



Implementing Websense Enterprise within Distributed Enterprises

Contents

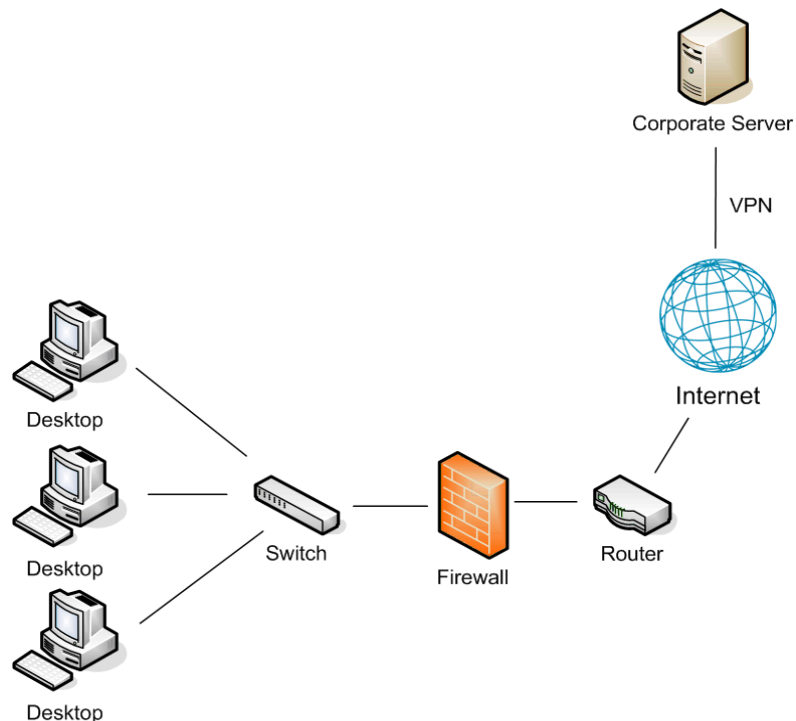
Network Topology	3	Calculating TCP Connections	9
Deploying Websense Enterprise	4	Optimizing Performance	9
Deployment Models	7	Internet Connection Speed	9
Regional Offices	7	Distance from the Websense Enterprise Server	10
Expanding Regional Offices	7	Hardware Performance	10
National or Worldwide Offices	8	Caching	10
Secure VPN Connections	9	Best Practices for Distributed Enterprises	11

Distributed enterprises are corporations with large numbers of remote locations, ranging from dozens to thousands of small offices. Typically, there are between 5 and 50 employees at each remote office, many of whom 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.

Network Topology

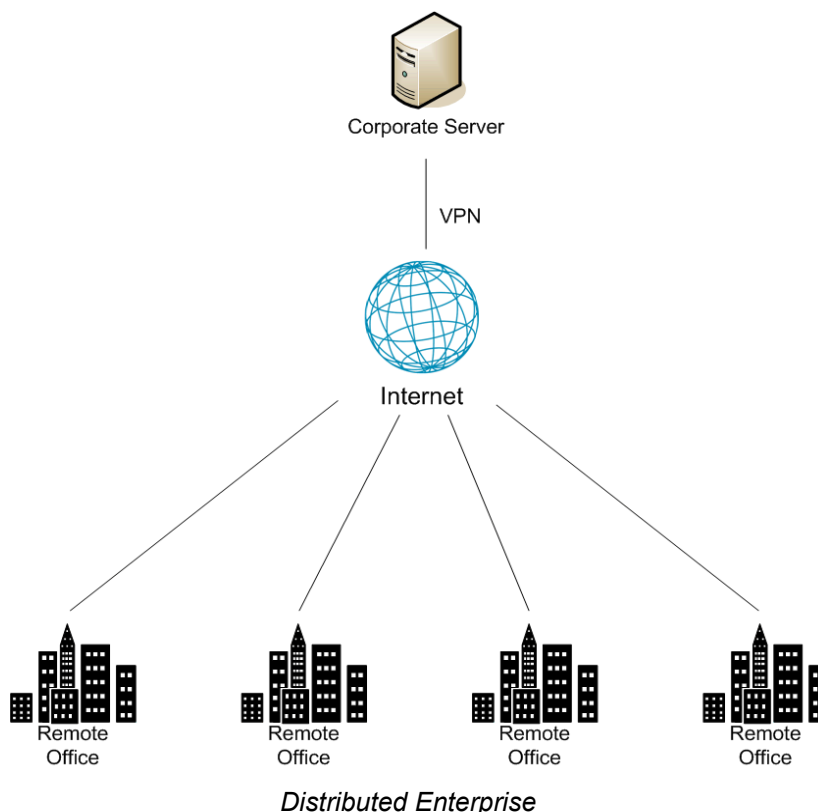
Each remote office firewall in a decentralized network is connected directly to the Internet, rather than to a corporate WAN, to reduce network infrastructure costs. This is usually accomplished through a small office/home office (SOHO) firewall connected to an ISDN, DSL/cable, or T1 connection. Except 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. The entire network is set up and configured by a corporate IT employee who does not remain on-site after installation.

The following diagram shows the network topology of this type of remote office.



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.



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.

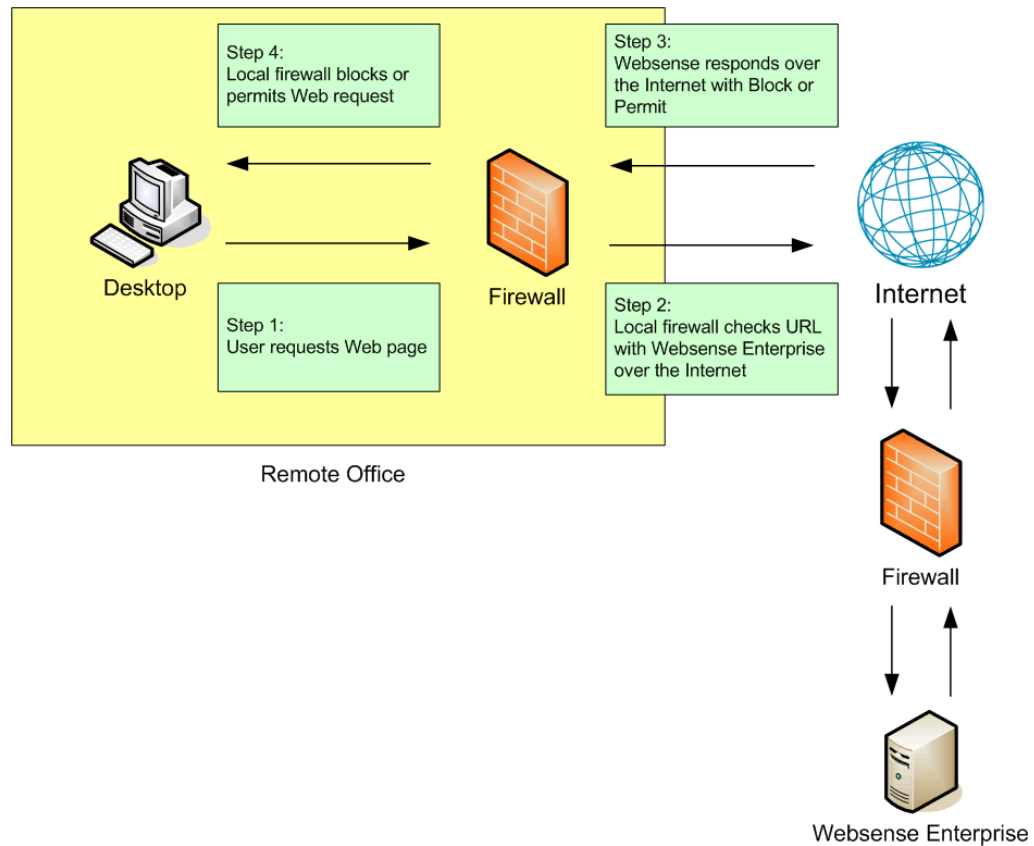
Deploying Websense Enterprise

In 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

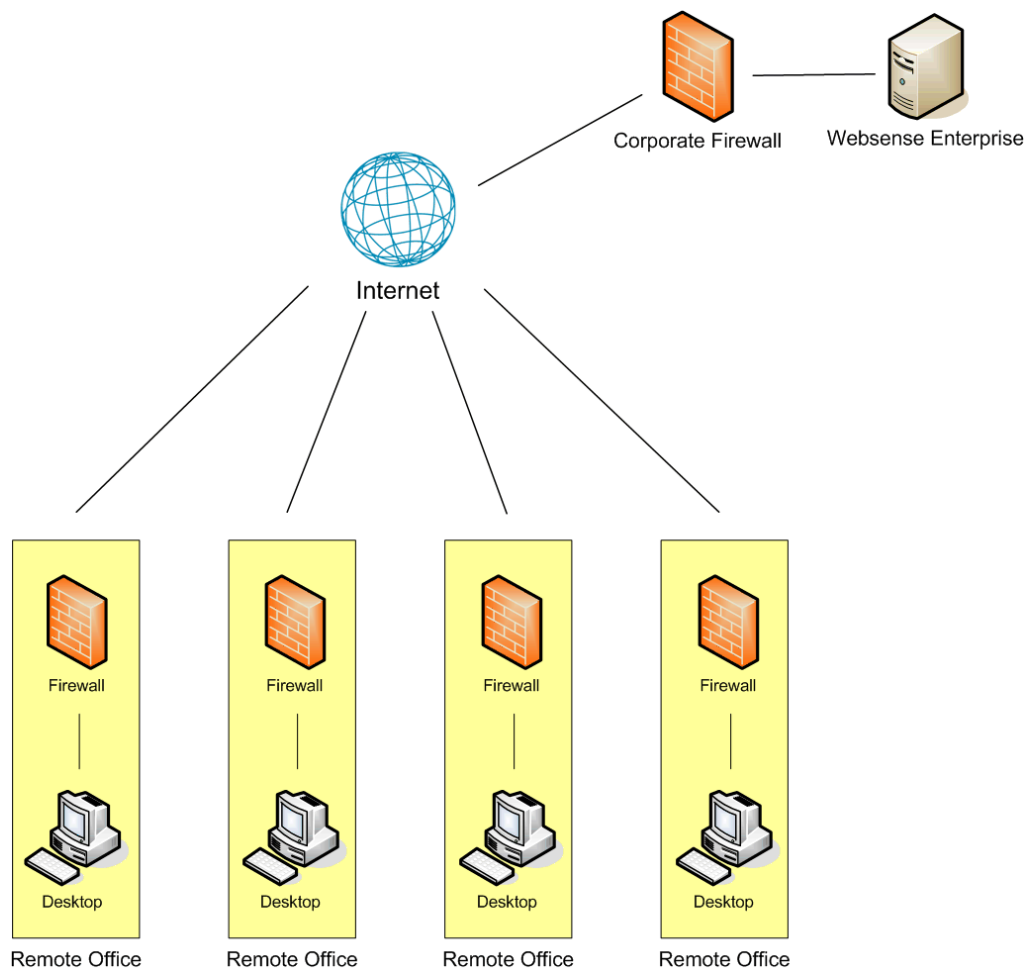
Enterprise is accessible from the Internet, the Websense machine should be protected by a firewall that allows URL lookup requests to pass through. The SOHO firewall at each remote office is then configured to communicate with the centralized Websense machine instead of a local Websense machine. To the firewall, there is no distinction between accessing Websense Enterprise over the Internet and accessing it through a LAN connection at a remote office.

The following diagram shows how a remote office can communicate with Websense Enterprise over the Internet.



Remote Office Communication Strategy

An entire distributed enterprise, with multiple remote offices, might be deployed as follows.



Distributed Enterprise Communicating with Websense Enterprise

Websense has tested this configuration in cooperation with several of its integration partners, including Juniper Networks, Cisco, and Check Point. Juniper Networks was instrumental in providing assistance with deployment and performance tests. However, the same deployment methodology described here 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://ww2.websense.com/global/en/ProductsServices/PartnerIntegrations/>

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. Overall, there are three general deployment models for distributed enterprises:

- ◆ **Regional Offices:** Remote offices located within one region.
- ◆ **Expanding Regional Offices:** Remote offices located within one region, with a growing number of employees and/or offices.
- ◆ **National or Worldwide Offices:** Remote offices located nationally or globally.

These three deployment models are discussed in the following sections.

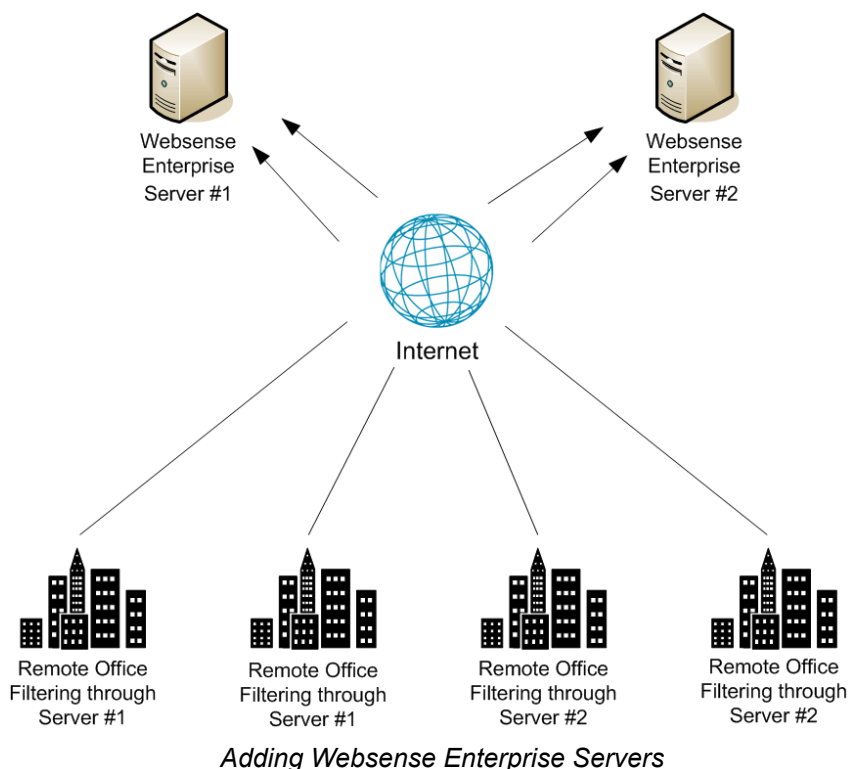
Regional Offices

The simplest Websense Enterprise deployment for a distributed enterprise is for a network composed of remote offices in a single region, such as Los Angeles 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 the diagram on [page 6](#).

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 will allow 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.
- ◆ **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.



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.

Calculating TCP Connections

When Internet requests are sent from hundreds of remote-office firewalls, the number of TCP connections opened to the Websense Enterprise server may be more than the Websense machine can accept. When the remote office firewalls exceed the allowed number of connections opened to Websense, the firewalls will either block all subsequent requests or permit all requests, depending upon how they are configured.

To calculate the number of connections required for a Websense Enterprise deployment and the number of Websense machines that will be needed under different traffic loads, refer to the sizing information in the technical white paper titled *Adjusting Persistent TCP Connections for Filtering in a Distributed Enterprise* found at:

<http://ww2.websense.com/global/en/SupportAndKB/ProductDocumentation/>

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. 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.

It is also important to 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, such as a Juniper Networks NetScreen-5XP, 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 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.

It is recommended 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 the Websense machine should take no more than 100 ms to provide satisfactory browsing speeds.

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. For the system requirements of a high performance Websense machine suitable for a distributed enterprise, refer to the technical white paper titled *Adjusting Persistent TCP Connections for Filtering in a Distributed Enterprise* or to the *Websense Enterprise Deployment Guide*.

The speed of the SOHO firewall is also an important consideration. A slower firewall will require additional time to contact Websense Enterprise, resulting in slower overall Web page responses. A faster firewall at each remote office will process the Websense response in less time and provide faster overall performance.

Caching

Four Websense partners have included a filtering enhancement that significantly improves performance with Websense Enterprise for distributed enterprises. Juniper Networks, Check Point, Cisco, and SonicWALL 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 four 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 document, 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 your distributed enterprise:

- ◆ **Response caching:** Deploy Websense with a firewall that supports Websense response caching (such as products from Juniper Networks, Check Point, Cisco, or 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 100 ms 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 provided by Websense.
- ◆ **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 is 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 will be 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).