Deploying with Websense Content Gateway

Websense Content Gateway is deployed as an add-on module with Websense Web Security or Websense Web Filter.

Websense Content Gateway can also be combined with Websense Web Security and Websense Active Security Module to create the Websense Web Security Gateway.

The Content Gateway module offers:

- ◆ SSL decryption/encryption
- Automatic categorization of dynamic Web 2.0 sites
- Automatic categorization of new, unclassified sites
- Proxy/cache

This document provides system recommendations and a brief overview of deploying Websense Content Gateway with Websense Web filtering software. For more information deploying Web filtering software, see the *Websense Web Security and Web Filtering Guide*, and the supplement for your network size.

For more information on Websense Content Gateway, see the *Websense Content Gateway Installation Guide* and the online help system.

System recommendations

Table 1

Websense Content Gateway

Hardware	 CPU Quad-Core Intel Xeon processor, 2.8 GHz or faster RAM 4 GB 	 Hard drives—2 disks: 100 GB for the operating system, Websense Content Gateway, and temporary data. 100 GB for storage (caching). This disk: Must be a raw disk Must be dedicated Must <i>not</i> be part of the RAID.
Operating system	 Red Hat Enterprise Linux (RHEL) Advanced Server Release 4, Update 5, kernel 2.6.9-55 	
Network connection		
Router	WCCP 1.0 routers support HTTP only. If your site is processing other protocols, such as HTTPS, your router must be WCCP2-enabled. For SSL Manager, the router must support WCCP2.	
	A Cisco router must be running IOS 12.2.	
—or—		
Layer 4 switch	You may be using a Layer 4 switch rather than a router. The switch requires the EMI or IP services image of the 12.2SE or later IOS release to support WCCP.	

Deployment overview

Websense Content Gateway is installed only on a Linux machine. Websense Web filtering software and its reporting components can be installed on either Windows or Linux machines. Running reporting on a Windows system provides more reporting features.

Websense Content Gateway can be connected to the Network via a WCCP-compliant router or a Layer 4 switch.



Figure 1 Basic deployment scenario

Websense Content Gateway can also be deployed with a load balancer to distribute the processing of Internet requests.



Figure 2 Deployment with load balancing

Deployment options

Websense Content Gateway can be deployed:

- ♦ As a Web proxy cache
- In a cache hierarchy
- In a cluster
- ♦ As an SSL server

As a Web proxy cache

When Websense Content Gateway is deployed as a Web proxy, user requests for Web content pass through Websense Content Gateway on the way to the destined Web server (origin server). If the cache contains the requested content, it serves the content directly. If the cache does not have the requested content, Websense Content Gateway acts as a proxy, fetching the content from the origin server on the user's behalf, while keeping a copy to satisfy future requests.

Websense Content Gateway provides the following proxy caching options:

- *Explicit proxy caching,* where the user's client software must be configured to send requests directly to Websense Content Gateway.
- Transparent proxy caching, where user requests are automatically injected into a Websense Content Gateway cache on their way to the eventual destination. Users request Internet content as usual, without any browser configuration, and the proxy serves their requests. The user's client software (typically a browser) is unaware that it is communicating with a proxy.

In a cache hierarchy

Websense Content Gateway can participate in flexible cache hierarchies, where Internet requests not fulfilled in one cache can be routed to other regional caches, taking advantage of their contents and proximity. In a hierarchy of proxy servers, Websense Content Gateway can act either as a parent or child cache, either to other Websense Content Gateway systems or to other caching products.

Websense Content Gateway can be a member of an HTTP cache hierarchy and an ICP (Internet Cache Protocol) cache hierarchy.

In a cluster

Websense Content Gateway scales from a single node into multiple nodes that form a cluster, improving system performance and reliability. The proxy detects the addition or removal of nodes. If Websense Content Gateway's virtual IP failover option is enabled, Websense Content Gateway maintains a pool of virtual IP addresses that it assigns to the nodes of the cluster. Websense Content Gateway can detect hard node

failures (such as power supply or CPU failures) and reassign IP addresses of the failed node to the operational nodes.

Websense Content Gateway has the following clustering modes:

- *Management-only mode*, where you can administer all the nodes in a cluster at the same time. Nodes automatically share configuration information.
- *Full-clustering mode*, where the node caches act as a single aggregate cache. A Websense Content Gateway cluster distributes its cache across its nodes into a single, virtual object store, rather than replicating the cache node by node.

A fully clustered Websense Content Gateway system provides a single system image to both users and administrators, appearing as a single virtual server. Fullclustering mode includes management-only mode.

As an SSL server

If your subscription includes SSL Manager, data can be decrypted and then reencrypted as it travels from the client to the origin server. SSL Manager includes a complete set of certificate-handling capabilities.