Symantec™ Data Loss Prevention Integration Guide for Squid Web Proxy

Version 11.0

Symantec

Symantec Data Loss Prevention Integration Guide for Squid Web Proxy

Documentation version: 11.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrades protection
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

About Squid Web Proxy integration

This chapter includes the following topics:

About integrating Squid Web Proxy with Network Prevent (Web)

Symantec Data Loss Prevention supports integrating Squid Web Proxy 3.0 with Network Prevent (Web) to inspect HTTP traffic, and to block or modify traffic that violates configured policies. You integrate the proxy using the Internet Content Adaptation Protocol (ICAP) interface provided in Squid 3.0 and a request modification (REQMOD) definition that proxies unencrypted traffic to Network Prevent (Web).

The Squid Web Proxy integration supports only forward-proxy mode deployments using ICAP request modification (REQMOD) mode. HTTP blocking is supported. Squid also supports HTTP content removal when a request is found to violate Symantec Data Loss Prevention policies.

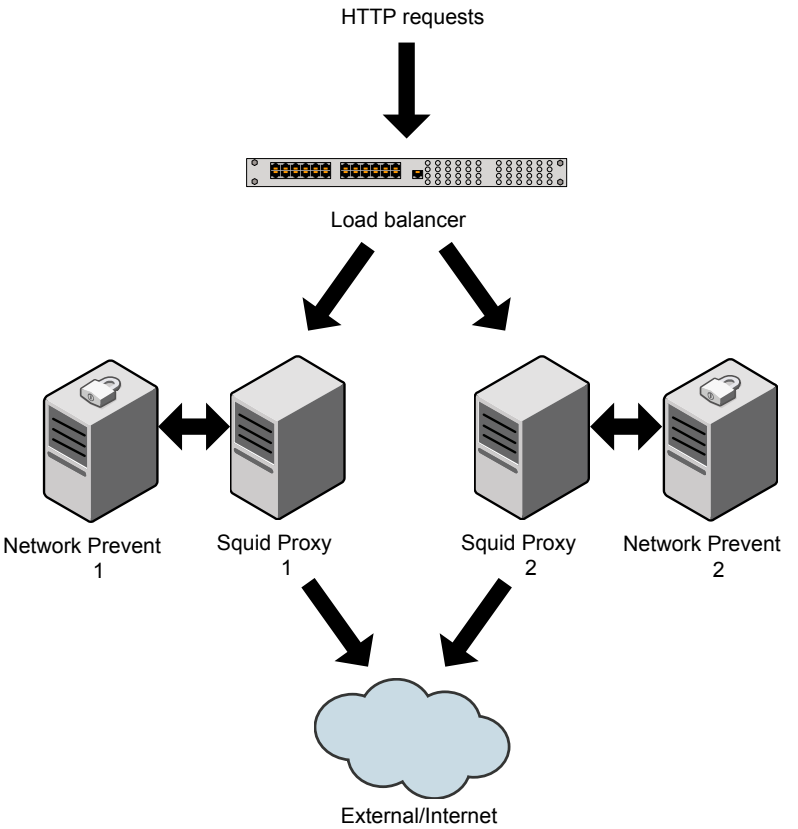
Reverse proxy configurations (RESPMOD mode) are not supported. Inspection of encrypted (SSL) content is not supported. Native or tunneled FTP monitoring and blocking is not supported.

See the *Symantec Data Loss Prevention Administration Guide* for more information about Network Prevent (Web) features.

About load balancing with Squid Web Proxy deployments

A single Squid Web Proxy server does not provide a mechanism for load balancing to multiple Network Prevent (Web) servers in the ICAP interface. To use multiple Network Prevent (Web) servers with Squid, you must deploy separate Squid Web Proxy servers and associate each proxy with a dedicated Network Prevent (Web) Server. To load balance requests, use a third-party load balancing solution to distribute outbound requests to the configured Squid Web Proxy servers. In this configuration, each Squid server communicates with only one Network Prevent (Web) server.

Figure 1-1 Load balancing with Squid Web Proxy



Squid Web Proxy requirements for integrating with Network Prevent (Web)

To integrate Squid Web Proxy with Network Prevent (Web), you must use Squid 3.0 stable release on a supported Linux computer. Symantec has tested Squid with stable release 20 (`squid-3.0.STABLE20`). See http://www.squid-cache.org for information about downloading and installing the proxy software.

When you compile the Squid source code, you must enable the ICAP interface option by specifying the `--enable-icap-client` option.

See "Installing Squid Web Proxy for integration with Network Prevent (Web)" on page 14.

You will also need to compile with features that are appropriate for your proxy deployment. See *Compiling Squid* for a list and description of common compilation options. This document is available from http://www.squid-cache.org. Also refer to the Squid FAQ at http://wiki.squid-cache.org/SquidFaq for information about compiling and using Squid.

After compiling and installing Squid, you must edit the `squid.conf` configuration file to define a REQMOD service to proxy requests to a deployed Network Prevent (Web) Server.

See "Configuring Squid for integration with Network Prevent (Web)" on page 16.

Chapter 2

Integrating Squid Web Proxy with Network Prevent (Web)

This chapter includes the following topics:

Integrating Squid Web Proxy with Network Prevent (Web)

Follow these steps to integrate Squid with Network Prevent (Web).

Table 2-1 Steps for integrating Squid with Network Prevent (Web)

Step	Action	Description
Step 1	Install Network Prevent (Web).	Install one or more Network Prevent (Web) detection servers that you will use to inspect content that is forwarded from a Squid proxy server. For more information, see the *Symantec Data Loss Prevention Installation Guide* for Linux or Windows.

Table 2-1 Steps for integrating Squid with Network Prevent (Web) *(continued)*

Step	Action	Description
Step 2	Configure Network Prevent (Web).	Configure your installed Network Prevent (Web) detection servers using instructions in the *Symantec Data Loss Prevention Administration Guide*.
Step 3	Install Squid Web Proxy with the ICAP interface.	See "Installing Squid Web Proxy for integration with Network Prevent (Web)" on page 14.
Step 4	Configure Squid and the ICAP interface.	See "Configuring Squid for integration with Network Prevent (Web)" on page 16.

Installing Squid Web Proxy for integration with Network Prevent (Web)

Follow these steps to install and compile Squid Web Proxy for integration with Network Prevent (Web).

To install and compile Squid Web Proxy

1. Download the official `squid-3.0.STABLE20.tar.gz` source code distribution from http://www.squid-cache.org/Versions/v3/3.0/.
2. Move to the directory in which you will unpack the Squid source code directory.
3. Uncompress the Squid source file download. For example:

   ```
   tar xzf ~/downloads/squid-3.0.STABLE20.tar.gz
   ```

   Replace *~/downloads* with the path to the downloaded source file.
4. Move to the newly-created Squid source code directory:

   ```
   cd ./squid-3.0.STABLE20
   ```

5 Compile Squid using the `--enable-icap-client` compiler option. The `--enable-icap-client` option is required to build the ICAP interface used to integrate with Network Prevent (Web). For example:

```
./configure --enable-icap-client
```

You will generally specify additional compiler options to enable or disable features as required for your Squid deployment. See *Compiling Squid* at http://wiki.squid-cache.org/SquidFaq/CompilingSquid for information about common compiler options. Or, use the following command to view a complete list of Squid compiler options:

```
./configure -h
```

6 Make and install Squid using the following two commands:

```
make
make install
```

7 After installing the proxy, configure the ICAP interface to proxy supported requests to Network Prevent (Web) for inspection.

See "Configuring Squid for integration with Network Prevent (Web)" on page 16.

Note: To uninstall Squid, return to the directory in which you compiled the application (for example, `~/downloads/squid-3.0.STABLE20`). Then enter the command `make uninstall`.

About starting and stopping Squid Web Proxy

You can run Squid Web Proxy either as a foreground process or as a daemon. When you first install squid, run the proxy as a foreground process and send debugging information to stderr. This helps you view configuration errors or validate that the application is running. For example:

```
/usr/sbin/squid -N -d1
```

Replace `/usr/sbin` with the correct installation directory.

After you have finished configuring Squid, omit the `-N` and `-d1` options to run the process as a daemon and turn off debugging messages. Refer the Squid log files to diagnose any runtime problems. See http://wiki.squid-cache.org/SquidFaq/SquidLogs for more information.

If you make any changes to the `squid.conf` configuration file while Squid is running, shut down and restart Squid to reload the configuration.

To stop Squid, use the `-k shutdown` option:

```
/usr/sbin/squid -k shutdown
```

See the Squid documentation or type `squid -?` to learn more about Squid command line options.

Configuring Squid for integration with Network Prevent (Web)

Squid manages all runtime configuration options in the `squid.conf` configuration file. This file is installed by default in `/etc/squid/squid.conf`. (If you used a different installation prefix when compiling Squid, the configuration file is placed in the directory you specified.) The default `squid.conf` file contains sample entries that you can uncomment and modify for your deployment.

To integrate Squid with Network Prevent (Web), you must configure the following features in `squid.conf`.

Table 2-2 Configuring Squid for Network Prevent (Web) integration

Step	Task	Description
Step 1	Configure an ACL and ICAP service definition for a Network Prevent (Web) Server.	See "Configuring a Squid ACL and ICAP service for Network Prevent (Web)" on page 16.
Step 2	Configure general ICAP connectivity options.	See "Configuring Squid ICAP connectivity options" on page 18.

Configuring a Squid ACL and ICAP service for Network Prevent (Web)

Each Squid installation must have the appropriate ACLs and rules for the local server and for the protocols you want to support. The default `squid.conf` file contains ACL and rule definitions for the cache monitor process, localhost, and for various protocols. You can modify these as needed for your Squid deployment. You must also create a dedicated ACL for the Network Prevent (Web) Server protocols and HTTP methods that you want to monitor, as described in the following procedure.

The ICAP service definition specifies the URL and options used to connect to Network Prevent (Web) for ICAP requests. Use the instructions below to create

an ICAP service that sends REQMOD requests to a configured Network Prevent (Web) Server. Note that Squid 3.0 also requires an `icap_class` directive that includes the service in the ICAP service chain.

To configure a Squid ACL and ICAP service

1 Open the `squid.conf` configuration file in a text editor.

See "Configuring Squid for integration with Network Prevent (Web)" on page 16.

2 Add the following ACL and rule definition for Network Prevent (Web):

```
acl vontu_reqmod_http_upload method POST PUT
```

Note: The example request method ACL does not specify the HTTP GET method because GET requests can generate large volumes of network traffic. If you choose to inspect GET requests, first see the *Symantec Data Loss Prevention Administration Guide* for guidelines on enabling GET processing. Then enable GET processing by adding GET to the ACL definition in `squid.conf`.

---

3 Add the following directive to define an ICAP service for Network Prevent (Web):

```
icap_service vontu_reqmod reqmod_precache 1 icap://prevent_address:prevent_port/reqmod
```

Replace *`prevent_address`* and *`prevent_port`* with the actual address and port number of your Network Prevent (Web) Server. For example: icap://myprevent.mycompany.com:1344/reqmod.

The `reqmod_precache` option is required. It specifies that requests are processed over the ICAP interface before the requests are cached.

The `1` specifies that Squid should allow the request to bypass the ICAP interface if the Network Prevent (Web) Server is unavailable. If you disable bypass mode (by specifying `0`), users receive an ICAP error instead of a normal response if the Network Prevent (Web) Server is unavailable.

4 Add the new ACL to an `icap_access` directive for the Network Prevent (Web) Server ICAP service. Also define the `icap_class` directive and add it to the ICAP service chain:

```
icap_class class_vontu_reqmod vontu_reqmod
icap_access class_vontu_reqmod allow vontu_reqmod_http_upload
```

5 Configure general ICAP connectivity options for Squid.

See "Configuring Squid ICAP connectivity options" on page 18.

Configuring Squid ICAP connectivity options

The `squid.conf` file uses a series of configuration directives to control the basic behavior of the ICAP interface. These directives affect the way in which Squid negotiates ICAP connections with Network Prevent (Web) Server. The directives also control the how user name and IP information is communicated to servers over ICAP.

To configure ICAP connection options

1 Open the `squid.conf` configuration file in a text editor.

See "Configuring Squid for integration with Network Prevent (Web)" on page 16.

2 Create a new section in the configuration file to add ICAP connection directives. For example, add the line:

```
# ICAP client parameters.
```

3 Add the following directives to configure the Squid proxy ICAP connection with Network Prevent (Web) Server. Note that the default `squid.conf` file also describes many of these directives.

Directive	Sample value	Description
`icap_enable`	`on`	Set this directive to “on” to enable the ICAP module.
`icap_io_timeout`	`70`	The amount of time in seconds to wait to establish an ICAP connection.
`icap_service_failure_limit`	`20`	The number of connection failures that are permitted when attempting to connect to Network Prevent (Web) Server.
`icap_service_revival_delay`	`30`	The time (in seconds) to wait before retrying the ICAP server after a connection failure.
`icap_preview_enable`	`on`	Enable the ICAP Preview feature so to speed ICAP message handling with Network Prevent (Web) Server. Note that this feature is disabled by default.
`icap_preview_size`	`0`	Change this value from the default value (-1) so that the Network Prevent (Web) Server can override the ICAP preview size.
`icap_persistent_connections`	`on`	Specifies that Squid should maintain a persistent connection to Network Prevent (Web) Server.
`icap_send_client_ip`	`on`	Specifies that Squid include the X-Client-IP header in ICAP requests to Network Prevent (Web) Server. Network Prevent (Web) uses the client IP address in this header to indicate the source of the incident.

Directive	Sample value	Description
`icap_send_client_username`	`on`	Specifies that Squid sends the authenticated HTTP client user name to the ICAP service when it is available. Network Prevent (Web) can include the user name in Symantec Data Loss Prevention incidents if the header is available in the X-Authenticated-User header. Use `icap_client_username_header` to specify the header in which to include the user name. Use `icap_client_username_encode` to specify the encoding for the user name.
`icap_client_username_header`	`X-Authenticated-User`	Specifies the header in which to store the authenticated HTTP client user name (when `icap_send_client_username` is set to `on`).
`icap_client_username_encode`	`on`	Specifies whether the authenticated HTTP client user name is encoded with Base64 transfer encoding.

4 Restart Squid to use the revised `squid.conf` file.

See "About starting and stopping Squid Web Proxy" on page 15.

Index

X