WEBSENSE.
Enterprise

v5.5

Websense Enterprise®
Deployment Guide

Websense Enterprise® Deployment Guide

Contents

List of Figures

List of Tables

CHAPTER 1 | Introduction

Thank you for choosing Websense Enterprise® v5.5, the leading Employee Internet Management system. Using Websense provides you with a highly effective Internet filtering service.

The *Websense Enterprise v5.5 Deployment Guide* provides an overview of how Websense Enterprise should be deployed on your network, plus operating system and hardware requirements. The information in this document is especially useful for planning your deployment before installing the product.

Websense Enterprise consists of a series of components that work together to monitor Internet requests, log activity, and apply filters as needed. The configuration of the machines on which the components are installed is dependent on the network size, amount of Internet requests, and the capability of those machines.

This chapter provides a brief introduction to the Websense Enterprise components.

The remaining chapters in this document include:

◆ *Chapter 2, General Deployment Recommendations*—provides an introduction to deployment, the network sizes and considerations, operating system recommendations for each component, hardware recommendations, and tips for maximizing your system performance.

◆ *Chapter 3, Network Configuration*—discusses deployment across single and multiple segment networks.

◆ *Chapter 4, Configuring Network Agent*—discusses where Network Agent should be located, settings, and configurations in relation to hubs, switches and gateways.

◆ *Chapter 5, Implementing Websense Enterprise within Distributed Enterprises*—discusses the deployment of Websense Enterprise over a distributed enterprise network with remote offices.

◆ *Appendix A, Minimum System Requirements for Websense Enterprise Components*— provides the minimum requirements to run each Websense component.

Websense Enterprise Components

Table 1 provides a brief description of the Websense Enterprise components that are discussed in this guide. Table 2, on page 13, provides a brief description of the Websense Enterprise Reporting components that are discussed in this guide. Reviewing these component descriptions helps to clarify the interaction of the components, which are discussed in the ensuing chapters.

Table 1 Websense Enterprise Components

Component	Definition
DC Agent[1]	An optional component that polls the workstations to transparently identify users so Websense Enterprise can filter them according to particular policies assigned to users or groups. The DC Agent should not reside in a particular domain. The DC Agent also should not be installed on a domain controller.
eDirectory Agent [1, 2]	An optional component that works with a Novell eDirectory server to transparently identify users so Websense Enterprise can filter them according to particular policies assigned to users or groups.
Filtering Service (formerly EIM Server)	Receives Internet requests, determines the appropriate filtering policy, and either permits the request or sends the appropriate block message.
Logon Agent[1]	Detects users as they log on to Windows domains in your network. The Logon Agent works together with the Websense User Service, and can run on Windows, Linux or Solaris. Logon Agent can also be used with a Windows- *or* LDAP-based directory service. A client-based logon application informs the Logon Agent when a user logs on. The logon application only runs on Windows-based client machines.
Network Agent	Detects network activity to support the Bandwidth Optimizer, Protocol Management, IM attachments, and reporting on bytes transferred and duration of a session.
	In the Stand-Alone edition, Network Agent also provides all HTTP and HTTPS filtering.
Policy Server	Stores Websense Enterprise configuration information and communicates this data to the other Websense Enterprise components. Policy Server also logs event messages for Websense components, regardless of where they are located.
RADIUS Agent[1, 3]	An optional component enables Websense Enterprise to transparently identify users who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection (depending on your configuration). RADIUS Agent can be used in conjunction with Windows-based or LDAP-based directory services. Websense Enterprise then can filter the users according to particular policies assigned to users or groups.
User Service[4]	Communicates with your environment's Directory Service to enable you 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 Directory Service, Windows Active Directory (via LDAP,) Sun Java System Directory Server (via LDAP), SunONE Directory Service (via LDAP) or Novell eDirectory (via LDAP).

Table 1 Websense Enterprise Components

Component	Definition
Websense Enterprise Manager	Administrative interface that communicates with Policy Server to configure and manage the Websense Enterprise functionality.
Websense Enterprise Real-Time Analyzer (RTA)[5]	Displays the real-time status of the traffic filtered by Websense Enterprise. RTA graphically displays bandwidth information and shows requests by category or protocol. • Web server—either Apache or Microsoft IIS (Apache is included in the installation package).
Websense Master Database	A downloadable collection of over 5 million Internet sites, representing over 800 million pages, each categorized by content. Protocols are also contained in this database.

1. Websense, Inc. supports certain combinations of transparent identification agents within the same network, or on the same machine. Generally, it is recommended to run one agent of a particular type on one machine. See *Deploying Transparent Identification Agents*, page 21 for more information.

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.) Refer to the *Transparent Identification of Users in Websense Enterprise* technical white paper for more information. This white paper can found on the Websense Product Documentation site—http://www.websense.com/support/documentation.

4. Only one User Service installation is allowed for each Policy Server that is installed in your system.

5. Only one RTA installation is allowed for each Policy Server that is installed in your system.

Websense Enterprise Reporting Components

All reporting modules and their components rely on Websense Enterprise. The reporting components are always installed after Websense Enterprise. For this release, Reporting components all run on Windows.

For more information on how Websense Enterprise Reporter and Websense Enterprise work together, refer to the *Websense Enterprise Reporter Administration Guide*.

For more information on how Websense Enterprise Explorer and Websense Enterprise work together, refer to the *Websense Enterprise Explorer Administration Guide*.

For more information on installing Websense Enterprise Reporter and Websense Enterprise Explorer, refer to the *Websense Enterprise Reporter Installation Guide*.

Table 2 Websense Enterprise Reporting Components

Component	Definition
Required Reporting components	Log Server, Log Database and the Database Engine are required to run Websense Enterprise Reporter, Websense Enterprise Explorer and the Log Database Manager.
Database Engine	Required that you obtain and install 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.

Table 2 Websense Enterprise Reporting Components

Component	Definition
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 Websense Enterprise Reporter and Websense Enterprise Explorer to create reports.
Log Server	Records and stores Internet activity on your network in the Log Database. Only one Log Server can be installed for each Log Database that is installed.
Log Database Manager	Web-based application that assists in managing the size of the Log Database, utilizing purge and archive functions. Log Database Manager only uses the database that is currently connected to the Log Server and must run on the same machine as the Log Server.
Reporter	Client-based application that creates a variety of reports that can be generated automatically, sent via email or printed
Websense Enterprise Explorer	A Web-based application that generates a variety of easy-to-understand summary reports from data stored in the Log Database as well as archived data. Explorer utilizes a: • Web server—either Apache or Microsoft IIS (Apache is included in the installation package). • Web browser—Microsoft Internet Explorer (not included in installation).

General Deployment Recommendations

Websense Enterprise can be deployed in different configurations, depending on the size and characteristics of the network, as well as your filtering needs. Websense Enterprise components can be installed together on one machine, or distributed across multiple machines, depending on the operating systems and the size of the network.

See Table 1 and Table 2 in Chapter 1 for a list and definitions of Websense Enterprise components.

This chapter describes four network sizes and includes system and deployment recommendations. The deployment recommendations are divided into the following network size ranges:

◆ Small (1–500 users)

◆ Medium (500–2,500 users)

◆ Large (2,500–10,000 users)

◆ Enterprise (10,000 + users)

These ranges are intended as general guidelines only. For networks that are larger or experience high volumes of Internet activity, a different deployment design might be necessary than is suggested for a given range of users to provide the necessary processing power to monitor the Internet requests. The location of some components is also limited to certain operating systems.

Depending on the size and configuration of your network, you may need to install multiple instances of certain components, such as Network Agent, the Websense Enterprise Reporter client application, Websense Enterprise Manager, the Transparent ID Agents, or Filtering Service.

The recommendations in this manual exceed the minimum requirements to allow you to optimize component performance. Performance may also be improved if you use more powerful machines for the more process intensive components, such as the Log Server and database engine (Microsoft SQL, MSDE, MySQL).

NOTE

The recommendations in this chapter allow for some network growth and an increasing number of Internet requests. As your network reaches the upper limits for a particular network size, you should revisit these recommendations to ensure your system is configured to optimize each component's performance.

Operating System Requirements

The tables in this section provide operating system requirements for the Websense Enterprise components.

Depending on the size of the network, the component and the deployment of Websense Enterprise, the components may be installed together on the same machine or installed on separate machines. Network Agent, Websense Enterprise Manager, DC Agent, eDirectory Agent, RADIUS Agent, and the Reporter client application can be installed on separate machines using their own installation programs. These installation programs are downloadable from the Websense Web site.

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

The following table lists each component and its recommended operating systems.

Table 3 Components and Required Operating Systems

Component	Operating System Requirements
DC Agent	• Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
eDirectory Agent[1]	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8 - v9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 SP1 or higher (Standard or Enterprise)
Filtering Service	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8 - v9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
Log Database	• The Log Database is dependant upon the database engine, MSDE or Microsoft SQL, and not the operating system. • If you are running Websense Enterprise Explorer for Unix, the Log Database runs on MySQL, and is dependant on the database engine, not the operating system.
Log Database Manager	• Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
Log Server	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris 8 - 9[2] • Windows 2000 Server SP3 or higher, or Advanced Server SP1 • Windows Server 2003 (Standard or Enterprise)

Table 3 Components and Required Operating Systems

Component	Operating System Requirements
Logon Agent	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris 8 - 9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
Network Agent	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris 8 - 9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
Policy Server	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8- v9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
RADIUS Agent[3]	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8 - v9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 SP1 or higher (Standard or Enterprise)
Real-Time Analyzer[4]	• Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
User Service[5]	• Red Hat Linux v9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8 -v 9[2] • Windows 2000 Server SP3 or higher • Windows Server 2003 (Standard or Enterprise)
Websense Enterprise Explorer[4] (Web server)	• Red Hat Linux 9 • Red Hat Enterprise Linux AS, ES and WS v3.0 • Solaris v8 - v9 • Windows 2000 Server SP3 • Windows 2003 Server (Web, Enterprise or Standard)
Websense Enterprise Manager	• Solaris v8 - v9[2] • Windows NT 4.0 SP 6a (Workstation or Server) • Windows 2000 SP3 or higher (Professional or Server) • Windows Server 2003 (Standard or Enterprise)
Websense Enterprise Reporter client application	• Windows 2000 SP3 or higher (Professional or Server) • Windows Server 2003 (Standard or Enterprise)

1. Requires Novell eDirectory 8.5 and later. NMAS authentication is supported.

2. Be sure to install the most current Solaris patch cluster before running the Websense Enterprise installer. Refer to the Sun Web site, http://www.sun.com, to download the latest patch cluster.

3. RADIUS Servers - most standard RADIUS servers are supported, including the following, which have been tested: Livingston (Lucent) 2.x, Cistron RADIUS server, Merit AAA, Microsoft IAS.

4. Real-Time Analyzer and Explorer also require Microsoft IIS v4.0 or 5.0 or Apache Web Server version 2.x or later. IIS is available from Microsoft. Apache software can be downloaded free from Apache, http://www.apache.org/.

5. Although User Service runs in the Linux and Solaris environments, it cannot use Windows directory services, (i.e., Windows NT Directory Service or Active Directory) from those platforms.

The following table lists the operating systems on which the Websense Enterprise components run.

Table 4 Operating Systems

Operating System	Component
Windows environment	
Windows 2000 Server, SP3 or higher (SP3 for Websense Enterprise Explorer) or Windows 2000 Advanced Server or Windows Server 2003 Standard and Enterprise Editions	All Websense Enterprise components: • Database Engine • DC Agent • eDirectory Agent • Filtering Service • Log Database Manager • Log Server • Logon Agent • Network Agent • Policy Server • RADIUS Agent • Real-Time Analyzer • User Service • Websense Enterprise Explorer • Websense Enterprise Manager • Websense Enterprise Reporter client application
Windows NT Server or Workstation, 4.0 SP 6a or Windows 98	• Websense Enterprise Manager • Websense Enterprise Reporter client application
Windows 2000 Professional, SP3 or higher	• Websense Enterprise Manager • Websense Enterprise Reporter client application
Windows XP Professional	• Websense Enterprise Manager • Websense Enterprise Reporter client application
Windows ME	• Websense Enterprise Manager

Table 4 Operating Systems

Operating System	Component
Linux environment	
Red Hat Linux 9 Red Hat Enterprise Linux AS (Advanced Server) v3.0 Red Hat Enterprise Linux ES (Enterprise Server) v3.0 Red Hat Enterprise WS (Workstation) v3.0	• eDirectory Agent • Filtering Service • Log Server • Logon Agent • Network Agent • Policy Server • RADIUS Agent • User Service[1] • Websense Enterprise Explorer for Unix
Solaris environment	
Solaris v8 - v9[2]	• eDirectory Agent • Filtering Service • Log Server • Logon Agent • Network Agent • Policy Server • RADIUS Agent • User Service[2] • Websense Enterprise Explorer for Unix

1. Although User Service runs in the Linux and Solaris environments, it cannot use Windows directory services, (i.e., Windows NT Directory Service, Active Directory) from those platforms.

2. Be sure to install the most current Solaris patch cluster before running the Websense Enterprise installer. Refer to the Sun website, http://www.sun.com, to download the latest patch cluster.

See the appropriate *Websense Enterprise Installation Guide* for integration specific operating system and CPU requirements.

The following sections provide hardware recommendations for deploying Websense Enterprise v5.5 in the supported network systems, within the listed network ranges.

Policy Server Limits

When deploying Websense Enterprise, certain installation dependencies must be considered:

◆ *One* User Service per Policy Server.

◆ *One* Real-Time Analyzer (RTA) per Policy Server.

◆ Up to *10* (ten) Filtering Services per Policy Server.

For more information on the interaction of Websense components, refer to the *Websense Enterprise v5.5 Installation Guide* for your integration and *Websense Enterprise v5.5 Administrator's Guide*.

The remainder of this section provides instructions for determining the number of Filtering Services needed for each Policy Server.

Number of Filtering Services allowed per Policy Server

You can have up to ten Websense Enterprise Filtering Services per Policy Server, if a quality network connection is established between the components. A quality connection is defined as one that provides a ping response of no greater than *30 milliseconds* (*ms*) between machines. See the *Testing the connection* section below.

Remote Filtering Service machines (those at a great physical distance communicating through a series of *jumps*) or those behind firewalls, may need their own Policy Servers. If additional Policy Servers must be deployed, you can use the *Central Policy Distribution* feature to push your policies out to the remote Policy Server machines. See the *Websense Enterprise v5.5 Administrator's Guide* for more information on Central Policy Distribution.

Testing the connection

Run a ping test to verify the response time and connection between the machines running Policy Server and Filtering Service. The response time must be no more than 30 ms.

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.

For interpreting the results, see the following information.

Linux or Solaris results

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

```
[root@localhost root]# ping 11.22.33.444
PING 11.22.33.444 (11.22.33.444) 56(84) bytes of data.
64 bytes from 11.22.33.444: icmp_seq=2 ttl=127 time=0.417 ms
64 bytes from 11.22.33.444: icmp_seq=3 ttl=127 time=0.465 ms
64 bytes from 11.22.33.444: icmp_seq=4 ttl=127 time=0.447 ms
64 bytes from 11.22.33.444: icmp_seq=1 ttl=127 time=0.854 ms
```

Ensure that `time=`*x.xx* `ms` is less than 30 ms.

If the time is greater than 30 ms, then one of the components must be installed on a machine at a different location on the network.

Windows results

In Windows, the results are similar to these:

```
C:\>ping 11.22.33.444
Pinging 11.22.33.444 with 32 bytes of data:
Reply from 11.22.33.444: bytes=32 time=14ms TTL=63
Reply from 11.22.33.444: bytes=32 time=15ms TTL=63
Reply from 11.22.33.444: bytes=32 time=14ms TTL=63
Reply from 11.22.33.444: bytes=32 time=15ms TTL=63
Ping statistics for 11.22.33.444:
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 less than 30 ms. If the time is greater than 30 ms, then one of the components must be installed on a machine at a different location on the network.

Deploying Transparent Identification Agents

The Websense transparent identification feature allows Websense to filter Internet requests from users in your directory service, without prompting users to manually authenticate.

Websense currently provides four optional components for identifying users transparently in various environments.

◆ DC Agent
◆ eDirectory Agent
◆ Logon Agent*
◆ RADIUS Agent

*The Logon Agent pushes out a logon application to Windows-based clients.

When using one of these agents, Websense, Inc. recommends only one instance of an agent should be installed on your network. In deployments that cover multiple locations or remote offices, more than one instance of an agent may be needed.

> **NOTE**
>
> The DC Agent should not be installed on a domain controller.

For example:

◆ DC Agent—one instance can handle multiple domains. The need for additional DC Agent installations is dependant 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 is related to the amount Internet requests generated by users on the network. If your network is large (10,000+ users), you may benefit from installing DC Agent on multiple machines. This installation provides ample space for DC Agent files that are continually populated with user information.
◆ eDirectory Agent—one instance per each Directory.
◆ Logon Agent—one instance for each Filtering Service that is installed.
◆ RADIUS Agent—one instance for each RADIUS server.

Websense, Inc. supports certain combinations of transparent identification agents within the same network, or on the same machine. See *Combining Transparent Identification Agents*.

For more information on transparent identification agents, see the *Transparent Identification of Users in Websense Enterprise v5.5* white paper. See the *Websense Enterprise v5.5 Administrator's Guide* for more information on configuring these agents, or installing multiple types of agents. For installation instructions for the transparent identification agents, refer to your *Websense Enterprise v5.5 Installation Guide*.

These documents can be found on the Websense Product Documentation site—
http://www.websense.com/support/documentation

Combining Transparent Identification Agents

Websense, Inc. supports certain combinations of the agent components within the same network, or on the same machine. Generally, it is recommended to run one agent of a particular type on one machine. If your network configuration requires multiple agents, it is best to install them on separate machines. However, you can configure Websense to work with multiple agents on a single machine in some cases.

Supported combinations for Websense Enterprise v5.5 are listed in Table 5, on page 22.

Table 5 Transparent Agent Combinations

Combination	Same machine?	Same network?	Configuration required
Multiple DC Agents	No	Yes	Ensure that all instances of DC Agent can communicate with Filtering Service.
Multiple RADIUS Agents	No	Yes	Configure both agents 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, you can have both Agents installed, with only one active Agent.)
DC Agent + Logon Agent	Yes	Yes	Configure both agents to communicate with Filtering Service. By default, each agent uses a unique port, so port conflicts are not an issue unless these ports are changed.
RADIUS Agent + Logon Agent	Yes	Yes	Configure all agents to communicate with Filtering Service. See Websense Knowledge Base article #1115.
eDirectory Agent + Logon Agent	No	No	Websense does not support communication with both Windows and Novell directory services in the same deployment. However, you can have both agents installed, with only one active agent.

Table 5 Transparent Agent Combinations

Combination	Same machine?	Same network?	Configuration required
RADIUS Agent + eDirectory Agent	Yes	Yes	Configure both agents to communicate with Filtering Service. When adding Agents to Websense Enterprise Manager, use an IP address to identify one, and a machine name to identify the other. See the *Transparent Identification of Users in Websense Enterprise v5.5* 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.

Small Networks: 1–500 Users

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

The deployment recommendations cover each of these operating systems to start using Websense Enterprise. You may need additional machines to run certain components as the network grows and Internet requests increase. On average, a small network has one to 100 requests per second. More powerful machines may be needed in a higher traffic, small network.

Websense Enterprise 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 will be filtered by Websense Enterprise.

Network Considerations

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

◆ Filtering Service can receive Internet requests from the gateway or integration device (if any) or Network Agent.

◆ Network Agent must have bi-directional visibility of Internet traffic that uses protocols that are not Web-based, such as instant messaging, chat, streaming media, peer-to-peer file sharing, file transfer (such as FTP), mail, and others. *Appendix A* of the *Websense Enterprise Administrator's Guide* lists these protocols.

◆ Network Agent must be deployed in the network at a single location where it can monitor all Internet traffic on the internal network.

◆ *IMPORTANT*: to ensure the integrity of your firewall, *do not* install Websense Enterprise components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, a dedicated machine runs Websense Enterprise components, and a second dedicated machine runs Reporting components. The separate dedicated machines may be combined into one machine with a Pentium 4, 3 GHz processor. Table 6 provides a recommended deployment. Figure 1, page 27 provides a synopsis of a Windows small network deployment. As the

network grows and the number of Internet requests increases, you may need to spread the deployment of components to additional, non-dedicated machines to improve processing performance on the dedicated machines.

Table 6 Windows Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1[1]	• DC Agent • eDirectory Agent[2] • Filtering Service • Logon Agent • Policy Server • RADIUS Agent[2] • Real-Time Analyzer - Requires Apache or IIS Web server • Network Agent • User Service • Websense Master Database • Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 2 GB of free disk space
Dedicated Machine #2[1]	• Explorer - Requires Apache or IIS Web server • Log Database • Log Database Manager • Log Server • Microsoft SQL Server or MSDE • Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 40 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Network Agent[4]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Transparent ID Agent[2] (DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent)	**Windows**[3] • Pentium 4, or greater • 256 MB RAM

Table 6 Windows Deployment in a Small Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	◆ Websense Enterprise Manager	**Windows**[3] ◆ Pentium 4, or greater ◆ 256 MB RAM

1. The separate dedicated machines may be combined into one machine with a Pentium 4, 3 GHz processor.

2. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

3. See Table 4, on page 18, to verify operating system support for each component.

4. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.

In Figure 1, page 27, Websense Enterprise is installed in a central location where it can receive Internet requests and manage both HTTP traffic (from the gateway, via the integration partner) and non-HTTP traffic (protocol requests from Network Agent).
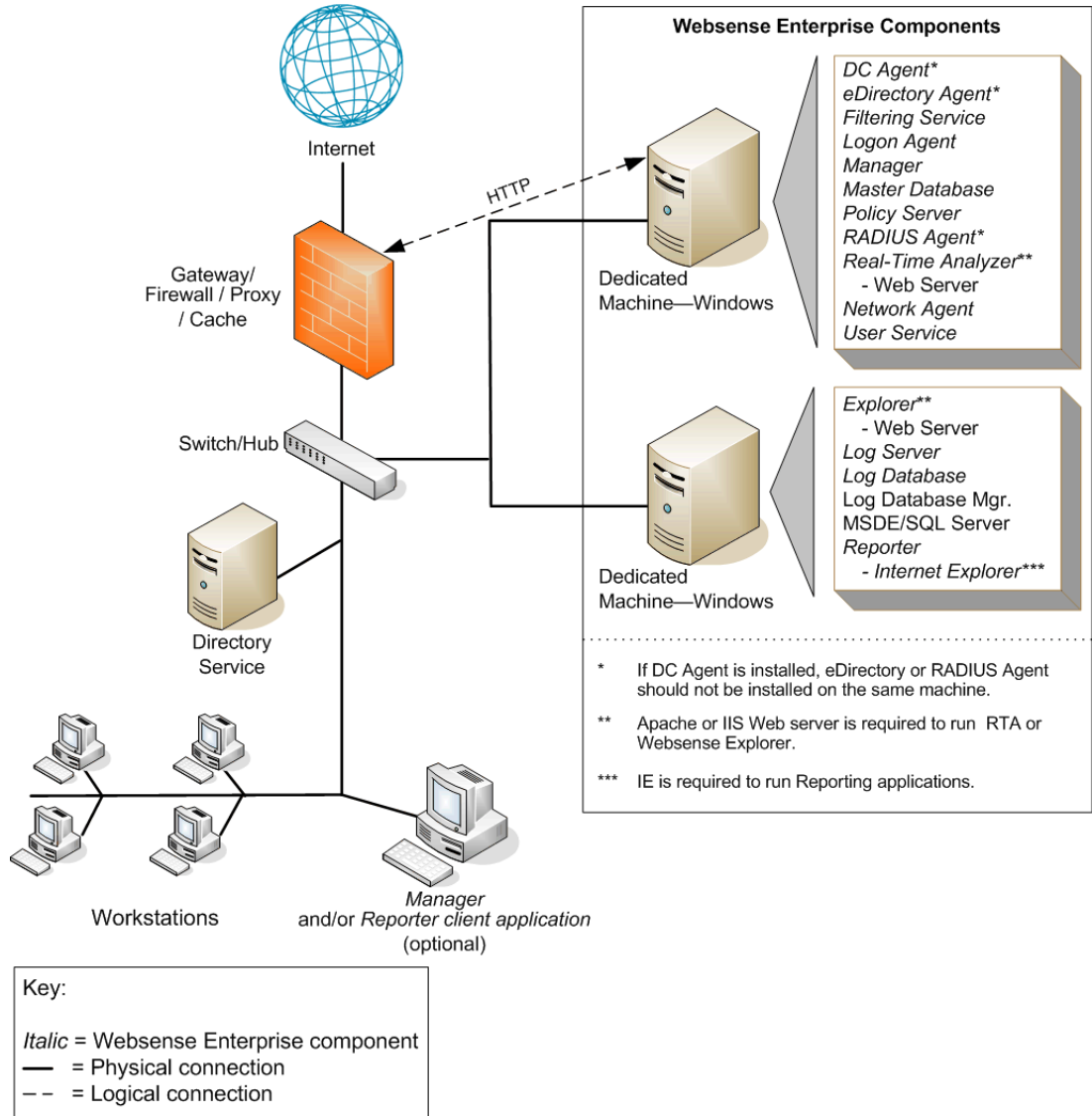
Figure 1   Synopsis of Windows Deployment in a Small Network

✓   **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a small Windows network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Linux Deployment Recommendations

If you want to run Websense Enterprise in a small network on a Linux machine, you need at least one Windows machine to run certain components. The following table provides a breakdown of the recommended deployment. Figure 2, page 30 provides a synopsis of a Linux deployment in a medium network.

Table 7 Linux Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database	**Linux**[3] • Pentium 4, or greater • 512 MB RAM • 2 GB of free disk space

Dedicated Machine #2	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[3]
		• Pentium 4, or greater
		• 512 MB RAM
		• 40 GB of free disk space

Dedicated Machine #2[4]	• Explorer for Unix - Requires Apache • Log Database • Log Server • MySQL	**Linux**[3] • Pentium 4, or greater • 512 MB RAM • 40 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires Apache or IIS Web server • Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		

Table 7 Linux Deployment in a Small Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[5]	**Linux**[3] • Pentium 4, or greater • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4 or greater • 256 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Linux**[3] (eDirectory Agent or RADIUS Agent only) • Pentium 4, or greater • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in Linux and Solaris environments, it cannot use Windows directory services, (i.e., Windows NT Directory Service or Active Directory) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

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

5. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.

Websense Enterprise Components

Internet

Gateway/
Firewall / Proxy
/ Cache

HTTP

Dedicated
Machine 1—Linux

eDirectory Agent
Filtering Service
Logon Agent
Master Database
Network Agent
Policy Server
RADIUS Agent
User Service*

Switch/Hub

Dedicated
Machine 2—Windows

—or—

Explorer**
- Web Server
Log Server
Log Database
Log Database Mgr.
MSDE/SQL Server
Reporter
- *Internet Explorer****

Directory
Service

Dedicated
Machine 2—Linux

Explorer for Unix**
- Apache
Log Server
Log Database
MySQL

Workstations

Manager
and/or *Reporter client application*
(optional)

Additional Windows Machine

DC Agent*
Manager
Real-Time Analyzer**
- Web Server

*   User Service must be installed on a Windows
    machine if DC Agent is being used.

**   Apache or IIS Web server is required to run RTA or
    Websense Explorer.

***   IE is required to run Reporting applications.

Key:

Italic = Websense Enterprise component
___ = Physical connection
_ _ . = Logical connection

Figure 2 Synopsis of Linux Deployment for a Small Network

✔ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise
components in a small Linux network. Depending on the configuration of your
network, the components may be deployed differently. Certain components, such
as Network Agent, also may be deployed on multiple segments.

Solaris Deployment Recommendations

If you want to run Websense Enterprise in a small network on a Solaris machine, you need at least one Windows machine to run certain components. The following table provides a breakdown of the recommended deployment. Figure 3, page 33 provides a synopsis of a Solaris deployment in a small network.

Table 8 Solaris Deployment in a Small Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	- eDirectory Agent[1] - Filtering Service - Logon Agent - Network Agent - Policy Server - RADIUS Agent[1] - User Service[2] - Websense Master Database - Websense Enterprise Manager	**Solaris**[3] - UltraSPARC IIIi 512 MB RAM 2 GB of free disk space.
Dedicated Machine #2	- Explorer - Requires Apache or IIS Web server - Log Database - Log Database Manager - Log Server - Microsoft SQL Server or MSDE - Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] - Pentium 4, or greater 512 MB RAM 40 GB of free disk space
Dedicated Machine #2[4]	- Explorer for Unix - Requires Apache - Log Database - Log Server - MySQL	**Solaris**[3] - UltraSPARC IIIi 512 MB RAM 40 GB of free disk space.
Additional Machine (not dedicated)	- DC Agent - Real-Time Analyzer - Requires Apache or IIS Web server	**Windows**[3] - Pentium 4, or greater 512 MB RAM 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines.		
See Table 3, on page 16 for component and operating system compatibility.		

Table 8 Solaris Deployment in a Small Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[5]	**Solaris**[3] • UltraSPARC IIIi • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Solaris**[3] (eDirectory Agent or RADIUS Agent only) • UltraSPARC IIIi • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 256 MB RAM **Solaris**[3] • UltraSPARC IIIi • 512 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service, Active Directory) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

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

5. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
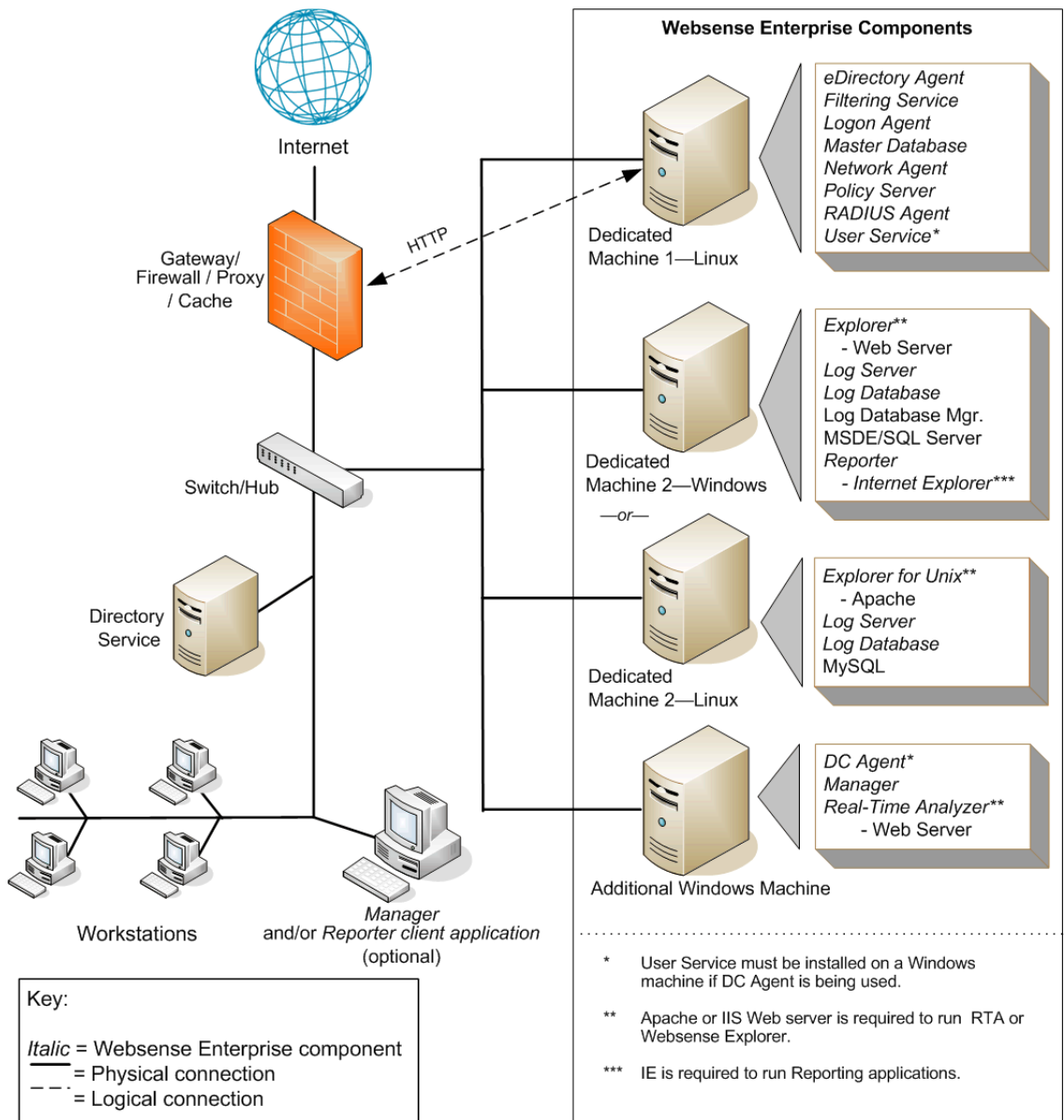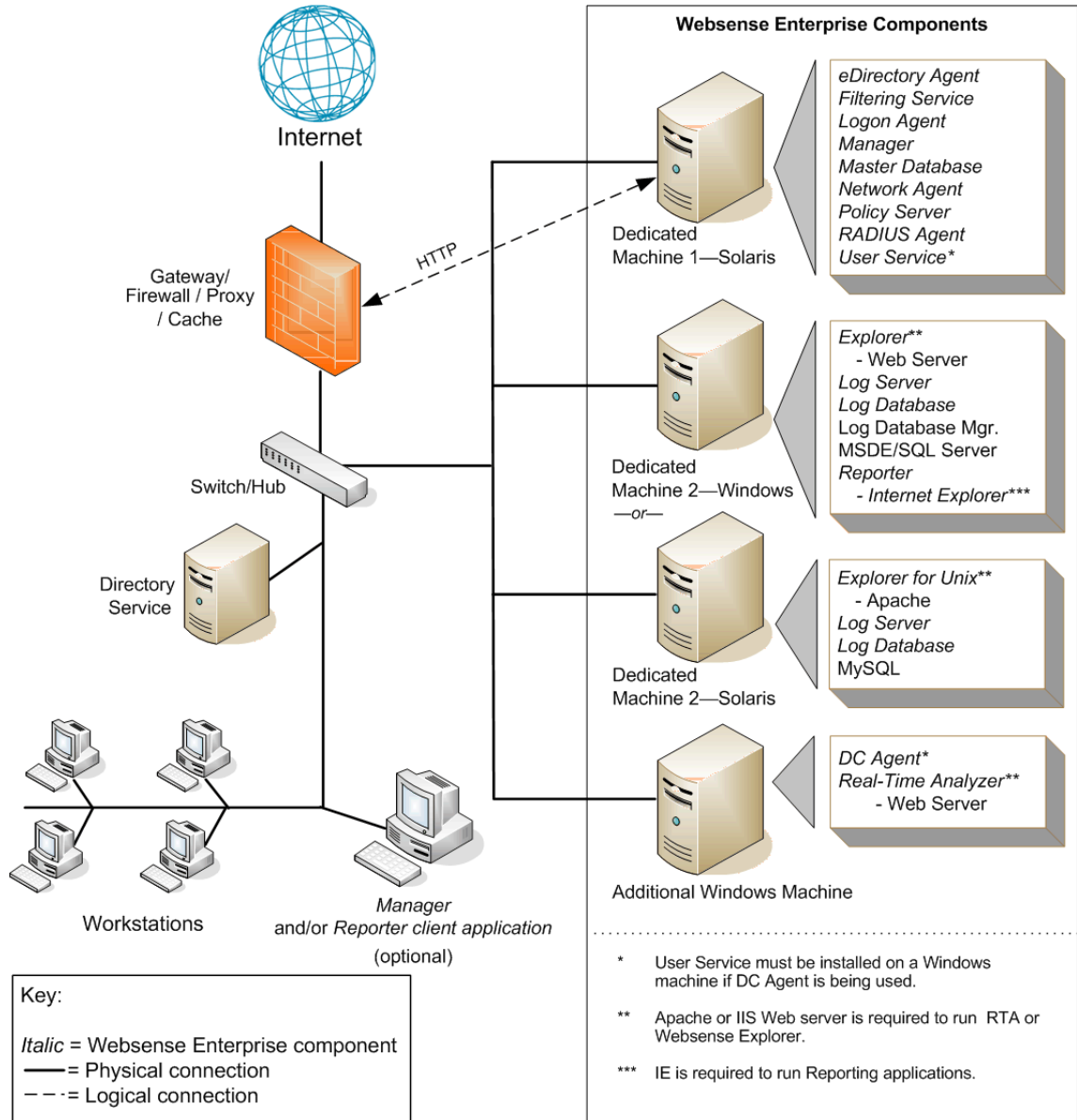
Figure 3 Synopsis of Solaris Deployment for a Small Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a small Solaris network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Medium Networks: 500–2,500 Users

In a medium network, Websense Enterprise components should be distributed on two or more dedicated machines, depending on your operating environment. Like the small network deployment, one machine runs Websense Enterprise, plus either Apache or IIS Web server. The machine on which Websense Enterprise is installed can be running a Windows Server, Linux or Solaris operating system. Linux and Solaris systems may require an additional dedicated Windows machine to run certain components that only run in a Windows environment. 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 may be needed in a higher traffic, medium network.

Websense Enterprise 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 will be filtered by Websense Enterprise.

Network Considerations

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

◆ Filtering Service can receive Internet requests from the gateway or integration device (if any) or from Network Agent.

◆ Network Agent must have bi-directional visibility of Internet traffic that uses protocols that are not web-based, such as instant messaging, chat, streaming media, P2P file sharing, file transfer (such as FTP), mail, and others. *Appendix A* of the *Websense Enterprise Administrator's Guide* lists these protocols.

◆ Network Agent must be deployed at a location where the agent can monitor all Internet traffic on the internal network. If one instance of Network Agent cannot see all Internet traffic, multiple Network Agents must be deployed. Each Network Agent must be located where it can see all Internet traffic on the segment that it is deployed to monitor.

◆ Multiple Filtering Services can be deployed, connected to one Policy Server. This deployment is useful for remote or isolated sub-networks. See *Number of Filtering Services allowed per Policy Server*, page 20, for more information.

◆ *IMPORTANT*: To ensure the integrity of your firewall, *do not* install Websense Enterprise components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, two dedicated machines are recommended to run Websense Enterprise in a medium network. The following table provides a breakdown of the recommended deployment. Figure 4, page 37 provides a synopsis of a Windows deployment in a medium network.

Table 9 Windows Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• DC Agent • eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent[1] • User Service • Websense Master Database • Websense Enterprise Manager	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM • 2 GB of free disk space

Dedicated Machine #2[3]	• Explorer
	  - Requires Apache or
	    IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet
	    Explorer 5.5 or later
		Windows[2]
		• Pentium 4, 2.0 GHz processor, or greater
		• 512 MB RAM
		• 100 GB of free disk space

Additional Machine (not dedicated)	• Real-Time Analyzer
	  - Requires IIS or
	    Apache Web Server
		Windows[2]
		• Pentium 4, or greater
		• 512 MB RAM
		• 1 GB of free disk space

Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Network Agent[4]	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM

Additional Machine (optional)	• Reporter client application
	  - Requires Internet
	    Explorer 5.5 or later
		Windows[2]
		• Pentium 4, or greater
		• 512 MB RAM

Table 9 Windows Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] (DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent)	**Windows**[2] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[2] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

2. See Table 4, on page 18, to verify operating system support for each component.

3. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

4. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.

In Figure 4, page 37, Websense Enterprise is installed in a central location where it can monitor and filter both HTTP traffic (from the gateway, via the integration partner) and non-HTTP traffic (from a switch or hub).

Websense Enterprise Components

Internet

HTTP

Gateway/
Firewall / Proxy
/ Cache

Dedicated
Machine 1—Windows

DC Agent*
eDirectory Agent*
Filtering Service
Logon Agent
Manager
Master Database
Network Agent
Policy Server
RADIUS Agent*
User Service

Switch/Hub

Dedicated
Machine 2—Windows

Explorer**
   - Web Server
Log Server
Log Database
Log Database Mgr.
MSDE/SQL Server
Reporting
   - *Internet Explorer****

Directory
Service

Real-Time Analyzer**
   - Web Server

Additional Windows Machine

*   If DC Agent is installed, eDirectory or RADIUS Agent
       should not be installed on the same machine.

**   Apache or IIS Web server is required to run RTA or
       Websense Explorer.

*** IE is required to run Reporting applications.

Workstations

Manager
and/or *Reporter client application*
(optional)

Key:

Italic = Websense Enterprise component
——— = Physical connection
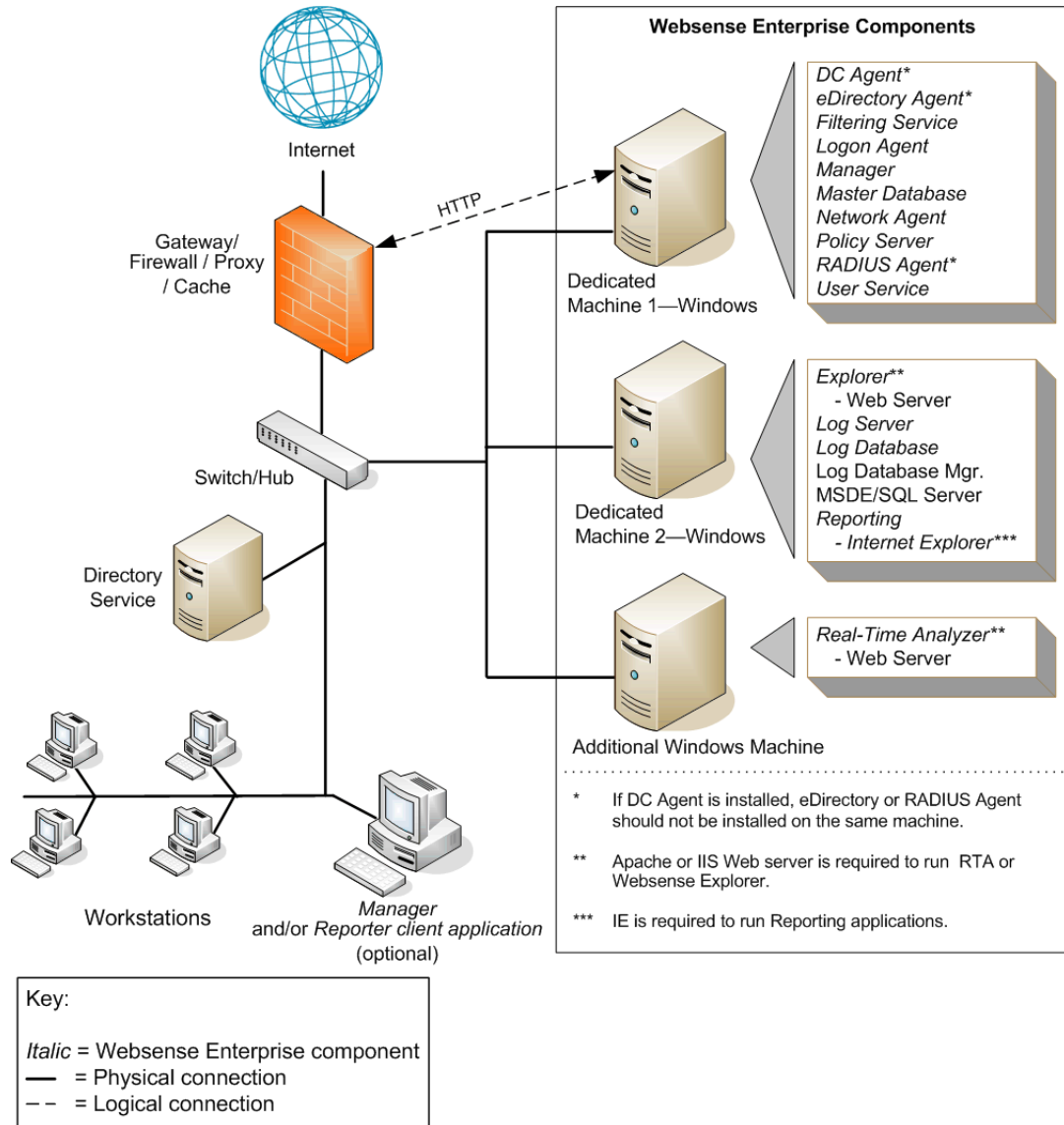– – = Logical connection

Figure 4 Synopsis of Windows Deployment for a Medium Network

NOTE

This diagram provides an overview of the distribution of the Websense Enterprise components in a medium Windows network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Linux Deployment Recommendations

If you want to run Websense Enterprise in a medium network on a Linux machine, you need at least two Windows machines to run certain components. The following table provides a breakdown of the recommended deployment. Figure 5, page 40 provides a synopsis of a Linux deployment in a medium network.

Table 10 Linux Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database	**Linux**:[3] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM • 2 GB of free disk space

Dedicated Machine #2[4]	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[3]
		• Pentium 4, 2.0 GHz processor, or greater
		• 512 MB RAM
		• 100 GB of free disk space

Dedicated Machine #2[5]	• Explorer for Unix - Requires Apache • Log Database • Log Server • MySQL	**Linux**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM • 100 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server • Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		

Table 10 Linux Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[6]	**Linux**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Linux**[3] (eDirectory Agent or RADIUS Agent only) • Pentium 4, or greater • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in the Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service, Active Directory) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

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

6. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
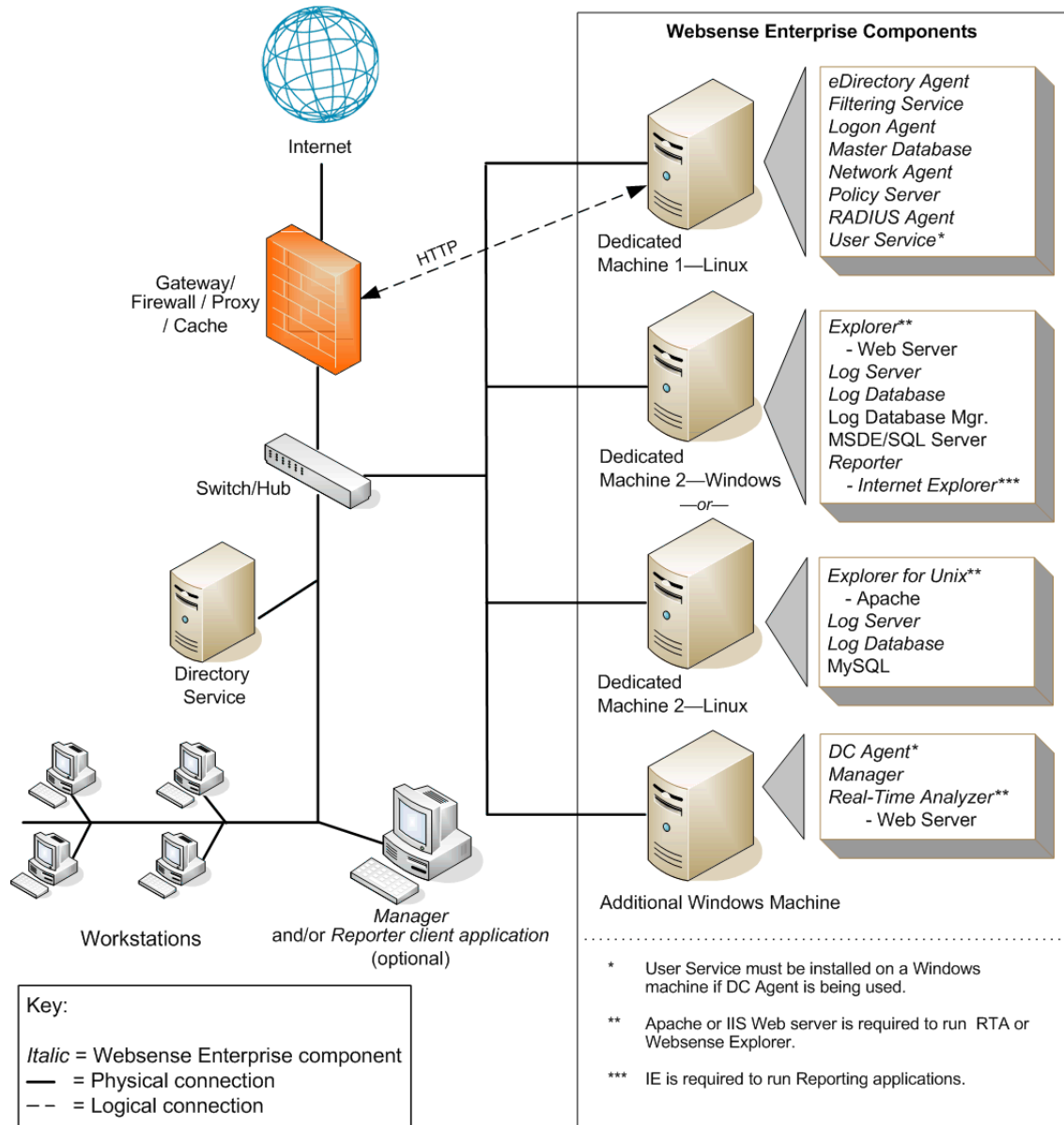
Figure 5 Synopsis of Linux Deployment for a Medium Network

> **NOTE**
>
> ✔ This diagram provides an overview of the distribution of the Websense Enterprise components in a medium Linux network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Solaris Deployment Recommendations

If you want to run Websense Enterprise in a medium network on a Solaris machine, you need at least two Windows machines to run certain components. The following table provides a breakdown of the recommended deployment. Figure 6, page 43 provides a synopsis of a Solaris deployment in a medium network.

Table 11 Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • RADIUS Agent[1] • Policy Server • User Service[2] • Websense Master Database • Websense Enterprise Manager	**Solaris**[3] • UltraSPARC IIIi • 1 GB RAM • 2 GB of free disk space
Dedicated Machine #2[4]	• Explorer -Requires Apache or IIS Web server • Log Database • Log Database Manager • Log Server • Microsoft SQL Server or MSDE • Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM • 100 GB of free disk space
Dedicated Machine #2[5]	• Explorer for Unix - Requires Apache • Log Database • Log Server • MySQL	**Solaris**[3] • UltraSPARC IIIi • 512 MB RAM • 100 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		

Table 11 Solaris Deployment in a Medium Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[6]	**Solaris**[3] • UltraSPARC IIIi • 512 MB RAM **Windows**[3] • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 512 MB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Solaris**[3] (eDirectory Agent or RADIUS Agent only) • UltraSPARC IIIi • 256 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Solaris**[3] • UltraSPARC IIIi • 512 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in the Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service configuration option,) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

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

6. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
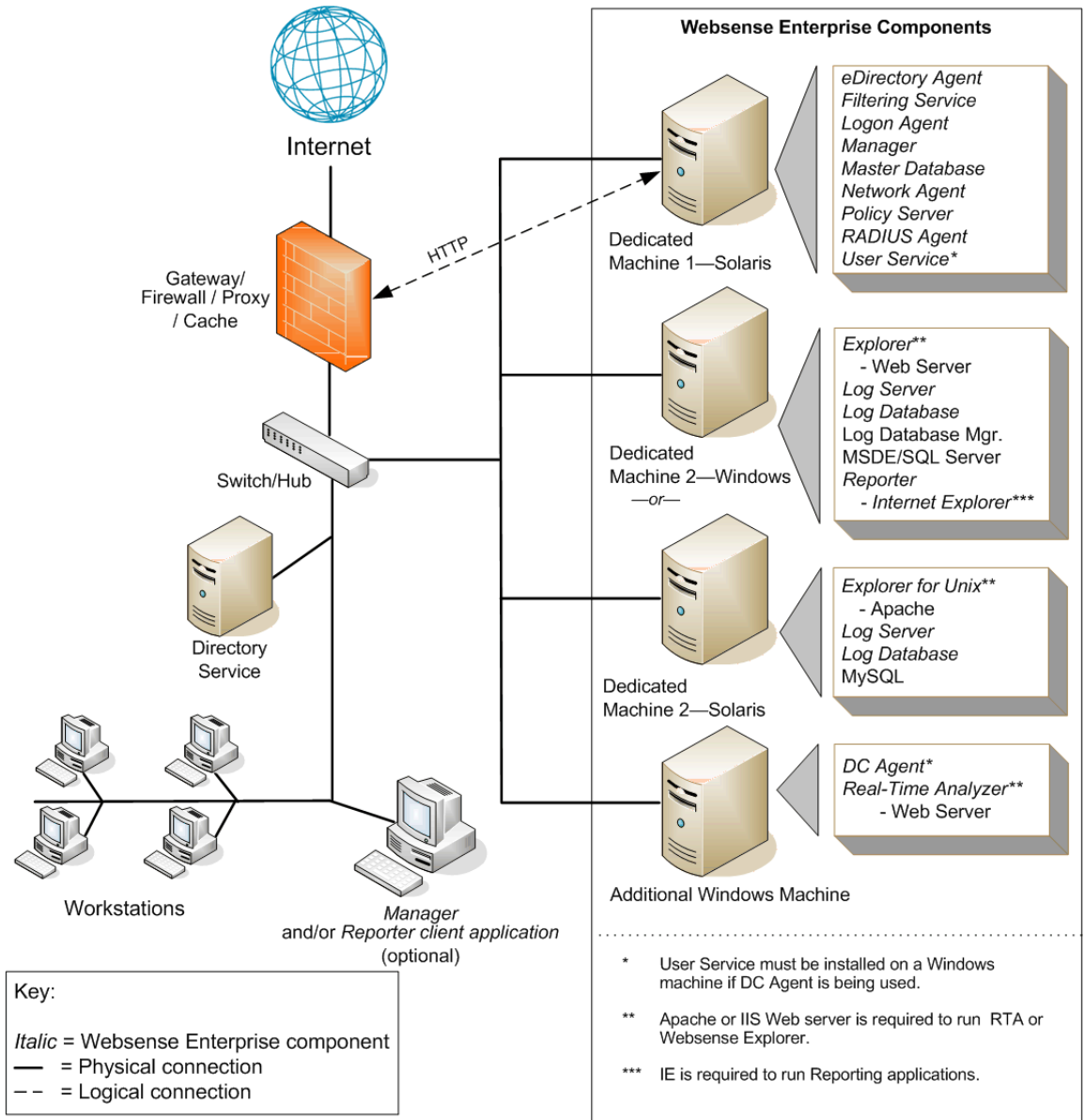
Figure 6 Synopsis of Solaris Deployment for a Medium Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a medium Solaris network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Large Networks: 2,500–10,000 Users

In a large network, Websense Enterprise components should be distributed on two or more dedicated machines, depending on your operating environment. The deployment on dedicated machines is the same as a medium network deployment. However, 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.

Websense Enterprise 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 will be filtered by Websense Enterprise.

Network Considerations

To ensure effective filtering, Websense Enterprise 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 have bi-directional visibility of Internet traffic that uses protocols that are not web-based, such as instant messaging, chat, streaming media, P2P file sharing, file transfer (such as FTP), mail, and others. *Appendix A* of the *Websense Enterprise Administrator's Guide* lists these protocols.

◆ Network Agent should be deployed in the network at a location where it can monitor all Internet traffic on the internal network.

◆ For larger networks, install multiple Network Agents, with each monitoring an IP address range or network segment. Depending on the size and traffic on the network, multiple Network Agents may be needed in order to capture all network traffic and prevent overloading of servers. You may want to put Network Agents on dedicated servers to increase overall throughput.

◆ Multiple Filtering Services can be deployed, connected to one Policy Server. This deployment is useful for remote or isolated sub-networks. See *Number of Filtering Services allowed per Policy Server*, page 20 for more information.

◆ *IMPORTANT*: To ensure the integrity of your firewall, *do not* install Websense Enterprise components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, two dedicated machines are recommended to run Websense Enterprise on a large network. The following table provides a breakdown of the recommended deployment. Figure 7, page 47 provides a synopsis of a Windows deployment in a large network.

Table 12 Windows Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• DC Agent • eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent[1] • User Service • Websense Master Database • Websense Enterprise Manager	**Windows**[2] • Xeon, 3.0 GHz processors, or greater • 1 GB RAM • 2 GB of free disk space

Dedicated Machine #2[3]	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[2]
		• Dual Xeon, 2.0 GHz processors, or greater
		• 1 GB RAM
		• 200 of free disk space utilizing a disk array[4]
		• High speed disk access

Additional Machine (not dedicated)	• Real-Time Analyzer - Requires IIS or Apache Web Server	**Windows**[2] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Network Agent[5]	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[2] • Pentium 4, or greater • 1 GB RAM

Table 12 Windows Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] (DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent)	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[2] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

2. See Table 4, on page 18, to verify operating system support for each component.

3. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

4. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

5. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
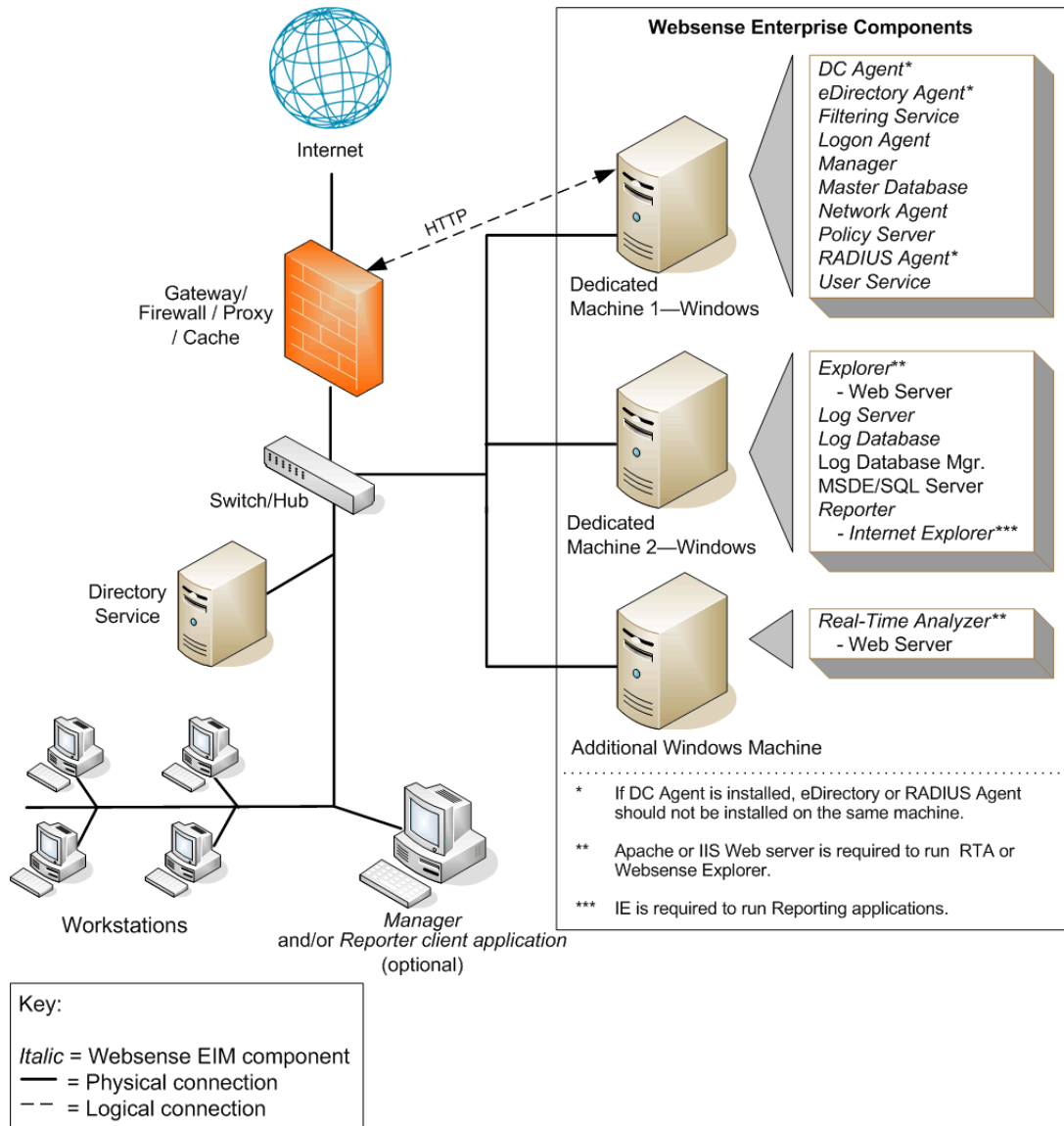
Figure 7 Synopsis of Windows Deployment for a Large Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a large Windows network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Linux Deployment Recommendations

If you want to run Websense Enterprise in a large network on a Linux machine, you also need at least two Windows machines to run certain components. The following table provides a breakdown of the recommended deployment. Figure 8, page 50 provides a synopsis of a Linux deployment in a large network.

Table 13 Linux Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Logon Agent • Filtering Service • Network Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database	**Linux**[3] • Xeon, 3.0 GHz processors, or greater • 1 GB RAM • 2 GB of free disk space
Dedicated Machine #2[4]	• Explorer - Requires Apache or IIS Web server • Log Database • Log Database Manager • Log Server • Microsoft SQL Server or MSDE • Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Dual Xeon, 2.0 GHz processors, or greater • 1 GB RAM • 200 GB of free disk space utilizing a disk array[5] • High speed disk access
Dedicated Machine #2[6]	• Explorer for Unix - Requires Apache • Log Database • Explorer Unix Log Server • MySQL	**Linux**[3] • Dual Xeon, 2.0 GHz processors, or greater • 1 GB RAM • 200 GB of free disk space utilizing a disk array[7] • High speed disk access
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server • Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		

Table 13 Linux Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[8]	**Linux**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Linux**[3] (eDirectory Agent or RADIUS Agent only) • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Linux**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service configuration option,) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. Depending on the configuration of the machine, Microsoft SLQ Server and the Log Database may need to be run on a separate machine than the Log Server and the Reporter client application. Log Database Manager and Log Server must run on the same machine.

5. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

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

7. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

8. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
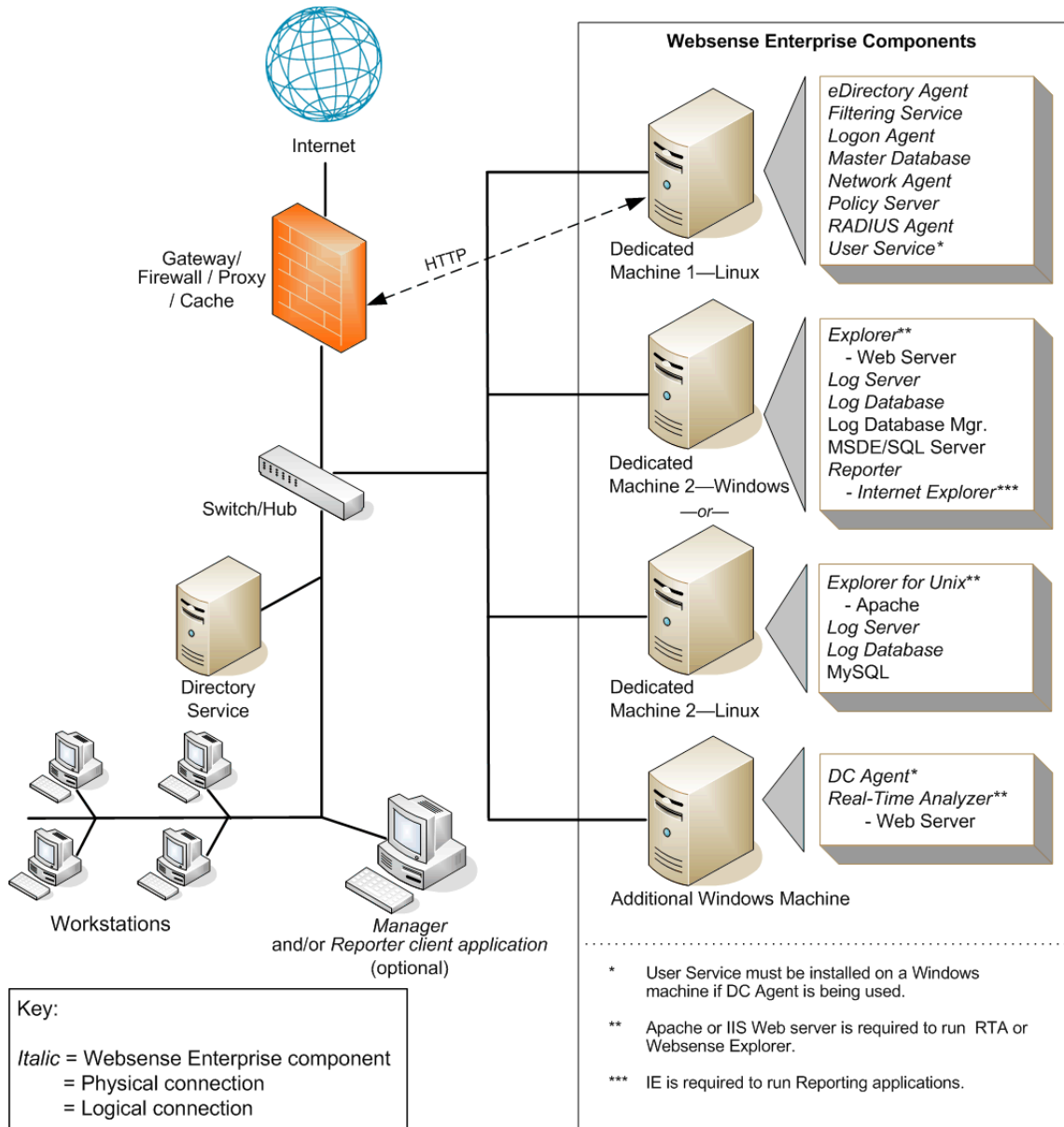

Figure 8 Synopsis of Linux Deployment for a Large Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a large Linux network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Solaris Deployment Recommendations

If you want to run Websense Enterprise in a large network on a Solaris machine, you also need at least two Windows machines to run certain components. The following table provides a breakdown of the recommended deployment. Figure 9, page 53 provides a synopsis of a Solaris deployment in a large network.

Table 14 Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Network Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database • Websense Enterprise Manager	**Solaris**[3] • UltraSPARC IV • 1 GB RAM • 2 GB of free disk space

Dedicated Machine #2[4]	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[3]
		• Dual Xeon, 2.0 GHz processors, or greater
		• 1 GB RAM
		• 200 GB of free disk space utilizing a disk array[5]
		• High speed disk access

Dedicated Machine #2[6]	• Explorer for Unix - Requires Apache • Log Database • Explorer Unix Log Server • MySQL	**Solaris**[3] • UltraSPARC IV • 1 GB RAM • 200 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server	**Windows**[3] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		

Table 14 Solaris Deployment in a Large Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent[7]	**Solaris**[3] • UltraSPARC IV • 512 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Solaris**[3] (eDirectory Agent or RADIUS Agent only) • UltraSPARC IIIi • 256 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Solaris**[3] • UltraSPARC IIIi • 256 RAM **Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in the Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service configuration option,) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

5. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability

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

7. 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 in a small network. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.
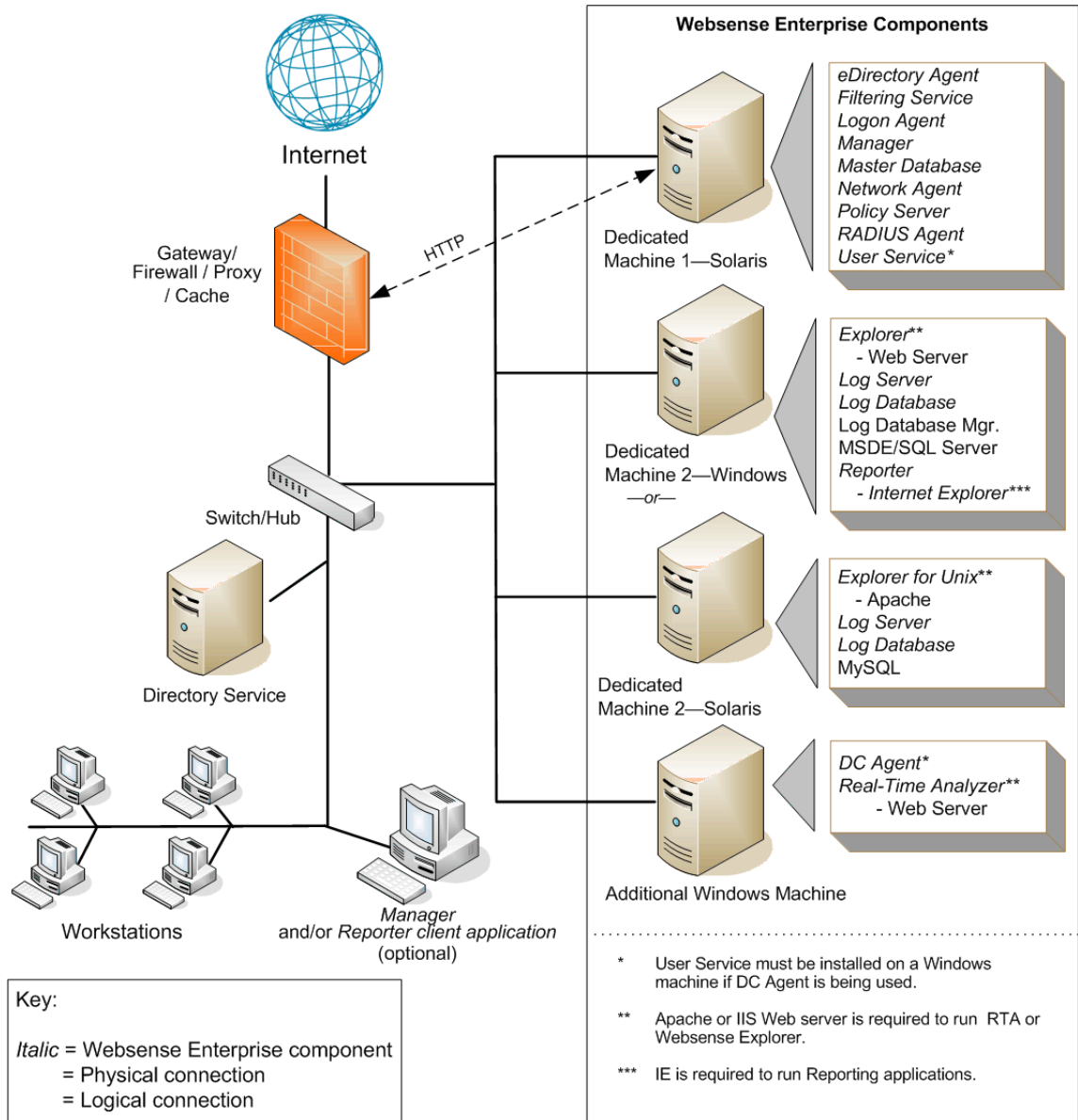

Figure 9 Synopsis of Solaris Deployment for a Large Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in a large Solaris network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Enterprise Networks: 10,000+ Users

In an enterprise network, Websense Enterprise components should be distributed on three 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.

Websense Enterprise 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 will be filtered by Websense Enterprise.

Network Considerations

To ensure effective filtering, Websense Enterprise 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 have bi-directional visibility of Internet traffic that uses protocols that are not web-based, such as instant messaging, chat, streaming media, P2P file sharing, file transfer (such as FTP), mail, and others. *Appendix A* of the *Websense Enterprise Administrator's Guide* lists these protocols.

◆ Network Agent must be located to see all Internet requests for the network it is deployed to monitor.

Depending on the size and traffic volume on the network, multiple Network Agents may be needed in order to capture all network traffic and prevent overloading of the monitoring machines. In such a deployment, each Network Agent monitors an IP address range or network segment. You may want to put Network Agents on dedicated servers to increase overall throughput.

◆ Multiple Filtering Services can be deployed, connected to one Policy Server. This deployment is useful for remote or isolated sub-networks. See *Number of Filtering Services allowed per Policy Server*, for more information.

◆ *IMPORTANT*: To ensure the integrity of your firewall, *do not* install Websense Enterprise components on the firewall machine.

Windows Deployment Recommendations

In a Windows environment, three dedicated machines are recommended to run Websense Enterprise in an enterprise network. The following table provides a breakdown of a recommended deployment. provides a synopsis of a Windows deployment in an enterprise network.

Table 15 Windows Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Policy Server • RADIUS Agent[1] • User Service • Websense Master Database • Websense Enterprise Manager	**Windows**[2] • Xeon, 3.0 GHz processor, or greater for 10,000 to 25,000 users Dual Xeon 3.20 GHz, or greater for more than 25,000 users. • 2 GB RAM • 2 GB of free disk space
Dedicated Machine #2	• Network Agent	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM • 1 GB of free disk space
Dedicated Machine #3[3]	• Apache or IIS Web server • Explorer • Log Database • Log Database Manager • Log Server • Microsoft SQL Server or MSDE • Reporter client application	**Windows**[2] • Dual Xeon, 2.0 GHz processor, or greater for 10,000 to 25,000 users. Quad Xeon 3.20 GHz for greater than 25,000 users. • 2 GB RAM or more, on Quad machine - 6 GB • 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 IIS or Apache Web Server	**Windows**[2] • Pentium 4, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines.		
Additional Machine (optional)	• Network Agent	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[2] • Pentium 4, or greater • 1 GB RAM

Table 15 Windows Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Additional Machine (optional)	• Transparent ID Agent[1] (DC Agent, eDirectory Agent, Logon Agent, or RADIUS Agent)	**Windows**[2] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[2] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

2. See Table 4, on page 18, to verify operating system support for each component.

3. 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 Reporter client application. The Log Database Manager and the Log Server must run on the same machine.

4. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.
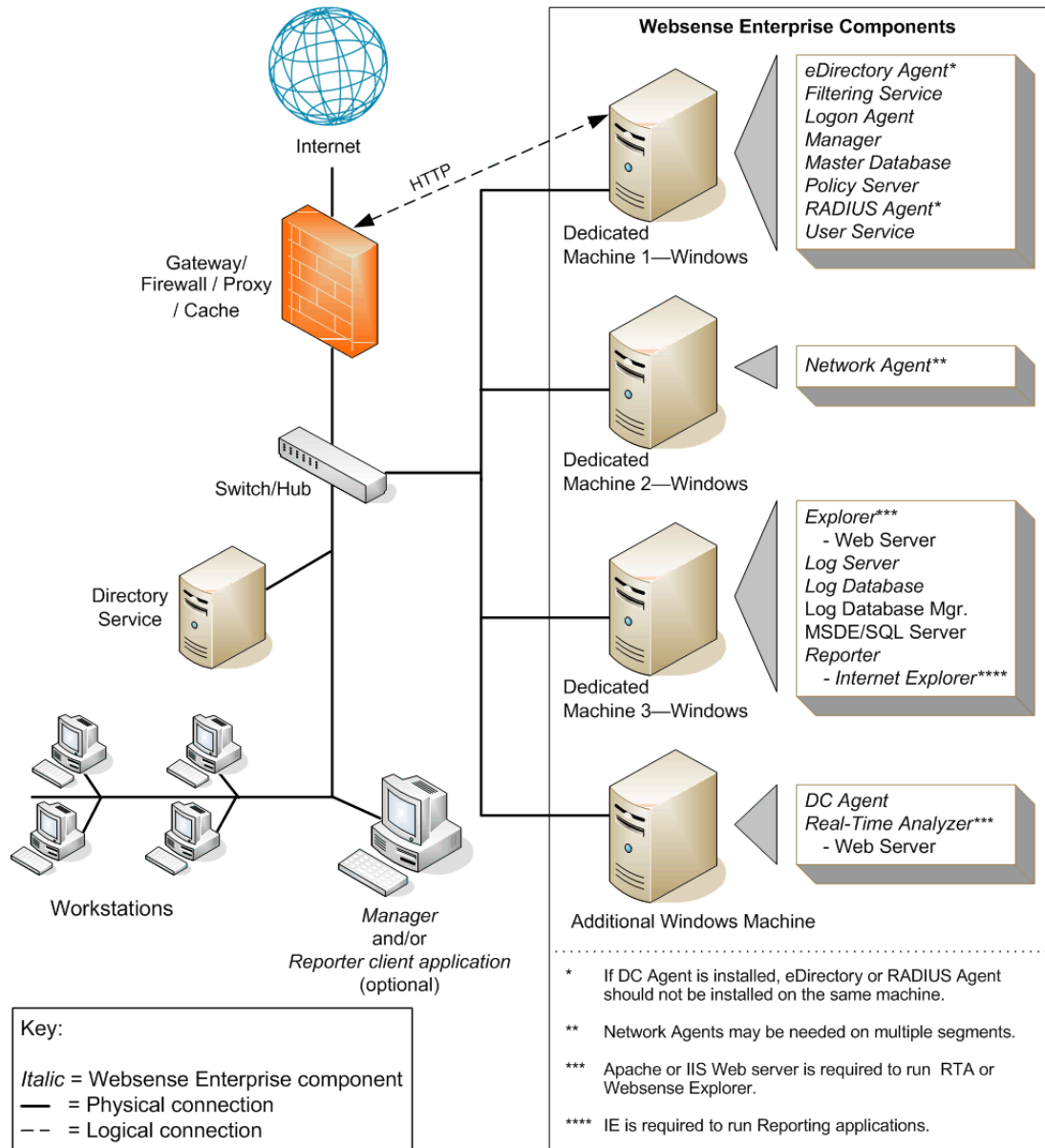
Figure 10 Synopsis of Windows Deployment for an Enterprise Network

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in an enterprise Windows network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple network segments.

Linux Deployment Recommendations

If you want to run Websense Enterprise in an enterprise network on a Linux machine, you also need at least two Windows machines to run certain components. The following table provides a breakdown of a recommended deployment. provides a synopsis of a Linux deployment in an enterprise network.

Table 16 Linux Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database	**Linux**[3] • Xeon, 3.0 GHz processor, or greater for 10,000 to 25,000 users Dual Xeon 3.20 GHz, or greater for more than 25,000 users. • 2 GB RAM • 2 GB of free disk space
Dedicated Machine #2	• Network Agent[4]	**Linux**[3] • Xeon, 3.0 GHz processor, or greater for 10,000 to 25,000 users Dual Xeon 3.20 GHz, or greater for more than 25,000 users. • 1 GB RAM • 1 GB of free disk space **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM • 1 GB of free disk space

Dedicated Machine #3[5]	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[3]
		• Dual Xeon, 2.0 GHz processor, or greater for 10,000 to 25,000 users. Xeon 3.20 GHz for greater than 25,000 users.
		• 2 GB RAM or more
		• 200 GB of free disk space utilizing a disk array[6]
		• High speed disk access

Dedicated Machine #3[7]	• Explorer for Unix - Requires Apache • Log Database • Explorer Unix Log Server • MySQL	**Linux**[3] • Dual Xeon, 2.0 GHz processor, or greater for 10,000 to 25,000 users. Xeon 3.20 GHz for greater than 25,000 users. • 2 GB RAM or more • 200 GB of free disk space utilizing a disk array[6] • High speed disk access

Table 16 Linux Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server • Websense Enterprise Manager	**Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM • 1 GB of free disk space
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent	**Linux**[3] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows**[3] • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Linux**[3] (eDirectory Agent or RADIUS Agent only) • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 256 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. The eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service, Active Directory) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. 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). See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.

5. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

6. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

7. A separate installation of Websense Enterprise Explorer for Unix is also available. This Explorer for Unix only runs with Explorer Unix Log Server and utilizes a MySQL database. The Unix and Windows Reporting products are not cross-platform compatible.
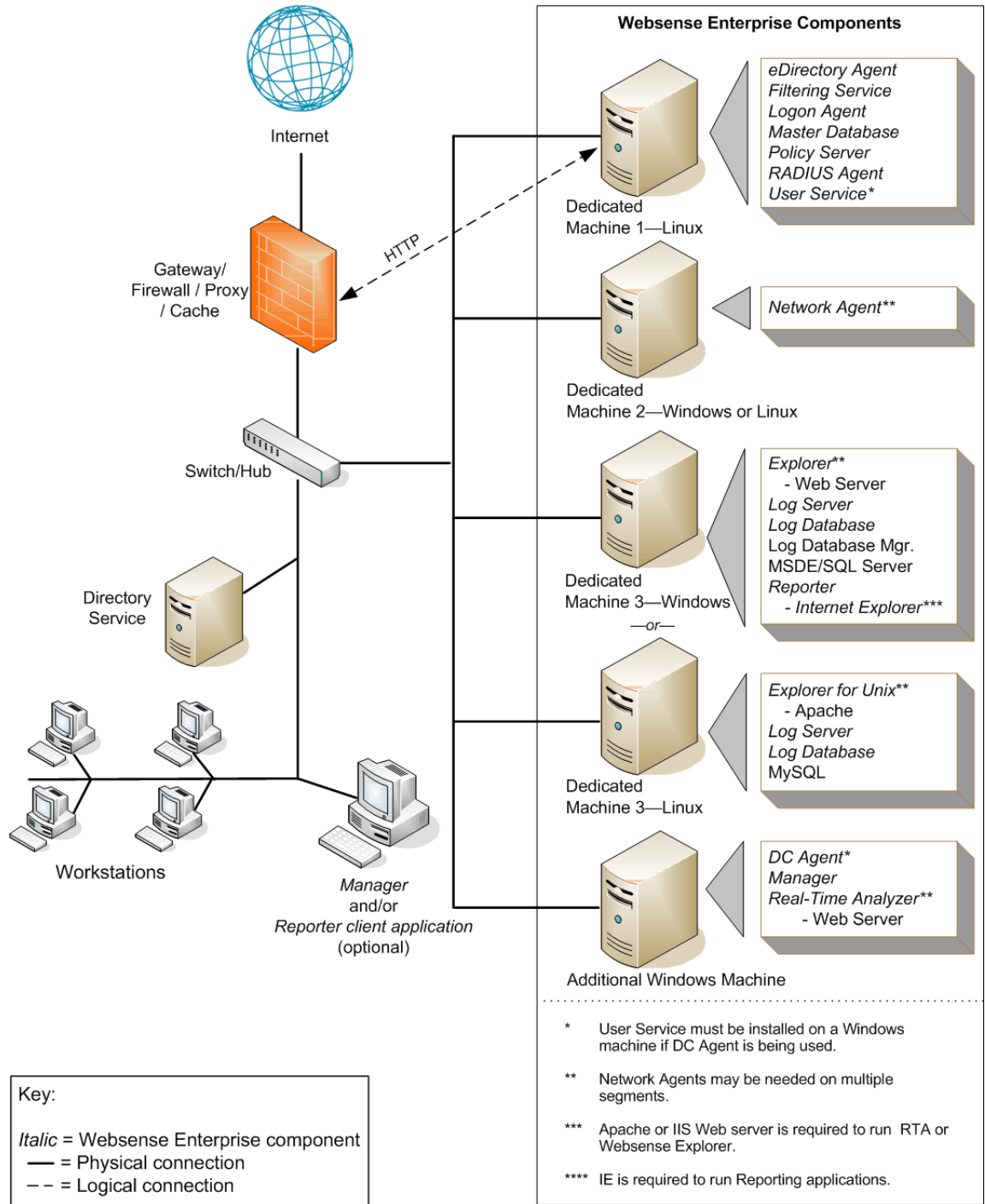
Websense Enterprise Components

Internet

Gateway/
Firewall / Proxy
/ Cache

HTTP

Switch/Hub

Directory
Service

Workstations

Manager
and/or
Reporter client application
(optional)

Dedicated
Machine 1—Linux

eDirectory Agent
Filtering Service
Logon Agent
Master Database
Policy Server
RADIUS Agent
User Service*

Dedicated
Machine 2—Windows or Linux

Network Agent**

Dedicated
Machine 3—Windows

Explorer**
   - Web Server
Log Server
Log Database
Log Database Mgr.
MSDE/SQL Server
Reporter
   - Internet Explorer***

—or—

Dedicated
Machine 3—Linux

Explorer for Unix**
   - Apache
Log Server
Log Database
MySQL

Additional Windows Machine

DC Agent*
Manager
Real-Time Analyzer**
   - Web Server

*   User Service must be installed on a Windows
       machine if DC Agent is being used.

**   Network Agents may be needed on multiple
       segments.

*** Apache or IIS Web server is required to run RTA or
       Websense Explorer.

**** IE is required to run Reporting applications.

Key:

Italic = Websense Enterprise component
—— = Physical connection
– – = Logical connection

Figure 11 Synopsis of Linux Deployment for an Enterprise Network

✔ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in an enterprise Linux network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Solaris Deployment Recommendations

If you want to run Websense Enterprise in an enterprise network on a Solaris machine, you also need at least two Windows machines to run certain components. The following table provides a breakdown of a recommended deployment. Figure 12, page 65 provides a synopsis of a Solaris deployment in an enterprise network.

Table 17 Solaris Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Dedicated Machine #1	• eDirectory Agent[1] • Filtering Service • Logon Agent • Policy Server • RADIUS Agent[1] • User Service[2] • Websense Master Database • Websense Enterprise Manager	**Solaris**[3] • UltraSPARC IV • 2 GB RAM • 2 GB of free disk space
Dedicated Machine #2	• Network Agent[4]	**Solaris**[3] • UltraSPARC IV • 1 GB RAM **Windows**[3] • Dual Xeon, 2.0 GHz processors, or greater • 1 GB RAM

Dedicated Machine #3[5]	• Explorer
	  - Requires Apache or IIS Web server
	• Log Database
	• Log Database Manager
	• Log Server
	• Microsoft SQL Server or MSDE
	• Reporter client application
	  - Requires Internet Explorer 5.5 or later
		Windows[3]
		• Dual Xeon, 2.0 GHz processor, or greater for 10,000 to 25,000 users. Xeon 3.20 GHz for greater than 25,000 users.
		• 2 GB RAM or more
		• 200 GB of free disk space utilizing a disk array[6]
		• High speed disk access

Dedicated Machine #3[7]	• Explorer for Unix - Requires Apache • Log Database • Explorer Unix Log Server • MySQL	**Solaris**[3] • UltraSPARC IV • 2 GB RAM • 200 GB of free disk space
Additional Machine (not dedicated)	• DC Agent • Real-Time Analyzer - Requires IIS or Apache Web Server	**Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM • 1 GB of free disk space

Table 17 Solaris Deployment in a Enterprise Network

Machine	Software	Hardware Recommendations
Websense Enterprise Manager, the Websense Enterprise Reporter client application and the agents can be installed with other components on dedicated machines, and also can be installed on multiple machines. Multiple installations provide easier access for the Manager and the Reporter client application, and improved processing of the Internet requests by the agents. These additional installations do not require dedicated machines. See Table 3, on page 16 for component and operating system compatibility.		
Additional Machine (optional)	• DC Agent[1]	**Windows**[3] • Pentium 4, or greater • 256 MB RAM
Additional Machine (optional)	• Network Agent	**Solaris**[3] • UltraSPARC IV • 1 GB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 1 GB RAM
Additional Machine (optional)	• Reporter client application - Requires Internet Explorer 5.5 or later	**Windows only**[3] • Pentium 4, or greater • 1 GB RAM
Additional Machine (optional)	• Transparent ID Agent[1] (eDirectory Agent, Logon Agent, or RADIUS Agent)	**Solaris**[3] (eDirectory Agent or RADIUS Agent only) • UltraSPARC IIIi • 256 MB RAM **Windows**[3] • Pentium 4, 2.0 GHz processor, or greater • 256 MB RAM
Additional Machine (optional)	• Websense Enterprise Manager	**Windows**[3] • Pentium 4, or greater • 256 MB RAM **Solaris**[3] • UltraSPARC IIIi • 512 MB RAM

1. eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported. DC Agent only runs on a Windows machine.

2. Although User Service runs in Linux and Solaris environments, it cannot use Windows directory services, (i.e., the Windows NT Directory Service, Active Directory) from those platforms. If DC Agent is used, User Service must be installed on another Windows machine.

3. See Table 4, on page 18, to verify operating system support for each component.

4. Network Agent can run on either the Solaris machine, Dedicated Machine #2, or a separate Windows machine (but not the machine running the Reporting components). See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information on deploying Network Agent.

5. 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 Reporter client application. Log Database Manager and Log Server must run on the same machine.

6. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

7. A separate installation of Websense Enterprise Explorer for Unix is also available. This Explorer for Unix only runs with Explorer Unix Log Server and utilizes a MySQL database. The Unix and Windows Reporting products are not cross-platform compatible.
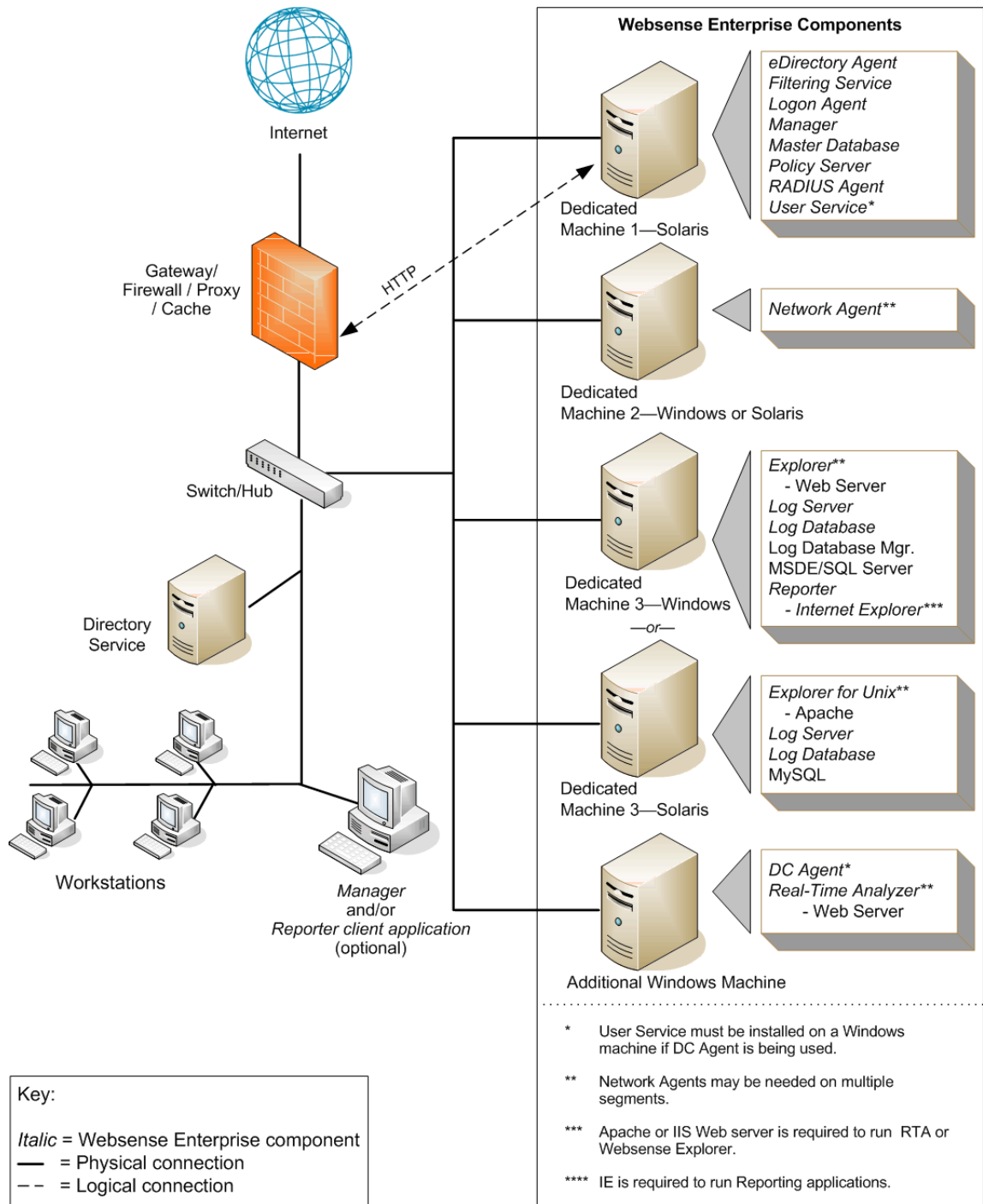
Figure 12 Synopsis of Solaris Deployment in an Enterprise Environment

✓ **NOTE**

This diagram provides an overview of the distribution of the Websense Enterprise components in an enterprise Windows network. Depending on the configuration of your network, the components may be deployed differently. Certain components, such as Network Agent, also may be deployed on multiple segments.

Websense Enterprise Stand-Alone Edition

The **Websense Enterprise Stand-Alone Edition** allows you to deploy the product utilizing Network Agent instead of a third party firewall, network appliance or proxy server. Network Agent detects all Internet requests, both URL and protocol requests, Network Agent checks with Filtering Service to see if the Internet request should be blocked. Besides its role as a standalone filtering agent, Network Agent also calculates the number of bytes transferred and sends a request to Filtering Service to log this information.

For more information about the deploying the Stand-Alone Edition, refer to the *Websense Enterprise Installation Guide for the Stand-Alone Edition*.

The Stand-Alone Edition runs on the following operating systems.

◆ Red Hat Linux 9

◆ Red Hat Linux ES, AS and WS v3.0

◆ Solaris v8 - v9

◆ Windows 2000 Server, SP3 or higher

◆ Windows Server 2003

The optional Websense Enterprise Reporter can run along with the Stand-Alone Edition. However Reporter should be run on a separate *Windows* machine, due to the amount of processing related to reporting. Although Reporter does not run on Linux or Solaris, the Stand-Alone edition can be run on these operating systems in conjunction with Reporter running on Windows.

In a Linux environment, Websense Enterprise Manager, along with Logon Agent and DC Agent (if they are used) must be installed on a Windows machine.

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. That machine must be able to monitor all Internet traffic from the internal network.

Table 18, on page 67, provides system recommendations for deploying the Stand-Alone edition, according to network size. System needs can vary, depending on the amount of Internet requests made by the users.

On average, requests per second are approximately as follows:

◆ 1 - 499 users = 1-100 requests/sec

◆ 500 - 2,499 users = 100 - 500 requests/sec

◆ 2,500 - 9,999 users = 500 - 2,250 requests/sec

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

Table 18 Stand-Alone System Recommendations

Network Size	Single Server Deployment (Windows or Linux)[1] [2]	Reporting Deployment (Windows Only)
1 - 499 users	• Pentium 4, 2.40 GHz, or greater • 1 GB RAM • 2 GB of free disk space	• Pentium 4, 2.40 GHz, or greater • 512 MB RAM • 40 GB of free disk space • MSDE or Microsoft SQL Server is required
500 - 2,499 users	• Pentium 4, 2.40 GHz, or greater • 1 GB RAM • 2 GB of free disk space	• Pentium 4, 2.0 GHz processor, or greater • 512 MB RAM • 100 GB of free disk space • MSDE or Microsoft SQL Server is required for reporting
2,500 - 9,999 users[3]	• Load Balancing Required • Xeon, 3.0 GHz, or greater • 1 GB RAM • 2 GB of free disk space	• Dual Xeon, 2.0 GHz processors, or greater • 1.5 GB RAM • 200 GB of free disk space utilizing a disk array[4] • High speed disk access • Microsoft SQL Server is required for reporting

1. *IMPORTANT*: To ensure the integrity of your firewall, *do not* install Websense Enterprise components on the firewall machine.

2. IMPORTANT: eDirectory or RADIUS Agent can be installed on the same machine as Filtering Service or installed on a separate server on the same network. eDirectory Agent cannot be installed on the same machine as the Reporting components. Running eDirectory Agent and DC Agent in the same deployment is not currently supported.

3. Two Network Agents, running on separate machines is required for a network of this size. A Pentium 4 with a 2 GHZ or greater processor and 256 MB of RAM is recommended for running Network Agent.

4. The Microsoft SQL database and the Log Database need a disk array, running RAID level 10, to increase I/O reliability.

Maximizing System Performance

By making some adjustments to your Websense Enterprise components, you can improve the filtering and logging response times, throughput, and CPU performance for the machine running the components. Performance optimizations on the Websense Enterprise system can be made in the following areas:

◆ Network Agent

◆ Real-Time Analyzer (RTA)

◆ Logging of bytes transferred

◆ Database engine (MSDE or Microsoft SQL Server)

Network Agent

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

If you are running Websense Enterprise in a high load environment and/or with a high capacity connection to the Internet, such as a T3 connection, consider installing Network Agent on multiple machines, each designated to monitor a specific portion of the network. This deployment increases throughput and provides the load.

> *i* **IMPORTANT**
>
> Network Agent must be installed so that it can have bi-directional visibility of the internal network or segment traffic that it is to monitor.
>
> If multiple Network Agents are installed, each network segment must be monitored by one Network Agent. An IP address range monitored by one Network Agent must not be overlapped by 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 of the other ports. *Multiple Segment Network*, page 74 and *Network Agent Location*, page 77 discuss locating Network Agent in more detail.

Real-Time Analyzer (RTA)

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

◆ Websense Enterprise system performance gains can be made by increasing the CPU speed, or number of CPUs, and the amount of RAM when RTA is installed with Filtering Service or Network Agent on the same machine.

◆ If CPU spikes continue, consider moving RTA to another machine, separate from Filtering Service and Network Agent. This change provides maximum Websense Enterprise system performance.

◆ Memory consumption can be managed via the Real-Time Analyzer system settings. Consult the *Websense Enterprise Administration Guide* for more information.

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

HTTP Reporting

Certain integration products can track HTTP requests and pass that information to Websense Enterprise. Websense Enterprise uses this data create logs to track the HTTP traffic.

Network Agent also can track bandwidth activity: bytes sent and received, and the duration for each permitted Internet request. Network Agent can then request that Websense Enterprise create a log with this data. If both Network Agent and the integration partner are providing logging data, these activities result in twice the CPU usage by Filtering Service.

Utilizing Network Agent allows the Websense Enterprise to report more HTTP details because the integration does not pass as much information to Websense Enterprise as Network Agent.

To avoid this additional processing, enable *HTTP Reporting* in Network Agent Local Settings dialog box in the Websense Enterprise Manager. With this feature enabled, Websense Enterprise does not log the HTTP requests coming from the integration partner, but instead relies on Network Agent to log that traffic. Refer to the Network Agent chapter in the *Websense Enterprise Administrator's Guide* for more information on configuring Network Agent.

If you plan on to activate full logging capabilities, consider installing Network Agent and Real-Time Analyzer together on a separate machine from Filtering Service. Refer to your *Websense Enterprise Installation Guide* for details.

Database Engine

Log Server and Websense Enterprise Reporter can use either Microsoft Database Engine (MSDE) or Microsoft SQL Server. Websense Enterprise Explorer for Unix uses MySQL. Only *one* Log Server can be installed for each Log Database used in your Websense Enterprise installation.

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 and then archive on a daily or weekly basis. MSDE allows the Log Databases to grow up to 1.5 GB. Upon reaching this maximum size, MSDE automatically 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 your database is frequently rolling over, consider purchasing Microsoft SQL Server 2000 Standard Edition to upgrade your database to a more scalable platform on which to build. Microsoft SQL Server can be optimized, while MSDE cannot. Microsoft SQL Server includes the Microsoft SQL Client Tools that allow you to check the size of a database created in either MSDE or Microsoft SQL.

> **NOTE**
>
> Consult the *Websense Enterprise Reporter Administrator's Guide* for detailed information about selecting the appropriate database engine for your deployment.

◆ Ensure you have applied the latest service packs. Microsoft SQL Server 2000 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 also can be tuned, where as MSDE cannot.

Microsoft SQL Server operations under high loads are resource intensive and can be a point of performance bottleneck for the Websense Enterprise system. Performance can be improved by implementing one or more of the following:

◆ Improve CPU performance to alleviate CPU contention between Log Server and the Microsoft SQL Server:

- Increase the CPU speed and/or number of CPUs on the system.
- Consider installing the Microsoft SQL Server on its own dedicated machine.

◆ Consider disk space usage and requirements, and ensure adequate space is available to accommodate the growth of the database.

◆ Use a disk array controller with multiple drives to increase I/O bandwidth.

◆ Run Microsoft SQL Server and the Log Server on separate machines if Websense Enterprise is monitoring a high volume of Internet traffic.

◆ Increase the RAM on the Microsoft SQL Server machine. By increasing the RAM, you reduce time-consuming disk I/O operations.

> **NOTE**
> Consult the Microsoft Web site for more detailed information on Microsoft SQL Server performance optimization.

MySQL

Websense Enterprise Explorer for Unix requires MySQL. The MySQL database must be a licensed installation of v4.0x or v4.1. MySQL requires that a license be purchased if the database is installed for commercial use.

For more information on MySQL, go to MySQL web site: 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 five 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.

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).

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 one (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 varies, depending on Internet usage.

Logging Hits

If the Log Database is configured to record each hit, calculate the disk space required 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).

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 a 500 user deployment, the Log Database could use 2.5 GB per month.

The Log Database requires 30 GB of disk space for one 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. Turning off full logging decreases the size of each entry and your database by a factor of four, thus saving disk space.

Full URLs are automatically enabled if the WebCatcher module is enabled.

Consolidation

Consolidation helps to reduce the size of the database by recording multiple visits to the same URL by the same user just once. 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 hit. If consolidation is turned off and the user revisits the site later, another hit is logged. With consolidation on, multiple hits or visits to the same site are logged as a single record.

Consolidation is turned *on* by default.

Factors that Impact the Size of the Database

The smaller the database, the faster reports can be run. Some other variables that can impact the size of the database include:

◆ Protocol filtering and logging. If protocol filtering is logged, it will increase the size of the database.

◆ Archiving data on a periodic basis. Log Database Manager can be used to schedule the archiving of the database, to decrease the size of the database.

Logging Database Strategy

Using the calculations provided for logging hits and visits, without logging full URLs, the data for one year would require:

◆ 600 GB for hits
◆ 120 GB for visits

Such large amounts of data would significantly slow down reporting functions. Also, you should not keep live data for one year due to the large amount of disk space required.

As an alternative, you can use the Websense Enterprise Database Manager to archive older data, such as data older than three months. The older data could be written to a secondary database, that could be compressed, backed up, and archived for one year. The primary database would continue to be used for logging and generating reports.

✔ **NOTE**
Reports cannot be run from compressed data.

For instructions on the Database Manager, refer to the *Websense Enterprise v5.5 Reporting Administrator's Guide*.

Network Configuration

Websense Enterprise can be deployed across virtually any type of network. When all Websense Enterprise components are installed on one machine, this machine must be able to receive Internet requests from the integration (firewalls, proxy server) and see the network traffic for those workstations that Network Agent is defined to monitor. Network Agent monitors protocols by *sniffing* the wire. Internet requests are routed to Websense Enterprise by the Websense integration product (a firewall, router, proxy server, or network appliance). In the Stand-Alone Edition, Network Agent provides the HTTP, HTTPS and FTP Internet filtering. When Websense Enterprise components are deployed across multiple machines in a network, Network Agent must be installed where can it see all Internet traffic.

How Websense Enterprise 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 whole network via a central connection point, such as a router, bridge, switch or 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 one Network Agent, while multiple segments may require multiple Network Agent to ensure that each segment is monitored.

Single Segment Network

A single segment network is a logically connected nodes operating in the same portion of the network. These nodes can be PCs, printers, other networked devices. In a such a network, Websense Enterprise and Network Agent must be installed where they can monitor Internet traffic across the entire network. Figure 13 shows the Websense Enterprise Stand-Alone Edition installed in a central location to see both HTTP and non-HTTP protocol traffic.
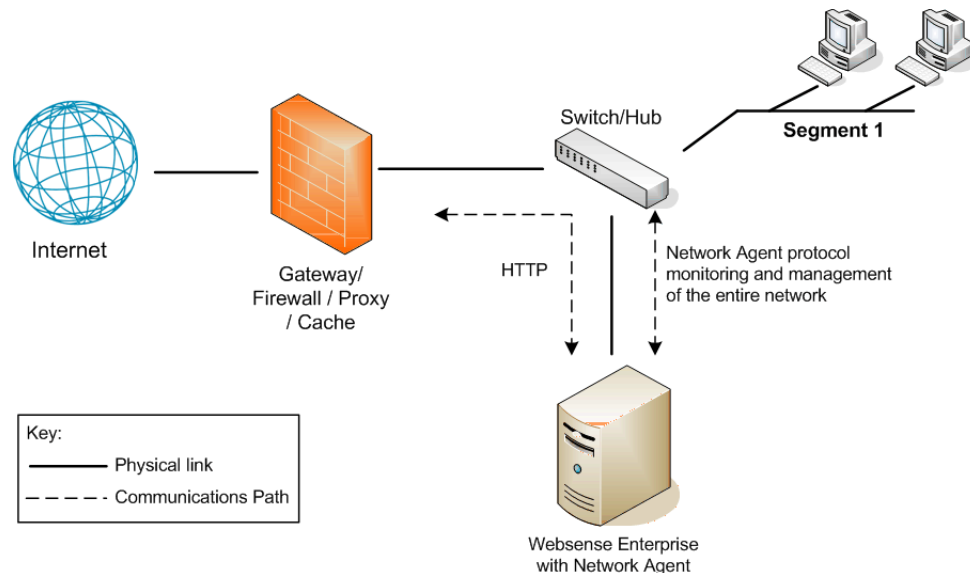
Figure 13 Websense Enterprise in a Single Segment Network

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 may serve as traffic control, preventing unneeded traffic from being sent to a segment. In this environment, you must plan where to deploy the Websense Enterprise components 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 and communicate with Network Agent. Each Network Agent must be able to see all traffic on the segment or segments that it is designated to monitor.

Multiple Network Agents may be needed in a multiple segment network to capture all network traffic. If multiple Network Agents are needed, the machines with Network Agents can be connected at a *single point* on the network or a Network Agent can be installed on each segment to monitor and manage all the traffic on its segment.

> **NOTE**
> A maximum of four (4) Network Agents can be used with each instance of Filtering Service.

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

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 and each Network Agent.

In Figure 14, 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 Enterprise 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 14, the switch is connected to the gateway. This location allows the Network Agents to monitor network traffic for all the network segments. The Network Agents must be configured to monitor only one network segment or range of IP addresses. When setting the IP range for one Network Agent, ensure that the range does not overlap the range covered by another Network Agent.
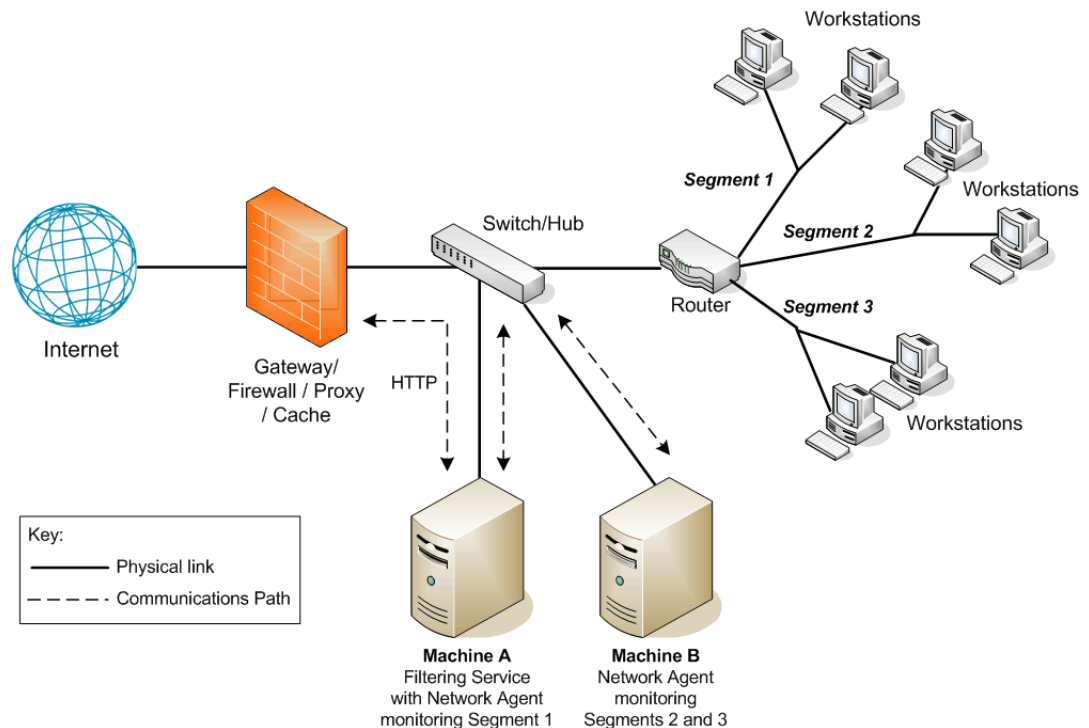
Figure 14 Websense Enterprise in a Multi-Segment Network

Distributed Network Agent Placement

The network in Figure 15 contains a single Filtering Service with three Network Agents, one for each segment of the network. This deployment can be useful for networks with satellite offices, for example.

A maximum of four (4) Network Agents is allowed per each Filtering Service.

Filtering Service (Machine C) must be installed in a location where it is able to receive and manage traffic 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 (Machine 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 of the traffic passing through that switch.

In the diagram below, 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.
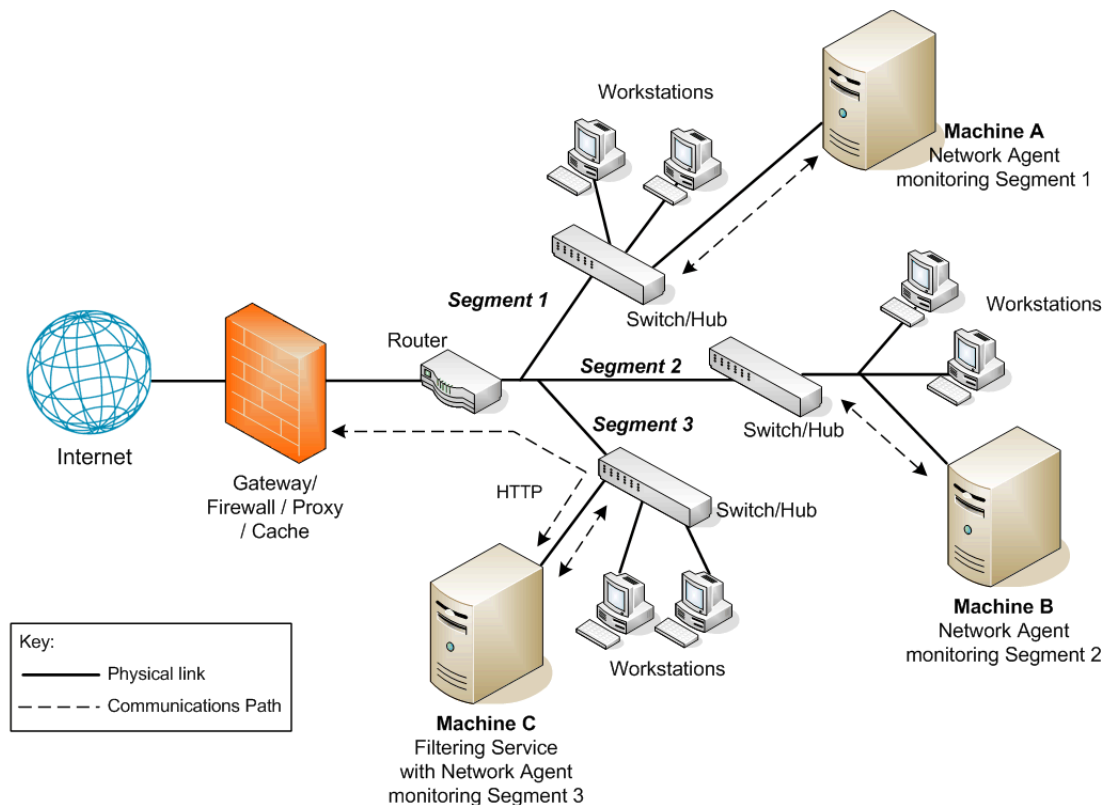
Figure 15 Multiple Network Agents in a Multi-Segmented Network

Configuring Network Agent

Network Agent must be installed in a location where it can monitor all network traffic going out to the Internet and replies coming back from the Internet. This monitoring must be done on the *internal* side of the firewall.

> *i* **IMPORTANT**
> Network Agent can only monitor and manage traffic that passes through the network device (switch, hub, or gateway) to which it is attached. This chapter discusses various network configurations with Network Agent.

The machine running a Network Agent can access the network via a switch or a hub, as discussed in the *Hub Configuration*, page 79 and *Switched Configuration*, page 80 sections. Network Agent can be installed on the same machine as an integration product, as discussed in the *Gateway Configuration* section of this chapter.

Network Agent Location

Network Agent must be able to see all Internet traffic on the network to filter effectively. This configuration can mean multiple installations of Network Agent in some cases.

For example, it can be useful to have multiple Network Agents for larger or high-traffic organizations. In this situation, you might place Network Agents on each of your internal network segments, as an example. A maximum of four (4) Network Agents is allowed per each Filtering Service.

> *i* **IMPORTANT**
> Do NOT install Network Agent on a machine running a firewall.

Here are some common scenarios for Network Agent installation:

◆ On a dedicated machine, connected to an unmanaged, unswitched hub located between an external router and your network.

◆ Connected to a switch or router. You must 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. 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 all the other ports. The span port mirrors all the traffic that passes through that particular switch.

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

If the machine running Network Agent is connected to multiple ports on the switch or router via multiple network interface cards (NICs), then the NICs together must be able to see all network traffic. See *Using Multiple NICs*, page 85 for information.

The diagrams in this chapter illustrate various methods in which Network Agent can interface with your network. Multiple Network Agents may be required under some configuration scenarios. See *Chapter 3 Network Configuration* for more information.

Network Agent Settings

Network Agent settings are configured in Websense Enterprise Manager. You must specify global settings (for all Network Agents, if there is more than one), 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 in the system and determines what every Network Agent installed should do with requests to machines in your network.

Global Settings define your network by providing a list of IP addresses or IP address ranges in your network that the Network Agents need to monitor.

By default, Network Agent does not monitor site, protocol, or application requests to machines within the network.

◆ *Local Settings* — apply to individual Network Agents or NICs. Local Settings identify 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 your internal network. By default, Network Agent monitors requests from all internal machines it sees. Websense Enterprise filters Internet content requested from these machines. Local Settings allow you to configure how much of the internal network each Agent *sees*. Then, you can optionally specify any desired exceptions to the default monitoring behavior. You can also customize Network Agent's behavior for machines using multiple Network Interface Cards (NICs).

Hub Configuration

At the simplest level, a network hub provides a central connection 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 of the ports to see all of the traffic. Network Agent must be able to see the traffic for the segments it is assigned to monitor.
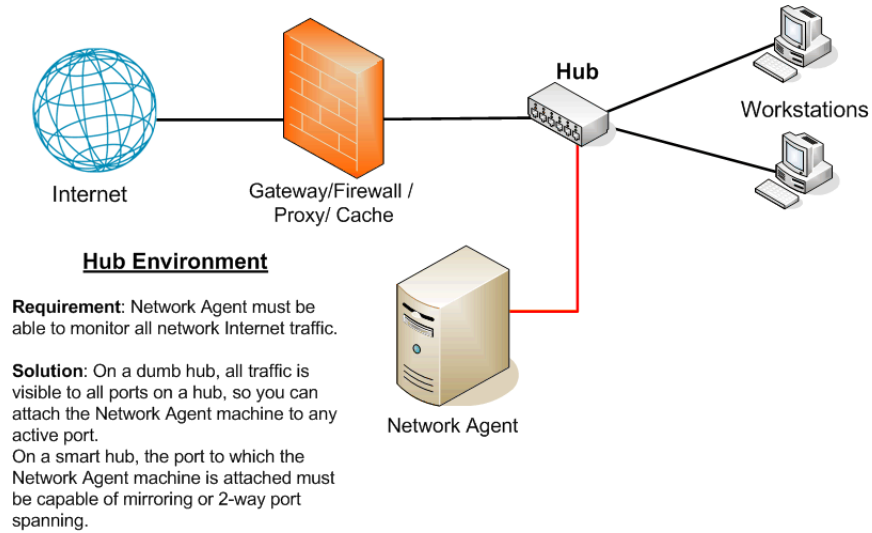
Figure 16 Network Agent Configured through a Hub

Switched Configuration

A switch is a hub 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 with Network Agent must be connected at a point where it can monitor all Internet traffic for your 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 all the other ports. The span port mirrors all the traffic that passes through that particular switch.

> ✔ **NOTE**
>
> Not all switches support port spanning or 2-way port mirroring. Contact your switch vendor to determine if your 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 report to Filtering Service, resulting in blank or inaccurate reports and possibly faulty protocol management and bandwidth optimization.

Figure 17 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.
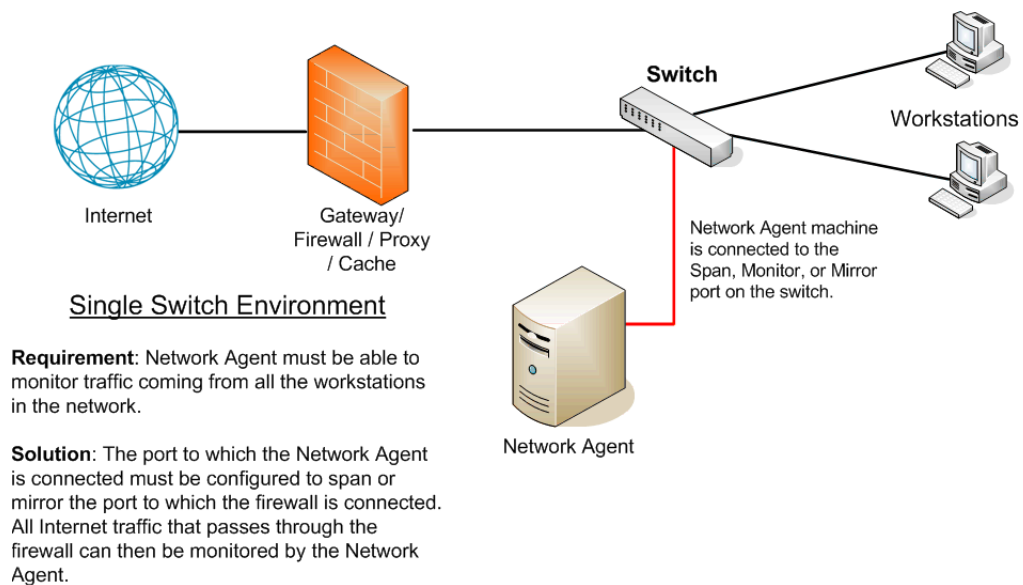
Figure 17 Simple Deployment in a Switched Environment

Figure 18 shows the addition of two more switches, Switch #1 and Switch #2, to create two 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.
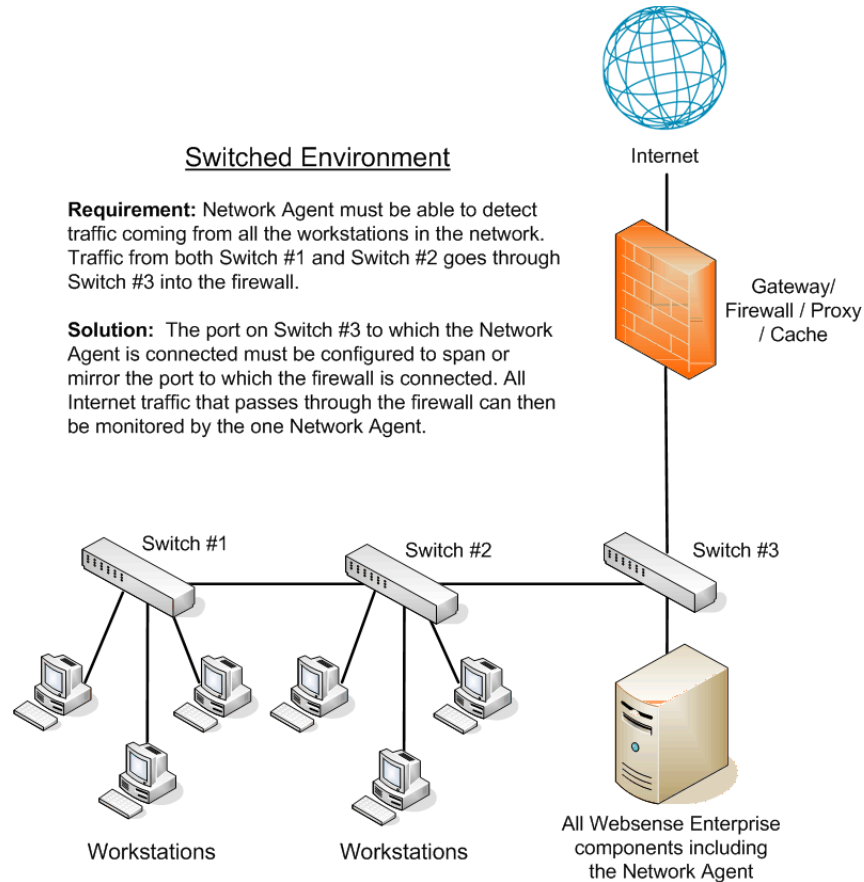
Figure 18 Multiple Subnets in a Switched Environment

Like Figure 18, Figure 19 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.
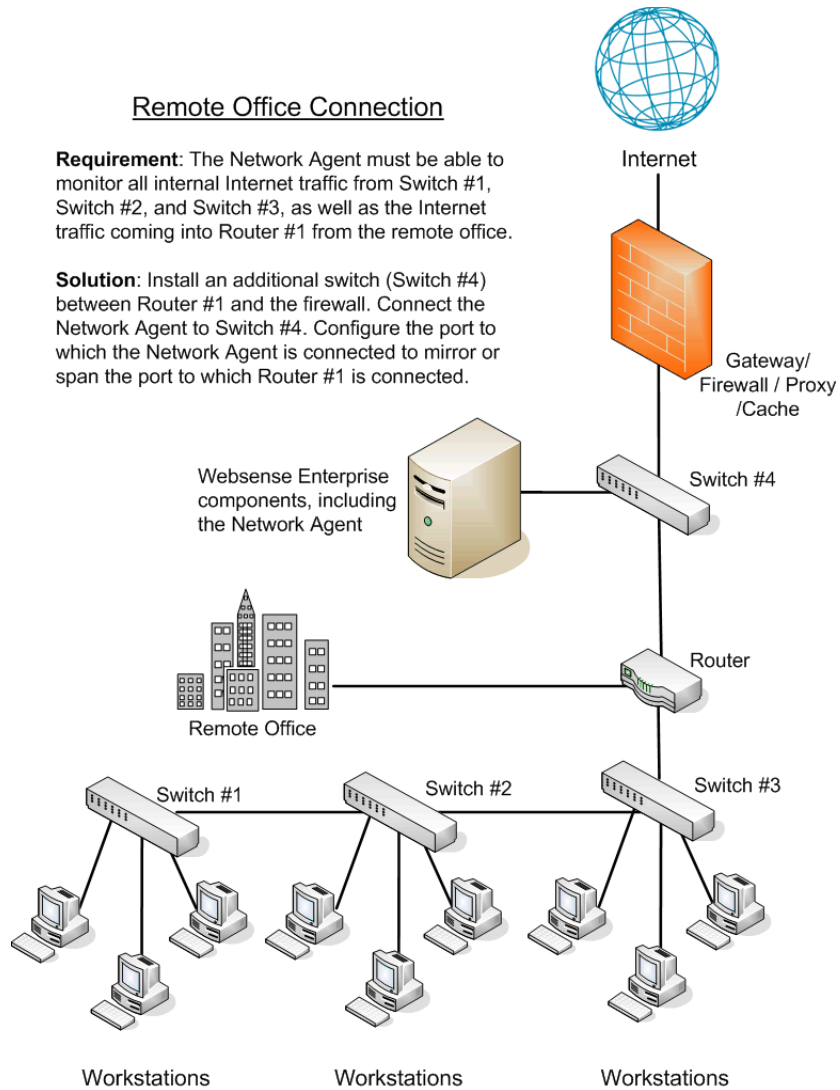
Figure 19 Switched Environment with a Remote Office Connection

Switched Networks with Multiple Network Agents

On a busy network, you may need to install multiple Network Agents and assign them to monitor various IP address ranges in your network. Figure 20 illustrates a network in which individual Network Agents monitor their network segments.

If you install multiple Network Agents, consider the following:

◆ A maximum of four (4) Network Agents is allowed per each Filtering Service.

◆ Deploy the Network Agents so that together they can filter the entire network. Partial deployment results in the loss of filtering capabilities and log data for the network segments not watched by Network Agent. A maximum of four Network Agents can be deployed per Filtering Service.

◆ IP address ranges for the each Network Agent must not overlap. Overlapping IP ranges result in inaccurate network bandwidth measurements and improper bandwidth-based filtering.

For example, if the IP addresses in your network range from 111.222.333.0 to 111.222.333.20, one Network Agent should cover 111.222.333.0 to 111.222.333.10 and the second Network Agent should cover 111.222.333.11 to 111.222.333.20.

Each of the Network Agents' IP address ranges are entered in the Local Settings dialog box that is accessed through Websense Enterprise Manager. For more information on configuring Network Agent, refer to the *Network Agent* chapter in the *Websense Enterprise Administrator's Guide*.
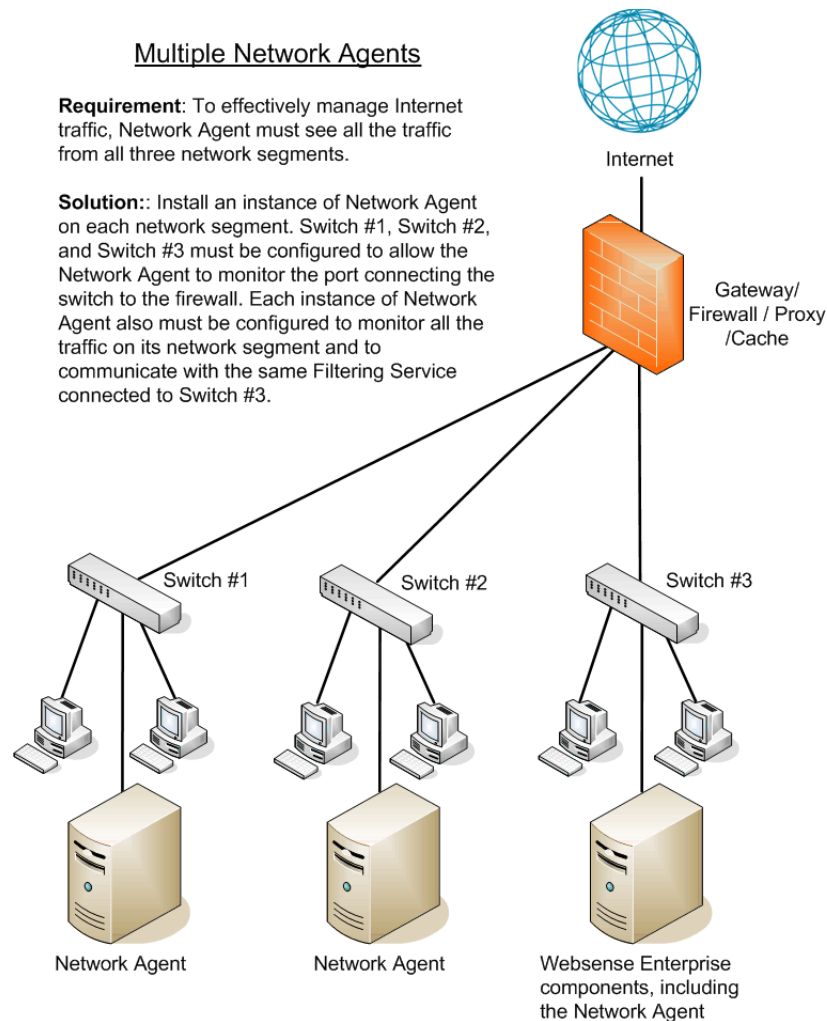
Figure 20 Multiple Network Agents in a Switched Environment

Gateway Configuration

A gateway provides a connection between two networks, with either the same or different protocols. The gateway can provide the connection between your 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 supported on the Windows operating system only and should only be 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 21 shows Network Agent monitoring the Internet traffic at the proxy gateway or caching appliance directly attached to the firewall.
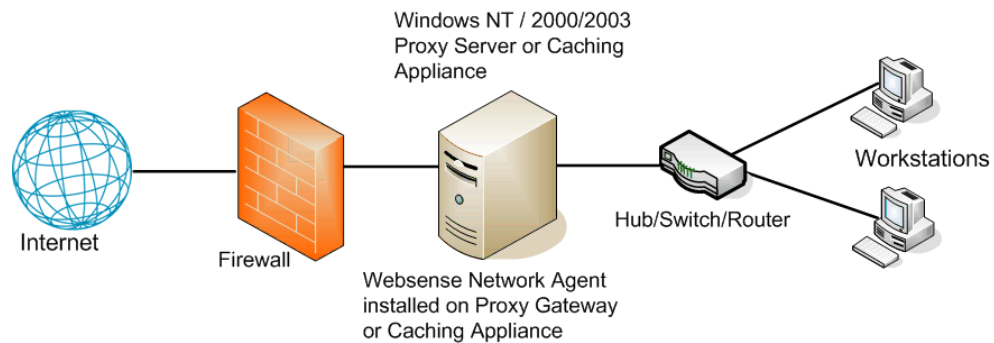
Figure 21 Network Agent Installed on the Gateway

Firewall Recommendations

Network Agent needs to monitor Internet requests on the *internal* network from inside of the firewall. *Do not* install Network Agent on a firewall.

Using Multiple NICs

Network Agent is capable of working with multiple network interface cards (NICs) if they are installed in the machine on which Network Agent is running.

If the machine running Network Agent has multiple NICs installed:

◆ Only one instance of Network Agent needs to be installed on the machine running with multiple NICs.

◆ Separate NICs can be assigned to monitor and to block.

  ■ The NICs must be in the same network segment in order for one NIC to be used for monitoring and another to be used for blocking

  ■ If the Network Agent machine has multiple NICs performing monitoring, each NIC used for blocking can only be associated with one monitoring NIC.

    For example: If network segment A is different from network segment B, then capturing NIC1 must use only NIC1 for blocking, and capturing NIC2 must use only NIC2 for blocking.

  ■ The port used for monitoring must be configured to use either mirroring or 2-way port spanning, plus the card must be in *promiscuous* mode, so that Network Agent can detect Internet requests from all the workstations. Contact your NIC vendor to determine if promiscuous mode is supported, and if so, how it can be enabled.

  ■ The NIC used for monitoring can be set for *stealth mode*, but must be used with a NIC that is assigned an IP address for communication. See your *Websense Enterprise Installation Guide* for instructions to configure the stealth mode.

◆ The NICs can also be used to monitor different segments of the network.

  ■ At least one of the NICs must be assigned for blocking.

During the installation, you are prompted to identify the NIC that Websense Enterprise will use for communication. If Network Agent is being installed, you are also prompted to identify the NIC that you want Network Agent to use to monitor Internet traffic. For more information, see the *Websense Enterprise Installation Guide* for your integration.
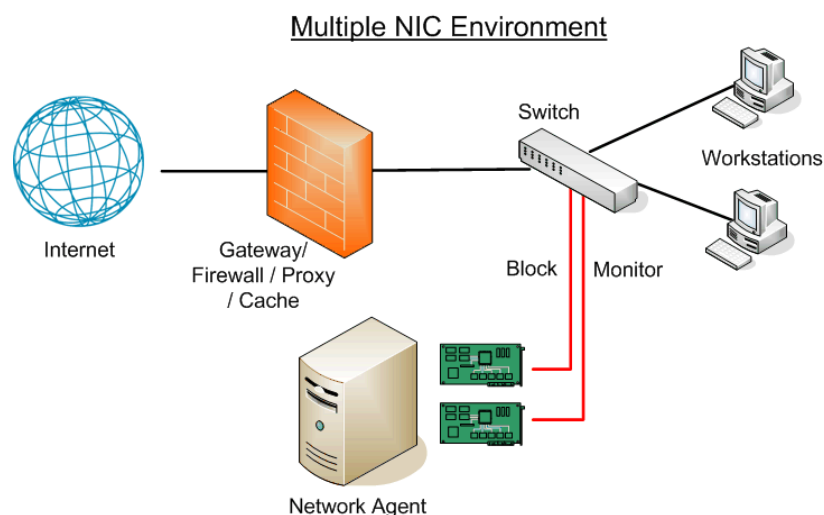
Figure 22 Dual NIC Configuration

Implementing Websense Enterprise within Distributed Enterprises

Distributed enterprises are corporations with large numbers of remote locations, ranging from dozens to thousands of small offices. Typically, between 5 and 50 employees work at each remote office, many of which have Internet access, and no dedicated IT staff. Some of these organizations use a decentralized network topology that provides each remote office with its own Internet connection. The challenge then becomes to apply consistent, cost effective filtering of Internet requests across the entire organization. Websense Enterprise servers, deployed regionally and communicating over the Internet, can apply uniform filtering policies to hundreds of remote offices from a central location.

✓ NOTE

This chapter discusses how Websense Enterprise can be deployed to effectively filter a distributed enterprise network. For more specific recommendations related to how the components should be deployed and the types of machines on which they should be deployed, refer to *Chapter 2, General Deployment Recommendations*.

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. This is usually accomplished through a small office/home office (SOHO) firewall connected to an ISDN, DSL/cable, or T1 connection. Except for corporate application data that may traverse a VPN connection, each outbound Internet request from a remote office is sent through a local Internet service provider (ISP) to the Internet.

, shows the network topology of this type of remote office.
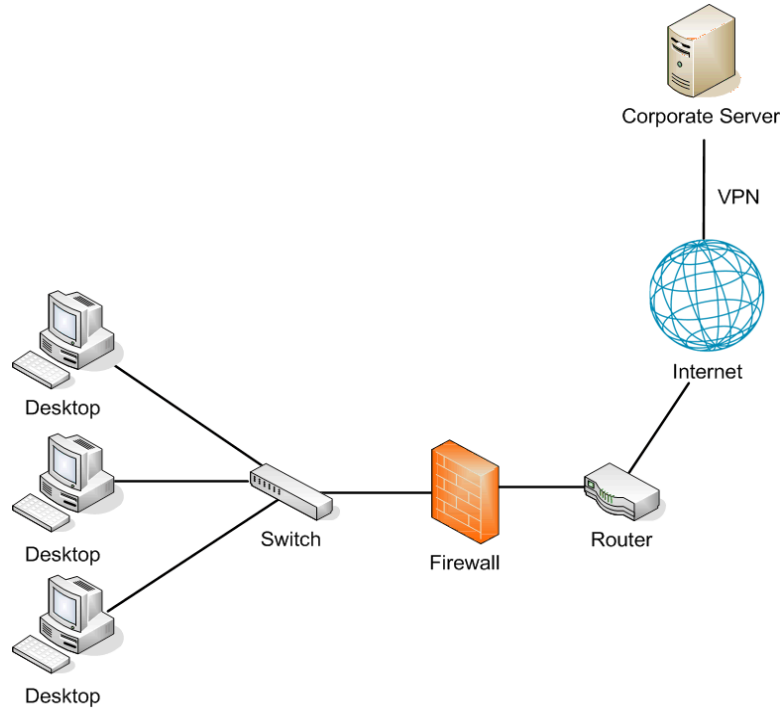
Figure 23 Remote Office Topology in a Decentralized Network

A large distributed enterprise can have hundreds, or even thousands, of such remote offices connected to the corporate network through the Internet.
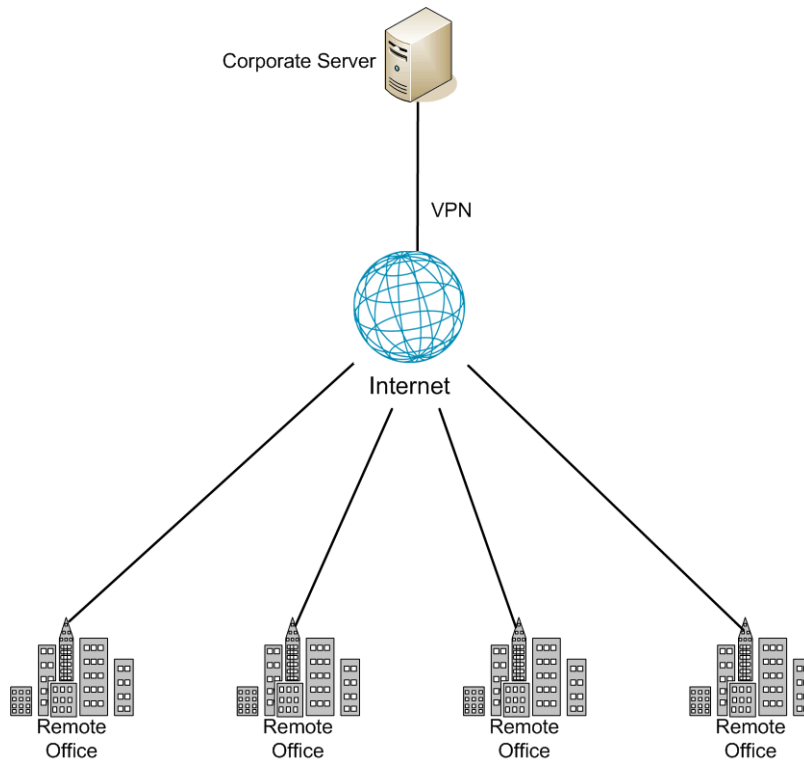
Figure 24 Distributed Enterprise

Distributed enterprises that employ remote Internet connectivity have a complex set of filtering considerations.

- ◆ Remote offices must have Internet access.
- ◆ Internet access is provided by independent ISPs, 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 remote office.
- ◆ Given the relative low speed of the Internet connection at each remote office, a moderate level of additional latency caused by the filtering product is acceptable.
- ◆ All remote offices can be filtered according to the same acceptable-use policies.

Deploying Websense Enterprise in a Distributed Enterprise

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

Rather than deploying Websense Enterprise at each remote office firewall, companies can deploy a Websense machine in a location geographically central to each of its remote offices. Since Websense Enterprise is accessible from the Internet, the Websense machine should be protected by a firewall that allows URL lookup requests to pass through. The SOHO firewall at each remote office is then configured to communicate with the centralized Websense machine instead of a local Websense machine. To the firewall, there is no distinction between accessing Websense Enterprise over the Internet and accessing it through a LAN connection at a remote office.

Figure 25 shows how a remote office can communicate with Websense Enterprise over the Internet.
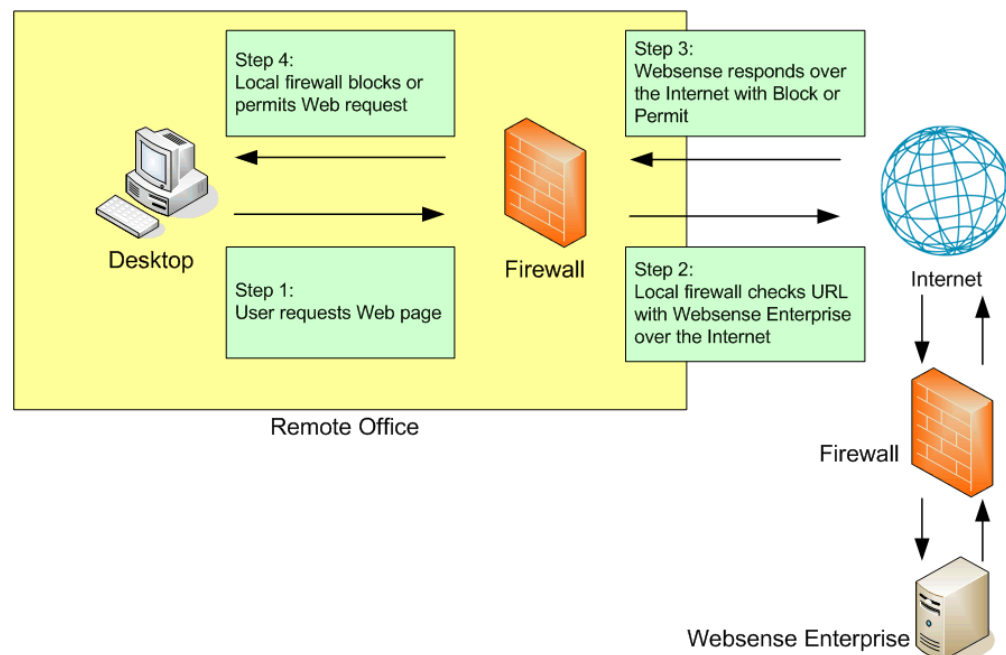
Figure 25 Remote Office Communication Strategy

An entire distributed enterprise, with multiple remote offices, might be deployed as follows.
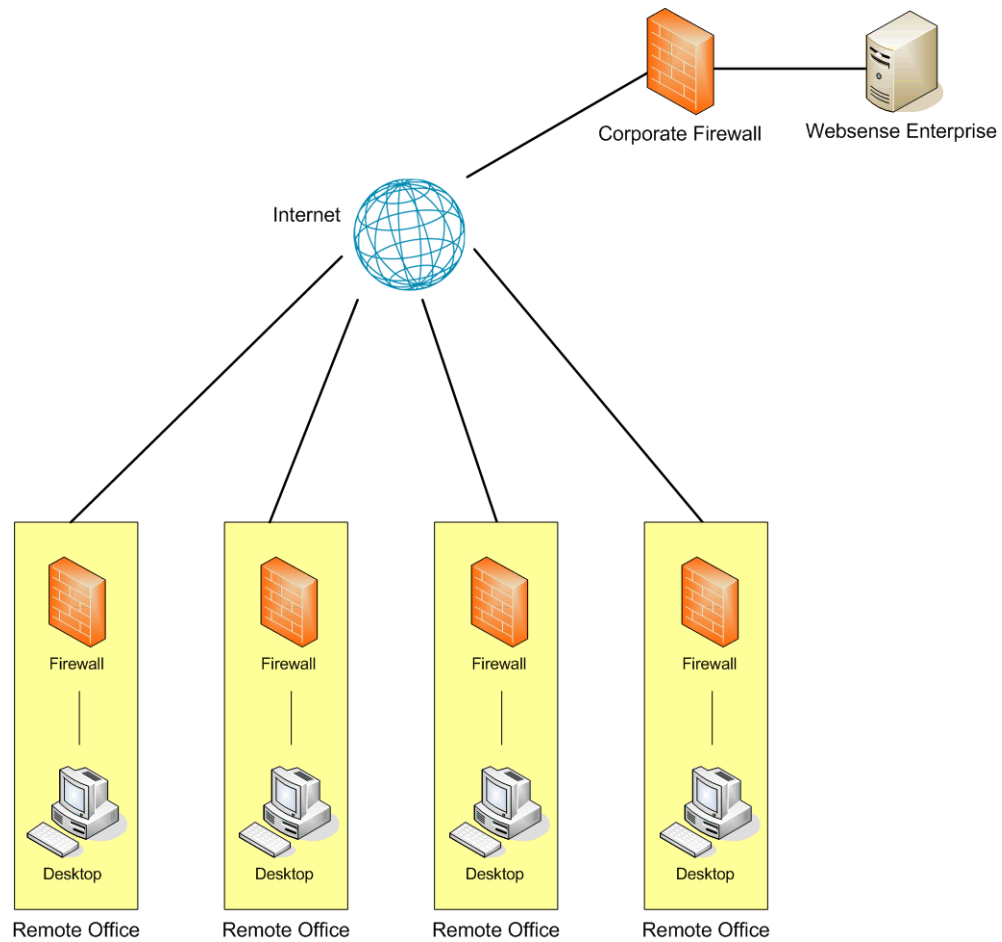
Figure 26 Distributed Enterprise Communicating with Websense Enterprise

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

   http://www.websense.com/products/integrations/index.cfm

This approach provides distributed enterprises with a Websense Enterprise solution for each remote office while eliminating the need for a separate Websense machine at each location. Centralized filtering benefits an organization by:

◆   Providing uniform filtering policies at each remote office.

◆   Eliminating the cost of additional hardware to provide filtering servers at each remote office.

◆   Allowing the enterprise to centrally configure, administer, and maintain a limited number of Websense server machines.

Deployment Models

Different deployment approaches may be required for enterprises with different needs. For example, an organization with 50 remote offices, all located in the same general region, will deploy Websense Enterprise differently than a company with remote offices spread throughout the world. This section discusses the three general deployment models available for distributed enterprises:

◆ Remote offices located within one region
◆ Remote offices located within one region, with a growing number of employees and/or offices
◆ Remote offices located nationally or globally

Regional Offices

The simplest Websense Enterprise deployment for a distributed enterprise is for a network composed of remote offices in a single region, such as San Diego County. Most organizations in this situation can deploy a single Websense machine, centrally located within that region, to provide filtering for all of their employees. See Figure 26, page 90.

Expanding Regional Offices

Some organizations deploy Websense Enterprise within a given region and later decide to increase the number of remote offices in that area. In this case, the organization can make two changes to compensate for the additional offices and employees.

◆ **Improve the performance of the existing Websense machine**: Increasing the RAM and CPU of the server running Websense Enterprise allows it to respond to larger amounts of users without additional latency. This is a good first step if the organization adds moderate head count or a few more offices. See *Chapter 2, General Deployment Recommendations* for hardware recommendations for various network sizes.

◆ **Deploy an additional Websense machine**: If significant numbers of new offices are added, however, the organization should deploy an additional Websense Enterprise server and distribute the remote offices between the two servers. This balances the load and provides optimum performance for each remote office. See Figure 27, page 92. See *Chapter 2, General Deployment Recommendations* for different scenarios for deploying Websense Enterprise components.
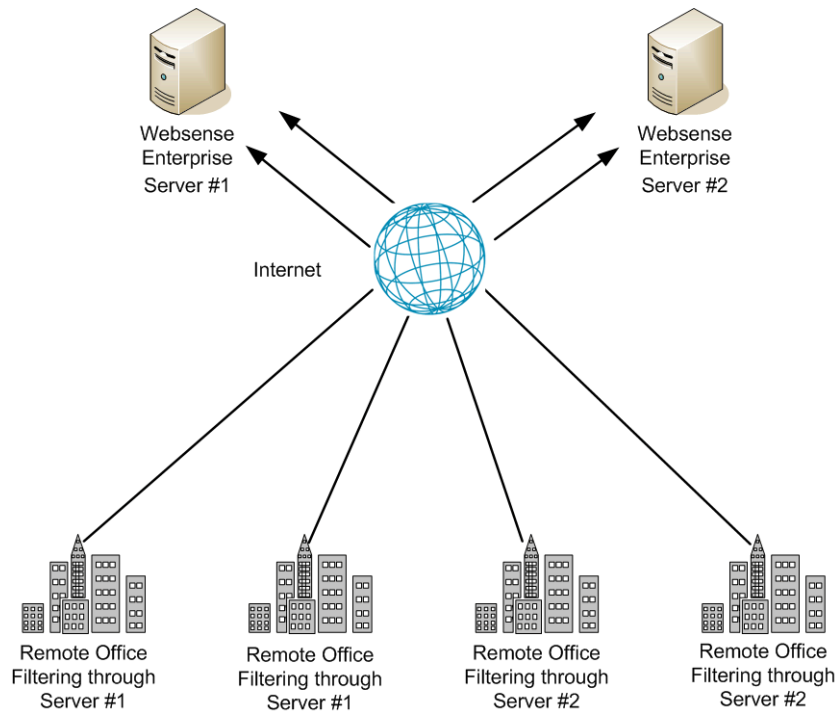
Figure 27 Adding Websense Enterprise Servers

Additional copies of Websense Enterprise 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, one or two Websense Enterprise servers would not suffice for the following reasons.

◆ Each remote office would be geographically distant from the Websense machine, causing each request lookup to have to travel further over the Internet to reach Websense Enterprise. This increases the total latency of the solution and may lead to slower Internet access for end users.

◆ Large numbers of employees would generate more Internet requests than recommended for one or two Websense machines, leading to delays in returning Web pages to requesting workstations.

Organizations in these situations should divide their offices into logical regions and deploy Websense Enterprise 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. They can then select a central office in each of the three regions in which to deploy a high-end Websense Enterprise server.

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 Websense Enterprise servers within that one area. Or, an enterprise may only have three offices in California with 100 to 250 employees at each office. In this case, a single Websense machine might be deployed for all three offices. This enterprise should also consider deploying Websense Enterprise 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 their Websense representative to plan their rollout strategy prior to deployment.

Secure VPN Connections

Some firewalls allow administrators to set up a secure VPN connection between the remote office firewalls and Websense Enterprise for URL lookup requests and replies. Permitted requests then are fulfilled directly from the Internet, providing an optimum combination of speed and security. See your firewall documentation for more information and to determine if your 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 *Chapter 2, General Deployment Recommendations* for information on deploying the RADIUS Agent. See your *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 Websense Enterprise servers 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 Websense Enterprise server may be exceeded. By default, each Websense Enterprise server machine 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 information for calculating the number of connections required for a Websense Enterprise deployment and the number of Websense machines that will be 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 your integration product to determine how to limit TCP connections. If your integration product cannot be reconfigured to open fewer connections, you may have to add additional Websense machines to handle the extra connections requested by the remote offices' firewalls.

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

Use the following formula to calculate the number of Websense connections required to filter Internet requests from remote offices.

Websense connections required =
{*# of integration machines*} x {*# of connections opened by each integration machine*}

To determine the number of Websense server machines your enterprise will need to filter the traffic from remote offices, divide the number of Websense connections required by the number of connections each Websense machine will be configured to accept.

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

System requirements for a high performance Websense machine are as follows:

- 2.0 GHz processor
- 2GB 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. Fewer connections require additional Websense machines 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 (one) for this example but may need to be higher as the load increases.

10 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Websense Machines Required
1000	1	1000	1
2000	1	1000	2
5000	1	1250	4

25 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Websense Machines Required
1000	1	1000	1
2000	1	1000	2
5000	1	1250	4

50 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Websense Machines Required
1000	1	1000	1-2
2000	1	1000	2-3
5000	1	1250	7-8

100 Users per Firewall

Number of Firewalls	Connections from Integration	Connections Allowed by Websense	Websense Machines Required
1000	1	500	2
2000	1	500	4
5000	1	500	10-11

Configuring Websense Connections

To increase the number of connections that Websense will accept:

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 the following 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, refer to the *Websense Enterprise v5.5 Administrator's Guide*.

Optimizing Performance

Websense Enterprise 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 a Websense Enterprise server, in most situations end users at remote offices are not aware of the filtering process unless they are blocked from a Web site. When deployed according to the guidelines listed here, end users should experience no more than one second of additional delay per request. Total latency, however, depends heavily on three factors:

◆ Speed (bandwidth) of the Internet connection at each remote office
◆ Distance from the remote office to the Websense machine
◆ Number of users and connections to the Websense machine
◆ Speed of the Websense machine

Internet Connection Speed

Overall filtering performance is highly 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 sufficiently fast to provide responsive URL lookups through Websense Enterprise. A 56K dial-up modem, on the other hand, is not recommended because of the additional time it would take 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 Enterprise Server

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 traverse, 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 Websense Enterprise server and the source of the request. The closer the server is to a remote office, the faster the Websense lookup and overall performance will be for the end user.

Websense recommends that distributed enterprises deploy their Websense Enterprise server 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 100ms 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), you can run:

◆ `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 superuser 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

See the respective Linux or UNIX man pages for more information on these commands and their options.

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 Enterprise server. 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 Enterprise, 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 Enterprise for distributed enterprises. NetScreen, Check Point, and Cisco firewalls cache the responses received from Websense Enterprise. This cache keeps track of common Web requests and the Websense response (Permit/Block) so the firewall does not have to check with Websense Enterprise for every requested Web page.

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

Websense recommends using a firewall from one of these three vendors when configuring remote offices for filtering. For information on determining if caching is appropriate for your environment, refer to the appropriate Websense Enterprise installation guide.

Best Practices for Distributed Enterprises

Enterprises with multiple remote offices often find it cost and time prohibitive to deploy Websense Enterprise 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 Enterprise in an efficient, high-performance, and cost-effective manner.

The following points summarize the main considerations in deploying Websense Enterprise in a distributed enterprise:

◆ **Response caching**: Deploy Websense with a firewall that supports Websense response caching (such as from Juniper, Check Point, Cisco, and SonicWall). Other network security products integrated with Websense Enterprise may also be used, but end-user performance may be higher with firewalls from one of these four vendors.

◆ **Distance to the Websense Enterprise server**: Deploy a Websense Enterprise server no more than 20 hops and 100ms from remote offices. Organizations with offices spread over a wider area should deploy one or more Websense Enterprise servers 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 your remote office firewalls. Increase the number of connections that Websense Enterprise will accept to accommodate the number of connections opened by the remote firewalls. Provide enough Websense Enterprise servers 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 Enterprise in distributed enterprises.

◆ **Server speed**: Websense Enterprise servers 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 in enabled,

and a performance problem with the Internet causes Websense lookups to take longer than normal, users at each remote office will still be able to access the Internet. Filtering is automatically 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 Enterprise server for maximum security (if supported by the firewall).

Minimum System Requirements for Websense Enterprise Components

This appendix provides the minimum requirements needed to run each component of Websense Enterprise.

These components generally are installed together in various scenarios, depending on the number of Internet requests generated in a network. In the event a component needs to be installed on a separate machine, this appendix provides the minimum requirements needed for running each component. The minimum requirements may not be suitable in all environments, as requirements increase with greater Internet usage, such as in larger networks. See *Chapter 2 General Deployment Recommendations* for specific deployment recommendations.

For component definitions, see Table 1, Websense Enterprise Components, on page 12.

To verify the required operating system versions for each component, see Table 4, Operating Systems, on page 18. This chapter contains two main sections: *Websense Enterprise Components* and *Websense Enterprise Reporting Components*, page 103.

Websense Enterprise Components

This section contains the minimum requirements for the Websense Enterprise components.

DC Agent

The DC Agent runs on Windows 2000 Server and Windows 2003 Server machines only, and requires:

◆ Pentium 4, or greater
◆ 256 MB of RAM

eDirectory Agent

The eDirectory Agent runs on Windows, Linux and Solaris machines.

Windows

◆ Pentium 4, or greater
◆ 256 MB of RAM

Linux

◆ Pentium 4, or greater
◆ 256 MB RAM

Solaris

◆ Sun UltraSPARC IIIi
◆ 1 GB RAM or more

Filtering Service

System requirements are listed separately for Windows and Linux machines.

> ✔ **NOTE**
>
> Virtual Memory should be set to less than 1.5 times the amount of RAM installed. This setting only applies to the Filtering Service machine that downloads the Websense Master Database.

Windows

- ◆ Pentium 4, or greater
- ◆ 512 MB RAM
- ◆ 1 GB of disk space

Linux

- ◆ Pentium 4, or greater
- ◆ 512 MB RAM
- ◆ 1 GB of disk space

Solaris

- ◆ UltraSPARC IIIi
- ◆ 512 MB RAM
- ◆ 1 GB of disk space

Policy Server

System requirements are listed separately for Windows, Solaris, and Linux machines.

Windows

- ◆ Pentium 4, or greater
- ◆ 512 MB RAM or more
- ◆ 512 MB GB of hard disk space

Linux

- ◆ Pentium 4, or greater
- ◆ 512 MB RAM
- ◆ 512 MB of hard disk space

Solaris

- ◆ UltraSPARC IIIi
- ◆ 512 MB RAM or more
- ◆ 512 MB of hard disk space

Network Agent

Network Agent runs on Windows, Solaris and Linux. For the most reliable performance, install Network Agent on an Ethernet network. Network Agent must have bidirectional access for both monitoring and filtering. Position the machine containing Network Agent to see the Internet requests from the internal network as well as the Internet response to the requesting workstations. See *Chapter 3 Network Configuration* and *Chapter 4 Configuring Network Agent* for more information.

> *i* **IMPORTANT**
> The network interface card (NIC) that you use for Network Agent must be in promiscuous mode. Check with the manufacturer of your interface to determine if your card supports this configuration.

Windows

   ◆ Pentium 4, or greater
   ◆ 256 MB of RAM
   ◆ 10 MB of hard disk space

Linux

   ◆ Pentium 4, or greater
   ◆ 256 MB RAM
   ◆ 10 MB of hard disk space

Solaris

   ◆ UltraSPARC IIIi
   ◆ 256 MB RAM or more
   ◆ 10 MB of hard disk space

RADIUS Agent

The RADIUS Agent runs on Windows, Linux and Solaris machines.

Windows

   ◆ Pentium 4, or greater
   ◆ 256 MB of RAM

Linux

   ◆ Pentium 4, or greater
   ◆ 256 MB RAM

Solaris

   ◆ Sun UltraSPARC IIIi
   ◆ 256 MB RAM

Real-Time Analyzer

Real-Time Analyzer runs on Windows only, and requires:

◆ Pentium 4, or greater
◆ 512 MB RAM
◆ Apache version 2 or higher, or Microsoft IIS version 4.0 and 5.0 server

> ✔ **NOTE**
> If you do not have one of the supported Web servers on your system, the Websense Enterprise installer provides the option of installing Apache.

User Service

User Service can be run on Solaris and Linux operating systems, but must be run on a Windows operating system when the DC Agent is used.

System requirements are listed separately for Windows, Solaris, and Linux.

Windows

◆ Pentium 4, or greater
◆ 512 MB RAM or more

Linux

◆ Pentium 4, or greater
◆ 512 MB RAM

Solaris

◆ UltraSPARC IIIi
◆ 512 MB RAM or more

Websense Enterprise Manager

The requirements are listed separately for Windows and Solaris installations. A Websense Enterprise Manager installed on a Windows or Solaris machine can configure a Policy Server installed on a Linux machine. Websense Enterprise Manager does not run on Linux.

Windows - all versions

◆ Pentium 4, or greater
◆ 256 MB RAM
◆ Internet Explorer or Netscape with Java support enabled (required to view online Help)
◆ Color depth set to 8-bit (256 colors) or greater
◆ 130 MB of free disk space

Solaris

The Websense Enterprise Manager cannot run on a non-GUI Solaris system. To run the Manager, you must have Common Desktop Environment (CDE), Java Virtual Machine (JVM) and a browser.

◆ UltraSPARC IIIi
◆ 256 MB RAM
◆ Internet Explorer or Netscape with Java support enabled (required to view online Help)
◆ Color depth set to 8-bit (256 colors) or greater
◆ 130 MB of disk space

Websense Enterprise Reporting Components

This section contains the minimum requirements for the Websense Enterprise reporting components.

Database Engine

The system requirements vary according to the database engine you use. Reporter works with either Microsoft Data Engine (MSDE) or Microsoft SQL Server. Websense recommends using MSDE in organizations with less Internet activity, and Microsoft SQL Server in organizations with higher volume.

The following database engines are supported:

◆ MSDE v2000 or higher. Other versions of MSDE are not supported. If you are currently using MSDE v7, upgrading to this version is supported
◆ SQL Server v7 or v2000 or higher
◆ Appropriate ODBC driver for the database version

MSDE

◆ Pentium 4, or greater
◆ 256 MB of RAM
◆ Windows 2000 Server, or Advanced Server (Service Pack 1), Windows 2003
◆ 3 GB disk space recommended (for one database)
◆ Microsoft Internet Explorer version 5.5 or later

Microsoft SQL Server

Enterprise Reporting supports Microsoft SQL Server 7.0 (Service Pack 1 or higher) and Microsoft SQL Server 2000 (Service Pack 1 or higher). Other versions of Microsoft SQL Server are not supported.

◆ 512 MB of RAM
◆ Windows 2000, Server, or Advanced Server (Service Pack 1), Windows 2003 Enterprise and Standard editions
◆ Microsoft Internet Explorer version 5.5 or later

Refer to Microsoft SQL Server documentation for more detailed system requirements.

Log Database

The Log Database requirements are dependant upon the database engine, MSDE or Microsoft SQL.

Log Database Manager

Log Database Manager must be installed on the same machine as Log Server.

◆ Websense Enterprise v5.5
◆ Websense Enterprise Reporter v5.5
◆ RAM on PC client machine: 256 MB minimum, 512 MB recommended
◆ Database Engine: MSDE v2000 or Microsoft SQL Server v7 or Microsoft SQL Server v2000
◆ Web Server: Microsoft IIS - version 4 or higher, or Apache Web Server - version 2.0.36 or higher
◆ Internet Explorer 5.5 or higher
◆ Archive or purge the Log Database before it consumes more than 50% of the available hard disk space
◆ RAM on client PC (the machine where the browser is used) 256 MB minimum, 512 MB recommended

Log Server

The Log Server can successfully log data for up to 99 Websense Filtering Services. Only one Log Server can be installed for each Log Database used in your installation:

◆ Pentium 4, or greater
◆ 256 MB of RAM
◆ Internet Explorer 5.01 or later

Reporter

◆ Pentium 4, or greater
◆ 256 MB of RAM
◆ Monitor: 800 x 600 or better resolution, with at least 256 colors recommended
◆ Microsoft Internet Explorer version 5.5 or later
◆ Valid print driver, appropriate to the operating system, selected as default. (Check the Websense Technical Support Web (http://www.websense.com/support/) site for a list of print drivers that are known to be incompatible with Reporter. Do not set one of these as the default print driver on the Reporter machine.)

Websense Enterprise Explorer

◆ Pentium 4, or greater
◆ 256 MB RAM
◆ Microsoft Internet Explorer - version 5.5 or higher
◆ Web Server: Microsoft IIS - version 4 or higher, or Apache Web Server - version 2.0.36 or higher
◆ Database Engine: MSDE v2000 or higher, or SQL Server v7 or v2000 or higher
◆ Appropriate ODBC driver for the database version
◆ Directory Service: To use the *Department Level Reporting* feature, you must be using one of the following directory services in your environment:
   ■ NTLM
   ■ Active Directory

Index