VYATTA, INC. | Vyatta System

Security

Reference Guide

Intrusion Protection System
Traffic Filtering
Web Filtering

Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

ISSUE DATE: April 2010

DOCUMENT REVISION. R6.0 v03

RELEASED WITH: R6.0

PART NO. A0-0219-10-0007

Table of Contents

Quick Reference to Commands

Use this section to help you quickly locate a command.

Quick List of Examples

Use this list to help you locate examples you'd like to try or look at.

Preface

This guide explains how to deploy security features of the Vyatta system. It describes the available commands and provides configuration examples.

This preface provides information about using this guide. The following topics are covered:

- Intended Audience
- Organization of This Guide
- Document Conventions
- Vyatta Publications

Intended Audience

This guide is intended for experienced system and network administrators. Depending on the functionality to be used, readers should have specific knowledge in the following areas:

- Networking and data communications
- TCP/IP protocols
- General router configuration
- Routing protocols
- Network administration
- Network security

Organization of This Guide

This guide has the following aid to help you find the information you are looking for:

- **Quick Reference to Commands**

  Use this section to help you quickly locate a command.

- **Quick List of Examples**

  Use this list to help you locate examples you'd like to try or look at.

This guide has the following chapters and appendixes:

Document Conventions

This guide contains advisory paragraphs and uses typographic conventions.

Advisory Paragraphs

This guide uses the following advisory paragraphs:

Warnings alert you to situations that may pose a threat to personal safety, as in the following example:

WARNING *Switch off power at the main breaker before attempting to connect the remote cable to the service power at the utility box.*

Cautions alert you to situations that might cause harm to your system or damage to equipment, or that may affect service, as in the following example:

CAUTION *Restarting a running system will interrupt service.*

Notes provide information you might need to avoid problems or configuration errors:

NOTE *You must create and configure network interfaces before enabling them for routing protocols.*

Typographic Conventions

This document uses the following typographic conventions:

`Monospace`	Examples, command-line output, and representations of configuration nodes.
`bold Monospace`	Your input: something you type at a command line.
bold	Commands, keywords, and file names, when mentioned inline. Objects in the user interface, such as tabs, buttons, screens, and panes.
italics	An argument or variable where you supply a value.
<key>	A key on your keyboard, such as <Enter>. Combinations of keys are joined by plus signs (“+”), as in <Ctrl>+c.
[*arg1* | *arg2*]	Enumerated options for completing a syntax. An example is [enable | disable].
num1–numN	A inclusive range of numbers. An example is 1–65535, which means 1 through 65535, inclusive.
arg1..argN	A range of enumerated values. An example is eth0..eth3, which means eth0, eth1, eth2, or eth3.
arg[*arg*...] *arg*[,*arg*...]	A value that can optionally represent a list of elements (a space-separated list in the first case and a comma-separated list in the second case).

Vyatta Publications

More information about the Vyatta system is available in the Vyatta technical library, and on www.vyatta.com and www.vyatta.org.

Full product documentation is provided in the Vyatta technical library. To see what documentation is available for your release, see the *Guide to Vyatta Documentation*. This guide is posted with every release of Vyatta software and provides a great starting point for finding the information you need.

Chapter 1: Intrusion Protection System

This chapter lists the commands for setting up intrustion detection and prevention, and traffic filtering on the Vyatta system.

This chapter presents the following topics:

- IPS Commands

IPS Commands

This chapter contains the following commands.

Configuration Commands	
content-inspection ips actions priority-1 <action>	Specifies the action to take for packets matching priority 1 IPS rules.
content-inspection ips actions priority-2 <action>	Specifies the action to take for packets matching priority 2 IPS rules.
content-inspection ips actions priority-3 <action>	Specifies the action to take for packets matching priority 3 IPS rules.
content-inspection ips actions other <action>	Specifies what to do with packets matching IPS rules with priority other than 1, 2, or 3.
content-inspection ips auto-update oink-code <code>	Records a Snort "oink code" for automatic Snort rule base updates.
content-inspection ips auto-update update-hour <hour>	Specifies the hour of the day for daily Snort rule base updates.
Operational Commands	
show ips log	Displays alerts logged by the IPS.
show ips summary	Displays a summary of all IPS alerts.
show ips update-log	Displays the history of automatic IPS rules updates.

content-inspection ips actions priority-1 <action>

Specifies the action to take for packets matching priority 1 IPS rules.

Syntax

set content-inspection ips actions priority-1 *action*

delete content-inspection ips actions priority-1

show content-inspection ips actions priority-1

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      actions {
         priority-1 [alert|drop|pass|sdrop]
      }
   }
}
```

Parameters

action	The action to take when a packet matches a priority 1 rule. Supported values are as follows: **alert**: Allows the packet and log an alert. **drop**: Drops the packet and log an alert. **pass**: Allows the packet and take no further action. **sdrop**: Drops packet but does not log an alert (that is, drops the packet silently).

Default

The default action is **drop**.

Usage Guidelines

Use this command to specify the action to take for packets matching priority 1 Intrusion Protection System (IPS) rules.

Use the **set** form of this command to specify the action.

Use the **delete** form of this command to restore the default action.

Use the **show** form of this command to display IPS priority 1 action configuration.

content-inspection ips actions priority-2 <action>

Specifies the action to take for packets matching priority 2 IPS rules.

Syntax

set content-inspection ips actions priority-2 *action*

delete content-inspection ips actions priority-2

show content-inspection ips actions priority-2

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      actions {
         priority-2 [alert|drop|pass|sdrop]
      }
   }
}
```

Parameters

action	The action to take when a packet matches a priority 2 rule. Supported values are as follows: **alert**: Allows the packet and log an alert. **drop**: Drops the packet and log an alert. **pass**: Allows the packet and take no further action. **sdrop**: Drops packet but does not log an alert (that is, drops the packet silently).

Default

The default action is **alert**.

Usage Guidelines

Use this command to specify the action to take for packets matching priority 2 Intrusion Protection System (IPS) rules.

Use the **set** form of this command to specify the action.

Use the **delete** form of this command to restore the default action.

Use the **show** form of this command to display IPS priority 2 action configuration.

content-inspection ips actions priority-3 <action>

Specifies the action to take for packets matching priority 3 IPS rules.

Syntax

set content-inspection ips actions priority-3 *action*

delete content-inspection ips actions priority-3

show content-inspection ips actions priority-3

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      actions {
         priority-3 [alert|drop|pass|sdrop]
      }
   }
}
```

Parameters

action	The action to take when a packet matches a priority 3 rule. Supported values are as follows: **alert**: Allows the packet and log an alert. **drop**: Drops the packet and log an alert. **pass**: Allows the packet and take no further action. **sdrop**: Drops packet but does not log an alert (that is, drops the packet silently).

Default

The default action is **alert**.

Usage Guidelines

Use this command to specify the action to take for packets matching priority 3 Intrusion Protection System (IPS) rules.

Use the **set** form of this command to specify the action.

Use the **delete** form of this command to restore the default action.

Use the **show** form of this command to display IPS priority 3 action configuration.

content-inspection ips actions other <action>

Specifies what to do with packets matching IPS rules with priority other than 1, 2, or 3.

Syntax

set content-inspection ips actions other *action*

delete content-inspection ips actions other

show content-inspection ips actions other

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      actions {
         other [alert|drop|pass|sdrop]
      }
   }
}
```

Parameters

action	The action to take when a packet matches a rule other than those having a priority of 1, 2, or 3. Supported values are as follows: **alert**: Allows the packet and log an alert. **drop**: Drops the packet and log an alert. **pass**: Allows the packet and take no further action. **sdrop**: Drops packet but does not log an alert (that is, drops the packet silently).

Default

The default action is **pass**.

Usage Guidelines

Use this command to specify what to do with packets matching Intrusion Protection System (IPS) rules other than rules with priority 1, 2, or 3.

Use the **set** form of this command to specify the action.

Use the **delete** form of this command to restore the default action.

Use the **show** form of this command to display IPS rule action configuration.

content-inspection ips auto-update oink-code <code>

Records a Snort “oink code” for automatic Snort rule base updates.

Syntax

set content-inspection ips auto-update oink-code *code*

delete content-inspection ips auto-update oink-code

show content-inspection ips auto-update oink-code

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      auto-update {
         oink-code text
      }
   }
}
```

Parameters

code	Mandatory if updates are to be received. The “oink” code generated at www.snort.org. This code is required in order to receive automatic IPS rule base updates from snort.org.

Default

None.

Usage Guidelines

Use this command to specify the “oink code” for downloading Snort rule updates.

The Vyatta system uses the Snort (www.snort.org) engine for intrusion detection. The Snort rule base can be automatically downloaded; however, in order to access Snort rule updates, you must register with the Snort organization and generate an “oink” code, which is used to authenticate the system.

Specify your oink code using this command. The Vyatta system uses this code when seeking rule base updates from the Snort organization.

A successful rule base update requires a restart of the Snort daemon. This restart can take five to ten seconds during which time the IPS will not be in effect.

Use the **set** form of this command to specify your Snort oink code.

Use the **delete** form of this command to remove Snort oink code configuration.

Use the **show** form of this command to display the configured Snort oink code.

content-inspection ips auto-update update-hour <hour>

Specifies the hour of the day for daily Snort rule base updates.

Syntax

set content-inspection ips auto-update update-hour *hour*

delete content-inspection ips auto-update update-hour

show content-inspection ips auto-update update-hour

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   ips {
      auto-update {
         update-hour u32
      }
   }
}
```

Parameters

hour	Mandatory if updates are to be received. The hour of the day at which to update the Snort rule base. The time is based on a 24-hour clock.

Default

None.

Usage Guidelines

Use this command to specify the hour of the day for Snort rule base updates.

A successful rule base update requires a restart of the Snort daemon. This restart can take five to ten seconds during which time the IPS will not be in effect.

Use the **set** form of this command to specify the hour of the day for rules updates.

Use the **delete** form of this command to remove the configuration.

Use the **show** form of this command to display the configuration.

show ips log

Displays alerts logged by the IPS.

Syntax

show ips log

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to see alerts logged by the Vyatta Intrusion Protection System (IPS).

Examples

Example 1-1 shows the first screen of output for **show ips log**.

Example 1-1 "show ips log": Displaying ips events

```
vyatta@R1:~$ show ips log
================================================
IPS events logged since Fri Apr 18 23:08:33 2008
================================================
2008-04-19 01:04:36.972690 {ICMP} 76.75.95.195 -> 76.74.103.8
(misc-activity) Misc activity (priority 3)
[1:483:5] ICMP PING CyberKit 2.2 Windows
------------------------------------------------------------
------------
2008-04-19 01:04:38.410018 {ICMP} 76.75.95.195 -> 76.74.103.64
(misc-activity) Misc activity (priority 3)
[1:483:5] ICMP PING CyberKit 2.2 Windows
------------------------------------------------------------
------------
2008-04-19 01:04:38.410091 {ICMP} 76.75.95.195 -> 76.74.103.65
(misc-activity) Misc activity (priority 3)
[1:483:5] ICMP PING CyberKit 2.2 Windows
------------------------------------------------------------
------------
2008-04-19 01:04:38.413503 {ICMP} 76.75.95.195 -> 76.74.103.66
(misc-activity) Misc activity (priority 3)
```

```
[1:483:5] ICMP PING CyberKit 2.2 Windows
------------------------------------------------------------------
------------
2008-04-19 01:04:38.417576 {ICMP} 76.75.95.195 -> 76.74.103.67
(misc-activity) Misc activity (priority 3)
[1:483:5] ICMP PING CyberKit 2.2 Windows
------------------------------------------------------------------
------------
```

show ips summary

Displays a summary of all IPS alerts.

Syntax

show ips summary

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to see a summary of all Intrusion Protection System (IPS) alerts.

Examples

Example 1-2 shows the output for **show ips summary**.

Example 1-2 "show ips summary": Displaying a summary of IPS alerts

```
vyatta@R1:~$ show ips summary
Processing log files...
Done.

============================================================
Summary of IPS events logged since Fri Apr 18 23:08:33 2008
============================================================
  Total number of events: 22331

  Breakdown by priorities:
    Priority 2: 17120
    Priority 3: 5211

  Breakdown by classes:
    bad-unknown: 9983 (Potentially Bad Traffic)
    attempted-recon: 95 (Attempted Information Leak)
    misc-activity: 5211 (Misc activity)
    misc-attack: 7042 (Misc Attack)

  Breakdown by signatures:
    [1:469:3]: 93 (ICMP PING NMAP)
```

```
    [1:476:4]: 2 (ICMP webtrends scanner)
    [1:483:5]: 5189 (ICMP PING CyberKit 2.2 Windows)
    [1:486:4]: 10 (ICMP Destination Unreachable Communication
with Destination Host is Administratively Prohibited)
    [1:524:8]: 12 (BAD-TRAFFIC tcp port 0 traffic)
    [1:527:8]: 9983 (DELETED BAD-TRAFFIC same SRC/DST)
    [1:2003:8]: 3521 (MS-SQL Worm propagation attempt)
    [1:2004:7]: 3521 (MS-SQL Worm propagation attempt OUTBOUND)

  Breakdown by dates:
    2008-04-19: 510
    2008-04-20: 1132
    2008-04-21: 1101
    2008-04-22: 2363
    2008-04-23: 2788
    2008-04-24: 1200
    2008-04-25: 1119
    2008-04-26: 7190
    2008-04-27: 2653
    2008-04-28: 1219
    2008-04-29: 1056

vyatta@R1:~$
```

show ips update-log

Displays the history of automatic IPS rules updates.

Syntax

show ips update-log

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to see a history of automatic Intrusion Protection System (IPS) rules updates.

Note that the first time an update is run the IPS system takes a few minutes to update the snort rules and the log file is not created until the first update is complete - so running this command prior to the first update completing could produce a “log not found” error.

Examples

Example 1-3 shows the output for **show ips update-log**.

Example 1-3 “show ips update-log”: Displaying ips rules update history

```
vyatta@R1:~$ show ips update-log
2008-06-18-015801: Failed to get
http://www.snort.org/pub-bin/oinkmaster.cgi/foo/snortrules-snap
shot-2.7.tar.gz
2008-06-18-015801: Update aborted due to error. IPS rules not
updated.
vyatta@R1:~$
```

Chapter 2: Traffic Filtering

This chapter lists the commands for setting up traffic filtering on the Vyatta system.

This chapter presents the following topics:

- Traffic Filtering Commands

Traffic Filtering Commands

This chapter contains the following commands.

Configuration Commands	
content-inspection traffic-filter <filter>	Specifies which traffic is to be processed by Vyatta IPS functions.
Operational Commands	
None	

content-inspection traffic-filter <filter>

Specifies which traffic is to be processed by Vyatta IPS functions.

Syntax

set content-inspection traffic-filter {**preset all** | **custom** *rule*}

delete content-inspection traffic-filter

show content-inspection traffic-filter

Command Mode

Configuration mode.

Configuration Statement

```
content-inspection{
   traffic-filter {
      preset all
      custom text
   }
}
```

Parameters

preset all	All IPv4 traffic is processed by the IPS.
custom *rule*	Specifies the name of an IPv4 firewall rule set (defined under “firewall name”) defining the type of traffic to be processed by the IPS.

Default

All traffic is processed when IPS is enabled.

Usage Guidelines

Use this command to specify the kind of traffic to be processed by Intrusion Protection System (IPS) functions.

Even if the traffic filter is specified, traffic is processed by the IPS only when the **ips** configuration node is defined.

Use the **set** form of this command to designate traffic for IPS filtering.

Use the **delete** form of this command to restore default traffic filtering.

Use the **show** form of this command to display traffic filter configuration.

Chapter 3: Web Filtering

This chapter explains how to set up web filtering on the Vyatta system.

This chapter presents the following topics:

- Web Filtering Configuration
- Web Filtering Commands

Web Filtering Configuration

This section presents the following topics:

- Web Filtering Overview
- Order of Evaluation
- Web Filtering Configuration Examples

Web Filtering Overview

The Vyatta system can be configured to act as a web proxy server for web caching and web filtering. To learn more about using the Vyatta system as a web proxy, please see the *Vyatta IP Services Reference Guide*.

When acting as a web proxy, the Vyatta system can also provide web filtering (URL filtering). Web filtering is an important tool for managing web access to reduce exposure to web-based threats, limit legal liabilities by blocking objectionable content, increase productivity, and manage bandwidth usage. The Vyatta system provides basic web filtering services as part of the Vyatta Core. Vyattaguard enhanced web filtering is available a Vyatta Plus service.

Web filtering is available as part of the Vyatta Core system, providing access to a list of filtering categories in a community-updated “blacklist.”

This feature is available only in Vyatta Plus.

Vyattaguard advanced web filtering is available as a subscription-based Vyatta Plus service offering which includes expanded content categorization (50+) and a continually updated database containing 350 million+ categorized URLs, as well as the ability to create customized whitelists and blacklists with time and date controls.

Key feature of Vyattaguard include the following:

- 50+ content categories
- 350+ million classified URLs
- Dynamic classification of new URLs
- Best feed of compromised, malicious, and phishing URLs
- Near real-time blocking of newly classified and malicious sites
- Up to 64 custom categories
- Unlimited custom URL categorizations
- Broad international coverage

- International domain name support includes domains with special characters
- Blend of automatic and human classification
- Fast response time in classifying new sites
- Granular URL classifications support specific pages, paths, subdomains, and parent domains
- Multiple categories per URL
- Reputation-based filtering services

NOTE *The vyattaguard database is considerably larger than the standard database. For this reason systems, that use Vyattaguard require an additional 2GB of disk space over the standard disk space requirements.*

Order of Evaluation

It is important to keep in mind the order that the various commands are evaluated in order to understand the results of web filtering. All filters contained within rules are evaluated first (in rule number order) followed by all global filters (i.e. those not contained within a rule). The filters, either within a rule or global, are evaluated in the following order:

1) local-ok

2) local-block

3) allow-ipaddr-url

4) block-category

5) allow-category

6) local-block-keyword

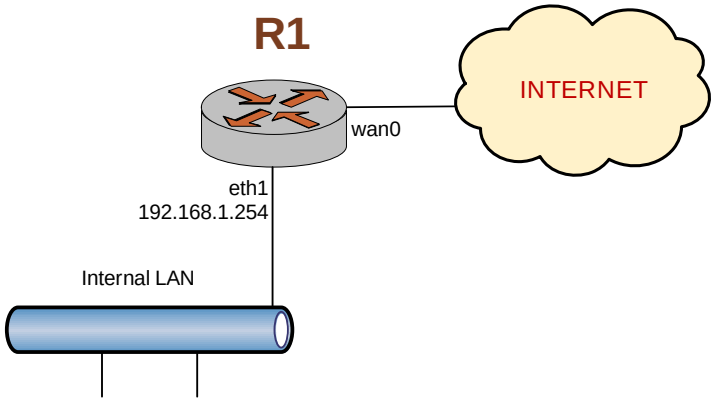
7) deafult-action

Web Filtering Configuration Examples

Figure 3-1 shows the web proxy deployment used in the examples in this section. In this scenario:

- Devices on the company’s internal LAN are accessing the Internet through the Vyatta system (R1).
- The web proxy is deployed on R1 to provide caching and web filtering functionality to employees accessing the Internet.

Figure 3-1 Web proxy



This section presents the following examples:

- Example 3-1 Blocking specific URLs
- Example 3-2 Verifying filtering
- Example 3-3 Filtering by content category
- Example 3-5 Allowing specific sites
- Example 3-6 Redirecting users
- Example 3-7 Handling different groups of users
- Example 3-8 Handling different time periods.
- Example 3-9 Creating a whitelist.

Blocking Specific URLs

Example 3-1 blocks specific URLs by explicitly specifying them using the **local-block** option, rather than by downloading and setting up a filter list. To block specific URLs on the Vyatta system, perform the following steps:

Example 3-1 Blocking specific URLs

Step	Command
Set the address to listen for requests on.	`vyatta@R1# set service webproxy listen-address 192.168.1.254` `[edit]`
Deny requests for the YouTube web site.	`vyatta@R1# set service webproxy url-filtering squidguard local-block youtube.com` `[edit]`

Example 3-1 Blocking specific URLs

Deny requests for the Facebook web site.	`vyatta@R1# set service webproxy url-filtering squidguard local-block facebook.com` `[edit]`
Commit the change	`vyatta@R1# commit` `[edit]`

Show the updated web proxy–related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  }`
	`}`
	`[edit]`

Verifying Filtering

You can verify that filtering is working for the previous example by enabling logging for the **local-block** category (“**log all”** would also work.). To view the results, use the **show webproxy blacklist log** command.

Example 3-2 enables logging for locally blocked URLs. To log web proxy functions in this way, perform the following steps:

Example 3-2 Verifying filtering

Step	Command
Set the web proxy to log everything filtered by the “local-block” option.	`vyatta@R1# set service webproxy url-filtering squidguard log local-block` `[edit]`
Commit the change	`vyatta@R1# commit` `[edit]`

Example 3-2 Verifying filtering

Show the updated web proxy–related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  log local-block`
	`  }`
	`}`
	`[edit]`

Filtering by Content Category

Example 3-3 uses a downloaded squidGuard database (downloaded using **update webproxy blacklists**) to filter web contents by content category. Customers using the Vyatta Plus advanced web filtering service, vyattaguard, would download a separate database (using **update webproxy vyattaguard**). In this example, web content is filtered for URLs related to advertisements, spyware, and gambling. To configure the web proxy in this way, perform the following steps:

Example 3-3 Filtering by content category

Step	Command
Block the ads category	`vyatta@R1# set service webproxy url-filtering squidguard block-category ads` `[edit]`
Block the spyware category	`vyatta@R1# set service webproxy url-filtering squidguard block-category spyware` `[edit]`
Block the gambling category	`vyatta@R1# set service webproxy url-filtering squidguard block-category gambling` `[edit]`
Commit the change	`vyatta@R1# commit` `[edit]`

Example 3-3 Filtering by content category

Show the updated web proxy–related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  block-category ads`
	`  block-category spyware`
	`  block-category gambling`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  log local-block`
	`  }`
	`}`
	`[edit]`

Filtering by Keyword

Example 3-4 uses keyword filtering to block access to sites that match a specific string of characters. In this example, access to all Chinese sites are blocked. To configure the web proxy in this way, perform the following steps:

Example 3-4 Filtering by keywords

Step	Command
Block access to Chinese sites.	`vyatta@R1# set service webproxy url-filtering squidguard local-block-keyword ".cn"` `[edit]`
Commit the change	`vyatta@R1# commit` `[edit]`

Example 3-4 Filtering by keywords

Show the updated web proxy–related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  block-category ads`
	`  block-category spyware`
	`  block-category gambling`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  local-block-keyword .cn`
	`  log local-block`
	`  }`
	`}`
	`[edit]`

Allowing Specific Sites

Example 3-5 enables sites that are blocked in virtue of being within a blocked category to be specifically allowed. In this example, the URL **www.company-ads.com** is specifically allowed, even though it falls within the blocked category of advertisements. To allow specific URLs, perform the following steps:

Example 3-5 Allowing specific sites

Step	Command
Allow users to access www.company-ads.com	`vyatta@R1# set service webproxy url-filtering squidguard local-ok www.company-ads.com` `[edit]`
Commit the change	`vyatta@R1# commit` `[edit]`

Example 3-5 Allowing specific sites

Show the updated web proxy–related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  block-category ads`
	`  block-category spyware`
	`  block-category gambling`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  local-block-keyword .cn`
	`  local-ok www.foobar.com`
	`  log local-block`
	`}`
	`[edit]`

Redirecting Users

By default, a user who tries to access a blocked site is sent to a pre-defined redirect site. The redirect site can be changed using the **redirect-url** command; another option is to display the reason (category) the requested URL was blocked.

Example 3-6 directs the system to display the category and URL of a blocked site when an access attempt is made by a user. To configure the web proxy in this way, perform the following steps:

Example 3-6 Redirecting users

Step	Command
Specify an HTTP query. The query shown in the example retrieves a squidGuard script that displays a blocked URL and the reason for blocking it. (Note the case in the query; HTTP queries are case-sensitive.)	`vyatta@R1# set service webproxy url-filtering squidguard redirect-url “http://192.168.1.254/cgi-bin/squidGuard-simple.cgi?targetclass=%t&url=%u”` `[edit]`
Commit the change.	`vyatta@R1# commit` `[edit]`

Example 3-6 Redirecting users

Show the updated webproxy-related configuration.	`vyatta@R1# show service webproxy`
	`listen-address 192.168.1.254 {`
	`}`
	`url-filtering {`
	`  squidguard {`
	`  block-category ads`
	`  block-category spyware`
	`  block-category gambling`
	`  local-block youtube.com`
	`  local-block facebook.com`
	`  local-block-keyword .cn`
	`  local-ok www.foobar.com`
	`  log local-block`
	`  redirect-url “http://192.168.1.254/cgi-bin/squidGuard-simple.cgi?targetclass=%t&url=%u”`
	`}`
	`[edit]`

Handling Different Groups of Users

To this point the examples assumed that all users would be treated equally. In the real world, some users need to be handled differently than others. The **source-group** command provides the ability to segregate users based on their specific IP address or the subnet that the are on.

Example 3-7 assumes the same network diagram as above (Example 3-1 Web proxy) but this time it is configured to address the needs of a school where system administrators, teachers, and students are each treated differently.

Example 3-7 Handling different groups of users

Step	Command
Remove the previous configuration.	`vyatta@R1# delete service webproxy url-filtering` `[edit]`
Commit the change.	`vyatta@R1# commit` `[edit]`
Redirect blocked requests to google.com	`vyatta@R1# set service webproxy url-filtering squidguard redirect-url “http://google.com”` `[edit]`

Example 3-7 Handling different groups of users

Create the administrators group (a single address).	vyatta@R1# **set service webproxy url-filtering squidguard source-group ADMIN address 10.0.5.15** [edit]
Create the teachers group (a single subnet).	vyatta@R1# **set service webproxy url-filtering squidguard source-group TEACHERS address 10.0.5.0/24** [edit]
Create the students group (the first of two subnets).	vyatta@R1# **set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.1.0/24** [edit]
Create the students group (the second of two subnets).	vyatta@R1# **set service webproxy url-filtering squidguard source-group STUDENTS address 10.0.2.0/24** [edit]
Create the rule to filter requests from the ADMIN group. In this case nothing gets filtered.	vyatta@R1# **set service webproxy url-filtering squidguard rule 10 source-group ADMIN** [edit]
Create the rule to filter requests from the TEACHERS group.	vyatta@R1# **set service webproxy url-filtering squidguard rule 20 source-group TEACHERS** [edit]
Block the "porn" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 20 block-category porn** [edit]
Block the "shopping" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 20 block-category shopping** [edit]
Create the rule to filter requests from the STUDENTS group.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 source-group STUDENTS** [edit]
Block the "adult" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 block-category adult** [edit]
Block the "warez" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 block-category warez** [edit]
Block the "drugs" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 block-category drugs** [edit]
Block the "filehosting" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 block-category filehosting** [edit]

Example 3-7 Handling different groups of users

Block the "audio-video" category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 30 block-category audio-video** [edit]
Commit the change.	vyatta@R1# **commit** [edit]

Show the new webproxy-related configuration.	vyatta@R1# **show service webproxy**
	listen-address 192.168.1.254 {
	}
	url-filtering {
	  squidguard {
	  redirect-url http://google.com
	  rule 10 {
	  source-group ADMIN
	  }
	  rule 20 {
	  block-category porn
	  block-category shopping
	  source-group TEACHERS
	  }
	  rule 30 {
	  block-category adult
	  block-category audio-video
	  block-category drugs
	  block-category filehosting
	  block-category warez
	  source-group STUDENTS
	  }
	  source-group ADMIN{
	  address 10.0.5.15
	  }
	  source-group STUDENTS {
	  address 10.0.1.0/24
	  address 10.0.2.0/24
	  }
	  source-group TEACHERS{
	  address 10.0.5.0/24
	  }
	  }
	}
	[edit]

Handling Different Time Periods

In the previous example the filtering rules applied at all times. In order to change the filtering for a group based on the day of the week and the time of day the **time-period** command is used.

Example 3-8 shows how to change the filtering based on time period. In this case, the teachers will be allowed to access sites in the “shopping” category but only during non-school hours.

Example 3-8 Handling different time periods.

Step	Command
Define the SCHOOLHOURS time period.	vyatta@R1# **set service webproxy url-filtering squidguard time-period SCHOOLHOURS days weekdays time “09:00-12:00, 13:00-16:00”** [edit]
Create a new rule to filter requests from the TEACHERS group.	vyatta@R1# **set service webproxy url-filtering squidguard rule 25 source-group TEACHERS** [edit]
Block only the “porn” category.	vyatta@R1# **set service webproxy url-filtering squidguard rule 25 block-category porn** [edit]
Apply the more restrictive rule (rule 20) to the teachers during school hours.	vyatta@R1# **set service webproxy url-filtering squidguard rule 20 time-period SCHOOLHOURS** [edit]
Apply the less restrictive rule (rule 25) to the teachers during non-school hours (using “!” to negate the time period).	vyatta@R1# **set service webproxy url-filtering squidguard rule 25 time-period !SCHOOLHOURS** [edit]
Commit the change.	vyatta@R1# **commit** [edit]

Example 3-8 Handling different time periods.

Show the new webproxy-related configuration.

```
vyatta@R1# show service webproxy
listen-address 192.168.1.254 {
}
url-filtering {
   squidguard {
      redirect-url http://google.com
      rule 10 {
         source-group ADMIN
      }
      rule 20 {
         block-category porn
         block-category shopping
         source-group TEACHERS
         time-period SCHOOLHOURS
      }
      rule 25 {
         block-category porn
         source-group TEACHERS
         time-period !SCHOOLHOURS
      }
      rule 30 {
         block-category adult
         block-category audio-video
         block-category drugs
         block-category filehosting
         block-category warez
         source-group STUDENTS
      }
      source-group ADMIN{
         address 10.0.5.15
      }
      source-group STUDENTS {
         address 10.0.1.0/24
         address 10.0.2.0/24
      }
      source-group TEACHERS{
         address 10.0.5.0/24
      }
   }
}
[edit]
```

Creating a Whitelist

The typical usage of web filtering is to allow access to all sites except those that are blocked using the various blocking filters. There are instances whare the general case is to block access to all sites except a chosen few - a “whitelist”.

Example 3-9 shows how to create a whitelist.

Example 3-9 Creating a whitelist.

Step	Command
Remove the previous configuration.	`vyatta@R1# delete service webproxy url-filtering` `[edit]`
Commit the change.	`vyatta@R1# commit` `[edit]`
Redirect blocked requests to google.com.	`vyatta@R1# set service webproxy url-filtering squidguard redirect-url “http://google.com”` `[edit]`
Set the default action to block access to all sites.	`vyatta@R1# set service webproxy url-filtering squidguard default-action block` `[edit]`
Allow access to “vyatta.com”.	`vyatta@R1# set service webproxy url-filtering squidguard local-ok vyatta.com` `[edit]`
Allow access to “vyatta.org”.	`vyatta@R1# set service webproxy url-filtering squidguard local-ok vyatta.org` `[edit]`
Allow access to “google.com”.	`vyatta@R1# set service webproxy url-filtering squidguard local-ok google.com` `[edit]`
Commit the change.	`vyatta@R1# commit` `[edit]`

Example 3-9 Creating a whitelist.

Show the new webproxy-related configuration.	vyatta@R1# **show service webproxy**
	listen-address 192.168.1.254 {
	}
	url-filtering {
	  squidguard {
	  default-action block
	  local-ok google.com
	  local-ok vyatta.com
	  local-ok vyatta.org
	  redirect-url http://google.com
	  }
	}
	[edit]

Web Filtering Commands

This chapter contains the following commands.

Configuration Commands	
service webproxy domain-block <domain>	Specifies a domain to block.
service webproxy domain-noncache <domain>	Specifies a domain that is not to be cached.
service webproxy reply-block-mime <mime-type>	Specifies a mime type to block.
service webproxy url-filtering squidguard	Blocks URLs in all categories.
service webproxy url-filtering squidguard allow-ipaddr-url	Specifies that direct IP address requests should be allowed.
service webproxy url-filtering squidguard auto-update update-hour <hour>	Sets the hour of the day at which to check for squidGuard database updates.
service webproxy url-filtering squidguard block-category <category>	Blocks web content by squidGuard database category.
service webproxy url-filtering squidguard default-action <action>	Specifies the default action to take for all traffic passing through the webproxy.
service webproxy url-filtering squidguard enable-safe-search	Enables Safe Search on many popular search engines.
service webproxy url-filtering squidguard local-block <address>	Defines a specific IP address or URL to be blocked.
service webproxy url-filtering squidguard local-block-keyword <keyword>	Defines a URL substring within a URL to be blocked.
service webproxy url-filtering squidguard local-ok <address>	Specifies an IP address or URL to allow.
service webproxy url-filtering squidguard log <category>	Enables logging for a squidGuard database category.
service webproxy url-filtering squidguard rule <rule-num>	Specifies a web filtering rule.
service webproxy url-filtering squidguard rule <rule-num> allow-ipaddr-url	Specifies that direct IP address requests should be allowed.
service webproxy url-filtering squidguard rule <rule-num> block-category <category>	Blocks web content by squidGuard database category within the rule.
service webproxy url-filtering squidguard rule <rule-num> default-action <action>	Specifies the default action to take for traffic within the rule.
service webproxy url-filtering squidguard rule <rule-num> description <desc>	Specifies a brief description for a web filtering policy rule.

service webproxy url-filtering squidguard rule <rule-num> enable-safe-search	Enables Safe Search on many popular search engines for a web filtering policy rule.
service webproxy url-filtering squidguard rule <rule-num> local-block <address>	Defines a specific IP address or URL to be blocked within the rule.
service webproxy url-filtering squidguard rule <rule-num> local-block-keyword <keyword>	Defines a URL substring within a URL to be blocked within the rule.
service webproxy url-filtering squidguard rule <rule-num> local-ok <address>	Specifies an IP address or URL to allow within the rule.
service webproxy url-filtering squidguard rule <rule-num> log <category>	Enables logging for a squidGuard database category within the rule.
service webproxy url-filtering squidguard rule <rule-num> redirect-url <url>	Specifies a URL to redirect users to when a blacklisted URL is requested within the rule.
service webproxy url-filtering squidguard rule <rule-num> source-group <group-name>	Specifies the source group to be used for the web filtering rule.
service webproxy url-filtering squidguard rule <rule-num> time-period <period-name>	Specifies the time period to be used for the web filtering rule.
service webproxy url-filtering squidguard redirect-url <url>	Specifies a URL to redirect users to when a blacklisted URL is requested.
service webproxy url-filtering squidguard source-group <group-name>	Specifies a web filtering source group.
service webproxy url-filtering squidguard source-group <group-name> address <addr>	Specifies an IPv4 address or subnet to include in the web filtering source group.
service webproxy url-filtering squidguard source-group <group-name> description <desc>	Specifies a brief description for a web filtering source group.
service webproxy url-filtering squidguard source-group <group-name> domain <domain>	Specifies a domain to include in a web filtering source group.
service webproxy url-filtering squidguard time-period <period-name>	Specifies a time period to be used in a web filtering rule.
service webproxy url-filtering squidguard time-period <period-name> days <day> time <time>	Specifies a day and time included in the time period.
service webproxy url-filtering squidguard time-period <period-name> description <desc>	Specifies a brief description for the time period.
service webproxy url-filtering squidguard vyattaguard mode	Specifies how the vyattaguard system will operate.
Operational Commands	
clear webproxy process	Restarts the webproxy service.

show webproxy blacklist categories	Displays all categories defined in the installed squidGuard database.
show webproxy blacklist domains	Displays all domains listed in the installed database.
show webproxy blacklist log	Displays the log for blacklisted URLs.
show webproxy blacklist search <filter>	Displays domains and/or URLs matching search text.
show webproxy blacklist urls	Displays all URLs in squidGuard database categories.
show webproxy log	Displays the web proxy log.
show webproxy vyattaguard categories	Displays all categories defined in the installed vyattaguard database.
show webproxy vyattaguard search <filter>	Displays domains and/or URLs in the vyattaguard database matching search text.
update webproxy blacklists	Updates the squidGuard database.
update webproxy vyattaguard	Updates the vyattaguard database.

clear webproxy process

Restarts the webproxy service.

Syntax

clear webproxy process

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to restart the webproxy service..

Examples

Example 3-11 displays output for **clear webproxy process**.

Example 3-10 Restarting the webproxy service

```
vyatta@R1> clear webproxy process
Restarting Squid HTTP Proxy 3.0: squid3
Waiting......................done.
.
vyatta@R1>
```

service webproxy domain-block <domain>

Specifies a domain to block.

Syntax

set service webproxy domain-block *domain*

delete service webproxy domain-block *domain*

show service webproxy domain-block

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      domain-block text
   }
}
```

Parameters

domain	Multi-node. The domain to block.

Default

None

Usage Guidelines

Use this command to block access to the specified domain. For example, specifying “facebook.com” will block all access to facebook.com, and specifying “.cn” will block all access to Chinese sites.

Use the **set** form of this command to specify the domain to block.

Use the **delete** form of this command to restore access to the domain.

Use the **show** form of this command to view the configuration.

service webproxy domain-noncache <domain>

Specifies a domain that is not to be cached.

Syntax

set service webproxy domain-noncache *domain*

delete service webproxy domain-noncache *domain*

show service webproxy domain-noncache

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      domain-noncache text
   }
}
```

Parameters

domain	Multi-node. The domain that is not to be cached.

Default

All domains are cached.

Usage Guidelines

Use this command to allow access to sites in a domain without caching them. For example, specifying “facebook.com” will allow access to “facebook.com” but the pages accessed will not be cached. This is useful when data on certain sites is sensitive and it caching it on the Vyatta system’s disk poses a security risk. It is also useful for working around problems with “If-Modified-Since” checking at certain sites.

Use the **set** form of this command to specify the domain that should not be cached.

Use the **delete** form of this command to restore caching of sites on the domain.

Use the **show** form of this command to view the configuration.

service webproxy reply-block-mime <mime-type>

Specifies a mime type to block.

Syntax

set service webproxy reply-block-mime *mime-type*

delete service webproxy reply-block-mime *mime-type*

show service webproxy reply-block-mime *mime-type*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      reply-block-mime text {
      }
   }
}
```

Parameters

mime-type	Mime type to block. Mime type are specified in a “type/sub-type” format. For example, the mime type for Quicktime video is “video/quicktime”, the mime type for .pdf files is “application/pdf”, and the mime type for .wav files is “audio/wav”.

Default

None.

Usage Guidelines

Use this command to specify the mime type to block.

Use the **set** form of this command to specify the mime type to block.

Use the **delete** form of this command to allow the mime type.

Use the **show** form of this command to view the mime type.

service webproxy url-filtering squidguard

Blocks URLs in all categories.

Syntax

set service webproxy url-filtering squidguard

delete service webproxy url-filtering squidguard

show service webproxy url-filtering squidguard

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {}
      }
   }
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command with no additional configuration nodes to block URLs in all squidGuard categories. Specifying additional nodes in the configuration tree under **squidguard** refines the URLs to be blocked.

Use the **set** form of this command to apply web filtering.

Use the **delete** form of this command to remove web filtering.

Use the **show** form of this command to view web filtering configuration.

service webproxy url-filtering squidguard allow-ipaddr-url

Specifies that direct IP address requests should be allowed.

Syntax

set service webproxy url-filtering squidguard allow-ipaddr-url

delete service webproxy url-filtering squidguard allow-ipaddr-url

show service webproxy url-filtering squidguard allow-ipaddr-url

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            allow-ipaddr-url
         }
      }
   }
}
```

Parameters

None.

Default

Direct IP address requests are blocked.

Usage Guidelines

By default, all accesses made directly to an IP address are blocked. Use this command to specify that direct IP address requests should not be blocked.

Use the **set** form of this command to allow direct IP address requests.

Use the **delete** form of this command to restore the default and block direct IP address requests.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard auto-update update-hour <hour>

Sets the hour of the day at which to check for squidGuard database updates.

Syntax

set service webproxy url-filtering squidguard auto-update update-hour *hour*

delete service webproxy url-filtering squidguard auto-update update-hour

show service webproxy url-filtering squidguard auto-update update-hour

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            auto-update {
               update-hour 0-23
            }
         }
      }
   }
}
```

Parameters

hour	The hour of the day (using a 24 hour clock) at which the web proxy service will check for database updates. Possible values range from 0 (12:00am) to 23 (11:00pm).

Default

The system will not check for database updates.

Usage Guidelines

Use this command to specify the hour of the day at which the system should check for database updates.

Use the **set** form of this command to set the hour of the day to check for database updates.

Use the **delete** form of this command to stop the system from checking for updates.

Use the **show** form of this command to view update hour configuration.

service webproxy url-filtering squidguard block-category <category>

Blocks web content by squidGuard database category.

Syntax

set service webproxy url-filtering squidguard block-category *category*

delete service webproxy url-filtering squidguard block-category *category*

show service webproxy url-filtering squidguard block-category

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            block-category text
         }
      }
   }
}
```

Parameters

category	Multi-node. The database category to block, or the keyword **all** to block all categories. You can block more than one category by creating multiple **block-category** configuration nodes.

Default

When the **squidguard** configuration node is defined with no block categories, all categories are blocked.

Usage Guidelines

Use this command to specify database categories to block.

The categories available will vary with the specific database. To view the categories defined in the installed database, issue the **show webproxy blacklist categories** command (see page 110).

Use the **set** form of this command to block a database category.

Use the **delete** form of this command to stop a database category from being blocked.

Use the **show** form of this command to view the database categories blocking configuration.

service webproxy url-filtering squidguard default-action <action>

Specifies the default action to take for all traffic passing through the webproxy.

Syntax

set service webproxy url-filtering squidguard default-action *action*

delete service webproxy url-filtering squidguard default-action

show service webproxy url-filtering squidguard default-action

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            default-action [allow|block]
         }
      }
   }
}
```

Parameters

action	The default action to take on all traffic passing through the webproxy. **allow**: Allow all traffic through by default. **block**: Block all traffic by default.

Default

Traffic is allowed through the webproxy.

Usage Guidelines

Use this command to specify the default action to take on traffic passing through the webproxy.

Use the **set** form of this command to specify the default action.

Use the **delete** form of this command to restore the default action to its default behavior.

Use the **show** form of this command to view the default action configuration.

service webproxy url-filtering squidguard enable-safe-search

Enables Safe Search on many popular search engines.

Syntax

set service webproxy url-filtering squidguard enable-safe-search

delete service webproxy url-filtering squidguard enable-safe-search

show service webproxy url-filtering squidguard

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            enable-safe-search
         }
      }
   }
}
```

Parameters

None.

Default

Safe Search is not enabled on any search engines.

Usage Guidelines

Use this command to modify requests to many popular search engines to perform Safe Search in order to filter out objectionable content. The search engines that are currently supported include: Google, Yahoo, MSN, and Bing.

Use the **set** form of this command to enable Safe Search on many popular search engines.

Use the **delete** form of this command to return URL filtering to its default (non-Safe Search) behavior.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard local-block <address>

Defines a specific IP address or URL to be blocked.

Syntax

set service webproxy url-filtering squidguard local-block *address*

delete service webproxy url-filtering squidguard local-block *address*

show service webproxy url-filtering squidguard local-block

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-block text
         }
      }
   }
}
```

Parameters

address	Multi-node. An IP address or URL to be blocked. You can block a number of IP addresses and/or URLs by creating multiple **local-block** configuration nodes.

Default

None.

Usage Guidelines

Use this command to specify an IP address or URL to be blocked. This allows you to block sites not belonging to a database category.

Use the **set** form of this command to block a specific IP address or URL.

Use the **delete** form of this command to stop an IP address or URL from being blocked.

Use the **show** form of this command to view individual blocking configuration.

service webproxy url-filtering squidguard local-block-keyword <keyword>

Defines a URL substring within a URL to be blocked.

Syntax

set service webproxy url-filtering squidguard local-block-keyword *keyword*

delete service webproxy url-filtering squidguard local-block-keyword *keyword*

show service webproxy url-filtering squidguard local-block-keyword

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-block-keyword text
         }
      }
   }
}
```

Parameters

keyword	Multi-node. A substring or regular expression (regex) matching a URL to be blocked. You can block a number of URLs by creating multiple **local-block-keyword** configuration nodes.

Default

None.

Usage Guidelines

Use this command to specify a substring or regular expression matching a URL to be blocked. This allows you to block sites not belonging to a database category.

NOTE *Use this command with caution as specifying a non-specific substring can match unintended URLs. In addition, this command is CPU intensive and can degrade performance.*

Use the **set** form of this command to specify the substring or regular expression to match.

Use the **delete** form of this command to remove the substring or regular expression from the configuration.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard local-ok <address>

Specifies an IP address or URL to allow.

Syntax

set service webproxy url-filtering squidguard local-ok *address*

delete service webproxy url-filtering squidguard local-ok *address*

show service webproxy url-filtering squidguard local-ok

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            local-ok text
         }
      }
   }
}
```

Parameters

address	Multi-node. An IP address or URL to allow.

Default

None.

Usage Guidelines

Use this command to allow an IP address or URL that blocked because it belongs to a squidGuard database category.

Use the **set** form of this command to specify an IP address or URL to allow.

Use the **delete** form of this command to return an IP address or URL in a blocked category to being blocked.

Use the **show** form of this command to view IP addresses and URLs being specifically allowed.

service webproxy url-filtering squidguard log <category>

Enables logging for a squidGuard database category.

Syntax

set service webproxy url-filtering squidguard log *category*

delete service webproxy url-filtering squidguard log *category*

show service webproxy url-filtering squidguard log

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            log text
         }
      }
   }
}
```

Parameters

category	Multi-node. The squidGuard database category to log, or the keyword **all** to log all categories.

Default

Web proxy web filtering is not logged.

Usage Guidelines

Use this command to direct the system to log filtering of squidGuard database categories.

Use the **set** form of this command to specify a database category to be logged.

Use the **delete** form of this command to stop the system from logging a database category.

Use the **show** form of this command to view database category logging configuration.

service webproxy url-filtering squidguard rule <rule-num>

Specifies a web filtering rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num*

delete service webproxy url-filtering squidguard rule *rule-num*

show service webproxy url-filtering squidguard rule *rule-num*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.

Default

None.

Usage Guidelines

Use this command to define a web filtering rule. web filtering rules are evaluated in a sequence according to rule number.

Use the **set** form of this command to specify a web filtering rule.

Use the **delete** form of this command to remove the web filtering rule.

Use the **show** form of this command to view the web filtering rule configuration.

service webproxy url-filtering squidguard rule <rule-num> allow-ipaddr-url

Specifies that direct IP address requests should be allowed.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **allow-ipaddr-url**

delete service webproxy url-filtering squidguard rule *rule-num* **allow-ipaddr-url**

show service webproxy url-filtering squidguard rule *rule-num* **allow-ipaddr-url**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               allow-ipaddr-url
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.

Default

Direct IP address requests are blocked.

Usage Guidelines

By default, all accesses made directly to an IP address are blocked. Use this command to specify that direct IP address requests should not be blocked.

Use the **set** form of this command to allow direct IP address requests.

Use the **delete** form of this command to restore the default and block direct IP address requests.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard rule <rule-num> block-category <category>

Blocks web content by squidGuard database category within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **block-category** *category*

delete service webproxy url-filtering squidguard rule *rule-num* **block-category** *category*

show service webproxy url-filtering squidguard rule *rule-num* **block-category**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               block-category text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
category	Multi-node. The database category to block, or the keyword **all** to block all categories. You can block more than one category by creating multiple **block-category** configuration nodes.

Default

When the **rule** is defined with no block categories, all categories are blocked within the rule.

Usage Guidelines

Use this command to specify database categories to block within the rule.

The categories available will vary with the specific database. To view the categories defined in the installed database, issue the **show webproxy blacklist categories** command (see page 110).

Use the **set** form of this command to block a database category.

Use the **delete** form of this command to stop a database category from being blocked.

Use the **show** form of this command to view the database categories blocking configuration.

service webproxy url-filtering squidguard rule <rule-num> default-action <action>

Specifies the default action to take for traffic within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **default-action** *action*

delete service webproxy url-filtering squidguard rule *rule-num* **default-action**

show service webproxy url-filtering squidguard rule *rule-num* **default-action**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               default-action [allow|block]
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
action	The default action to take on all traffic passing through the webproxy. **allow**: Allow all traffic through by default. **block**: Block all traffic by default.

Default

Traffic is allowed through the webproxy.

Usage Guidelines

Use this command to specify the default action to take on traffic within the rule.

Use the **set** form of this command to specify the default action.

Use the **delete** form of this command to restore the default action to its default behavior.

Use the **show** form of this command to view the default action configuration.

service webproxy url-filtering squidguard rule <rule-num> description <desc>

Specifies a brief description for a web filtering policy rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **description** *desc*

delete service webproxy url-filtering squidguard rule *rule-num* **description**

show service webproxy url-filtering squidguard rule *rule-num* **description**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               description text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
desc	A description of the policy rule. If the description contains spaces then it must be contained in double quotes.

Default

None.

Usage Guidelines

Use this command to specify a description of a web filtering policy rule.

Use the **set** form of this command to specify the description of the policy rule specified by the policy rule number.

Use the **delete** form of this command to remove the description of the policy rule specified by the policy rule number.

Use the **show** form of this command to view the description of the policy rule specified by the policy rule number.

service webproxy url-filtering squidguard rule <rule-num> enable-safe-search

Enables Safe Search on many popular search engines for a web filtering policy rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **enable-safe-search**

delete service webproxy url-filtering squidguard rule *rule-num* **enable-safe-search**

show service webproxy url-filtering squidguard rule *rule-num*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               enable-safe-search
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.

Default

Safe Search is not enabled on any search engines.

Usage Guidelines

Use this command to modify requests to many popular search engines to perform Safe Search in order to filter out objectionable content for this policy rule. The search engines that are currently supported include: Google, Yahoo, MSN, and Bing.

Use the **set** form of this command to enable Safe Search on many popular search engines for this policy rule.

Use the **delete** form of this command to return URL filtering for this policy rule to its default (non-Safe Search) behavior.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard rule <rule-num> local-block <address>

Defines a specific IP address or URL to be blocked within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **local-block** *address*

delete service webproxy url-filtering squidguard rule *rule-num* **local-block** *address*

show service webproxy url-filtering squidguard rule *rule-num* **local-block**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               local-block text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
address	Multi-node. An IP address or URL to be blocked within the rule. You can block a number of IP addresses and/or URLs by creating multiple **local-block** configuration nodes.

Default

None.

Usage Guidelines

Use this command to specify an IP address or URL to be blocked within the rule. This allows you to block sites not belonging to a database category.

Use the **set** form of this command to block a specific IP address or URL.

Use the **delete** form of this command to stop an IP address or URL from being blocked.

Use the **show** form of this command to view individual blocking configuration.

service webproxy url-filtering squidguard rule <rule-num> local-block-keyword <keyword>

Defines a URL substring within a URL to be blocked within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **local-block-keyword** *keyword*

delete service webproxy url-filtering squidguard rule *rule-num* **local-block-keyword** *keyword*

show service webproxy url-filtering squidguard rule *rule-num* **local-block-keyword**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               local-block-keyword text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
keyword	Multi-node. A substring or regular expression (regex) matching a URL to be blocked within the rule. You can block a number of URLs by creating multiple **local-block-keyword** configuration nodes.

Default

None.

Usage Guidelines

Use this command to specify a substring or regular expression matching a URL to be blocked within the rule. This allows you to block sites not belonging to a database category.

NOTE *Use this command with caution as specifying a non-specific substring can match unintended URLs. In addition, this command is CPU intensive and can degrade performance.*

Use the **set** form of this command to specify the substring or regular expression to match..

Use the **delete** form of this command to remove the substring or regular expression from the configuration.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard rule <rule-num> local-ok <address>

Specifies an IP address or URL to allow within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **local-ok** *address*

delete service webproxy url-filtering squidguard rule *rule-num* **local-ok** *address*

show service webproxy url-filtering squidguard rule *rule-num* **local-ok**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               local-ok text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
address	Multi-node. An IP address or URL to allow within the rule.

Default

None.

Usage Guidelines

Use this command to allow an IP address or URL (within the rule) that blocked because it belongs to a squidGuard database category.

Use the **set** form of this command to specify an IP address or URL to allow.

Use the **delete** form of this command to return an IP address or URL in a blocked category to being blocked.

Use the **show** form of this command to view IP addresses and URLs being specifically allowed.

service webproxy url-filtering squidguard rule <rule-num> log <category>

Enables logging for a squidGuard database category within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **log** *category*

delete service webproxy url-filtering squidguard rule *rule-num* **log** *category*

show service webproxy url-filtering squidguard rule *rule-num* **log**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               log text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
category	Multi-node. The squidGuard database category to log, or the keyword **all** to log all categories within the rule.

Default

Web proxy web filtering is not logged.

Usage Guidelines

Use this command to direct the system to log filtering of squidGuard database categories within the rule.

Use the **set** form of this command to specify a database category to be logged.

Use the **delete** form of this command to stop the system from logging a database category.

Use the **show** form of this command to view database category logging configuration.

service webproxy url-filtering squidguard rule <rule-num> redirect-url <url>

Specifies a URL to redirect users to when a blacklisted URL is requested within the rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **redirect-url** *url*

delete service webproxy url-filtering squidguard rule *rule-num* **redirect-url**

show service webproxy url-filtering squidguard rule *rule-num* **redirect-url**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               redirect-url text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
url	The URL to which to redirect users when the user attempts to access a blacklisted URL.

Default

Users attempting to access a blacklisted site are redirected to the global redirect URL.

Usage Guidelines

Use this command to specify a redirect URL for users attempting to access a filtered URL within the rule. If no redirect URL is specified within the rule then the global redirect URL is used.

NOTE *It is important to make sure that the redirect URL specified is not a blocked site. For example, if the* ***default-action*** *is set to* ***block*** *and the* ***redirect-url*** *is not included in the* ***local-ok*** *list then it will not be able to redirect the user as expected.*

Use the **set** form of this command to specify a redirect URL.

Use the **delete** form of this command to restore the default redirect URL.

Use the **show** form of this command to view redirect URL configuration.

service webproxy url-filtering squidguard rule <rule-num> source-group <group-name>

Specifies the source group to be used for the web filtering rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **source-group** *group-name*

delete service webproxy url-filtering squidguard rule *rule-num* **source-group**

show service webproxy url-filtering squidguard rule *rule-num* **source-group**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               source-group text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
group-name	Mandatory. The source group to be used for the web filtering rule.

Default

None.

Usage Guidelines

Use this command to specify the source group to be used for the web filtering rule. A source group must be specified. Source groups must be pre-defined using the **service webproxy url-filtering squidguard source-group <group-name>** command (see page 94) before they can be specified here.

Use the **set** form of this command to specify the source group to use for the web filtering rule.

Use the **delete** form of this command to remove the source group.

Use the **show** form of this command to view the source group configuration.

service webproxy url-filtering squidguard rule <rule-num> time-period <period-name>

Specifies the time period to be used for the web filtering rule.

Syntax

set service webproxy url-filtering squidguard rule *rule-num* **time-period** *period-name*

delete service webproxy url-filtering squidguard rule *rule-num* **time-period**

show service webproxy url-filtering squidguard rule *rule-num* **time-period**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            rule 1-1024 {
               time-period text
            }
         }
      }
   }
}
```

Parameters

rule-num	Multi-node. Defines a web filtering rule. The rule number specifies the order in which the rule is evaluated. Each rule must have a unique rule number. The range is 1 to 1024.
period-name	The time period to be used for the web filtering rule.

Default

The web filtering rule is valid at all times.

Usage Guidelines

Use this command to specify the time period to be used for the web filtering rule. Time periods must be pre-defined using the **service webproxy url-filtering squidguard time-period <period-name>** command (see page 102) before they can be specified here. Use "!" to negate the time period (i.e. include all times not specified in the time period definition).

Use the **set** form of this command to specify the time period to use for the web filtering rule.

Use the **delete** form of this command to remove the time period and make the web filtering rule valid at all times.

Use the **show** form of this command to view the time period configuration.

service webproxy url-filtering squidguard redirect-url <url>

Specifies a URL to redirect users to when a blacklisted URL is requested.

Syntax

set service webproxy url-filtering squidguard redirect-url *url*

delete service webproxy url-filtering squidguard redirect-url

show service webproxy url-filtering squidguard redirect-url

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            redirect-url text
         }
      }
   }
}
```

Parameters

url	The URL to which to redirect users when the user attempts to access a blacklisted URL. By default, users are redirected to a pre-defined site.

Default

Users attempting to access a blacklisted site are redirected to a pre-defined site.

Usage Guidelines

Use this command to specify a redirect URL for users attempting to access a filtered URL.

NOTE *It is important to make sure that the redirect URL specified is not a blocked site. For example, if the* ***default-action*** *is set to* ***block*** *and the* ***redirect-url*** *is not included in the* ***local-ok*** *list then it will not be able to redirect the user as expected.*

Use the **set** form of this command to specify a redirect URL.

Use the **delete** form of this command to restore the default redirect URL.

Use the **show** form of this command to view redirect URL configuration.

service webproxy url-filtering squidguard source-group <group-name>

Specifies a web filtering source group.

Syntax

set service webproxy url-filtering squidguard source-group *group-name*

delete service webproxy url-filtering squidguard source-group *group-name*

show service webproxy url-filtering squidguard source-group *group-name*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group text {
            }
         }
      }
   }
}
```

Parameters

group-name	Multi-node. A web filtering source group.

Default

None.

Usage Guidelines

Use this command to define a web filtering source group to provide a way to filter traffic from a specific set of addresses or subnets rather than filtering all traffic.

Use the **set** form of this command to specify a web filtering source group.

Use the **delete** form of this command to remove the web filtering source group.

Use the **show** form of this command to view the web filtering source group configuration.

service webproxy url-filtering squidguard source-group <group-name> address <addr>

Specifies an IPv4 address or subnet to include in the web filtering source group.

Syntax

set service webproxy url-filtering squidguard source-group *group-name* **address** *addr*

delete service webproxy url-filtering squidguard source-group *group-name* **address** *addr*

show service webproxy url-filtering squidguard source-group *group-name* **address** *addr*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group text {
               address text
            }
         }
      }
   }
}
```

Parameters

group-name	Multi-node. A web filtering source group.
addr	Multi-node. An IPv4 address or subnet that is part of the source group.

Default

None.

Usage Guidelines

Use this command to specify an IPv4 address or subnet to include in the source group.

Use the **set** form of this command to specify an IPv4 address or subnet.

Use the **delete** form of this command to remove the IPv4 address or subnet from the source group.

Use the **show** form of this command to view the address configuration.

service webproxy url-filtering squidguard source-group <group-name> description <desc>

Specifies a brief description for a web filtering source group.

Syntax

set service webproxy url-filtering squidguard source-group *group-name* **description** *desc*

delete service webproxy url-filtering squidguard source-group *group-name* **description**

show service webproxy url-filtering squidguard source-group *group-name* **description**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group text {
               description text
            }
         }
      }
   }
}
```

Parameters

group-name	Multi-node. A web filtering source group.
desc	A description of the source group. If the description contains spaces then it must be contained in double quotes.

Default

None.

Usage Guidelines

Use this command to specify a description of a web filtering source group.

Use the **set** form of this command to specify a description of a web filtering source group.

Use the **delete** form of this command to remove the description.

Use the **show** form of this command to view the description.

service webproxy url-filtering squidguard source-group <group-name> domain <domain>

Specifies a domain to include in a web filtering source group.

Syntax

set service webproxy url-filtering squidguard source-group *group-name* **domain** *domain*

delete service webproxy url-filtering squidguard source-group *group-name* **domain** *domain*

show service webproxy url-filtering squidguard source-group *group-name* **domain**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            source-group text {
               domain text
            }
         }
      }
   }
}
```

Parameters

group-name	Multi-node. A web filtering source group.
domain	A domain to be included in the source group (e.g. company.com).

Default

None.

Usage Guidelines

Use this command to specify a domain to include in a web filtering source group.

Use the **set** form of this command to specify a domain to include in a web filtering source group.

Use the **delete** form of this command to remove the a domain to include in a web filtering source group.

Use the **show** form of this command to view the configuration.

service webproxy url-filtering squidguard time-period <period-name>

Specifies a time period to be used in a web filtering rule.

Syntax

set service webproxy url-filtering squidguard time-period *period-name*

delete service webproxy url-filtering squidguard time-period *period-name*

show service webproxy url-filtering squidguard time-period *period-name*

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period text {
            }
         }
      }
   }
}
```

Parameters

period-name	The time period to be used in a web filtering rule.

Default

The rule is active at all times.

Usage Guidelines

Use this command to define a time period to be used in a web filtering rule. The web filtering rule is valid during the times specified.

Use the **set** form of this command to specify a time period to be used in a web filtering rule.

Use the **delete** form of this command to remove the time period configuration.

Use the **show** form of this command to view the time period configuration.

service webproxy url-filtering squidguard time-period <period-name> days <day> time <time>

Specifies a day and time included in the time period.

Syntax

set service webproxy url-filtering squidguard time-period *period-name* **days** *day* **time** *time*

delete service webproxy url-filtering squidguard time-period *period-name* **days** *day* [**time**]

show service webproxy url-filtering squidguard time-period *period-name* **days** *day* [**time**]

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period text {
               days [Mon|Tue|Wed|Thu|Fri|Sat|Sun|
                     weekdays|weekends|all] {
                  time text
               }
            }
         }
      }
   }
}
```

Parameters

period-name	The time period to be used in a web filtering rule.

day	A day (or days) within a time period specification. Supported values are as follows: **Mon**: The rule is valid on Mondays. **Tue**: The rule is valid on Tuesdays. **Wed**: The rule is valid on Wednesdays. **Thu**: The rule is valid on Thursdays. **Fri**: The rule is valid on Fridays. **Sat**: The rule is valid on Saturdays. **weekdays**: The rule is valid on weekdays. **weekends**: The rule is valid on weekends. **all**: The rule is valid on all days.
time	The time range (using 24 hour time representation) within the day specified. The format is **hh:mm-hh:mm**. Multiple ranges are supported. When multiple ranges are specified they must be separated by commas and enclosed in double quotes (e.g. “09:00-14:00, 18:00-24:00”).

Default

None.

Usage Guidelines

Use this command to specify a day (or days) and a time range within the time period definition.

NOTE *To filter url requests based on time period, at least one rule and one source group are required.*

Use the **set** form of this command to specify a day (or days) and a time range.

Use the **delete** form of this command to remove the day and/or time configuration.

Use the **show** form of this command to view the day and/or time configuration.

service webproxy url-filtering squidguard time-period <period-name> description <desc>

Specifies a brief description for the time period.

Syntax

set service webproxy url-filtering squidguard time-period *period-name* **description** *desc*

delete service webproxy url-filtering squidguard time-period *period-name* **description**

show service webproxy url-filtering squidguard time-period *period-name* **description**

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            time-period text {
               description text
            }
         }
      }
   }
}
```

Parameters

period-name	The time period to be used.
desc	A description of the policy rule. If the description contains spaces then it must be contained in double quotes.

Default

None.

Usage Guidelines

Use this command to specify a description of a time period.

Use the **set** form of this command to specify the description of the time period.

Use the **delete** form of this command to remove the description of the time period.

Use the **show** form of this command to view the description of the time period.

service webproxy url-filtering squidguard vyattaguard mode

Specifies how the vyattaguard system will operate.

Availability

Vyatta Plus

Syntax

set service webproxy url-filtering squidguard vyattaguard mode [**local-only | net-only | normal**]

delete service webproxy url-filtering squidguard vyattaguard mode

show service webproxy url-filtering squidguard vyattaguard mode

Command Mode

Configuration mode.

Configuration Statement

```
service {
   webproxy {
      url-filtering {
         squidguard {
            vyattaguard {
               mode {
                  local-only
                  net-only
                  normal
               }
            }
         }
      }
   }
}
```

Parameters

local-only	Use only the local vyattaguard database to classify a URL.

net-only	Use only the remote vyattaguard database to classify a URL.
normal	Use the local vyattaguard database to classify a URL. If no classification can be made, try the remote vyattguard database. This is the default.

Default

Both the local database and network classification are used.

Usage Guidelines

Use this command to specify how the vyattaguard system will operate. The **net-only** mode would typically be used on systems with disk space constraints that would not be able to house the entire vyattaguard database. Vyatta recommends 2GB of additional disk space to house the vyattguard database.

Use the **set** form of this command to specify how the vyattaguard system will operate.

Use the **delete** form of this command to return the vyattaguard fetaure to its default operational mode.

Use the **show** form of this command to view the vyattaguard mode configuration.

show webproxy blacklist categories

Displays all categories defined in the installed squidGuard database.

Syntax

show webproxy blacklist categories

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to display all database categories that are available in the squidGuard database that is currently installed.

Examples

Example 3-11 displays categories for a squidGuard database.

Example 3-11 Displaying database categories

```
vyatta@R1> show webproxy blacklist categories
ads
aggressive
audio-video
drugs
gambling
hacking
mail
porn
proxy
redirector
spyware
suspect
violence
warez
vyatta@R1>
```

show webproxy blacklist domains

Displays all domains listed in the installed database.

Syntax

show webproxy blacklist domains

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to display all the domains in the installed squidGuard database. Domains from all database categories are shown.

Examples

Example 3-12 shows the first few domains displayed from an installed database.

Example 3-12 Displaying database domains

```
vyatta@R1> show webproxy blacklist domains
101com.com
101order.com
103bees.com
1100i.com
123banners.com
123found.com
123pagerank.com
180searchassistant.com
180solutions.com
207.net
247media.com
247realmedia.com
24pm-affiliation.com
:
:
```

show webproxy blacklist log

Displays the log for blacklisted URLs.

Syntax

show webproxy blacklist log

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to display the system's record of URLs that have been filtered.

Examples

Example 3-13 shows sample output of **show webproxy blacklist log**.

Example 3-13 Displaying the blacklist log

```
vyatta@R1> show webproxy blacklist log
2008-09-03 18:12:01 [12027] Request(default/gambling/-)
http://www.goldenpalacepoker.com 10.1.0.173/- - GET
2008-09-04 10:00:44 [12988] Request(default/spyware/-)
http://www.180solutions.com 10.1.0.173/- - GET
vyatta@R1>
```

show webproxy blacklist search <filter>

Displays domains and/or URLs matching search text.

Syntax

show webproxy blacklist search *filter*

Command Mode

Operational mode.

Parameters

filter	The filter text.

Usage Guidelines

Use this command to search for domains or URLs within the installed squidGuard database. All domains or URLs matching the filter string are shown.

Examples

Example 3-14 lists the IP addresses in the installed database that begin with “206.132.42”.

Example 3-14 Searching for an IP address or URL in a database

```
vyatta@R1> show webproxy blacklist search 206.132.42
porn/domains     206.132.42.195
porn/domains     206.132.42.197
porn/domains     206.132.42.200
porn/domains     206.132.42.201
porn/domains     206.132.42.206
porn/domains     206.132.42.212
porn/domains     206.132.42.213
porn/domains     206.132.42.215
porn/domains     206.132.42.218
porn/domains     206.132.42.219
porn/domains     206.132.42.231
porn/domains     206.132.42.250
porn/domains     206.132.42.251
```

```
porn/domains     206.132.42.253
warez/domains     206.132.42.196
warez/domains     206.132.42.208
vyatta@R1>
```

show webproxy blacklist urls

Displays all URLs in squidGuard database categories.

Syntax

show webproxy blacklist urls

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display all the URLs in squidGuard database categories.

Examples

Example 3-15 shows the first few entries of sample output of **show webproxy blacklist urls**.

Example 3-15 Displaying blacklisted URLs

```
vyatta@R1> show webproxy blacklist urls
thisisarandomentrythatdoesnotexist.com/foo
thisisarandomentrythatdoesnotexist.com/foo
134.121.0.99/~dcarp
165.21.101.33/~mp3mania
194.134.35.11/mp3forever
194.134.35.12/mp3forever
194.134.35.17/mp3forever
194.145.63.33/bg-mp3
195.141.34.45/mp3millennium
195.141.34.45/mp3sweden
195.66.60.36/mhs00160
195.96.96.198/~brouns
205.188.134.217/h0tp00lman
209.202.218.12/mb/honzicek
:
:
```

show webproxy log

Displays the web proxy log.

Syntax

show webproxy log

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to display the web proxy log.

Examples

Example 3-16 displays a portion of the web proxy log.

Example 3-16 Viewing the web proxy log

```
vyatta@R1> show webproxy log
1220642370.525    708 172.16.117.25 TCP_REFRESH_MODIFIED/200
17825 GET
http://newsrss.bbc.co.uk/rss/newsonline_world_edition/front_pag
e/rss.xml - DIRECT/212.58.226.29 text/xml
1220642699.568    830 172.16.117.25 TCP_MISS/200 46448 GET
http://sb.google.com/safebrowsing/update? -
DIRECT/209.85.133.136 text/html
1220644499.691   1274 172.16.117.25 TCP_MISS/200 53832 GET
http://sb.google.com/safebrowsing/update? -
DIRECT/209.85.133.93 text/html
1220645984.836     34 172.16.117.25 TCP_MISS/302 694 GET
http://en-us.fxfeeds.mozilla.com/en-US/firefox/headlines.xml -
DIRECT/63.245.209.121 text/html
1220645984.881     31 172.16.117.25 TCP_MISS/302 736 GET
http://fxfeeds.mozilla.com/firefox/headlines.xml -
DIRECT/63.245.209.121 text/html
:
:
```

show webproxy vyattaguard categories

Displays all categories defined in the installed vyattaguard database.

Availability

Vyatta Plus

Syntax

show webproxy vyattaguard categories

Command Mode

Operational mode.

Parameters

None

Usage Guidelines

Use this command to display all database categories that are available in the vyattaguard database that is currently installed.

show webproxy vyattaguard search <filter>

Displays domains and/or URLs in the vyattaguard database matching search text.

Availability

Vyatta Plus

Syntax

show webproxy vyattaguard search *filter*

Command Mode

Operational mode.

Parameters

filter	The filter text.

Usage Guidelines

Use this command to search for domains or URLs within the installed vyattaguard database. All domains or URLs matching the filter string are shown.

update webproxy blacklists

Updates the squidGuard database.

Syntax

update webproxy blacklists

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to initiate an update to the squidGuard database. If no databases have been installed, the system allows you to download and install one.

Examples

Example 3-17 shows the system interaction for downloading a first squidGuard database.

Example 3-17 Downloading a squidGuard database

```
vyatta@R1> update webproxy blacklists
No url-filtering blacklist installed
Would you like to download a blacklist? [confirm][y]
--2008-09-10 01:32:15--
http://squidguard.mesd.k12.or.us/blacklists.tgz
Resolving squidguard.mesd.k12.or.us... 198.236.66.41
Connecting to squidguard.mesd.k12.or.us|198.236.66.41|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 5459348 (5.2M) [application/x-gzip]
Saving to: `/tmp/blacklists.gz'

100%[=======================================================
=============================================================
=====================>] 5,459,348    408K/s   in 13s
```

```
2008-09-10 01:32:29 (407 KB/s) - `/tmp/blacklists.gz' saved
[5459348/5459348]

Uncompressing blacklist...
```

update webproxy vyattaguard

Updates the vyattaguard database.

Availability

Vyatta Plus

Syntax

update webproxy vyattguard

Command Mode

Operational mode.

Parameters

None.

Usage Guidelines

Use this command to initiate an update to the vyattaguard database. If no databases have been installed, the system allows you to download and install one.

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
AS	autonomous system
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DLCI	data-link connection identifier
DMI	desktop management interface
DMZ	demilitarized zone
DN	distinguished name
DNS	Domain Name System

DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EGP	Exterior Gateway Protocol
ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Ouput
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol

MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit
NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PAT	Port Address Translation
PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RA	router advertisement
RIB	Routing Information Base
RIP	Routing Information Protocol

RIPng	RIP next generation
RS	router solicitation
Rx	receive
SLAAC	Stateless address auto-configuration
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
ToS	Type of Service
Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network