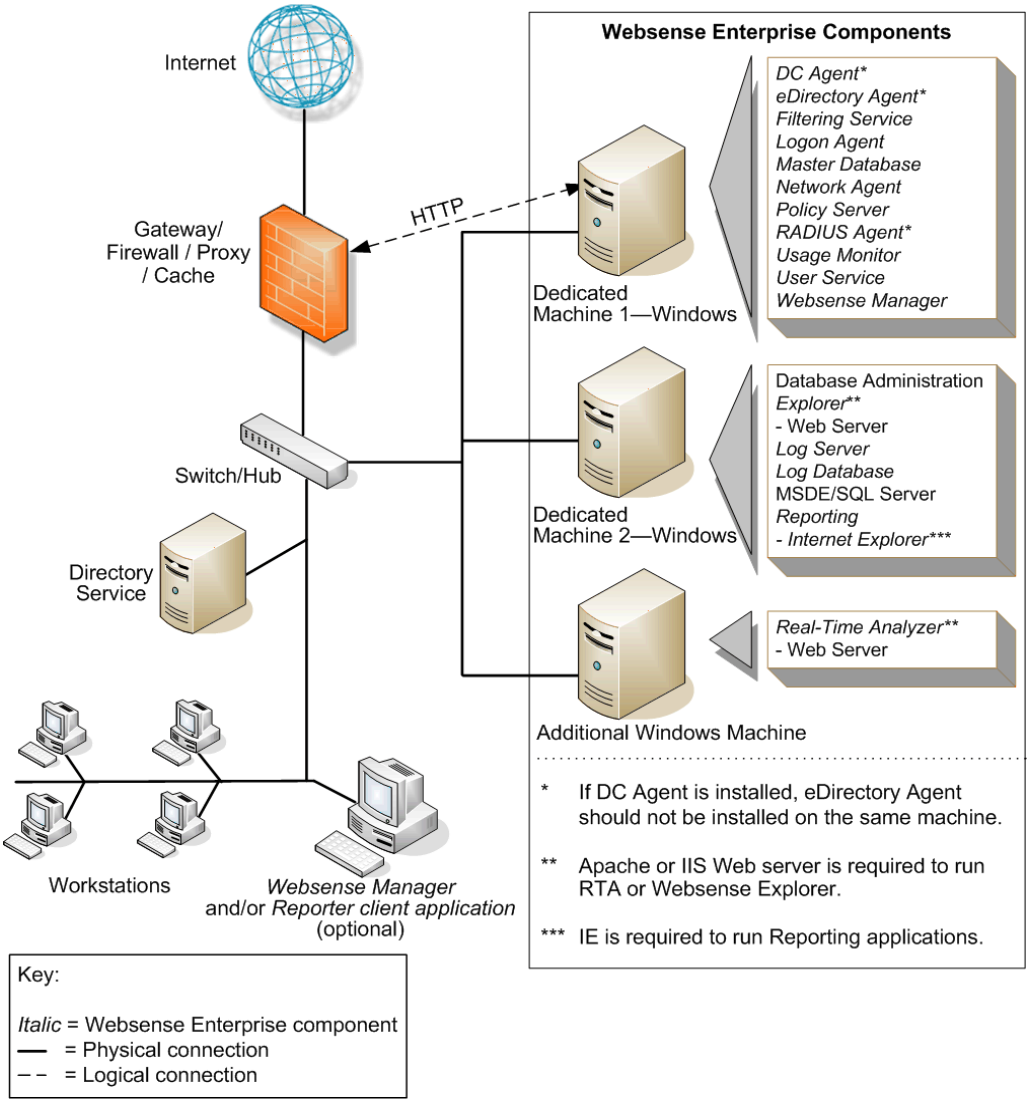

Figure 4 Concept of Windows Deployment—Medium Network

Linux/Solaris Deployment Recommendations

To run Websense software in a medium network on a Linux or Solaris machine, at least 1 Windows machine is needed to run some components. Table 13 provides deployment recommendations. Figure 5, page 80 provides an overview of a Linux or Solaris deployment in a medium network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 13 Linux or Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Transparent ID Agent:[1] – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Linux** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IIIi • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.

Table 13 Linux or Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #2[2]	• Database Administration • Explorer – Requires IIS or Apache web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005 or MSDE 2000 • Reporter client application	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 100 GB of free disk space
Dedicated Machine #2[3]	• Explorer for Unix – Requires Apache web server • Log Database • Unix Log Server • MySQL 5.0	**Linux** • Pentium 4, 2.0 GHz or greater • 1 GB RAM • 100 GB of free disk space **Solaris** • UltraSPARC IIIi • 1 GB RAM • 100 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 1 GB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		

Table 13 Linux or Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Filtering Service – Websense Master Database	An additional machine or machines running Filtering Service may be needed, depending on the volume of internet requests. **Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IIIi • 1 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (optional)	• Network Agent	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM **Solaris** • UltraSPARC IIIi • 1 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 512 MB RAM

Table 13 Linux or Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent (Windows only) – eDirectory Agent – Logon Agent – RADIUS Agent	**Linux** or **Windows** • Pentium 4, or greater • 256 MB RAM **Solaris** • UltraSPARC IIIi • 256 MB RAM • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Depending on the configuration of the machine, Microsoft SQL Server and the Log Database may need to run on a separate machine than Log Server and the Reporting applications.
3. A separate installation of Explorer for Unix is also available. This Explorer only runs with Unix Log Server, and utilizes a MySQL database (a licensed install of v4.0x or v4.1). The Unix and Windows Reporting products are not cross-platform compatible.

Figure 5, page 80 illustrates the distribution of the Websense components in a medium Linux or Solaris network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments

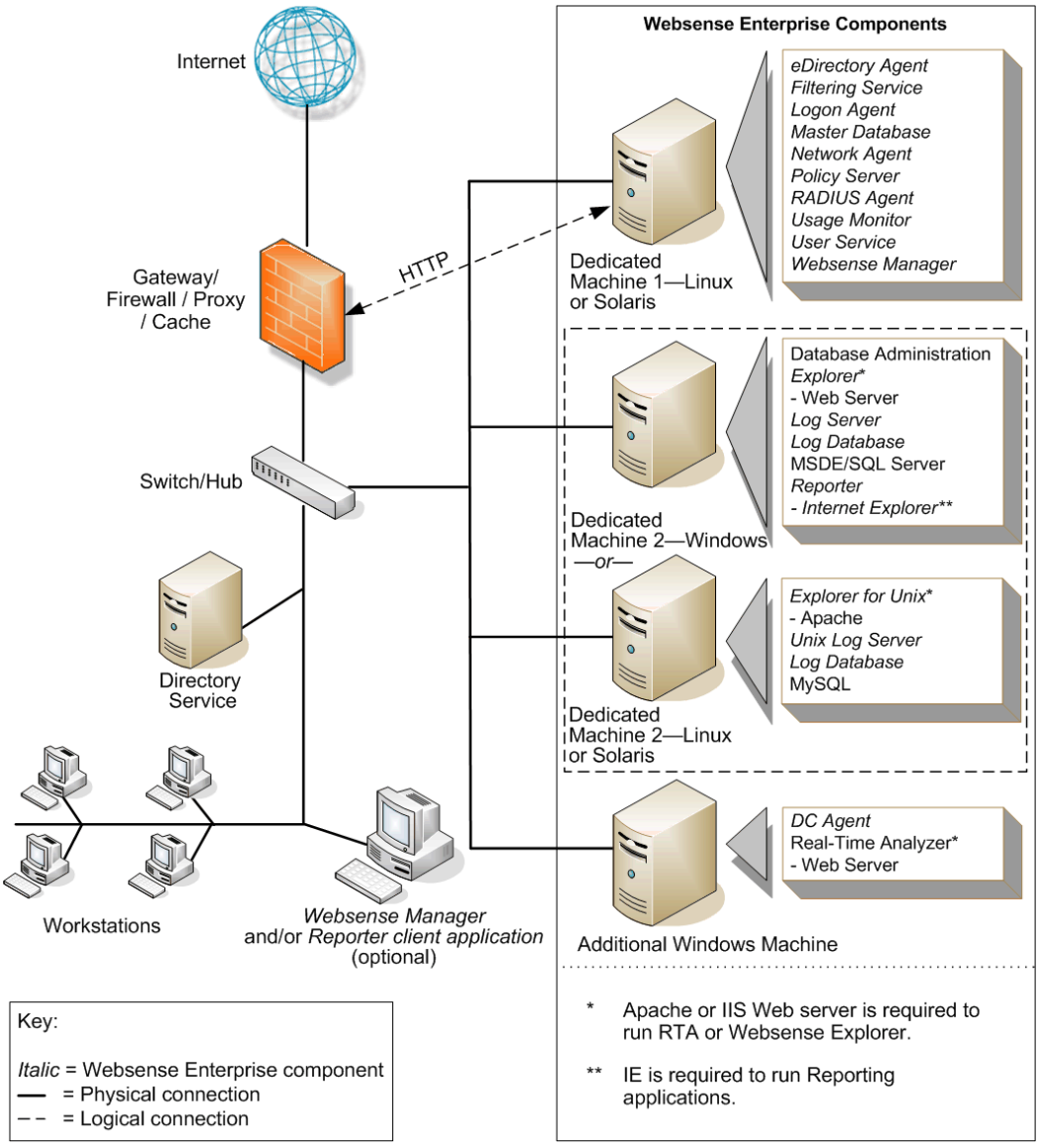

Figure 5 Concept of Linux Deployment—Medium Network

Large Networks: 2,500–10,000 Users

In a large network, Websense components should be distributed on 2 or more dedicated machines, depending on the operating environment. The deployment on dedicated machines is similar to a medium network deployment.

Due to the increased traffic on a large network, more powerful processors and more RAM are recommended for each dedicated machine. On average, a large network has 500 to 2,250 requests per second. More powerful machines may be needed in a higher traffic, large network.

Note

Dedicated machines are recommended for running some Websense components. The tables in this section list possible configurations for these dedicated machines. Only Websense components and applications related to running those components are installed the dedicated machine.

Network Considerations

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

- In a multi-segmented network, Filtering Service must be installed where it can both receive and filter internet requests from the integration partner 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. Each Network Agent monitors an IP address range or network segment. For more information, see *Chapter 5: Deploying Network Agent*.
- Network Agent must have bidirectional visibility of internet traffic to filter non-HTTP traffic, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and other network protocols.
- Multiple Network Agents are needed to capture all network traffic and prevent overloading of servers. The number of Network Agents needed depends on the network size and volume of internet requests. Network Agent can be installed on a dedicated machine to increase overall throughput.

- If User Service is installed on a Linux or Solaris machine and Network Agent is used for protocol filtering, then Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block pages.
- Up to 10 Filtering Services can be connected to 1 Policy Server. This deployment is useful for remote or isolated sub-networks. A Policy Server may be able to handle more than 10 Filtering Services. However, inconsistent filtering may occur if the number of Filtering Services exceeds the capacity of the Policy Server. For more information, see *Number of Filtering Services Allowed per Policy Server*, page 32.
  - Since a maximum of 5000 connections per Policy Server is recommended, multiple Policy Servers may be needed. Central Policy Distribution can be used to apply 1 policy across all Policy Servers.
- As a network grows and the number of internet requests increase, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
- *IMPORTANT*: To ensure the integrity of the firewall, *do not* install Websense components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, 2 dedicated machines are recommended to run Websense software on a large network. Table 14, on page 83 provides a breakdown of the recommended deployment. Figure 6, page 86 provides an overview of a Windows deployment in a large network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 14 Windows Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Transparent ID Agent:[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Windows** • Dual Xeon, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2[2]	• Database Administration • Explorer – Requires Apache or IIS web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005 or MSDE 2000 • Reporter client application	**Windows**[2] • Dual Xeon, 2.0 GHz or greater • 1 GB RAM • 200 of free disk space utilizing a disk array[3] • High speed disk access
Optional Dedicated Machine	• Network Agent	**Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM

Table 14 Windows Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (not dedicated)	• Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Filtering Service – Websense Master Database	An additional machine or machines running Filtering Service may be needed, depending on the volume of internet requests. **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent	**Windows** • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Windows** • Pentium 4, or greater • 512 MB RAM

Table 14 Windows Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Websense Manager	**Windows** • Pentium 4, or greater • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Depending on the configuration of the machine, Microsoft SQL Server and the Log Database may need to run on a separate machine from Log Server and the Reporting applications.
3. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.

Figure 6, page 86 illustrates the distribution of the Websense components in a large Windows network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

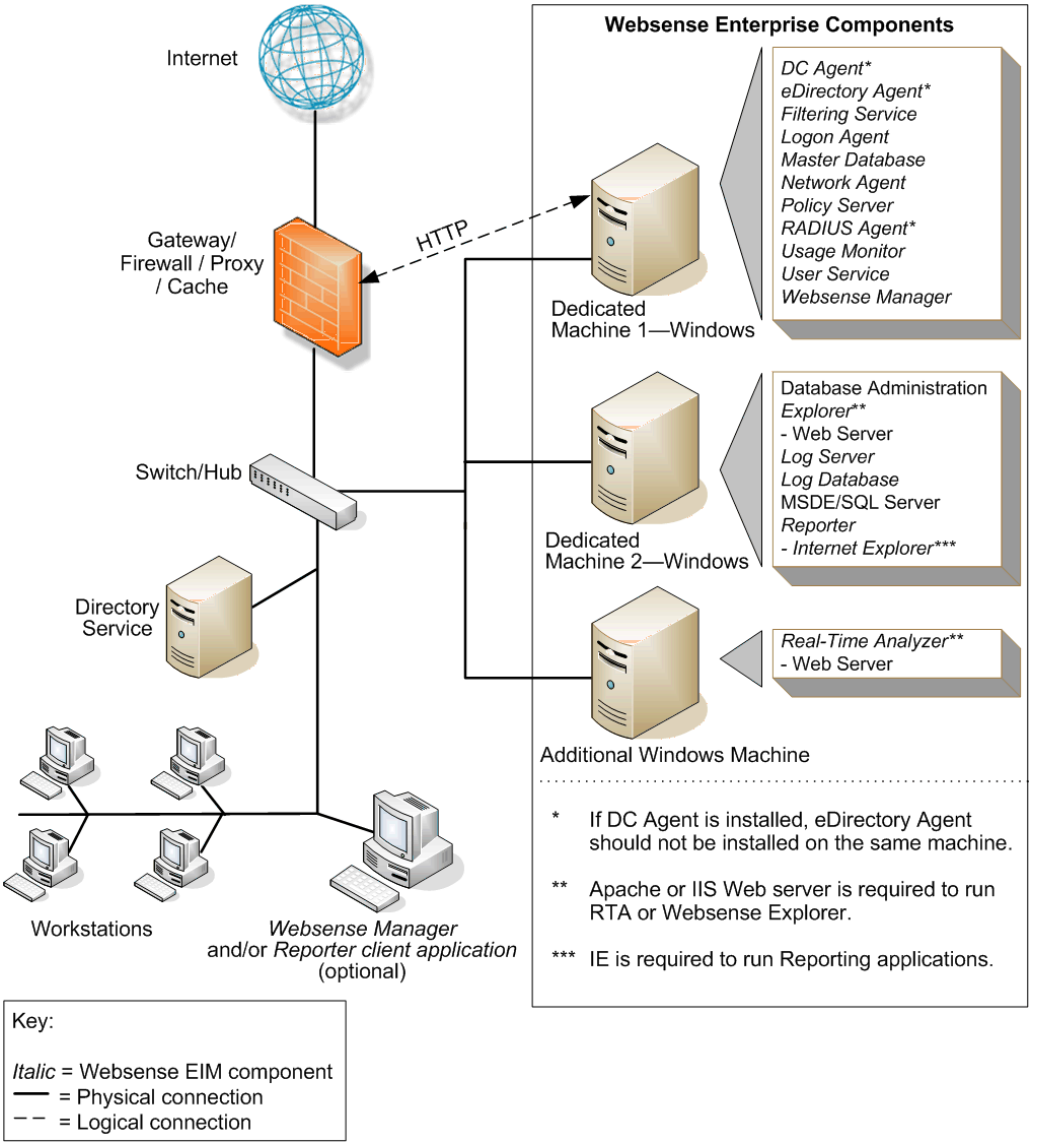

Figure 6 Concept of Windows Deployment—Large Network

Linux/Solaris Deployment Recommendations

To run Websense software in a large network on a Linux or Solaris machine, at least 1 Windows machine is needed to run some components. Table 15 provides a breakdown of the recommended deployment. Figure 7, page 91 provides an overview of a Linux or Solaris deployment in a large network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

Note

Network Agent can be deployed with the filtering components or on a separate machine for improved performance. Network Agent should *not* be deployed on the same machine as response-critical components. For more information, see *Chapter 5: Deploying Network Agent*.

Table 15 Linux or Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Network Agent • Policy Server • Transparent IS Agent:[1] – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Linux** • Dual Xeon, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.

Table 15 Linux or Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #2[2]	• Database Administration • Explorer – Requires IIS or Apache web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005 or MSDE 2000 • Reporter client application	**Windows** • Dual Xeon, 3.0 GHz or greater • 1 GB RAM • 200 GB of free disk space utilizing a disk array[3] • High speed disk access
Dedicated Machine #2[2,4]	• Explorer for Unix – Requires Apache web server • Log Database • Unix Log Server • MySQL 5.0	**Linux** • Dual Xeon, 3.0 GHz or greater • 1 GB RAM • 200 GB of free disk space utilizing a disk array[3] • High speed disk access **Solaris** • UltraSPARC IV • 1 GB RAM • 200 GB of free disk space
Optional Dedicated Machine	• Network Agent	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM **Solaris** • UltraSPARC IV • 1 GB RAM

Table 15 Linux or Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Filtering Service – Websense Master Database	An additional machine or machines running Filtering Service may be needed, depending on the volume of internet requests. **Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 1 GB RAM

Table 15 Linux or Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent (Windows only) – eDirectory Agent – Logon Agent – RADIUS Agent	**Linux** or **Windows** • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM **Solaris** • UltraSPARC IIIi • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Linux** or **Windows** • Pentium 4 or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 RAM
Additional Machine (optional)	• Websense Manager	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Depending on the configuration of the machine, the database engine and the Log Database may need to be run on a separate machine than the Log Server and the Reporting applications.
3. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.
4. A separate installation of Explorer for Unix is also available. This Explorer only runs with Unix Log Server, and utilizes a MySQL database (a licensed install of v4.0x or v4.1). The Unix and Windows Reporting products are not cross-platform compatible.

Figure 7, page 91 illustrates the distribution of the Websense components in a large Linux or Solaris network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

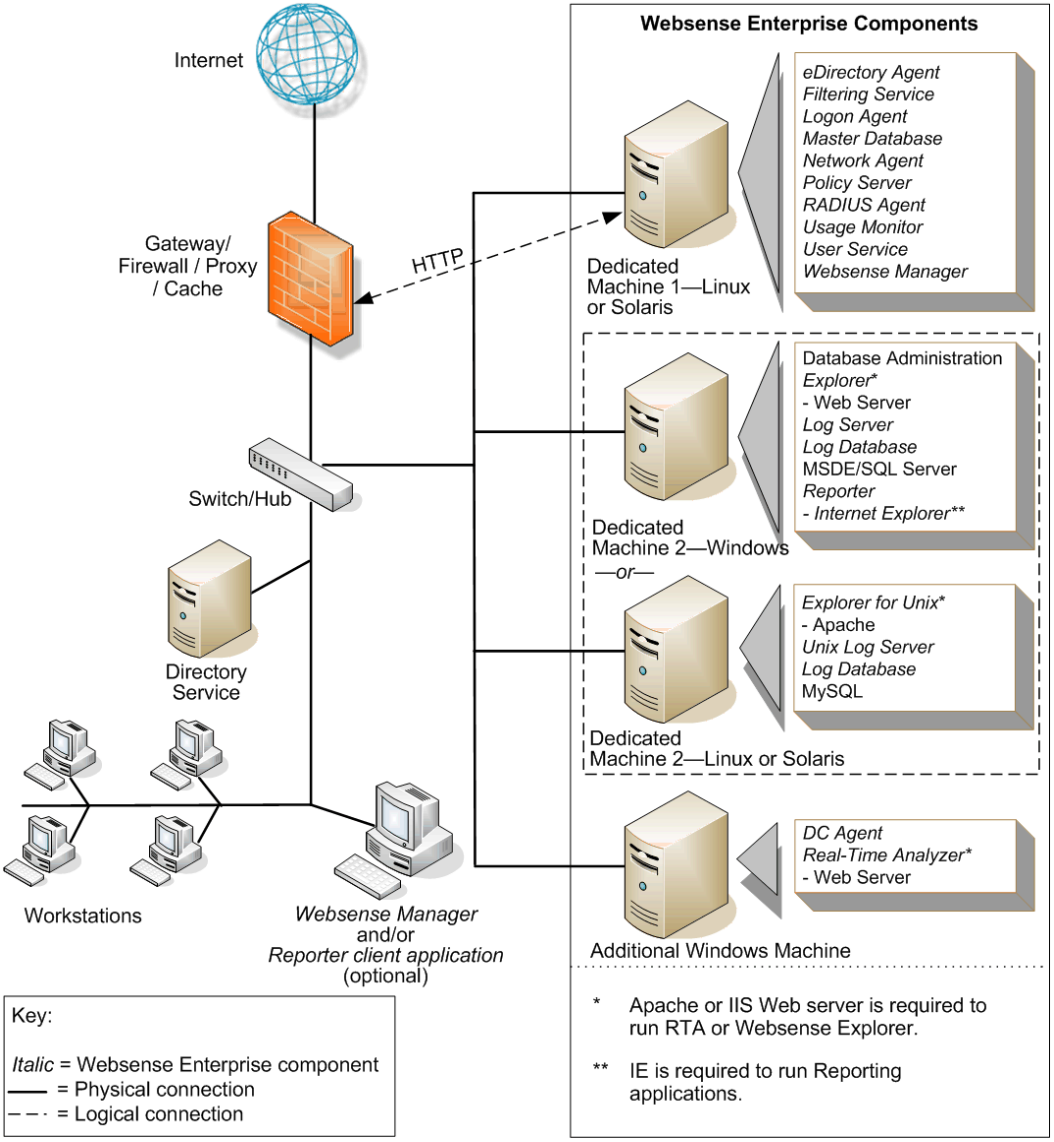

Figure 7 Concept of Linux Deployment—Large Network

CHAPTER 4

Deploying in Networks with Over 10,000 Users

Websense software can be deployed in different configurations, depending on the size and characteristics of the network and filtering needs. Websense components can be installed together on 1 machine, or distributed across multiple machines. Deployment depends on the operating systems, the network size, and volume of internet requests.

Most components can be installed on separate machines using the Websense installation program.

Table 1 and Table 2 in Chapter 1 describe Websense components.

This chapter describes system and deployment recommendations for these ranges:

- Enterprise (10,000–25,000 users)
- Very Large Enterprise (25,000+ users)

Networks with less than 10,000 users are discussed in *Chapter 3: Deploying in Networks up to 10,000 Users*.

The network ranges are intended as general guidelines only. Deployment designs vary between networks, depending on the configuration of the network, operating systems installed, and the volume of internet activity.

Because of the size of the network, multiple instances of certain components must be installed, such as Network Agent and Filtering Service. Multiple instances of other components, such as the Reporter client application, Websense Manager, or the transparent ID agents, may also be needed.

This manual provides system recommendations to optimize Websense component performance. Performance also can be improved by using more powerful machines for resource intensive components, such as the Log Server and database engine (Microsoft SQL, MSDE, MySQL).

In environments with a large number of workstations, installing multiple instances of Filtering Service for load balancing purposes may be appropriate.

Some load balancing configurations, however, permit the same user to be filtered by different Filtering Services, depending on the current load

Note

- These recommendations allow for some network growth and an increase in internet requests. As the network reaches the upper limits for a particular network size, revisit these recommendations to ensure the system is configured to optimize each component's performance.
- Websense software supports TCP/IP-based networks only. If the network uses both TCP/IP and non-IP based network protocols, only those users on the TCP/IP portion of the network are filtered by Websense software.

Enterprise Networks: 10,000–25,000 Users

In an enterprise network, Websense components should be distributed on 3 dedicated machines. Processor and RAM requirements for the respective dedicated machines are the same as a large network deployment for each operating system. Unlike the smaller networks, Network Agent and Filtering Service are installed on separate machines.

Note

Dedicated machines are recommended for running some Websense components. The tables in this section list possible configurations for these dedicated machines. Only Websense components and applications related to running those components are installed the dedicated machine.

Network Considerations

To ensure effective filtering, Websense software must be installed as follows:

- 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 partner 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. Each Network Agent monitors an IP address range or network segment. For more information, see *Chapter 5: Deploying Network Agent*.
- Network Agent must have bidirectional visibility of internet traffic to filter non-HTTP traffic, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and other network protocols.
- Multiple Network Agents are needed to capture all network traffic and prevent overloading of servers. The number of Network Agents needed depends on the network size and volume of internet requests. In an enterprise network, Network Agent needs to be installed on a dedicated machine to increase overall throughput.
- If User Service is installed on a Linux or Solaris machine and Network Agent is used for protocol filtering, then Samba client (v2.2.8a or later) is required on the machine running User Service to enable Windows workstations to display protocol block pages.
- Due to the size of the network, multiple Filtering Services must be deployed. Up to 10 Filtering Services can be connected to 1 Policy Server. This deployment is useful for remote or isolated sub-networks. A Policy Server may be able to handle more than 10 Filtering Services. However, inconsistent filtering may occur if the number of Filtering Services exceeds the capacity of the Policy Server. For more information, see *Number of Filtering Services Allowed per Policy Server*, page 32.
  - Since a maximum of 5000 connections per Policy Server is recommended, multiple Policy Servers may be needed. Central Policy Distribution can be used to apply 1 policy across all Policy Servers.
- As a network grows and the number of internet requests increase, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
- *IMPORTANT*: To ensure the integrity of the firewall, *do not* install Websense components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, 3 dedicated machines are recommended to run Websense software in an enterprise network. Table 16 provides a breakdown of a recommended deployment. Figure 8, page 99 provides an overview of a Windows deployment in an enterprise network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

The recommendations in this section are general guidelines. Contact Field Service Engineering for assistance in deploying Websense software in an enterprise network.

Table 16 Windows Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Policy Server • Transparent ID Agent: [1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Windows** • Dual Xeon, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2	• Network Agent	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM

Table 16 Windows Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #3[2]	• Database Administration • Explorer – Requires Apache or IIS web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005 • Reporter client application	**Windows** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM or more • 200 GB of free disk space utilizing a disk array[3] • High speed disk access
Additional Machine (not dedicated)	• Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing.		
Additional Machine (optional)	• Filtering Service – Websense Master Database	Additional machines running Filtering Service are needed. The number of machines needed depends on the volume of internet requests. **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.

Table 16 Windows Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Network Agent	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent	**Windows** • Pentium 4, 2.0 GHz or greater • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Windows** • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Websense Manager	**Windows** • Pentium 4, or greater • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Depending on the configuration of the machine, Microsoft SQL Server and the Log Database may need to run on a separate machine than Log Server and the Reporting applications. The Database Administration and the Log Server must run on the same machine.
3. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.

Figure 8, page 99 illustrates the distribution of the Websense components in a Windows enterprise network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

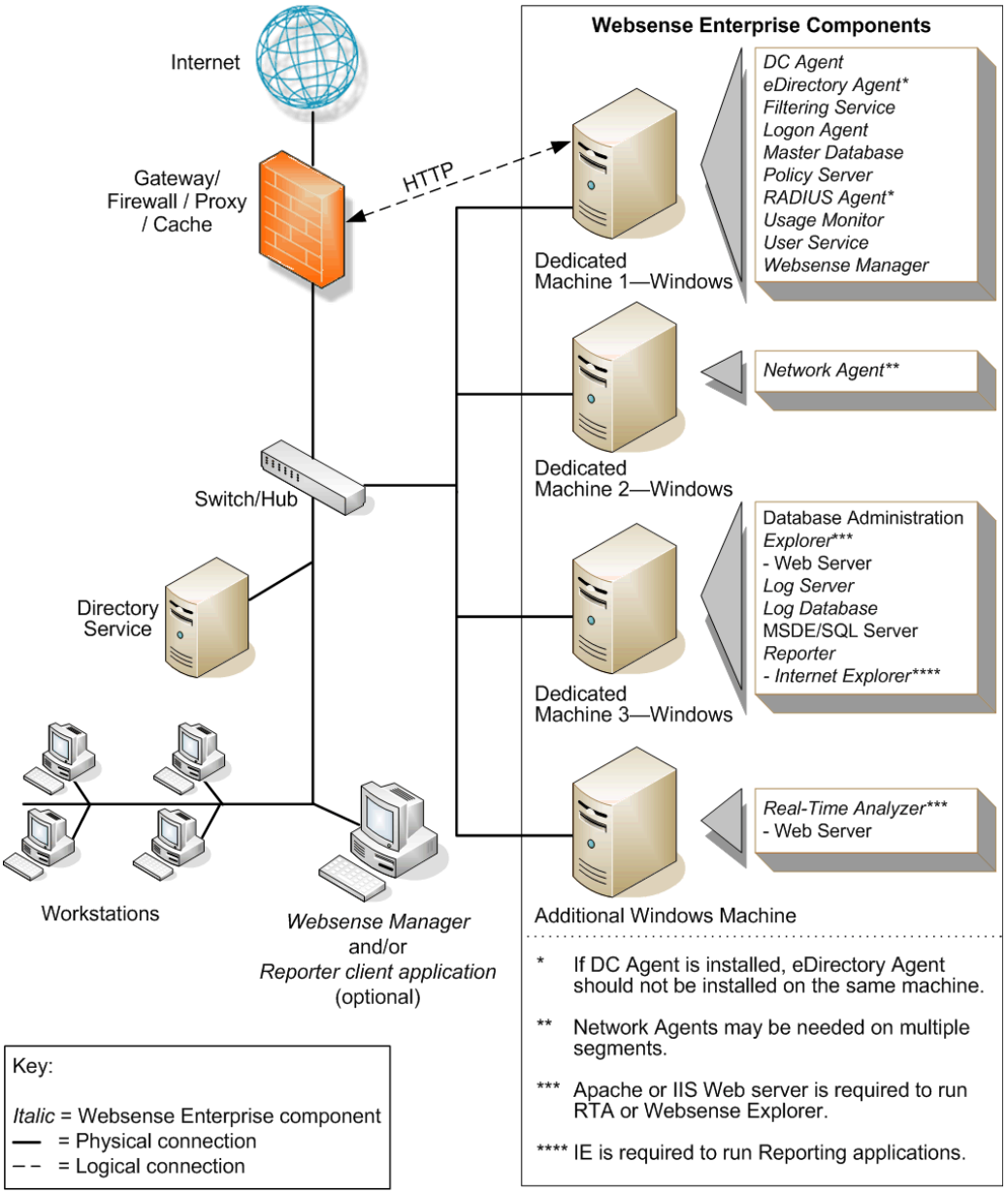

Figure 8 Concept of Windows Deployment—Enterprise Network

Linux/Solaris Deployment Recommendations

To run Websense software in an enterprise network on a Linux or a Solaris machine, at least 1 Windows machine is needed to run some components. Table 17 provides a breakdown of a recommended deployment. Figure 9, page 104 provides an overview of a Linux or Solaris deployment in an enterprise network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

The recommendations in this section are general guidelines. Contact Field Service Engineering for assistance in deploying Websense software in an enterprise network.

Table 17 Linux or Solaris Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Policy Server • Transparent ID Agent:[1] – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Linux** • Dual Xeon, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2	• Network Agent[2]	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM **Solaris** • UltraSPARC IV • 2 GB RAM

Table 17 Linux or Solaris Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #3[3]	• Database Administration • Explorer – Requires Apache or IIS web server • Log Database • Log Server – Requires Internet Explorer 5.5 or later • Microsoft SQL Server 2000/2005 • Reporter client application	**Windows** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM or more • 200 GB of free disk space utilizing a disk array[4] • High speed disk access
Dedicated Machine #3[5]	• Explorer for Unix – Requires Apache web server • Log Database • Unix Log Server • MySQL 5.0	**Linux** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM or more • 200 GB of free disk space utilizing a disk array[4] • High speed disk access **Solaris** • UltraSPARC IV • 4 GB RAM • 200 GB of free disk space utilizing a disk array[4] • High speed disk access
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, 3.0 GHz or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing.		

Table 17 Linux or Solaris Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Filtering Service – Websense Master Database	Additional machines running Filtering Service are needed. The number of machines depends on the volume of internet requests. **Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (optional)	• Network Agent	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM **Solaris** • UltraSPARC IV • 2 GB RAM
Additional Machine (optional)	• Reporter client application	**Windows** • Pentium 4, or greater • 1 GB RAM

Table 17 Linux or Solaris Deployment in an Enterprise Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent (Windows only) – eDirectory Agent Logon Agent – RADIUS Agent	**Linux** or **Windows** • Pentium 4, 2.0 GHz or greater • 256 MB RAM **Solaris** • UltraSPARC IIIi • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Network Agent can run on either the Linux machine, Dedicated Machine #2, or a separate Windows machine (but not the machine running the Reporting components). For more information, see *Chapter 5: Deploying Network Agent*.
3. Depending on the configuration of the machine, the database engine and the Log Database may need to run on a separate machine than Log Server and the Reporting applications.
4. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.
5. A separate installation of Explorer for Unix is also available. This Explorer only runs with Unix Log Server, and utilizes a MySQL database (a licensed install of v4.0x or v4.1). The Unix and Windows Reporting products are not cross-platform compatible.

Figure 9, page 104 illustrates the distribution of the Websense components in a Linux or Solaris enterprise network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

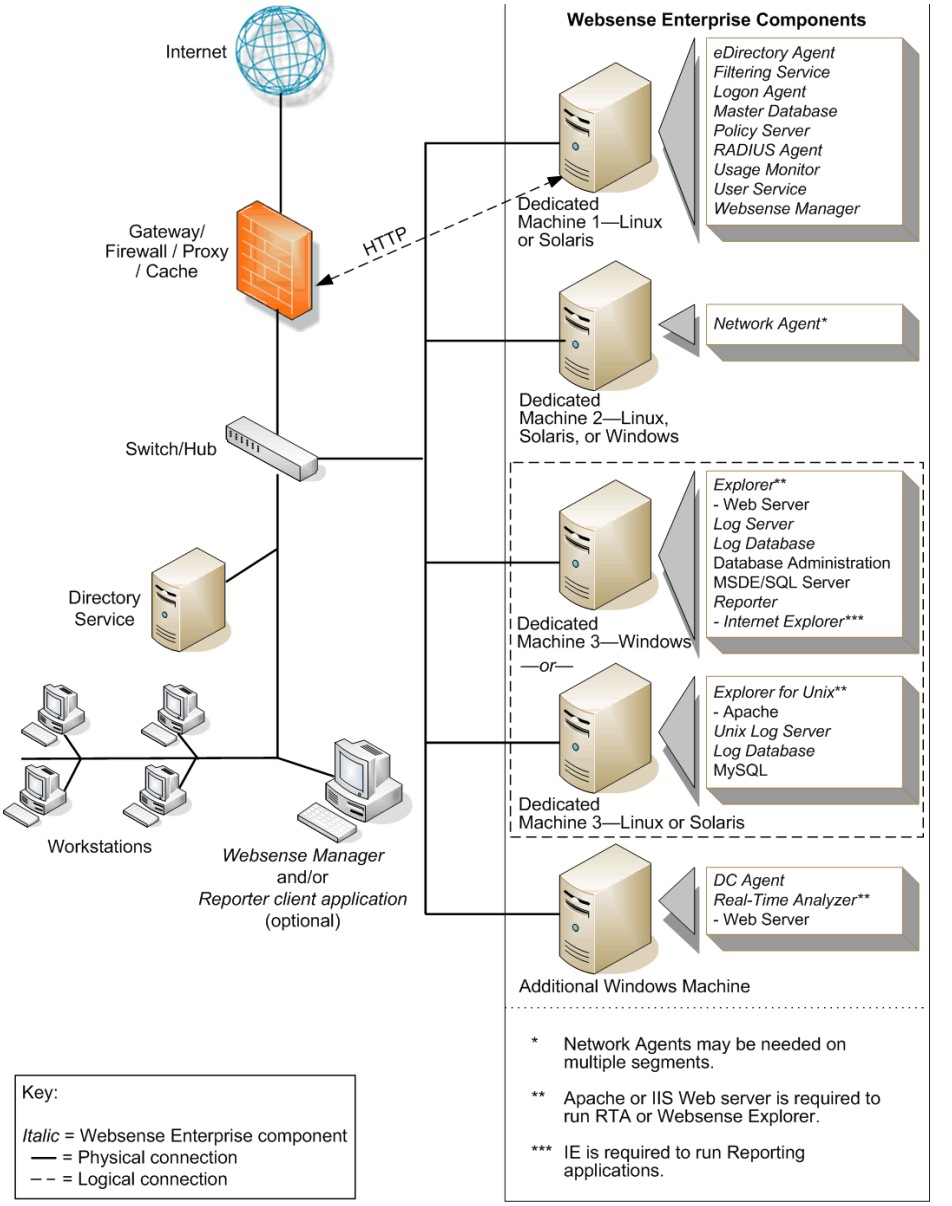

Figure 9 Concept of Linux Deployment—Enterprise Network

Very Large Enterprise Networks: 25,000+

In an very large enterprise network, Websense components should be distributed on 3 dedicated machines. Processor and RAM requirements for the respective dedicated machines are the same as an enterprise network deployment for each operating system. Unlike the smaller networks, Network Agent and Filtering Service are installed on separate machines.

> **Note**
> Dedicated machines are recommended for running certain Websense components. The tables in this section list possible configurations for these dedicated machines. Only Websense components and applications related to running those components are installed the dedicated machine.

Network Considerations

To ensure effective filtering, Websense software must be installed as follows:

- 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 partner 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. Each Network Agent monitors an IP address range or network segment. For more information, see *Chapter 5: Deploying Network Agent*.
- Network Agent must have bidirectional visibility of internet traffic to filter non-HTTP traffic, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and other network protocols.
- Multiple Network Agents are needed to capture all network traffic and prevent overloading of servers. The number of Network Agents needed depends on the network size and volume of internet requests. In an enterprise network, Network Agent needs to be installed on a dedicated machine to increase overall throughput.
- If User Service is installed on a Linux or Solaris machine and Network Agent is used for protocol filtering, then Samba client (v2.2.8a or later) is

required on the machine running User Service to enable Windows workstations to display protocol block pages.

- Due to the size of the network, multiple Filtering Services must be deployed. Up to 10 Filtering Services can be connected to 1 Policy Server. This deployment is useful for remote or isolated sub-networks. A Policy Server may be able to handle more than 10 Filtering Services. However, inconsistent filtering may occur if the number of Filtering Services exceeds the capacity of the Policy Server. For more information, see *Number of Filtering Services Allowed per Policy Server*, page 32.
  - Since a maximum of 5000 connections per Policy Server is recommended, multiple Policy Servers may be needed. Central Policy Distribution can be used to apply 1 policy across all Policy Servers.
- As a network grows and the number of internet requests increase, components can be deployed to additional, non-dedicated machines to improve processing performance on the dedicated machines.
- *IMPORTANT*: To ensure the integrity of the firewall, *do not* install Websense components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, 3 dedicated machines are recommended to run Websense software in a very large enterprise network. Table 18 provides a breakdown of a recommended deployment. Figure 8, page 99 provides an overview of a Windows deployment in an enterprise network.

The recommendations in this section are general guidelines. Contact Field Service Engineering for assistance in deploying Websense software in a very large enterprise network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements

Table 18 Windows Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Policy Server • Transparent ID Agent:[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent • User Service • Usage Monitor • Websense Manager	**Windows** • Quad Xeon, 3.20 GHz or greater • 4 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2	• Network Agent	**Windows** • Dual Xeon, 3.20 GHz or greater • 2 GB RAM
Dedicated Machine #3	• Database Administration • Log Server	**Windows** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM • 100 GB of free disk space utilizing a disk array
Dedicated Machine #4	• Log Database • Microsoft SQL Server 2000	**Windows** • Quad Xeon, 3.20 GHz or greater • 6 GB RAM or more • 500 GB of free disk space utilizing a disk array[2] • High speed disk access

Table 18 Windows Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Additional Dedicated Machines	• Filtering Service – Websense Master Database	Additional machines running Filtering Service are needed. The number of machines needed depends on the volume of internet requests. **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (not dedicated)	One or both: • Reporter client application • Explorer (Web server) – Requires Apache or IIS web server	**Windows** • Pentium 4, 3.0 GHz or greater • 1 GB RAM
Additional Machine (not dedicated)	• Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing.		
Additional Machine (optional)	• Network Agent	**Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM

Table 18 Windows Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent – eDirectory Agent – Logon Agent – RADIUS Agent	**Windows** • Pentium 4, 2.0 GHz or greater • 256 MB RAM
Additional Machine (optional)	• Usage Monitor	**Windows** • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Windows** • Pentium 4, or greater • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.

Figure 10, page 110 illustrates the distribution of the Websense components in a very large Windows enterprise network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

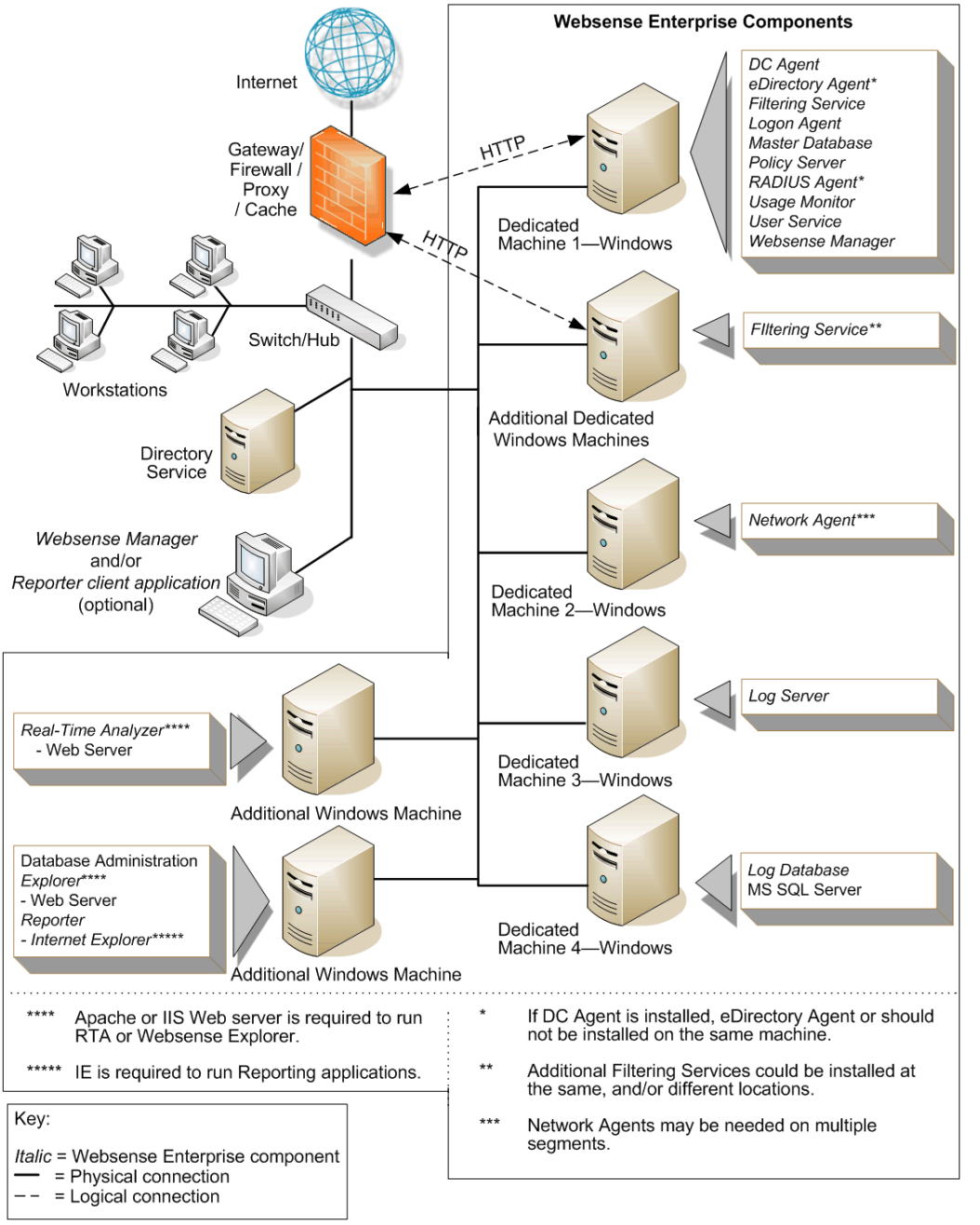

Figure 10 Concept of Windows Deployment—Very Large Enterprise

Linux/Solaris Deployment Recommendations

To run Websense software in an enterprise network on a Linux or Solaris machine, at least 1 Windows machine is needed to run some components. Table 19 provides a breakdown of a recommended deployment. Figure 9, page 104 provides an overview of a Linux or Solaris deployment in an enterprise network.

See Table 3, on page 20 and Table 4, on page 27 for a complete list of operating system and other application requirements.

The recommendations in this section are general guidelines. Contact Field Service Engineering for assistance in deploying Websense software in a very large enterprise network.

Table 19 Linux or Solaris Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• Filtering Service – Websense Master Database • Policy Server • Transparent ID Agent:[1] – eDirectory Agent – Logon Agent – RADIUS Agent[1] • User Service • Usage Monitor • Websense Manager	**Linux** • Quad Xeon, 3.20 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Dedicated Machine #2	• Network Agent[2]	**Linux** or **Windows** • Dual Xeon, 3.20 GHz, or greater • 2 GB RAM **Solaris** • UltraSPARC IV • 2 GB RAM

Table 19 Linux or Solaris Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Dedicated Machine #3	• Database Administration • Log Server	**Windows** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM or more
Dedicated Machine #3	• Unix Log Server	**Linux** • Dual Xeon, 2.0 GHz or greater • 4 GB RAM or more **Solaris** • UltraSPARC IV • 4 GB RAM
Dedicated Machine #4	• Log Database • Microsoft SQL Server 2000	**Windows** • Quad Xeon, 3.20 GHz or greater • 6 GB RAM or more • 500 GB of free disk space utilizing a disk array[3] • High speed disk access
Dedicated Machine #4	• Log Database • MySQL 5.0	**Linux** • Quad Xeon 3.20 GHz or greater • 6 GB RAM or more • 500 GB of free disk space utilizing a disk array[3] • High speed disk access **Solaris** • UltraSPARC IV • 6 GB RAM • 500 GB of free disk space

Table 19 Linux or Solaris Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Additional Dedicated Machines	• Filtering Service – Websense Master Database	Additional machines running Filtering Service are needed. The number of machines depends on the volume of internet requests. **Linux** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Solaris** • UltraSPARC IV • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space. **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM • 10 GB of free disk space Free space must comprise at least 20% of the total disk space.
Additional Machine (not dedicated)	One or both: • Explorer (Web server) – Requires Apache or IIS web server • Reporter client application	**Windows** • Pentium 4, or greater • 1 GB RAM

Table 19 Linux or Solaris Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Additional Machine (not dedicated)[4]	• Explorer for Unix – Requires Apache web server • Web browser	**Linux** • Pentium 4, or greater • 1 GB RAM **Solaris** • UltraSPARC IV • 1 GB RAM
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer – Requires Apache or IIS web server – Internet Explorer 5.5 or later	**Windows** • Pentium 4, 2.0 GHz or greater • 512 MB RAM • 1 GB of free disk space
While multiple Websense components can be installed on dedicated machines, Websense Manager and the Reporter client application also can be installed on additional machines to provide easier access. The transparent ID agents and Network Agent also can be installed on multiple machines to improve processing.		
Additional Machine (optional)	• Network Agent	**Linux** or **Windows** • Pentium 4, 3.0 GHz or greater • 2 GB RAM **Solaris** • UltraSPARC IV • 2 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] – DC Agent (Windows only) – eDirectory Agent – Logon Agent – RADIUS Agent	**Linux or Windows** • Pentium 4, 3.0 GHz or greater • 256 MB RAM **Solaris** • UltraSPARC IIIi • 256 MB RAM

Table 19 Linux or Solaris Deployment in a Very Large Enterprise

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Usage Monitor	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM
Additional Machine (optional)	• Websense Manager	**Linux** or **Windows** • Pentium 4, or greater • 512 MB RAM **Solaris** • UltraSPARC IIIi • 512 MB RAM

1. Transparent ID agents can be deployed alone or in certain combinations. For more information, see *Deploying Transparent Identification Agents*, page 37.
2. Network Agent can run on either the Linux machine, Dedicated Machine #2, or a separate Windows machine (but not the machine running the Reporting components). For more information, see *Chapter 5: Deploying Network Agent*.
3. The Log Database needs a disk array, running RAID level 10, to increase I/O reliability and performance.
4. A separate installation of Explorer for Unix is also available. This Explorer only runs with Unix Log Server, and utilizes a MySQL database (a licensed install of v4.0x or v4.1). The Unix and Windows Reporting products are not cross-platform compatible.

Figure 11, page 116 illustrates the distribution of the Websense components in a very large Linux enterprise network. This drawing is not a required configuration; the components may be deployed differently or on multiple segments.

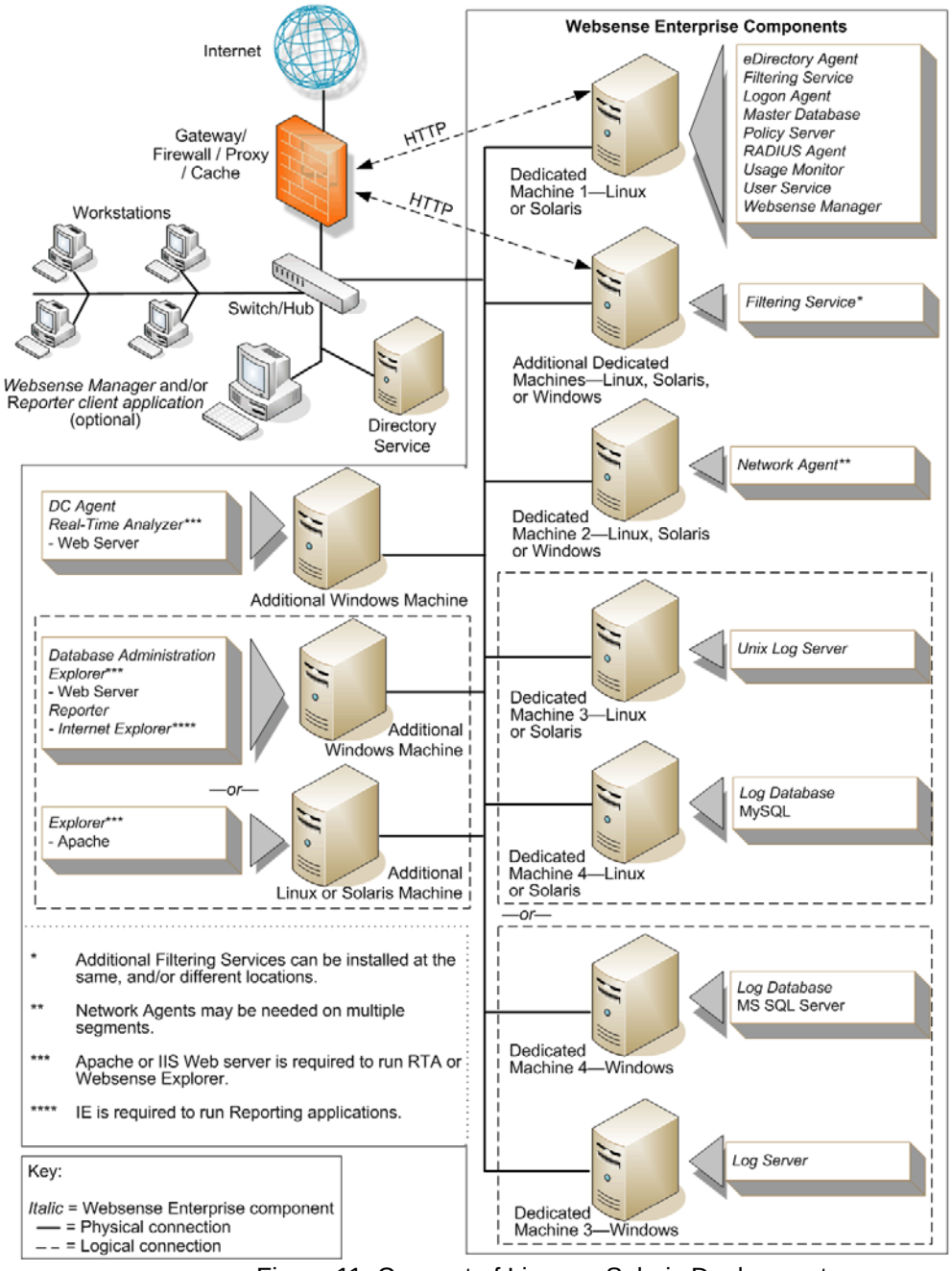

Figure 11 Concept of Linux or Solaris Deployment—
Very Large Enterprise Network

Implementing Websense Software Within Distributed Enterprises

Distributed enterprise networks have many remote locations, ranging from dozens to thousands of small offices. Typically, between 5 and 50 employees work at each remote office. Many of these offices have internet access and no dedicated IT staff. Some organizations use a decentralized network topology that provides each remote office with its own internet connection. The challenge is to apply consistent, cost effective filtering of internet requests across the entire organization. Websense filtering components are deployed regionally and communicate over the internet. Uniform filtering policies are applied to hundreds of remote offices from a central location.

Network Topology

Each remote office firewall in a decentralized network is connected directly to the internet, rather than to a corporate WAN, to reduce network infrastructure costs. A small office/home office (SOHO) firewall is connected to an ISDN, DSL/cable, or T1 connection. Except for corporate application data that may use a virtual private network (VPN) connection, each outbound internet request from a remote office is sent through a local internet service provider (ISP) to the internet.

Figure 12, page 118 shows the network topology of this type of remote office.

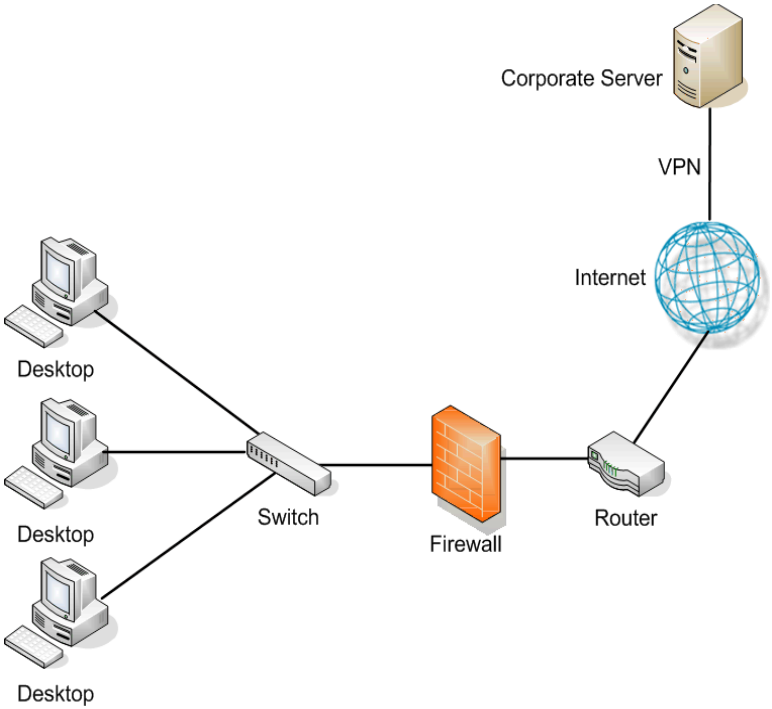

Figure 12 Remote Office Topology in a Decentralized Network

A large distributed enterprise, as shown in Figure 13, page 119, can have hundreds, or even thousands, of such remote offices connected to the corporate network through the internet.

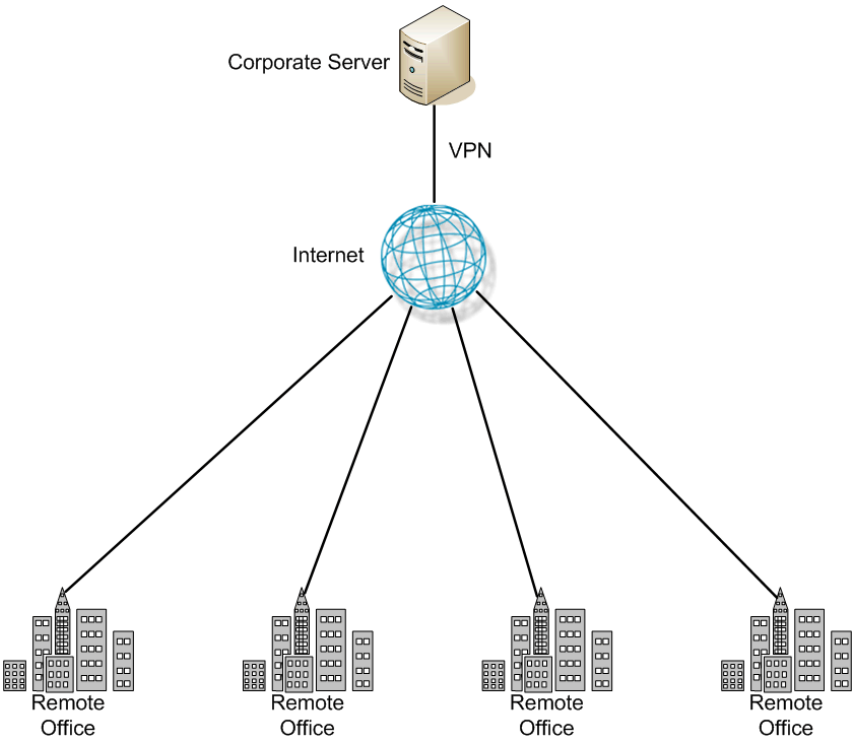

Figure 13 Distributed Enterprise

Distributed enterprises with remote internet connectivity have a complex set of filtering considerations. Remote Filtering and Citrix integration are discussed in *Chapter 2: General Deployment Recommendations*.

- Remote offices must have internet access.
- Internet access is provided by independent internet service providers, often using low to medium-bandwidth connections.
- Web page requests are sent directly to the internet and are not routed first through a central corporate network.
- Internet access must be filtered to allow only business-related, non-offensive content.
- Cost considerations prohibit deploying a filtering server at each office.
- Given the relative low speed of each office's internet connection, a slightly slower response caused by the filtering product is acceptable.
- All remote offices can be filtered according to the same policies.

Deploying Websense Software in a Distributed Enterprise

In centralized organizations which route all outbound internet requests through a single large internet connection, the server running Websense software is normally placed physically close to the firewall, proxy server, or network appliance. Remote offices in a distributed enterprise have a direct local connection to the internet, and no centralized point of control.

Rather than deploying Websense software at each remote office firewall, Websense components can be deployed in a geographically central location. Since Websense software is accessible from the internet, the Websense components should be protected by a firewall that allows URL lookup requests to pass through. A SOHO firewall at each remote office is configured to communicate with the centralized Websense components. The firewall does not distinguish between accessing Websense software over the internet and accessing it through a LAN connection at a remote office.

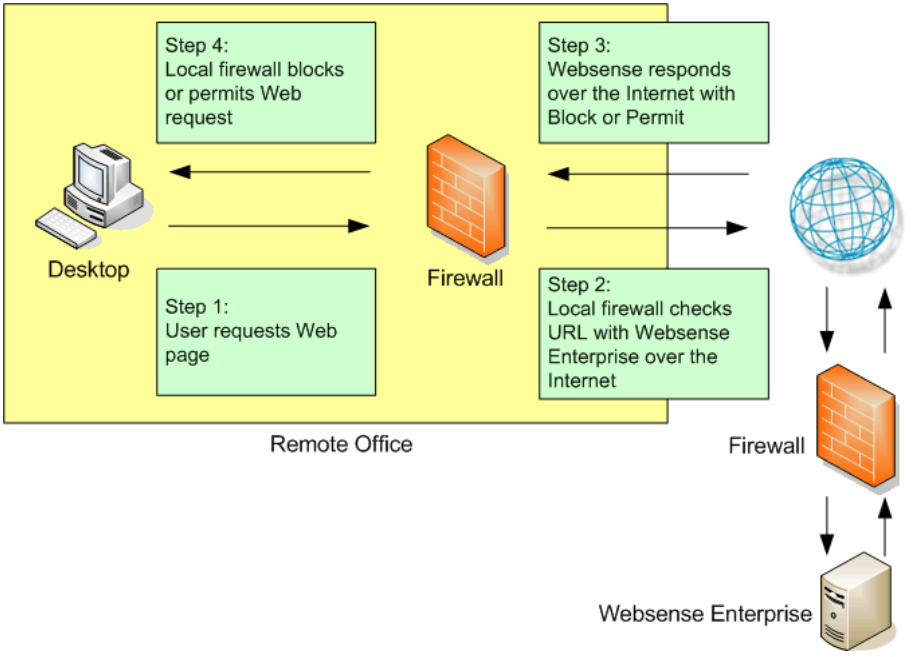

Figure 14 Remote Office Communication Strategy

Figure 15, page 121 illustrates an distributed enterprise, with multiple remote offices.

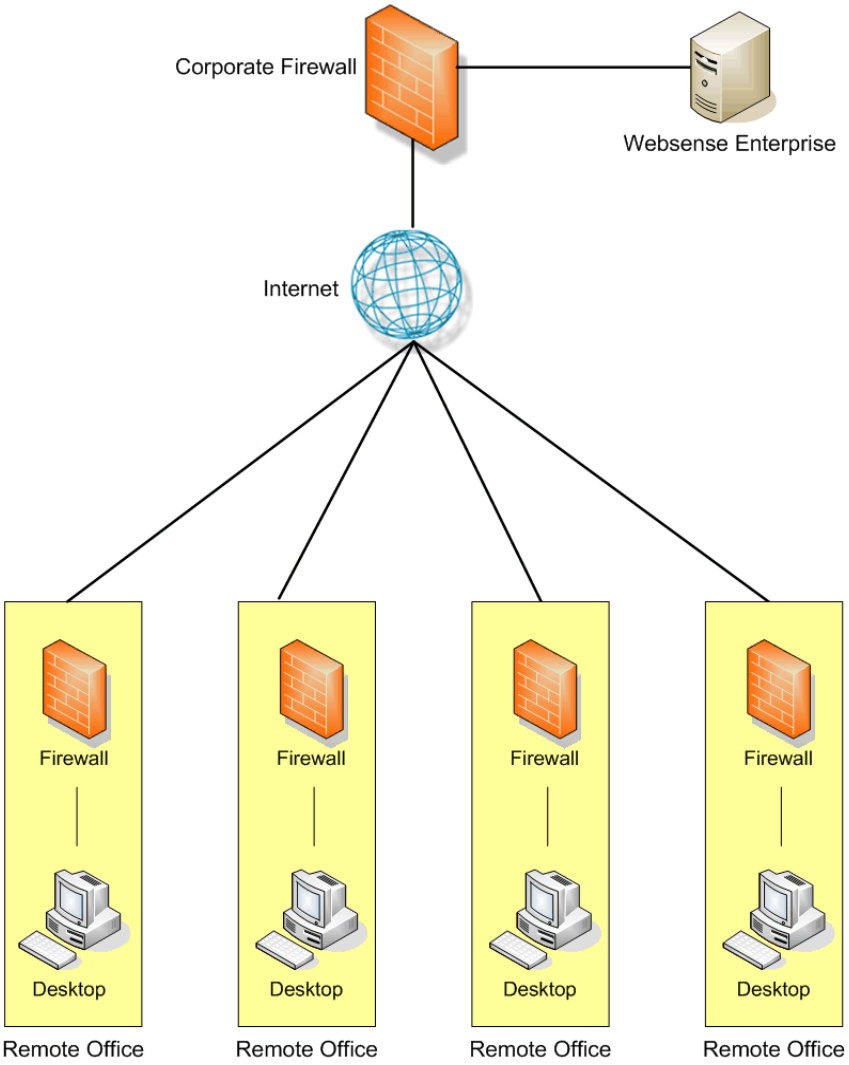

Figure 15 Distributed Enterprise Communicating with Websense Software

Websense has tested this configuration in cooperation with several of its integration partners. The same deployment methodology described here can be used with any network security product integrated with Websense software. A full list of Websense integrations can be found at:

www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/

Centralized filtering:

- Provides distributed enterprises with Websense filtering for each remote office.
- Eliminates the need for a separate Websense installation at each location.
- Provides uniform filtering policies at each remote office.
- Eliminates the cost of additional hardware to provide filtering servers at each remote office.
- Allows the enterprise to centrally configure, administer, and maintain a limited number of Websense filtering machines.

Deployment Models

Deployment scenarios vary with different enterprise configurations. For example, an organization with 50 remote offices, all located in the same general region, deploys Websense software differently than a company with remote offices spread throughout the world. This section discusses 3 of the general deployment models available for distributed enterprises:

- Remote offices located within 1 region
- Remote offices located within 1 region, with a growing number of employees or offices, or both
- Remote offices located nationally or globally

Regional Offices

The simplest Websense deployment for a distributed enterprise is a network composed of remote offices in a single region, such as San Diego County. Most organizations with this configuration can use a single Websense deployment, centrally located within that region, to provide filtering for all employees. See Figure 15, page 121.

Expanding Regional Offices

Some organizations deploy Websense software within a given region and later decide to increase the number of remote offices in that area. To compensate for the additional offices and employees, the organization can:

- **Improve the performance of the machines running Websense components**. Increasing the RAM and CPU of the server or servers running Websense components allows them to respond to larger amounts

of users without additional latency. This upgrade helps with a moderate increase in head count or the addition of a few more offices. This chapter and Chapter 3 contain hardware recommendations for different network sizes.

- **Deploy an additional machines to run Websense components.** If a significant number of new offices is added, the deployment of additional instances of certain Websense components distributes the load and provides optimum performance for each remote office. See Figure 16.

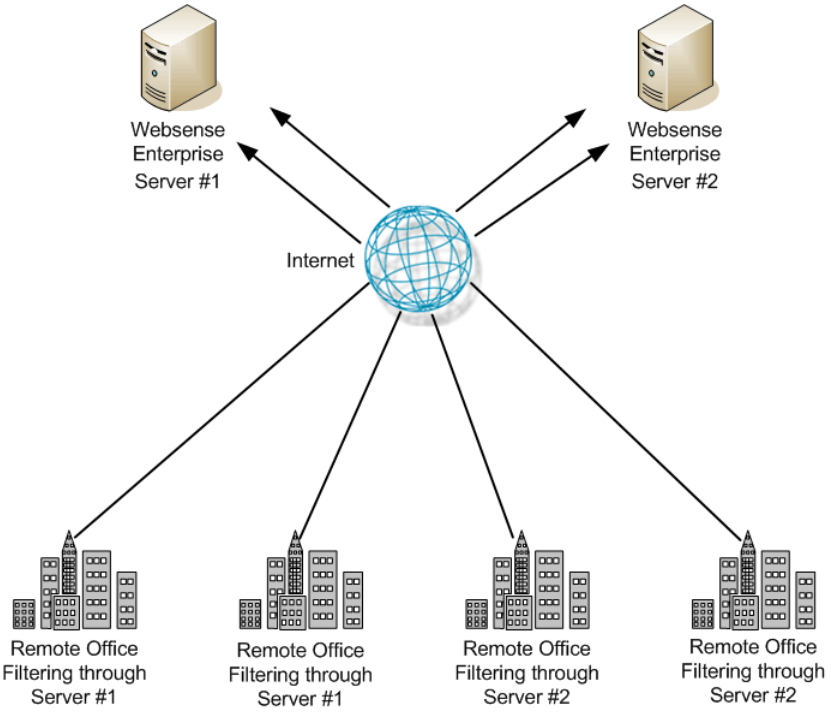

Figure 16 Adding Websense Filtering

Additional copies of Websense software can be deployed within the region as the number of offices continues to grow.

National or Worldwide Offices

Some organizations have hundreds of remote offices spread through a country or even around the world. In such cases, 1 or 2 Websense installations are not enough because:

- Each remote office is geographically distant from the Websense components. Request lookups would to have to travel further over the internet to reach Websense software. This distance increases the total latency of the response and may lead to slower internet access for end users.
- Large numbers of employees generate more internet requests than recommended for 1 or 2 Websense machines, leading to delays in returning web pages to requesting workstations.

These organizations should divide their offices into logical regions and deploy Websense software in each region. For example, a distributed enterprise might group their United States offices into a western region, a central region, and an eastern region. Websense software is deployed at a central office in each region.

The logical division of offices into regions depends on the location and grouping of remote offices and the total number of employees at each office. For example, a company with a large number of remote offices in a concentrated area, such as New York City, may need to deploy multiple machines running Websense software within that area. Or, an enterprise may only have 3 offices in California with 100 to 250 employees at each office. In this case, a single Websense installation might be deployed for all 3 offices. This enterprise also can deploy Websense software locally at each office (rather than using a distributed approach), particularly if an IT staff is present at each location.

Given the significant number of variables, large organizations should contact Websense Sales Engineering to plan a rollout strategy before deployment.

Secure VPN Connections

For URL lookup requests and replies, some firewalls allow administrators to set up a secure VPN connection between the remote office firewalls and Websense software. Permitted requests then are fulfilled directly from the internet, providing an optimum combination of speed and security. See the firewall documentation to determine if the firewall supports this capability.

If a RADIUS server is being used with the VPN service, a Websense RADIUIS Agent can be used for transparent user identification. See *Deploying Transparent Identification Agents*, page 37 for information on deploying the RADIUS Agent. See the *Websense Enterprise Installation Guide* for more information on installing the RADIUS Agent.

Calculating TCP Connections

In a distributed enterprise, internet requests may be sent to multiple Filtering Services from hundreds of remote-office firewalls that are configured for persistent TCP connections. In this type of deployment, the number of TCP connections available for a Filtering Service may be exceeded. By default, each Filtering Service is configured to accept a maximum of 500 connections. When the remote offices' firewalls exceed the maximum allowed number of connections that can be accepted by Websense, the firewalls either block all subsequent requests or permit all requests, depending upon how those firewalls are configured.

This section provides the instructions for calculating the number of connections required for a Websense deployment and the number of Filtering Service instances needed under different traffic loads.

Calculating Connections

The number of TCP connections opened by different integration products varies widely. In a distributed environment of remote offices, 1-3 connections should be sufficient for each remote office firewall, depending upon the load (number of requests per second) from each office. Contact the manufacturer of the integration product to determine how to limit TCP connections. If the integration product cannot be reconfigured to open fewer connections, additional Filtering Services may be needed to handle the extra connections requested by the remote offices' firewalls.

Note

Switching connections from TCP to UDP in a distributed enterprise may solve a connection problem. Consult the integration product documentation to determine if the integration can be configured for UDP connections.

To calculate the number of Websense connections required to filter internet requests from remote offices, multiply:

(number of integration machines) x (number of connections opened by each integration machine)

To calculate the number of Filtering Service instances an enterprise needs to filter the traffic from remote offices, divide:

(number of Websense connections required) / (number of connections each Filtering Service is configured to accept)

The maximum number of connections recommended for a Filtering Service running on a high performance machine is 1500 (500 connections times 3 TCP ports).

System requirements for a high performance machine running Filtering Service:

- Pentium 4, 3.0 GHz
- 2 GB RAM (including 1 MB of memory for each connection)

Sizing Information

Websense web filtering performance is dependent upon the machine's processor speed and available memory under a given load (requests per second). An increased load requires more CPU time and supports fewer connections. If fewer connections are supported, additional Filtering Service instances are required to filter the requests from the remote offices.

The following tables display sizing information for remote offices with differing numbers of users.

- Estimates are based on the system requirements for a high performance machine as described in the previous section.
- The number of connections from the integration has been set at 1 for this example but may need to be higher as the load increases.
- A remote location could have 1 or multiple firewalls, depending on the network configuration and user location. See the number of firewalls in the following tables.
- As the number of users increases, the required number of Filtering Service instances increases to meet the need to filter a greater number of internet requests.

Table 20 10 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense Software	Number of Filtering Service Instances
1000	1	1000	1
2000	1	1000	2

Table 20 10 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense Software	Number of Filtering Service Instances
5000	1	1250	4

Table 21 25 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense Software	Number of Filtering Service Instances
1000	1	1000	1
2000	1	1000	2
5000	1	1250	4

Table 22 50 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Number of Filtering Service Instances
1000	1	1000	1-2
2000	1	1000	2-3
5000	1	1250	7-8

Filtering Service faces an increased demand as more users are added behind a firewall. Due to the increased traffic, each installation of Filtering Service is able to handle fewer connections, as seen in the table below.

Table 23 100 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Number of Filtering Service Instances
1000	1	500	2
2000	1	500	4
5000	1	500	10-11

Configuring Websense Connections

The number of connections that Websense accepts can be increased.

Note

Contact Websense Technical Support for assistance with this procedure.

1. Stop the Websense Filtering Service.
2. Locate the `eimserver.ini` file in the **\bin** directory.
3. Make a backup copy of the `eimserver.ini` file.
4. Open the `eimserver.ini` file with a text editor.
5. Add this line to the file:

   `MaxWISPConnections=<number>`

   Where <*number*> is a value between 501 and 1500.
6. Save and close the file.
7. Restart Filtering Service.

For instructions on stopping and starting the Websense Filtering Service, see the *Websense Enterprise Administrator's Guide*.

Optimizing Network Performance

Websense software introduces minimal latency when deployed on a server physically close to a firewall, proxy server, or caching appliance. Websense has also tested the distributed deployment approach discussed in this document to ensure a similarly low level of delay. Latency is the time a network packet needs to reach its destination. Even though outbound web requests from remote offices must travel over the internet to the Websense installation, in most situations end users at remote offices are not aware of the filtering process unless they are blocked from a website. Total latency depends on these factors:

- Speed (bandwidth) of the internet connection at each remote office.
- Distance from the remote office to the machine running Websense filtering.
- Number of users and connections to the machine running Websense filtering.
- Speed of the Websense machine.

Internet Connection Speed

Overall filtering performance is dependent upon the speed of the internet connection at each remote office, which is determined when the parent corporation sets up the office. A DSL, cable, or T1 line is appropriate for an office of 5-25 employees and is fast enough to provide responsive URL lookups through Websense software. A 56K dial-up modem is not recommended because of the additional time needed to retrieve Websense responses.

IMPORTANT

Match an appropriate class of firewall to the number of employees at each remote site. For example, a remote office with 10 employees can use a SOHO-class firewall, while a remote office of 100 employees should use a firewall with greater capacity.

Distance from the Websense Machine

The internet is a large collection of servers and routers that pass data from point to point until it reaches its destination. The more points (hops) a Websense lookup request has to travel, the longer it takes the remote office to receive a reply and fulfill the end user's request. The number of hops required to reach the Websense machine, and the time required for each hop, is generally tied to the geographical distance between machine running Websense software and the source of the request. The closer the server is to a remote office, the faster the Websense lookup and overall performance improves for the end user.

Websense recommends that distributed enterprises deploy the Websense machine no more than 20 hops from each remote office. Similarly, the total trip for an ICMP (Internet Control Message Protocol) ping from each remote office to Websense machine should take no more than 100 ms to provide satisfactory browsing speeds.

Trip time for a ping and the number of hops can be determined through the use of commands.

From a DOS prompt (Windows):

- `ping`—test network connection and discover the total trip time.
- `tracert`—traces the route to the remote host.
- `pathping`—combines the ping and tracert functions.

From Linux/Solaris:

- `ping`—test network connection and discover the total trip time.
- `traceroute`—prints the route traffic takes to the remote host. This command requires super-user or administration privileges and has many options.
- `tracepath`—traces the route to the network host. This command has fewer options than traceroute, but can be used by all users.
- `netstat`—prints the network connections, routing tables, and other network data depending on the options that are entered

For more information on these commands and their options, see the Linux or Unix man pages.

Hardware Performance

The number of requests per second coming in from remote offices can be quite high, as can the number of connections being opened to the Websense machine. The Websense machine must be capable of handling the anticipated traffic load without adding to the latency of the system.

The speed of the SOHO (small office/home office) firewall is also an important consideration. A slower firewall requires additional time to contact Websense software, resulting in slower overall Web page responses. A faster firewall at each remote office processes the Websense response in less time and provides faster overall performance.

Caching

Certain Websense partners have included a filtering enhancement that significantly improves performance with Websense software for distributed enterprises. Juniper Networks NetScreen, Check Point, and Cisco firewalls cache the responses received from Websense software. This cache keeps track of common Web requests and the Websense response (Permit/Block) so the firewall does not have to check with Websense software for every requested Web page.

For example, if all employees of an organization are allowed to visit www.cnn.com, these firewalls allow the request to be fulfilled by the destination web server without first checking with Websense software (after the first request has been verified). This use of caching can dramatically improve performance.

Websense recommends using a firewall from 1 of these 3 vendors when configuring remote offices for filtering. For information on determining if caching is appropriate for the environment, see the appropriate *Websense Installation Guide*.

Best Practices for Distributed Enterprises

Enterprises with multiple remote offices often find it cost and time prohibitive to deploy Websense software at each location. Other companies do not have the network infrastructure in place to feed all outbound internet requests through a single, central control point. Using the guidelines and deployment methodologies outlined in this manual, together with careful planning, distributed enterprises can deploy Websense software in an efficient, high-performance, and cost-effective manner.

The main considerations in deploying Websense software in a distributed enterprise are:

- **Response caching**—deploy Websense with a firewall that supports Websense response caching (such as from Juniper Networks NetScreen, Check Point, and Cisco). Other network security products integrated with Websense software may also be used, but end-user performance may be higher with firewalls from mentioned vendors.
- **Distance to the Websense filtering machine**—deploy a machine running Websense software no more than 20 hops and 100ms from remote offices. Organizations with offices spread over a wider area should deploy 1 or more FIltering Services in each geographical region. Each server should conform to the CPU and RAM requirements described in *Chapter 2: General Deployment Recommendations*.
- **Configuring connections**—be sure to configure an adequate number of persistent TCP connections for all remote office firewalls. Increase the number of connections that Websense software accepts to accommodate the number of connections opened by the remote firewalls. Provide enough Filtering Services for the anticipated traffic.
- **Internet connection speed**—remote offices should use the fastest internet connection possible. Filtering is virtually undetectable when using a fast internet connection. Cable or DSL connections are the minimum requirement for use with Websense software in distributed enterprises.
- **Server speed**—Websense machines must be capable of handling the anticipated traffic load and the number of connections opened by the remote office firewalls. Deploy high performance machines.
- **Filtering policy when Websense is unavailable**—some firewalls and cache appliances give administrators the option of allowing Web requests

out to the internet—unfiltered by Websense—if they receive more internet requests than they can handle. If this feature is enabled, and a performance problem with the internet causes Websense lookups to take longer than normal, users at each remote office can still access the internet. Filtering is enabled again as soon as internet performance returns to normal. Websense recommends that administrators enable this option, if available.

- **VPN connection**—use a VPN connection between the remote office firewall and the Websense machine for maximum security (if supported by the firewall).

CHAPTER 5

Deploying Network Agent

How Websense components are deployed is dependent on the configuration of the network. Except for the simplest configurations, Ethernet networks are built of *segments*.

These segments serve as neighborhoods for a group of machines, which are connected to the rest of the network via a central connection point, such as a 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 single segment requires only 1 Network Agent, while multiple segments each may require a Network Agent to ensure that those segments are monitored.

A simple overview is provided for network configurations and Network Agent location.

Network Agent

Network Agent manages internet protocols (including HTTP, HTTPS, and FTP), by examining network packets and identifying the protocol. Network Agent queries the Filtering Service to determine if the protocol should be blocked, and logs the results of that query.

Network Agent, as with other integration products (a firewall, router, proxy server, or network appliance), route internet requests to Websense software for filtering.

Network Agent must be installed where can it see all internet requests for the machines it is assigned to monitor. For those machines, Network Agent must see all URL and protocol requests going out to the internet and replies coming

back from the internet. This monitoring must be done on the *internal* side of the corporate firewall.

Warning

- Do NOT install Network Agent on a machine running a firewall or Remote Filtering Server. Network Agent's packet capturing may not work properly if installed on a firewall machine.

Network Agent only monitors and manages traffic passing through the network device (switch, hub, or gateway) to which it is attached. Network Agent works with various network configurations, as discussed later.

The machine running a Network Agent can access the network via a switch or a hub, as discussed in *Hub Configuration*, page 144 and *Switched Configuration*, page 145.

Network Agent can be installed on the same machine as an integration product, as discussed in *Gateway Configuration*, page 150.

Multiple Network Agents may be needed, depending on the size, volume of internet requests and the network configuration.

Network Agent Settings

Network Agent settings are configured in Websense Manager. Global settings must be specified (for all Network Agents, if there is more than 1), and local settings for each particular Network Agent.

The *Global* and *Local* configurations are used to inform Network Agent which machines to monitor for traffic and which to ignore.

- *Global Settings*—apply to all Network Agents connected to the Policy Server. Global Settings determine what every Network Agent is to do with requests from machines in the network.

  Global Settings define a network by providing a list of IP addresses or IP address ranges in the network that the Network Agents need to monitor.
- *Local Settings*—apply to individual Network Agents. Local Settings identify the Filtering Service to which a Network Agent communicates, and how to handle traffic if Network Agent and Filtering Service cannot connect.

Local Settings determine how each particular Network Agent treats machines in the internal network. By default, Network Agent monitors requests from all internal machines and external hosts that it sees. Websense software filters internet content requested from these machines. Local Settings configure how much of the internal network each Network Agent sees. Then, exceptions can be specified to the default monitoring behavior. Network Agent's behavior can be customized for machines using multiple Network Interface Cards (NICs).

Network Agent Location

Network Agent must be able to see all internet traffic in both directions on the network segment that it is assigned to monitor. Multiple instances of Network Agent may be needed to monitor an entire network.

For example, it can be useful to have multiple Network Agents for larger or high-traffic organizations. In this situation, Network Agents can be placed on each internal network segment.

Some common scenarios for Network Agent installation include:

- On a dedicated machine, connected to an unmanaged, unswitched hub located between an external router and the network.
- Connected to a switch or router. Configure a switch or router to use mirroring or 2-way port spanning, so that Network Agent can detect internet requests from all the workstations.
- To monitor and filter internal traffic, such as instant messaging attachments, the Global settings must be configured to allow Network Agent to see the internal traffic. For more information, see the Network Agent chapter in the *Websense Enterprise Administrator's Guide*.

When using a switch, plug the Network Agent machine into the port on the switch that mirrors, monitors, or spans the traffic of the gateway port. The span port mirrors all the traffic that leaves the network segment to which the switch is attached.

> **Note**
>
> Not all switches support port spanning or mirroring. Contact the switch vendor to determine if the switch is capable of mirroring or port spanning, and to learn how to implement the correct configuration

The machine running Network Agent can use multiple network interface cards (NICs) to connect to multiple ports on the switch or router. See *Using Multiple NICs*, page 151 for information.

The following diagrams illustrate different methods in which Network Agent can interface with the network. Multiple Network Agents may be required under some configuration scenarios.

Single Segment Network

A single segment network is a series of logically connected nodes operating in the same portion of the network. These nodes can be PCs, printers, other networked devices. In a single segment network, Filtering Service and Network Agent must be installed where they can monitor internet traffic across the entire network. Figure 17, page 139 shows the Stand-Alone Edition installed in a central location to see both HTTP and non-HTTP protocol traffic.

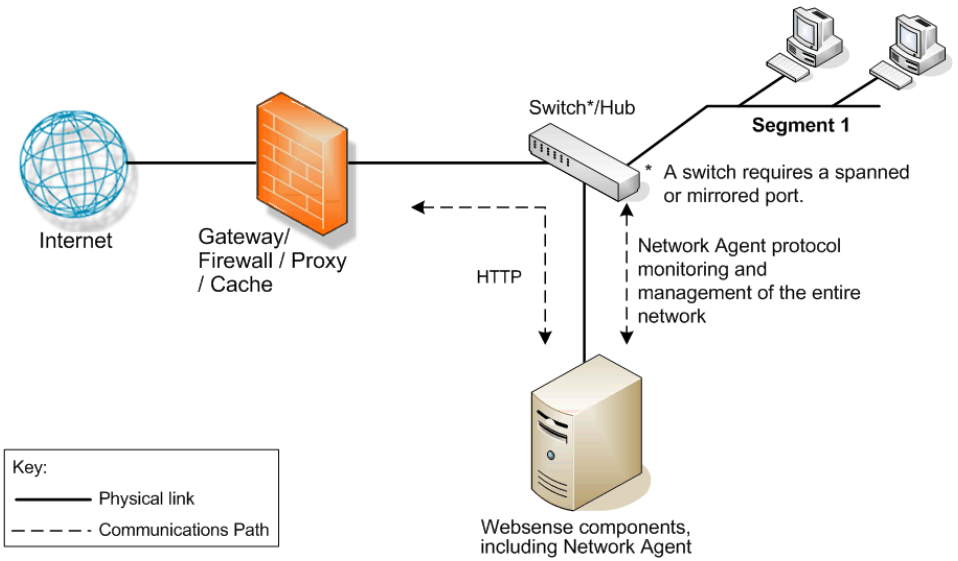

Figure 17 Websense Software in a Single Segment Network

To learn more about installing Network Agent in a network with a hub, see *Hub Configuration*, page 144. To learn more on installing Network Agent in a network with a switch, see *Switched Configuration*, page 145. To learn more about installing Network Agent in a network with a gateway, see *Gateway Configuration*, page 150.

Multiple Segment Network

Depending on the device connecting multiple 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 components must be deployed to allow the product to see all network traffic.

In a multiple segment network, Filtering Service must be installed in a location where it can receive and manage internet requests from the integration product, if any, and communicate with Network Agent. Each Network Agent must be able to see all internet requests on the segment or segments that it is designated to monitor.

Deploying Multiple Network Agents

Multiple Network Agents 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, although more agents may be allowed, depending on system and network configuration and the volume of internet requests.

If multiple Network Agents are installed:

- Deploy the Network Agents so that they can filter the entire network. Partial deployment results in incomplete filtering by protocol and bandwidth, and incomplete basic HTTP filtering (in Stand-Alone Edition), as well as the loss of log data from network segments not watched by the Network Agent.
- IP address ranges must not overlap between Network Agents. Overlapping IP ranges result in inaccurate logging and network bandwidth measurements, and improper bandwidth-based filtering.

  For example, if the network's IP range is 111.222.254.0 to 111.222.254.20, one Network Agent can cover 111.222.254.0 to 111.222.254.10 and the second Network Agent can cover 111.222.254.11 to 111.222.254.20.

  The IP address ranges for each Network Agent is entered in the Settings dialog box that is accessed through Websense Manager. For more information on configuring Network Agent, see the *Network Agent* chapter in the *Websense Enterprise Administrator's Guide*.
- Avoid deploying Network Agent across different LANs. If you install Network Agent on 111.x.x.x and configure it to communicate with a Filtering Service on 10.x.x.x through a variety of switches and routers, communication may be slow enough to prevent the Network Agent from blocking an internet request in time.

Examples are provided on the following pages for central and distributed Network Agent placement.

To learn more about installing Network Agent in a network with a hub, see *Hub Configuration*, page 144.

To learn more on installing Network Agent in a network with a switch, see *Switched Configuration*, page 145.

To learn more about installing Network Agent in a network with a gateway, see *Gateway Configuration*, page 150.

Central Network Agent Placement

A multiple segment network can be monitored from a single location. Filtering Service is installed where it can receive internet requests from both the integration product, if any, and each Network Agent.

In Figure 18, page 142, the first Network Agent is installed with Filtering Service on Machine A. This machine is connected to the network with a switch that is configured to mirror or span the traffic of network Segment 1.

A second Network Agent is installed on Machine B. This machine 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 of the network.

Both Network Agents are connected to the network in a location that is as far up the network chain as needed to see their respective segments' traffic and also communicate with other Websense components.

If the network contains multiple switches, the Network Agents 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 18, the switch is connected to the gateway. This location allows the Network Agents to monitor network traffic for all the network segments.

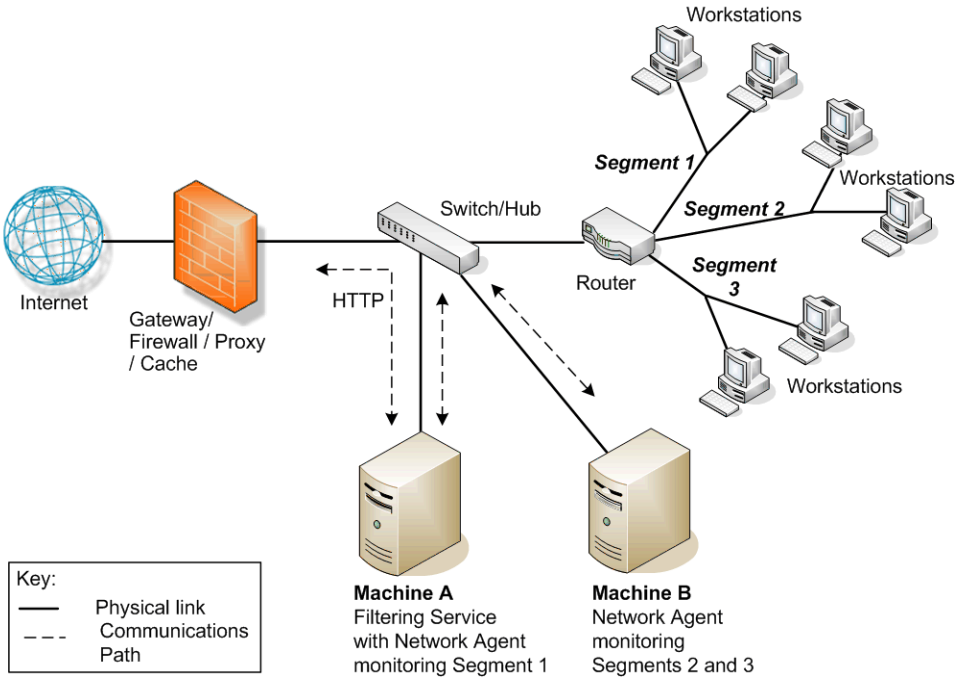

Figure 18 Websense Software in a Multi-Segment Network

Distributed Network Agent Placement

The network in Figure 19, page 143 contains a single Filtering Service with 3 Network Agents, 1 for each segment of the network. This deployment helps networks with satellite offices, for example.

Filtering Service (Machine C) must be installed in a location where it is able to receive and manage internet requests from both the integration product and each of the Network Agents (machines A and B), which are deployed on separate network segments. Machine C also has Network Agent installed.

Each Network Agent (machines A, B and C) is connected to the network segment using a switch. Each Network Agent machine is connected to a port on the switch that is configured to span or mirror all traffic passing through that switch.

See *Deploying Multiple Network Agents*, page 140 for more information on deploying multiple Network Agents.

In Figure 19, the switches are not connected in a series. However, each switch is connected to the router, which is connected to the gateway. Each Network Agent monitors all internet requests for its respective segment.

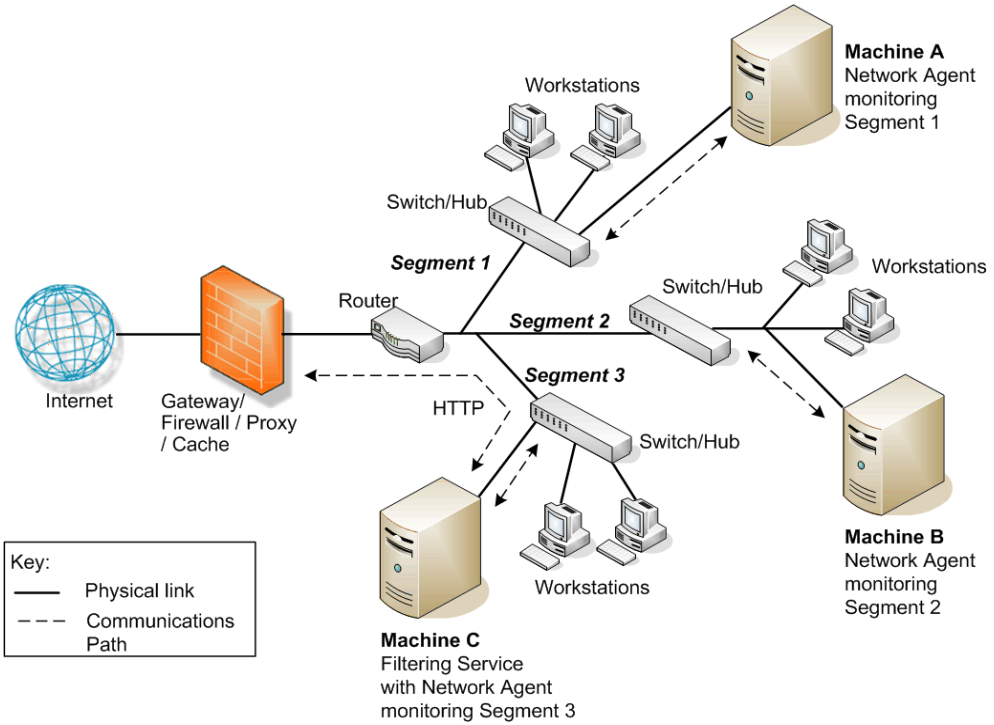

Figure 19 Multiple Network Agents in a Multi-Segmented Network

Hub Configuration

At the simplest level, a network hub provides a central connection point for the network segments and the devices on those segments. The port to which the Network Agent machine is attached to the hub is dependent on the type of hub. Some hubs broadcast traffic to all of their ports, while some smart hubs may not allow all ports to see all traffic. Network Agent must be able to see the traffic for the segments it is assigned to monitor.

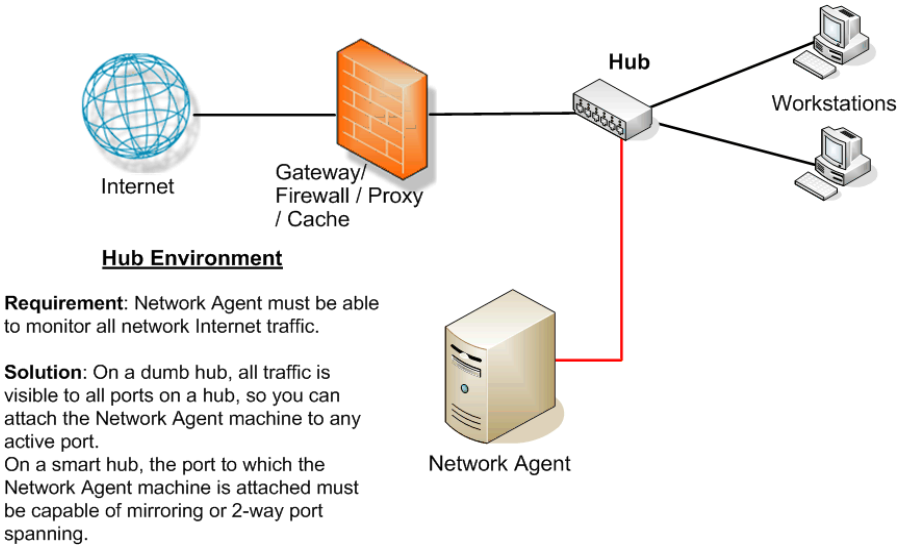

Figure 20 Network Agent Configured Through a Hub

Switched Configuration

A switch is a bridge that routes traffic between network segments. This control prevents all traffic from going to all segments, thus reducing congestion on the network. Since not all the 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.

To connect to the network using a switch, plug the Network Agent machine into the port on the switch that mirrors, monitors, or spans the traffic on the gateway or firewall port. The span port mirrors all the traffic that leaves the network segment.

Note

Not all switches support port spanning or 2-way port mirroring. Contact the switch vendor to determine if the switch is capable of supporting these functions and to learn how to implement the correct configuration. If these functions are not enabled or available, Network Agent is not able to properly monitor the network, resulting in blank or inaccurate reports, and possibly faulty protocol management and bandwidth optimization.

Figure 21, page 146 shows a network with a single switch. The machine running Network Agent is attached to the port from which it can see all traffic from the adjoining workstations. The subsequent illustrations provide scenarios with multiple switches and subnetworks.

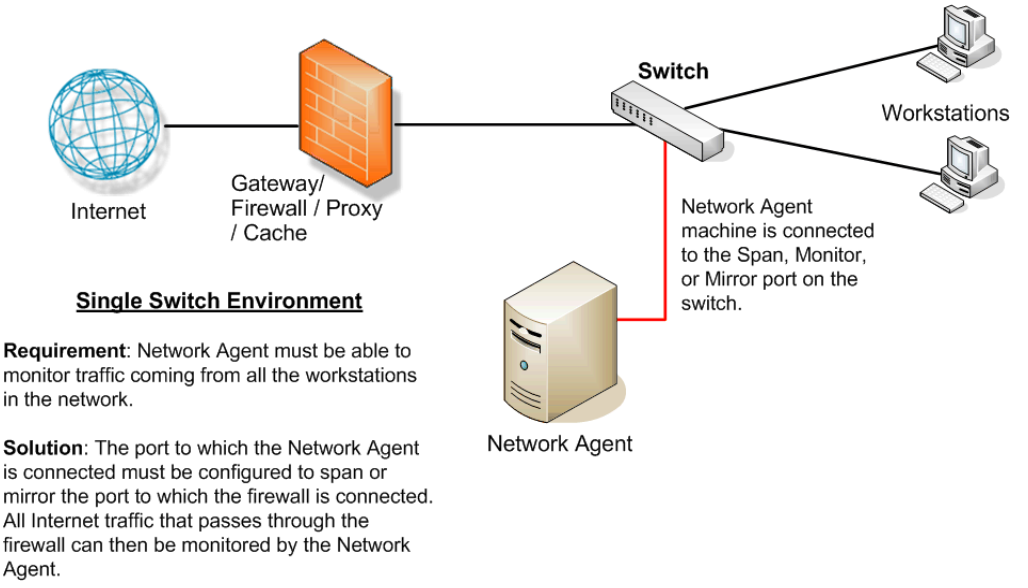

Figure 21 Simple Deployment in a Switched Environment

Figure 22, page 147 shows the addition of 2 more switches, Switch #1 and Switch #2, 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 because Network Agent is unable to see the network traffic.

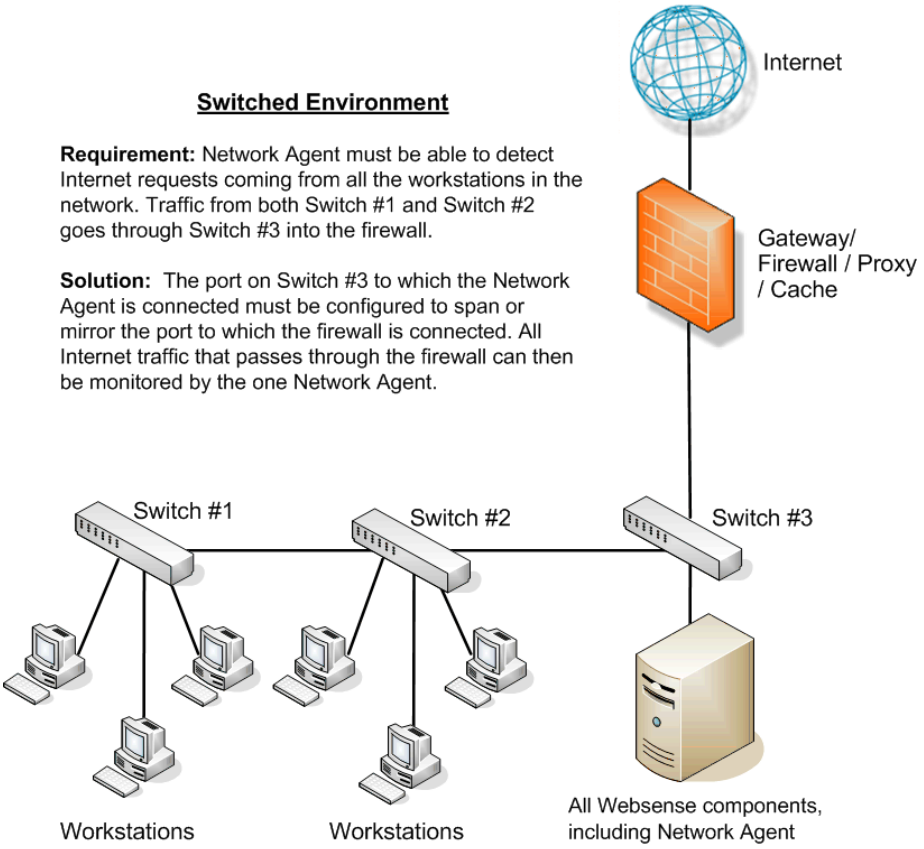

Figure 22 Multiple Subnets in a Switched Environment

Like Figure 22, Figure 23, page 148 contains multiple network segments. This network adds a router for communications from a remote office. The machine running Network Agent is connected to an additional switch.

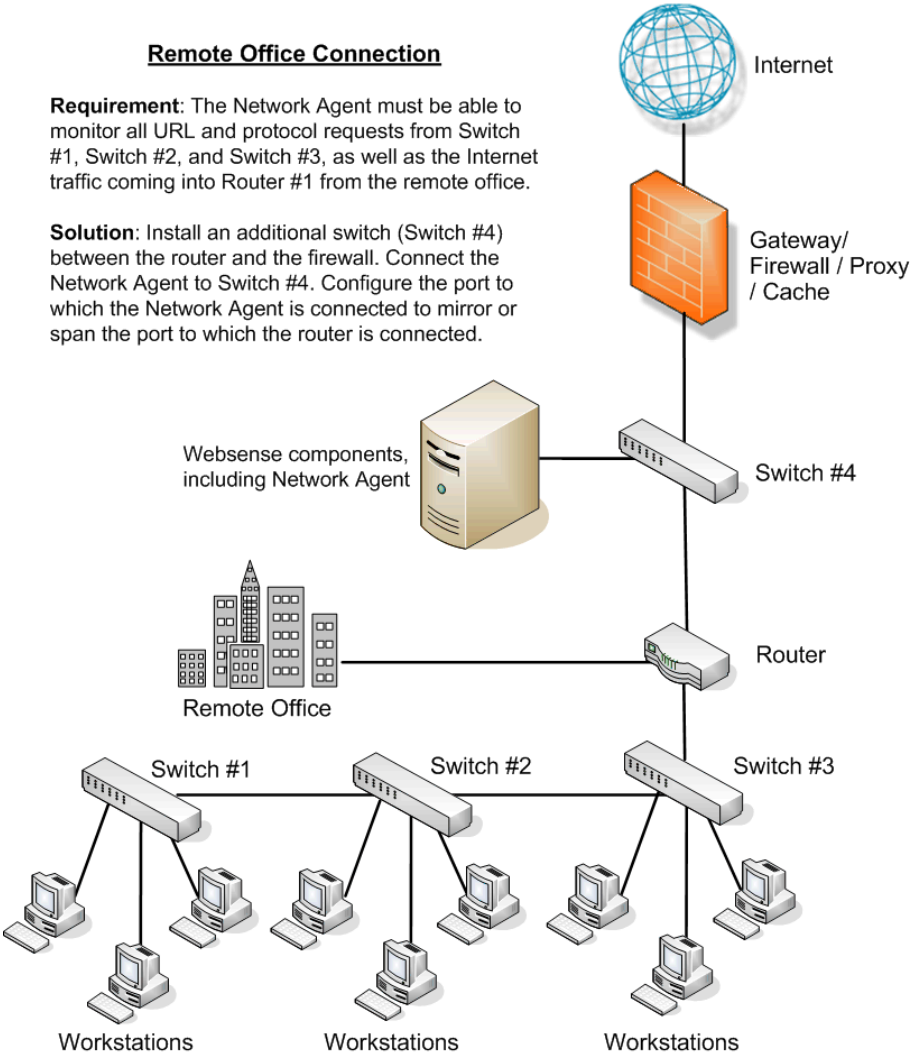

Figure 23 Switched Environment with a Remote Office Connection

Switched Networks with Multiple Network Agents

On a busy network, multiple Network Agents may be needed to monitor different IP address ranges in the network. Figure 24, page 149 illustrates a network in which individual Network Agents monitor their network segments.

See *Deploying Multiple Network Agents*, page 140 for more information on deploying multiple Network Agents.

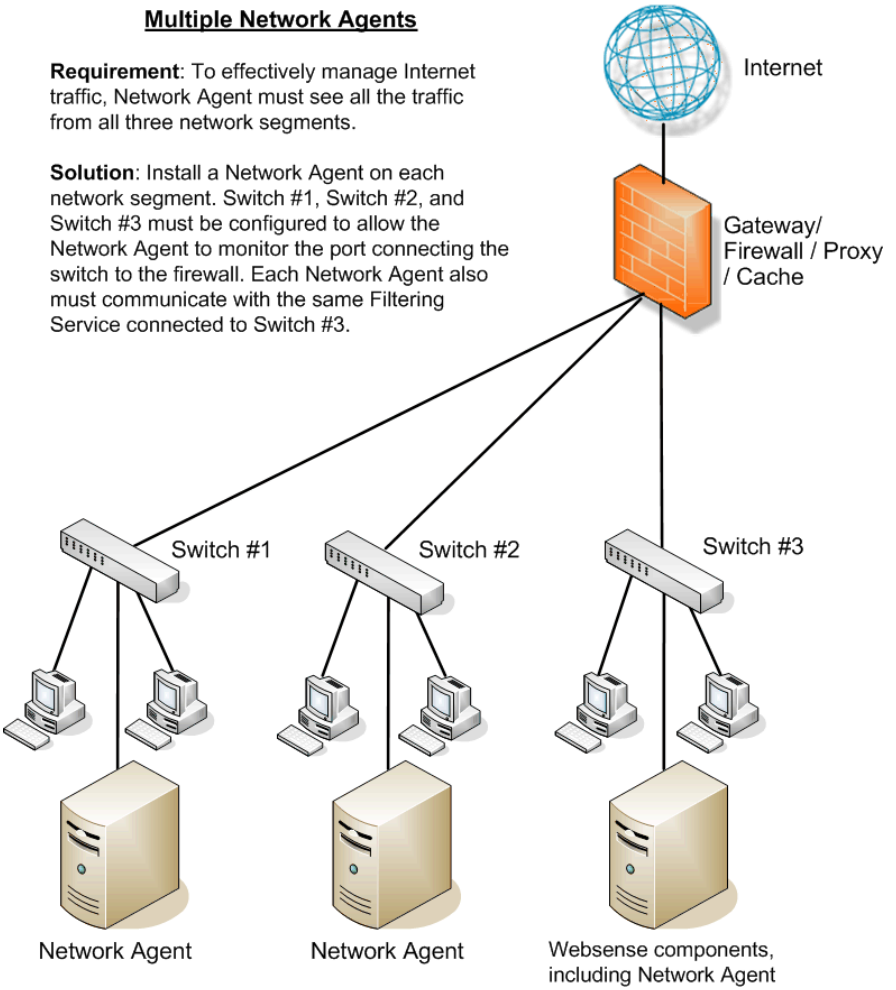

Figure 24 Multiple Network Agents in a Switched Environment

Gateway Configuration

A gateway provides a connection between 2 networks, with either the same or different network protocols. The gateway can provide the connection between the network and the internet.

Network Agent can be installed on the gateway machine, which allows Network Agent to manage and monitor all internet traffic. This gateway can either be a proxy server or a network appliance. *Do not* install Network Agent on a firewall.

IMPORTANT

This configuration 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 software

Figure 25 shows Network Agent monitoring the internet traffic at the proxy gateway or caching appliance directly attached to the firewall.

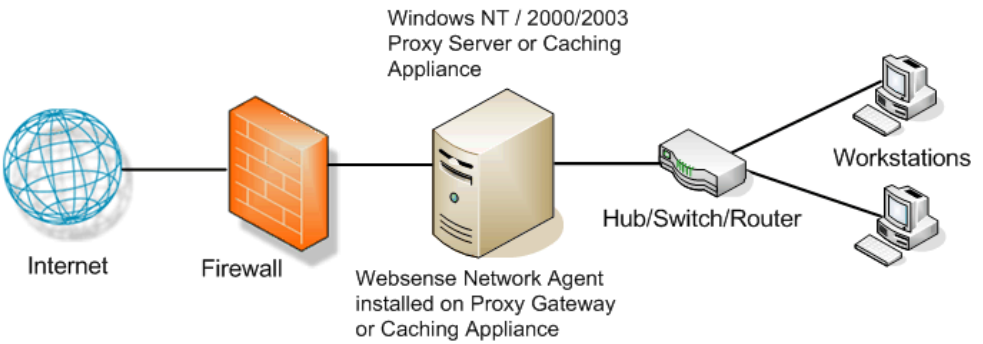

Figure 25 Network Agent Installed on the Gateway

Using Multiple NICs

Network Agent is capable of working with multiple network interface cards (NICs) installed in the same machine on which Network Agent is running. A practical limit of 5 NICs is recommended. The NICs can be connected to ports on the same network device (such as a switch or a router), or can be connected to different network devices.

If the machine running Network Agent has multiple NICs installed:

- Only 1 instance of Network Agent can be installed on the machine running with multiple NICs.
- The blocking (inject) NIC must have an IP address.
- A NIC can be designated to either monitor or block internet requests, or do both.
- The NICs can also be used to monitor different segments of the network.
- At least 1 NIC must be assigned for blocking.
- Separate NICs can be assigned to monitor and to block.
  - The NICs do not have to be assigned to the same network segment if separate NICs are used for monitoring and blocking.
  - A monitoring NIC must be able to see all internet traffic on the network segment that it is assigned to watch.
  - Multiple monitoring NICs can use the same blocking NIC.

    That blocking NIC needs to be able to send the block messages back to all machines assigned to these monitoring NICs, even if the machines are on a different segment.
  - A monitoring NIC can be set for *stealth mode* (no IP address). It must use a blocking NIC that is assigned an IP address for communication. For information on configuring the stealth mode, see the *Websense Enterprise Installation Guide*.
  - A blocking NIC, or a NIC configured to monitor and block, cannot be set to stealth mode.

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

For information on configuring multiple NICs, see the *Websense Enterprise Administration Guide*.

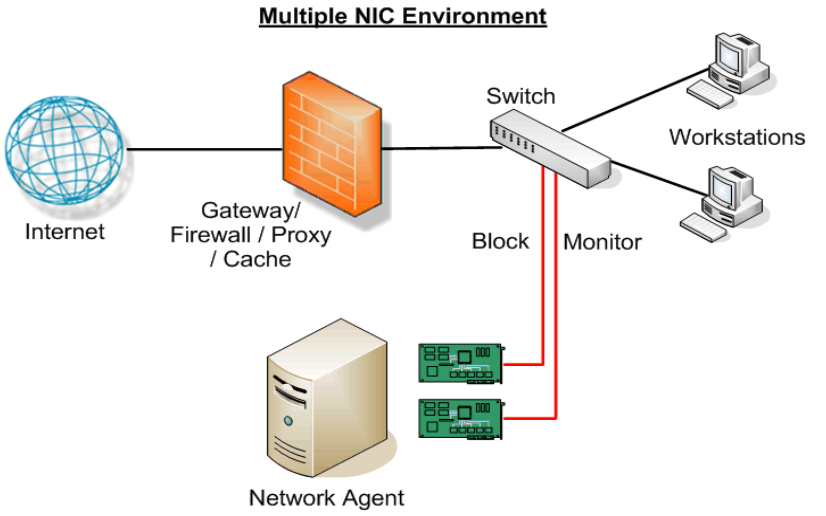

Figure 26 Dual NIC Configuration

NAT and Network Agent Deployment

Using Network Address Translation (NAT) on internal routers can prevent Network Agent from identifying the source IP addresses of client machines making internet requests.

If you deploy Network Agent to monitor traffic from multiple subnets *after* it passes through such a router, you must disable NAT. If NAT is not disabled, Network Agent sees the IP address of the router's external interface as the source of the request.

As an alternative, you can install Network Agent on a machine located *between* the NAT router and the clients to be monitored.

E

F

G

H

M

N

R

S

T

U