Symantec Web Security™ Deployment Guide

Symantec Web Security™ Deployment Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 2.0

PN: 07-30-00463

Copyright Notice

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Trademarks

Symantec and the Symantec logo are registered trademarks of Symantec Corporation and its subsidiaries. Symantec Web Security is the trademark of Symantec Corporation and its subsidiaries. Solaris is a registered trademark of Sun Microsystems, Inc. in the United States and other countries. Microsoft Internet Explorer is a registered trademark of Microsoft Corporation in the United States and other countries. Netscape Navigator is a registered trademark of Netscape Communications Corporation in the United States and other countries.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Two routines from an implementation by Eric Young of the Data Encryption Standard (DES) are included to encrypt access passwords. This DES code is Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com) All rights reserved. Redistribution and use in source and binary forms of DES, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

DES code disclaimer: “THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License.

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. Use that number of copies of the Software as have been licensed to you by Symantec under a License Module, provided that if the Software is part of a suite of Symantec software licensed to you, the number of copies you may use of all titles of the software in the suite, including the Software, may not exceed the total number of copies so indicated in the License Module in the aggregate, as calculated by any combination of licensed suite products. Your License Module shall constitute proof of your right make such copies. If no License Module accompanies, precedes, or follows this license, you may make one copy of the Software you are authorized to use on a single computer.

B. Make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. Use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

D. After written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license; and

E. If a single person uses the computer on which the Software is installed at least 80% of the time, that person may also use the Software on a single home computer.

You may not:

A. Copy the printed documentation which accompanies the Software;

B. Sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. Use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. Use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. Use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. Use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

4. Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items”, as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation”, as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401.

CONTENTS

Deploying Symantec Web Security™ 2.0

Using Symantec Web Security 9

Symantec Web Security deployment modes 10

Deploying Symantec Web Security as a proxy within a network 10

Symantec Web Security as a firewall plug-in that supports CVP 12

General deployment guidelines 13

Server sizing 13

DNS setup 14

Accompanying router/firewall settings 15

Browser settings 16

Specific deployment options and guidelines 17

Proxy deployment 17

Deployment as a CVP resource 18

Proxy vs. CVP 19

Deployment as a downstream proxy 22

Multiple proxy deployment 24

Other deployment-related options 25

Automatic browser configuration capabilities 25

Transparent proxy capabilities 25

Index

Deploying Symantec Web Security™ 2.0

This document contains the following:

- Using Symantec Web Security
- Symantec Web Security deployment modes
- General deployment guidelines
- Specific deployment options and guidelines
- Other deployment-related options

Using Symantec Web Security

Symantec Web Security protects your Web traffic (HTTP/FTP) by scanning for viruses and inappropriate content using leading antivirus and filtering technologies at the gateway. Symantec Web Security combines heuristic safety-net technologies with list-based techniques to protect against known and unknown virus threats and nonbusiness-related Web sites.

Symantec Web Security is available in three variations: a dedicated gateway virus scanner, a dedicated Web content filter, or an integrated antivirus and Web content filtering solution. The same executable is delivered for all three variants, with the different levels of functionality activated by different license keys. The *Symantec Web Security Implementation Guide* provides details on using the software.

This document helps you deploy Symantec Web Security on your network. It covers the basic deployment options, as well as the issues associated with each option.

This document addresses three general topics:

- How Symantec Web Security operates and the basic steps needed to ensure that it installs and runs smoothly, including the necessary DNS settings and the importance of proper server sizing.
- How Symantec Web Security can be used within your network, including the available deployment options (stand-alone proxy, CVP resource, and so on).
- Other tools and capabilities that exist to aid in the deployment, including the use of built-in capabilities (like the transparent proxy capability) and existing administrative tools for aiding in the deploying and maintaining of Symantec Web Security.

This document is not a detailed discussion of Symantec Web Security features. Detailed user information is contained in the *Symantec Web Security Implementation Guide*. Similarly, this document does not provide detailed configuration information about specific deployment-related devices (for example, how to configure your router to redirect packets to a designated proxy server). Wherever possible, links to documents that contain more detailed information are included.

Since Symantec Web Security is available in three variations, any discussions in this document pertaining to functions performed by Symantec Web Security in various deployment scenarios assume that the specific function being described (either virus scanning or Web content filtering) is available in the variation that you are deploying.

This document is updated periodically with the latest information on deployment options, tools, and operating tips available for Symantec Web Security. Check with a Symantec sales or technical support representative for the latest information.

Symantec Web Security deployment modes

Symantec Web Security can be deployed as a proxy within a network or as a plug-in to a firewall compliant with Content Vectoring Protocol (CVP).

Deploying Symantec Web Security as a proxy within a network

Symantec Web Security receives all outbound HTTP, HTTPS, and FTP requests from client computers within the network, since users' Web browsers have been configured to send those requests to the Symantec Web Security proxy.

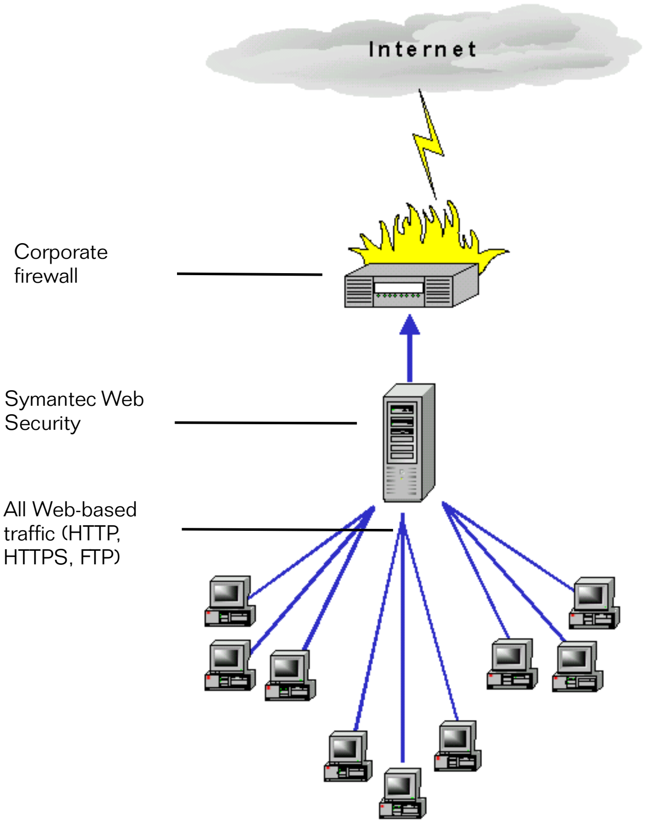
Symantec Web Security processes the requests to determine if the content is appropriate in accordance with the Web browsing policies set by the administrator.

One of the following occurs:

- If the requests are allowed, Symantec Web Security issues the requests to the Internet.
- Symantec Web Security denies the requests and the requests are prevented from going any further, and the requesting clients are notified.

Symantec Web Security receives the inbound HTTP, HTTPS, and FTP traffic and scans it for viruses and inappropriate content. Only allowed Web content and virus-free files are returned to the requesting clients.

Deploying Symantec Web Security as a proxy within a network is illustrated in the following figure.



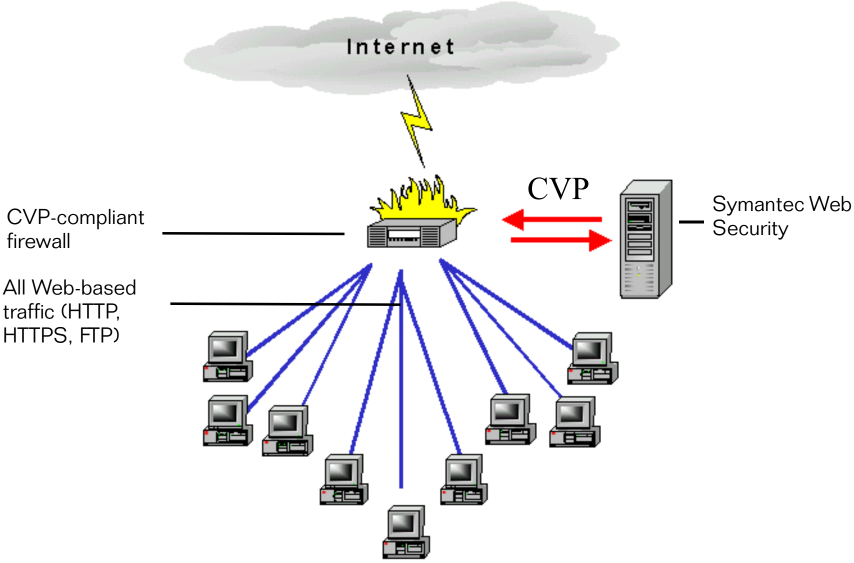
Symantec Web Security as a firewall plug-in that supports CVP

You can deploy Symantec Web Security as a CVP resource (or plug-in) to a CVP-compliant firewall as follows.

All inbound HTTP, HTTPS, and FTP traffic received by the firewall is passed using CVP to the designated CVP resource running Symantec Web Security for virus and content scanning. Symantec Web Security may be running on the same server as the firewall or on a separate server.

Symantec Web Security passes only the allowed and virus-free files back to the firewall. The allowed and virus-free files are passed to the client computer, and the filtered files are passed to the requesting users.

Deploying Symantec Web Security as a plug-in to a CVP-compliant firewall is illustrated in the following figure.



General deployment guidelines

This section discusses general guidelines that should be followed regardless of which deployment mode you choose. In additon, each deployment option is discussed in greater detail, including the advantages and disadvantages of each option.

For more information, see "Specific deployment options and guidelines" on page 17.

Server sizing

It is critical that the servers running Symantec Web Security are correctly sized to process the volume of anticipated Web traffic based on the number of users that might make simultaneous Web requests. Generally, about 20-40% of the total number of desktops/nodes within a network are making simultaneous requests. However, there are situations and organizations where this percentage is significantly higher. Sustained traffic loads of 1000 (or more) simultaneous users require more than one server running Symantec Web Security for optimal performance and redundancy.

Symantec system engineers and technical support staff can provide you with recommendations for processor speed, RAM, and hard disk configurations based on your anticipated or observed Web traffic.

The examples in this document illustrate single-server deployment. You have the choice of running multiple Symantec Web Security servers and deploying them using one of the following methods:

- Fully centralized deployments: Use one or more appropriately-sized Symantec Web Security servers at a central location that proxy and process requests. For example, an entire company or school district.
- Fully distributed deployments: Require an appropriately-sized Symantec Web Security server at each end-user site. For example, at branch office locations or schools within a district.
- Hybrid deployments: Mix the fully centralized and fully distributed approaches that involve placing dedicated and appropriately-sized servers at each of the end-user sites where the heaviest Internet traffic is expected, while lower-traffic sites proxy through servers located at a central site to complete the picture.

Deciding whether to use a fully centralized or fully distributed deployment is usually driven by the available bandwidth that connects the end-user sites and the point where the Internet connection is established. Cost is also a factor, which usually results in considering the hybrid deployment as a middle ground solution.

DNS setup

Proper DNS setup is critical to operating Symantec Web Security. Improperly configured DNS settings are responsible for a large number of installation and performance-related issues.

For more information, see the *Symantec Web Security Implementation Guide*.

The DNS server that is referenced/used by the server running Symantec Web Security must contain the following records:

- An A (address) record that maps the Symantec Web Security server's host name to its IP address. Each Symantec Web Security server requires an A record.
- A PTR (pointer) record that maps the Symantec Web Security server's IP address to its host name, including the domain name. Each Symantec Web Security server requires a PTR record.

To ensure that the DNS server entries are configured properly for each Symantec Web Security server being deployed, you must issue two nslookup commands:

- A command on the Symantec Web Security server's hostname to ensure that the address records are in effect.
- A second command on the Symantec Web Security server's IP address to ensure that the corresponding pointer records are in effect.

You should always be able to resolve both the Symantec Web Security server names as well as the corresponding IP addresses from computers other than the Symantec Web Security servers.

Accompanying router/firewall settings

Symantec Web Security can be configured to prevent unwanted Web traffic and viruses from entering your network. To prevent users from bypassing the content filtering and virus scanning settings/policies you have selected, enact appropriate rules (access lists) at the router and/or firewalls within your network. Configure your router or firewall so that it processes only HTTP, HTTPS, and FTP requests that originate from the Symantec Web Security server.

The fully distributed or hybrid deployment options described previously require using multiple Symantec Web Security servers distributed throughout the network. Settings can be added to prevent users from attempting to proxy through other Symantec Web Security servers within the network, since those servers might be enforcing less restrictive filtering and virus-scanning settings than the server the user should be using.

Additional settings to prevent users from switching to other Symantec Web Security servers are unnecessary in situations where multiple Symantec Web Security servers are intended to balance the traffic load from all users via a third-party load-balancing mechanism.

When such settings are enabled, an FTP request issued from a command line results in the request not being processed, since it does not originate from the Symantec Web Security server. If the proper settings are in place in the Web browser, visiting and downloading data from an FTP site from within a browser results in the request being processed and scanned for content and viruses by Symantec Web Security.

These settings should always be enabled, regardless of the means by which Web requests are being directed to the server running Symantec Web

Security (for example, whether you are using browser-based redirection of requests, or the available transparent proxying capabilities in Symantec Web Security).

Browser settings

In the proxy or CVP deployment modes, the HTTP, HTTPS, and FTP requests issued by users must be directed toward the server running Symantec Web Security.

In the proxy deployment, all HTTP, HTTPS, and FTP requests issued by users must be directed to the Symantec Web Security proxy server. This is accomplished using either browser redirection or transparent proxy.

Browser redirection

Browser redirection involves configuring each client browser to use the Symantec Web Security server as the HTTP, HTTPS, and FTP proxy. These settings can be made manually or by using automatic browser configuration provided by administration toolkits, such as the Internet Explorer Administration Kit.

Transparent proxy

Transparent proxying involves using the transparent proxy capabilities available in Symantec Web Security, in conjunction with associated software, to pass each client's HTTP, HTTPS, and FTP requests to the Symantec Web Security servers without having to explicitly set each client browser to point at the Symantec Web Security server.

Note: This option is available only when running Symantec Web Security on a Solaris® operating system.

Browser settings and CVP

When deploying Symantec Web Security as a CVP resource, it is not required that Web browser settings be changed to specify the Symantec Web Security server as the HTTP, HTTPS, and FTP proxy. The firewall performs the redirection of data to Symantec Web Security. While this appears to be a convenient and time-saving feature, it increases the processing load on the firewall and reduces the effectiveness of the content filter.

Even in deployments where Symantec Web Security is being used as a CVP resource, it can also be accessed as a proxy (both the proxy and CVP functionality are always available), so that after Symantec Web Security is deployed as a CVP resource, users can be made to transition over time to the higher-performing proxy implementation (using browser redirection to point to the Symantec Web Security server) without reinstalling or reconfiguring Symantec Web Security.

Specific deployment options and guidelines

This section covers the proxy and CVP deployment options in greater detail, including primary advantages and disadvantages associated with each option.

Proxy deployment

In proxy deployment, all unfiltered client HTTP, HTTPS, and FTP requests are directed to the Symantec Web Security server using the browser redirection or transparent proxy method.

The Symantec Web Security server applies initial filtering on the outbound request to ensure it is allowed in accordance with the settings for the user or client issuing the request.

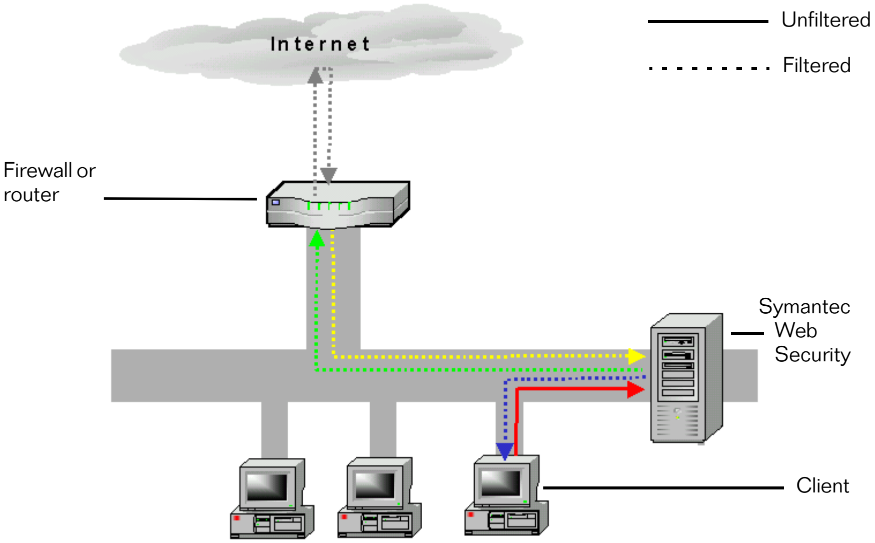
One of the following occurs:

- If the request is denied, it goes no further than the Symantec Web Security server, and a denial message is issued to the client.
- If the request is allowed, the Symantec Web Security server issues the filtered request to the Internet.

If the filtered request is allowed, the request goes to the Internet, returns through the firewall, and is routed back to the Symantec Web Security server.

The Symantec Web Security server applies additional scanning for viruses and filtering for content before delivering the virus-free and appropriate content to the client that issued the request.

A Symantec Web Security server deployed in proxy mode is illustrated in the following figure.



Deployment as a CVP resource

In CVP deployment, all unfiltered client HTTP, HTTPS, and FTP requests arrive at the CVP-compliant firewall.

An unfiltered request is made to the Internet. The resulting inbound unfiltered data is routed by the firewall to the Symantec Web Security server via CVP.

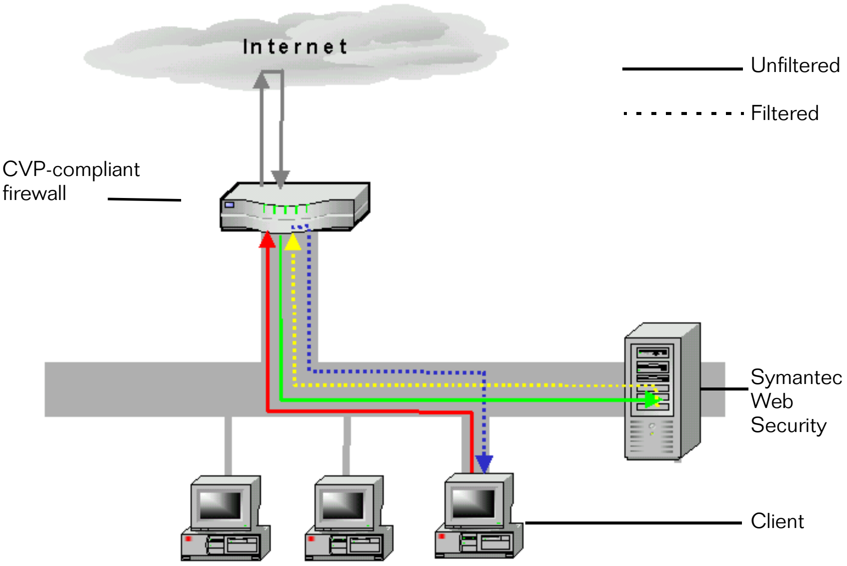
Symantec Web Security scans the data to ensure that it is virus-free and allowed in accordance with the browsing policy set for the user issuing the request.

After scanning, one of the following occurs:

- Symantec Web Security delivers the filtered virus-free and appropriate content back to the firewall.
- Symantec Web Security issues a denial notification.

The firewall routes the virus-free and appropriate content back to the client that issued the request.

A Symantec Web Security server deployed as a CVP resource is illustrated in the following figure.



Proxy vs. CVP

Based on traffic flow for proxy and CVP deployment, there are several reasons for choosing proxy deployment.

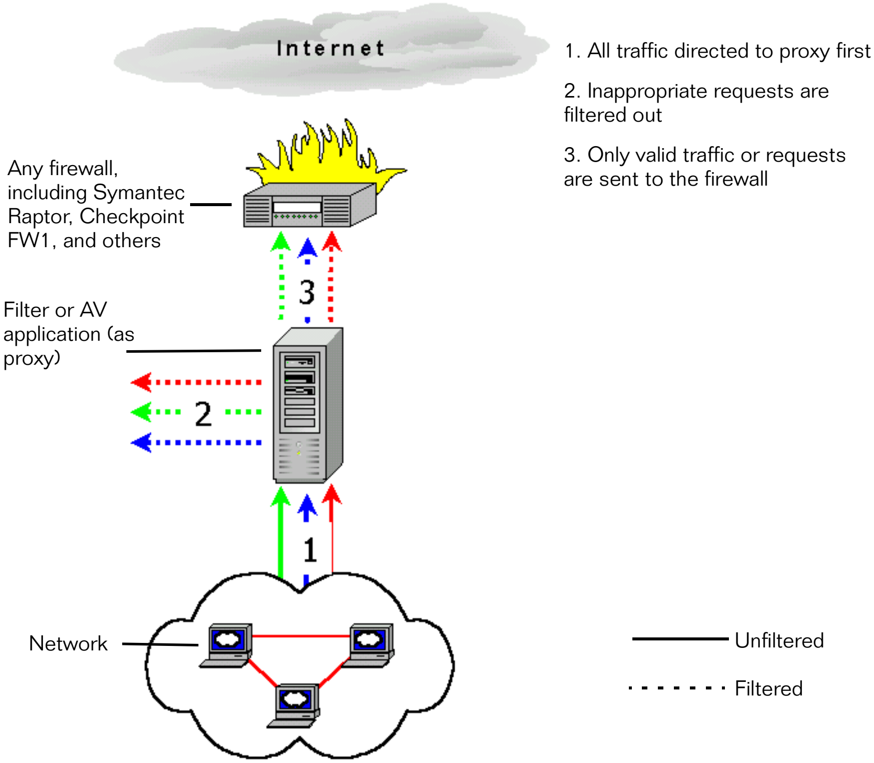
Proxy deployment advantages

Client requests are initially processed at the proxy, allowing Web browsing policies to be enforced at the earliest possible opportunity. Only requests that are initially filtered, and new requests that are not in Symantec Web Security's cache, proceed further. The initial scanning ensures that only allowed requests go out to the Internet and use the available bandwidth on your network.

In proxy mode deployment, filtering initially occurs on the outbound user request to ensure that it is allowed in accordance with the settings for the user issuing the request, and additional filtering occurs after the request is returned from the Internet to the firewall. During CVP deployment, a request is made to the Internet and the resulting inbound data is filtered only after being routed by the firewall to the Symantec Web Security server.

Proxy mode deployment of Symantec Web Security can work with any firewall, whether it is a CVP-compliant firewall or not. You can easily transition to the higher-performing proxy deployment even if Symantec Web Security is initially deployed as a CVP resource.

The proxy deployment option is illustrated in the following figure.

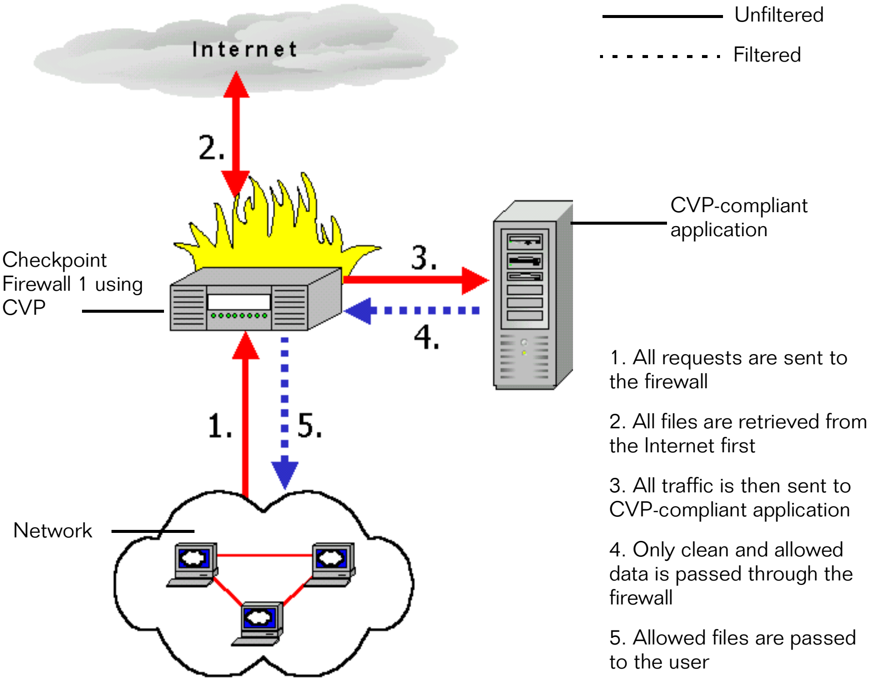

Internet
1. All traffic directed to proxy first
2. Inappropriate requests are filtered out
3. Only valid traffic or requests are sent to the firewall
Any firewall, including Symantec Raptor, Checkpoint FW1, and others
3
Filter or AV application (as proxy)
2
1
Network
Unfiltered
Filtered

CVP deployment option

CVP deployment is considered less involved than proxy deployment because client browsers do not require reconfiguration, as is required in proxy mode to point clients to the appropriate proxy. However, when Symantec Web Security is deployed in CVP mode, scanning of data for content and viruses occurs after the data is retrieved from the Internet, forcing your firewall to process a higher volume of traffic.

When a request is issued to the Internet by entering a hostname/URL in a user’s browser, CVP passes data to the Symantec Web Security server. This data is not the requested hostname/URL, but instead is the corresponding IP address obtained from a reverse DNS lookup performed by the CVP-compliant firewall. This reduces the effectiveness of any filter lists from any vendor because the IP addresses assigned to specific hosts are prone to change, and because of popular practices like virtual hosting (where several Web domains – each serving potentially different types of content – share a published/external IP address).

The CVP deployment option is illustrated in the following figure.



1. All requests are sent to the firewall

2. All files are retrieved from the Internet first

3. All traffic is then sent to CVP-compliant application

4. Only clean and allowed data is passed through the firewall

5. Allowed files are passed to the user

The sequence of events for both deployment options is summarized in the following table.

Using CVP	Using proxy
All user requests are passed to the firewall.	All user requests are passed to the proxy server.
All requested data is retrieved (before filtering).	All requests are filtered (first).

Using CVP	Using proxy
Data is passed to the filter or scanner for analysis.	Filtered requests are sent to the firewall.
Data is filtered or scanned.	Data is retrieved from the Internet.
Filtered data is passed back to the firewall.	Filtered data is passed back to the proxy.
Data is passed to the user.	Data is passed to the user.

With the advent of virtual hosting on the Internet, any Web filtering solution that relies solely on the list-based approach, and whose lists are comprised of IP addresses, is more prone to error from under- or over-filtering. In proxy or CVP mode, Symantec Web Security offers the list-based approach (with a database comprised of host names and IP addresses) and heuristics-based context-sensitive scanning in 14 languages to perform Web filtering.

Deployment as a downstream proxy

Symantec Web Security can be deployed as an initial, or downstream, proxy that receives HTTP, HTTPS, and FTP requests. After scanning, Symantec Web Securiy passes the data to an existing upstream proxy or caching appliance that might be on the network. This deployment is a slight variation of the standard proxy deployment.

All client HTTP, HTTPS, and FTP requests are directed to the Symantec Web Security server using the browser redirection or transparent proxy method.

As in standard proxy deployment, the Symantec Web Security server applies initial filtering on the outbound request.

One of the following occurs:

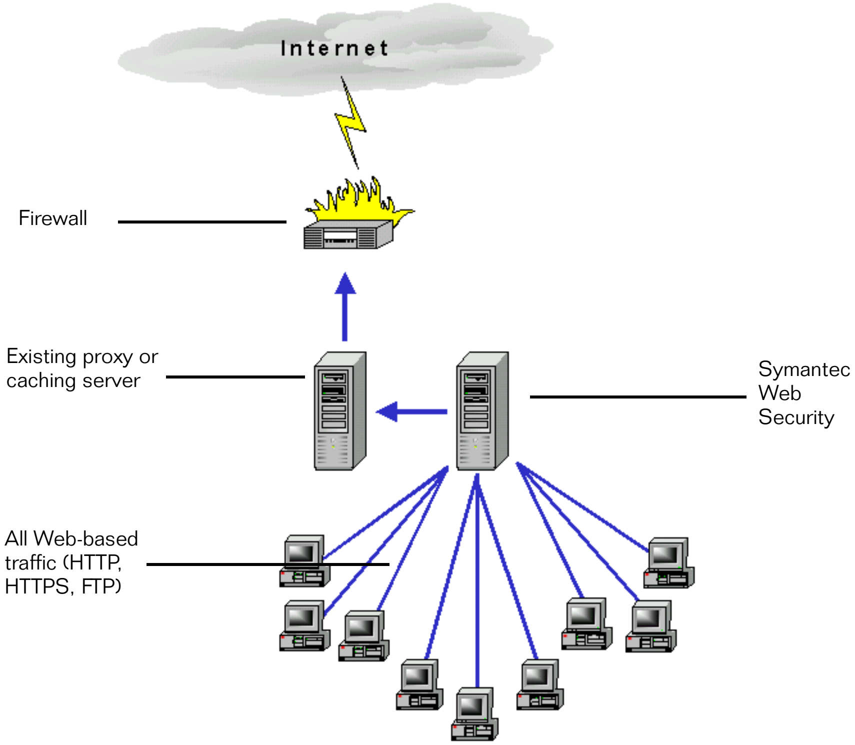
- If the request is not allowed, it does not pass the Symantec Web Security server and a denial message is issued to the client.
- If the request is allowed, the Symantec Web Security server passes the request to the next proxy by specifying the server name and port number of the upstream proxy in the proxy configuration section of Symantec Web Security's administrative interface

For more information, see the *Symantec Web Security Implementation Guide*.

The request goes out to the Internet, returns through the firewall, and is routed back to the Symantec Web Security server.

The Symantec Web Security server applies additional scanning for viruses and content before delivering the virus-free and appropriate content to the client that issued the request.

A Symantec Web Security server deployed as a downstream proxy is illustrated in the following figure.


Internet
Firewall
Existing proxy or caching server
Symantec Web Security
All Web-based traffic (HTTP, HTTPS, FTP)

While Symantec Web Security is a caching proxy, you can still turn the caching function off.

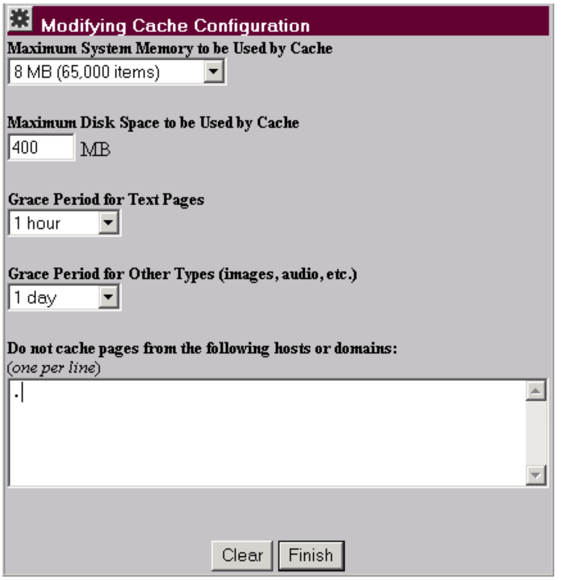
To turn the caching function off

1. In the Symantec Web Security Administrative interface, log on.
2. On the System object, click **Modify**.

3 In the Modify System dialog box, click **Cache Configuration.**

4 Click **Next**.

5 In the Modifying Cache Configuration dialog box under Do not cache pages from the following hosts or domains:, type a period (**.**).



Modifying Cache Configuration

Maximum System Memory to be Used by Cache: 8 MB (65,000 items)

Maximum Disk Space to be Used by Cache: 400 MB

Grace Period for Text Pages: 1 hour

Grace Period for Other Types (images, audio, etc.): 1 day

Do not cache pages from the following hosts or domains:
(one per line)
.

6 Click **Finish**.

If you are using Symantec Web Security downstream of or in conjunction with a dedicated, high-performance caching appliance, this option may help enhance performance.

Multiple proxy deployment

Symantec Web Security can be deployed using multiple servers throughout your network in a fully distributed or hybrid manner. You can also install multiple Symantec Web Security servers at a central site to perform virus and content scanning for the entire organization (fully centralized deployment), perhaps behind a load-balancing switch. In either scenario, all single-server deployment options are still available (along with the advantages and disadvantages of each), and all single-server guidelines still apply. When Symantec Web Security is deployed properly and the servers are properly sized and placed, it can be scaled to meet the virus and content scanning needs of virtually any organization.

If you are considering multiserver deployment of Symantec Web Security, contact a Symantec sales or technical support staff representative to recommend the best deployment options based on your specific needs and network topology.

Other deployment-related options

Two methods can be used to aid in deploying Symantec Web Security in proxy mode. Both of these methods deal with how HTTP, HTTPS, and FTP requests from clients are redirected to the Symantec Web Security server.

Automatic browser configuration capabilities

Web browser settings, including proxy settings, can be automatically and centrally specified and distributed. Administrative tools are available for the most commonly used browser types (Internet Explorer® and Netscape Navigator/Communicator®). For example, Internet Explorer offers automatic browser configuration using the Internet Explorer Administration Kit (IEAK).

For more information, see the following sites:

- http://www.microsoft.com/TechNet/IE/technote/deploygd/Part2-intro/CHAPTER4.asp
- http://www.microsoft.com/TechNet/IE/reskit/ie5/part5/ch21auto.asp
- http://home.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html

Transparent proxy capabilities

When deploying Symantec Web Security on a Solaris operating system, you can use the available transparent proxy capability to route requests to the Symantec Web Security server without specifying the proxy in each client browser. Instead, a feature of many modern routers is used that allows the default gateway (router) for the network to intercept Web traffic and redirect this data to the proxy server.

In addition to configuring Symantec Web Security to function in transparent proxy mode, the process also involves installing and configuring the available IP_Filter software to perform packet redirection to Symantec Web Security, as well as some router configuration.

The basic steps are listed as follows:

1 Enable transparent proxy support in Symantec Web Security using the Symantec Web Security administrative interface in the Modifying Proxy Configuration panel.

  This enables Symantec Web Security to accept non-proxy requests.

  For more information, see the *Symantec Web Security Implementation Guide*.

2 Install and configure IP_Filter so that it forwards packets to Symantec Web Security.

3 Configure your router to redirect packets originating from each client to the computer running IP_Filter (the server running Symantec Web Security).

Using transparent proxy services requires configuring a different set of rules on the router. In this case, an access list is used to select packets coming into the router that are destined for a Web or proxy server (port 80 or 8002). A policy route (or route map) is used to redirect those packets to the Symantec Web Security proxy. This prevents users from circumventing the Symantec Web Security proxy (for example, replacing the access lists).

Note: The IP_Filter software is available upon request from Symantec sales and technical support staff.

Once these steps are completed, the steps that a client's request takes are as follows:

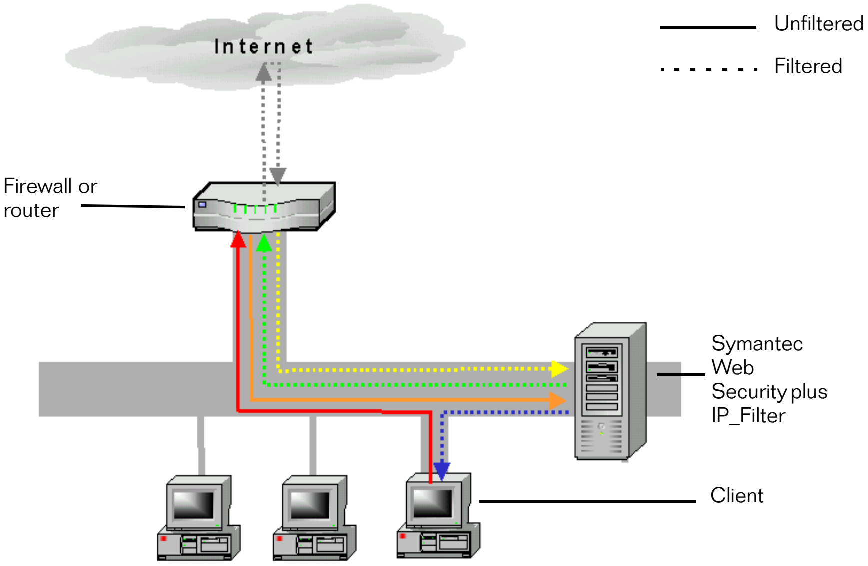
The unfiltered client request is sent to the router because no setting exists within the client browser to route it directly to the Symantec Web Security server. The router passes the unfiltered request to the Symantec Web Security server in accordance with the rules set on the router.

Symantec Web Security applies the initial scanning. As in standard proxy deployment, only allowed requests go further.

Allowed requests are sent through the router, and the data is retrieved from the Internet. The filtered data is routed to the Symantec Web Security server, where the next scan is performed.

The virus-free and appropriate content is delivered to the client that issued the request.

The steps a client's request takes when using transparent proxy capability are illustrated in the following figure.



Any packet redirection method (including transparent proxy and CVP) has a cost associated with it: increased load at the router or firewall. The increased load and accompanying reduced performance on the router or firewall must be weighed against the time, effort, and cost of manually reconfiguring browser settings.

The most effective method for reducing the router or firewall load is to use the browsers to send requests directly to the Symantec Web Security server. Packet redirection by transparent proxy is an effective means to quickly and transparently introduce the services provided by Symantec Web Security into your network. Ultimately, from a performance and router/ firewall load standpoint, it is probably most efficient to utilize transparent proxy services as a temporary measure until browser reconfiguration (ideally, via automatic browser configuration settings) can be implemented.

INDEX

A
access lists 15, 26
address record 14

C
caching proxy, truning off 23
CVP
  deployment 18
  deployment of Symantec Web Security using 12
  problems during deployment 20
  sequence of events during deployment 21
  setting Web browser using 16

D
deployment
  as downstream proxy 22
  factors in determining 14
  fully centralized 14
  fully distriburted 14
  hybrid 14
deployment guidelines 13
DNS
  required records 14
  setup 14
downstream proxy, deployment as 22

F
firewall settings 15
FTP, request issued from a command line 15

I
IP_Filter sortware, installing and configuring 25

M
multiple servers
  deployment using 14
  using proxy deployment with 24
  when to add settings 15

N
nslookup commands 15

P
proxy deployment 17
  advantages of 19
  on a stand-alone server 10
  sequence of events during 21
  using multiple servers 24
PTR record 14

R
router settings 15

S
server size
  considerations 13
  number of users 13
Solaris, running Symantec Web Security on 16
Symantec Web Security
  as a firewall plug-in 12
  functions of 9
  Implementation Guide 9, 10, 14
  proxy deployment within a network 10
  variations of 9

T
transparent proxy capabilities, on Solaris Operating System 25

V
virtual hosting

definition of 21
effect on list-based filtering 22

W

Web browser
automatic configuration capabilities 25
redirection 16
settings 16
settings when used with CVP 16
transparent proxy 16