JUNIPER NETWORKS

Application-Services

HTTP Content Management Configuration Guide

Release
11.4 R4

Published: 2012-07-10

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Application-Services HTTP Content Management Configuration Guide

Revision History
July 2012— HTTP Content Management Configuration Guide, Initial Release

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

HTTP Content Management Overview

HTTP Content Management (HCM) is an application used to inspect HTTP traffic. The software is also sometimes referenced as HTTP-Manager. HCM can be installed on an MX Series router that is running the corresponding version of the Junos OS release. HCM inspects HTTP traffic even if the default port 80 is not used for HTTP traffic. It is interoperable with ms, rms, and ams interface types. It supports fragmented HTTP request packets and GET, PUT, and POST requests. HCM supports the following features:

- **HTTP Tagging:** HTTP Tagging is a feature that enables the router to monitor HTTP transactions and match the HTTP transactions against the HTTP Tagging service rules. If an HTTP transaction matches a service rule configured for tag insertion, then a corresponding tag is inserted in that HTTP request. HTTP Tagging service rule contains a list of terms that are evaluated sequentially.

  The tag inserted in the HTTP request can be either a fixed string or a set of subscriber-specific attributes. If you have configured service rules to insert subscriber-specific attributes, the HTTP Content Management application interacts with PTSP to identify the subscribers who have sent any given HTTP request. The HTTP Content Management application resolves the subscriber-specific attributes and inserts the tags in the HTTP headers.

  The HTTP Tagging feature:

  - Enables you to define a configurable tag header in the HTTP tag inserted in the HTTP request.
  - Enables you to define a configurable list of subscriber-specific attributes in the HTTP tag inserted in the HTTP request.
  - Enables you to define a separator character that can be inserted between attributes in the HTTP tag inserted in the HTTP request.
  - Provides configuration knobs to configure specific HTTP tags based on the server address and the port used.
  - Enables you to maintain the statistics of HTTP requests on a per-rule or per-term basis for HTTP requests that have met the criteria for being tagged.
  - Provides a CLI command to view the current statistics for HTTP tag-insertion policies.

- **HTTP Error-redirect:** HTTP Error-redirect is a feature that enables the router to monitor HTTP transactions and match the HTTP transactions against the HTTP Error-redirect service rules. If an HTTP server returns an error code response that matches a service rule, the router replaces that HTTP status code with a redirect response to a landing page specified in the service rule. The HTTP error redirect service rule contains terms that are evaluated sequentially.

The HTTP Error-redirect feature:

- Provides configuration knobs to configure the HTTP status codes, size of the error response, landing page URL, and copying of the Host and Request-URI field in Request-Line from the original request into the redirect message in multiple policies.
- Enables you to maintain the statistics of HTTP requests on a per-rule or per-term basis for HTTP requests that have met the criteria for being redirected.
- Provides a CLI command to view the current statistics for HTTP Error-redirect policies.

- **HTTP URL Filtering and Logging:** HTTP URL Filtering and Logging is a feature that monitors and matches the HTTP transactions against preconfigured URLs and hostnames configured using HTTP URL Filtering service rules. If an HTTP transaction matches any of the preconfigured URLs or hostnames, a configured action that is specified by the service rule is enforced on that HTTP transaction. The following table lists the actions that can be configured in an HTTP URL Filtering service rule.

Action	Description
Discard	Discards all packets associated with the 5-tuple flow where the URL was seen. Initially, some packets may be accepted until the URL match is performed.
Reset	Resets all TCP-based transactions associated with the 5-tuple flow where the URL was seen. Initially, some packets may be accepted until the URL match is performed. This action triggers the transmission of a TCP RESET to both peers of the connection.
Log	Creates a log where the request and response can be logged. The request and response logs contain the 5-tuple flow, session identifier, timestamp, and the fields related to request and response.
Accept	Allows the HTTP transaction to proceed.
Count	Allows the HTTP transaction to proceed and collects statistics on the number of times a rule or term is matched for all service sets that the rule exists on for an individual PIC.

You can use the following combination of actions in an HTTP URL Filtering rule:

- Discard and Log (request only)
- Reset and Log (request only)
- Accept and Count
- Accept and Log
- Accept, Count, and Log

The HTTP URL Filtering feature:

- Enables the URLs configured in the router and the actions to specify a wildcard character “*” as:
  - A prefix for the “Host” portion of the HTTP request

- A suffix for the “request-URI” portion of the HTTP request

- Provides a CLI command to view the current statistics for HTTP URL Filtering policies.

HTTP Content Management features are configured using service rules. A service rule contains terms that are evaluated sequentially. Because HTTP Content Management features use different matching criteria, it is recommended that you create a different service rule for each HTTP Content Management feature that you want to configure. This makes it easier for you to define the combinations of matching criteria and corresponding actions for each service rule.

Related Documentation

- Configuring the HTTP Content Management Package on the Router on page 3
- Configuring HTTP Tagging on page 6
- Configuring HTTP Error-redirect on page 9
- Configuring HTTP URL Filtering and Logging on page 11
- Configuring HTTP Content Management Service Sets on page 15
- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Configuring the HTTP Content Management Package on the Router

You can configure the HTTP Content Management package on MX960, MX480, or MX240 routers. To configure the HTTP Content Management package on the router:

1. Enable the juniper provider-id statement to enable Juniper’s extension application packages to be deployed and run on the router.

   [edit system]

   ```
   extensions {
     providers {
       juniper {
         license-type juniper deployment-scope commercial;
       }
     }
   }
   ```

2. Before you install the HTTP Content Management package on the router, ensure that you have the appropriate version of the HTTP Content Management package for the Junos OS image you are using on the router. When you have confirmed that you have the right package, use the request system software add command to install the HTTP Content Management package. You would need to restart the CLI after the package is installed.

   ```
   user@router> request system software add http-manager-11.4R4.4-1-A1.1.tgz
   NOTICE: Validating configuration against package-name.
   NOTICE: Use the 'no-validate' option to skip this if desired.
   Checking compatibility with configuration

   Initializing...

   WARNING: cli has been replaced by an updated version:
   ```

```
CLI release 11.4R4 built by builder on 2012-07-4 02:36:22 UTC
Restart cli using the new version ? [yes,no] (yes)
Restarting cli ...
```

3. When the CLI has restarted, use the **show version** command to see whether the HTTP Content Management packages are installed.

```
user@router> show version
...
HTTP-Manager Management Component [11.4R4.4-1-A1.1]
HTTP-Manager Dataplane Component [11.4R4.4-1-A1.1]
user@router>..
```

4. If you want to upgrade the Junos OS image on a router that has the HTTP Content Management package installed, you should first save and then delete the HTTP Content Management configuration from the router.

   - To view the HTTP Content Management configuration, use the **user@router>extension juniper-http-manager show <section>** command.
   - To delete the HTTP Content Management configuration from the router, use the **user@router>extension juniper-http-manager delete <section>** command.
   - Any remnant HTTP Content Management configuration left on the router will be deleted when the Junos OS image is upgraded. So, ensure that you have saved all necessary HTTP Content Management configurations.
   - To delete the HTTP Content Management package from the router, use the **user@router>> request system software delete <http-manager-package>** command.
   - Reinstall the HTTP Content Management package on the router after you upgrade the Junos OS image on the router.

```
root@aulavik> show version
Hostname: aulavik
Model: mx480
JUNOS Base OS boot [11.4R4.4]
JUNOS Base OS Software Suite [11.4R4.4]
JUNOS Kernel Software Suite [11.4R4.4]
JUNOS Crypto Software Suite [11.4R4.4]
JUNOS Packet Forwarding Engine Support (M/T Common) [11.4R4.4]
JUNOS Packet Forwarding Engine Support (MX Common) [11.4R4.4]
JUNOS Online Documentation [11.4R4.4]
JUNOS Voice Services Container package [11.4R4.4]
JUNOS Border Gateway Function package [11.4R4.4]
JUNOS Services AACL Container package [11.4R4.4]
JUNOS Services LL-PDF Container package [11.4R4.4]
JUNOS Services PTSP Container package [11.4R4.4]
JUNOS Services Stateful Firewall [11.4R4.4]
JUNOS Services NAT [11.4R4.4]
JUNOS Services Application Level Gateways [11.4R4.4]
JUNOS Services Captive Portal and Content Delivery Container package [11.4R4.4]
JUNOS Services RPM [11.4R4.4]
JUNOS Services HTTP Content Management package [11.4R4.4]
JUNOS AppId Services [11.4R4.4]
JUNOS IDP Services [11.4R4.4]
```

```
JUNOS Services Crypto [11.4R4.4]
JUNOS Services SSL [11.4R4.4]
JUNOS Services IPSec [11.4R4.4]
JUNOS Runtime Software Suite [11.4R4.4]
JUNOS Routing Software Suite [11.4R4.4]
HTTP-Manager Management Component [11.4R4.4-1-A1.1]
HTTP-Manager Dataplane Component [11.4R4.4-1-A1.1]

root@aulavik> configure
Entering configuration mode

[edit]
root@aulavik# extension juniper-http-manager show
## Last changed: 2012-06-07 13:21:36 PDT
services {
   http-manager {
      traceoptions {
         level all;
         flag all;
      }
   }
}

[edit]
root@aulavik# extension juniper-http-manager delete

[edit]
root@aulavik# extension juniper-http-manager show

[edit]
root@aulavik# commit
commit complete

[edit]
root@aulavik# exit
Exiting configuration mode

root@aulavik> request system software delete http-manager-services
Removing package http-manager-services' ...
Removing /opt/sdk/service-packages/http-manager-services ...
Removing http-manager-services-xlr-11.4R4.4-1-A1.1.tgz from /var/sw/pkg ...
Notifying mspd ...

root@aulavik> request system software delete http-manager-mgmt
Removing package http-manager-mgmt' ...
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd: commit complete
Restarting mgd ...
Restarting http-manager ...

WARNING: cli has been replaced by an updated version:
CLI release 11.4R4.4 built by builder on 2012-05-14 19:51:45 UTC
Restart cli using the new version ? [yes,no] (yes)

Restarting cli ...
root@aulavik>

root@aulavik> show version
Hostname: aulavik
Model: mx480
```

JUNOS Base OS boot [11.4R4.4]
JUNOS Base OS Software Suite [11.4R4.4]
JUNOS Kernel Software Suite [11.4R4.4]
JUNOS Crypto Software Suite [11.4R4.4]
JUNOS Packet Forwarding Engine Support (M/T Common) [11.4R4.4]
JUNOS Packet Forwarding Engine Support (MX Common) [11.4R4.4]
JUNOS Online Documentation [11.4R4.4]
JUNOS Voice Services Container package [11.4R4.4]
JUNOS Border Gateway Function package [11.4R4.4]
JUNOS Services AACL Container package [11.4R4.4]
JUNOS Services LL-PDF Container package [11.4R4.4]
JUNOS Services PTSP Container package [11.4R4.4]
JUNOS Services Stateful Firewall [11.4R4.4]
JUNOS Services NAT [11.4R4.4]
JUNOS Services Application Level Gateways [11.4R4.4]
JUNOS Services Captive Portal and Content Delivery Container package [11.4R4.4]
JUNOS Services RPM [11.4R4.4]
JUNOS Services HTTP Content Management package [11.4R4.4]
JUNOS AppId Services [11.4R4.4]
JUNOS IDP Services [11.4R4.4]
JUNOS Services Crypto [11.4R4.4]
JUNOS Services SSL [11.4R4.4]
JUNOS Services IPSec [11.4R4.4]
JUNOS Runtime Software Suite [11.4R4.4]
JUNOS Routing Software Suite [11.4R4.4]

Related Documentation

- HTTP Content Management Overview on page 1
- Configuring HTTP Tagging on page 6
- Configuring HTTP Error-redirect on page 9
- Configuring HTTP URL Filtering and Logging on page 11
- Configuring HTTP Content Management Service Sets on page 15
- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Configuring HTTP Tagging

To configure HTTP Tagging rule sets:

1. Configure the **tag-rule** statement at the **http-manager** hierarchy level to specify a name for this rule.

   In the following example, the **tag-rule** statement is configured as *rule1*.

2. Configure the **term** statement at the **http-manager** hierarchy level to specify a numbered identity for each term in a rule.

   The **term** statement can be configured with an identity ranging from 1 through 255. In the following example, the **term** statement is configured as *1*.

3. Configure the **destination-address** statement at the **http-manager** hierarchy level to define the IP address.

This statement accepts a list of IPv4 or IPv6 IP addresses. In the following example, the **destination-address** statement is configured as a **from** clause inside a **term** called *1* inside a **tag-rule** called *rule1*. Using the **<except>** keyword forces a policy match if that address is not the destination address.

4. Configure the **destination-address-range** statement and specify a low-to-high IP address range.

   This statement accepts a list of IPv4 or IPv6 IP address ranges. In the following example, the **destination-address-range** statement is configured as a **from** clause inside a **term** called *1* inside a **tag-rule** called *rule1*. Using the **<except>** keyword forces a policy match if that address is not the destination address.

5. Configure the **destination-ports** statement and specify a list of ports.

   In the following example, the **destination-ports** statement is configured as a **from** clause inside a **term** called *1* inside a **tag-rule** called *rule1* and configured as *100*.

6. Configure the **destination-port-range** statement and specify a low-to-high port range.

   In the following example, the **destination-port-range** statement is configured as a **from** clause inside a **term** called *1* inside a **tag-rule** called *rule1* and configured as *1000* and *2000* for minimum value and maximum value respectively.

7. Configure the **destination-prefix-list** statement to reference a predefined prefix list.

   You can reference any address prefix-list configured in the router.

8. Configure the **x-forwarded-for** statement to apply a pair of address masks to the address.

   The two types of masks are specified by the **mask** or **or-value** statements. These address masks can be IPv4 or IPv6 addresses. If one of the masks is specified, then the other must also be specified. **<mask>** is logically joined to the IP address with an AND operator and then subsequently logically joined to the **<or-value>** with an OR operator. The resultant address is inserted into the packet along with the **x-forwarded-for** tag.

9. Configure the **tag** statement to specify a reference name for a tag definition.

   The tags are inserted in the order specified in the CLI.

10. Configure the **tag-header** statement to determine the tag header to apply to the HTTP header.

    The tag header string cannot contain the following characters: (,), <, >, @, “,”, ;, \, “””, /, [,], ?, =, {, and }. In the following example, the **tag-header** statement is configured under a **tag** statement named *httpmanager* inside a **then** clause inside a **term** called *1* and a **tag-rule** called *rule1*.

11. Configure the **tag-separator** statement to specify the separator character to be inserted between tag attributes.

    In the following example, the **tag-header** statement is configured under a **tag** statement named *httpmanager* inside a **then** clause inside a **term** called *1* and a **tag-rule** called *rule1*.

12. Configure the **tag-attribute** statement to specify a reference name for a tag attribute.

Multiple tag attributes can be defined per tag header. The order of insertion is determined by the attribute-id.

13. Configure the **radius-attribute**, **fixed-attribute**, or **subscriber-attribute** statements depending on the type of tag-attribute you want to configure.

    - If you want to configure a **radius-attribute** statement, specify the **radius-attribute-id** that corresponds to the numbered RADIUS attributes ranging from 1 through 255. When specified, the RADIUS attribute is looked up for the subscriber that the policy applies to, and the result is inserted into the packet.
    - If you want to configure a **fixed-attribute** statement, specify the **subscriber-id**. When specified, the **PTSP subscriber_id attribute** is looked up and inserted into the packet.
    - If you want to configure a **subscriber-attribute** statement, specify a text string that is used to look up a subscriber attribute. Ensure that all subscriber attributes are predefined in the services http-manager tag-attribute.

14. If you want to configure a rule set with multiple rules, configure the **tag-rule-set** statement and specify the name for the rule set.

    A rule set is a collection of rules ordered in the sequence in which they are entered. Rule sets are evaluated in the order in which they are configured in a service set.

15. Configure the **service-set** statement to create a service set for the tagging rules and the rule sets that you have created. See "Configuring HTTP Content Management Service Sets" on page 15 for more information.

Configuring HTTP Tagging Rule sets

```
services {
  http-manager {
    tag-rule rule1 {
      term 1 {
        from {
          destination-address {
            10.0.0.1/32;
          }
          destination-address-range {
            low 10.0.0.10 high 10.0.0.30;
          }
          destination-prefix-list {
            list1;
          }
          destination-ports 100;
          destination-port-range {
            low 1000 high 2000;
          }
        }
        then {
          tag tag1 {
            tag-header httpmanager;
            tag-separator :;
            tag-attribute 1 {
              radius-attribute 100;
            }
            tag-attribute 2 {
```

```
                fixed-attribute subscriber-id;
              }
            }
            x-forwarded-for {
              mask 0.255.255.255;
              or-value 168.0.0.0;
            }
            count;
          }
        }
      }
      tag-rule-set tagging1 {
        rule rule1;
      }
    }
  }
}
```

Related Documentation

- Configuring the HTTP Content Management Package on the Router on page 3
- Configuring HTTP Error-redirect on page 9
- Configuring HTTP URL Filtering and Logging on page 11
- HTTP Content Management Overview on page 1
- Configuring HTTP Content Management Service Sets on page 15
- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Configuring HTTP Error-redirect

To configure HTTP Error-redirect rule sets:

1. Configure the **redirect-rule** statement at the **http-manager** hierarchy level to specify a name for this rule.

   In the following example, the **redirect-rule** statement is configured as *rule2* .

2. Configure the **term** statement at the **http-manager** hierarchy level to specify a numbered identity for each term in a rule. The term statement can be configured with an identity ranging from 1 through 255.

   In the following example, the **term** statement is configured as *2*.

3. Configure the **http-status-code** statement and specify a list of error codes to match this term. The HTTP status code from a response is compared against these values.

   In the following example, the **http-status-code** statement is configured as a **from** clause inside a **term** called *2* inside a **redirect-rule** called *rule2*.

4. Configure the **maximum-content-length** statement and specify a threshold on the size of the HTTP response, in bytes.

   If the server's response is less than or equal to this value, this term matches the response. If the server's response is greater than this value, this term does not match

the response. In the following example, the **http-status-code** statement is configured as a **from** clause inside a **term** called *2* inside a **redirect-rule** called *rule2*.

5. Configure the **redirect-302** statement and specify the URL of the landing page to be included in the 302 redirect message sent to clients.

   This is a string that contains the complete URL. The following escape characters can be used in the string:

   - %h - Escape character that will be replaced by the "hostname" HTTP header content of the original HTTP request that triggered this response.
   - %u - Escape character that will be replaced by the URI content of the original HTTP request that triggered this response.

6. If you want to configure a rule set with multiple rules, configure the **redirect-rule-set** statement and specify the name for the rule set.

   A rule set is a collection of rules ordered in the sequence in which they are entered. Rule sets are evaluated in the order in which they are configured in a service set.

7. Configure the **service-set** statement to create a service set for the error-redirect rules and rule sets you have created. See "Configuring HTTP Content Management Service Sets" on page 15 for more information.

Configuring HTTP Error-redirect Rule sets

```
services {
  http-manager {
    redirect-rule rule2 {
      term 2 {
        from {
          http-status-code [ 403 404 ];
          maximum-content-length 50;
        }
        then {
          count;
          redirect-302 {
            location "%h/redirecturl.html";
          }
        }
      }
    }
    redirect-rule-set redirect1 {
      rule rule2;
    }
  }
}
```

Related Documentation

- Configuring the HTTP Content Management Package on the Router on page 3
- Configuring HTTP Tagging on page 6
- Configuring HTTP URL Filtering and Logging on page 11
- HTTP Content Management Overview on page 1
- Configuring HTTP Content Management Service Sets on page 15

- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Configuring HTTP URL Filtering and Logging

To configure HTTP URL Filtering rule sets:

1. Configure the **url-rule** statement at the **http-manager** hierarchy level to specify a name for this rule.

   In the following example, the **url-rule** statement is configured as *rule 3*.

2. Configure the **term** statement at the **http-manager** hierarchy level to specify a numbered identity for each term in a rule.

   The **term** statement can be configured with an identity ranging from 1 through 255. In the following example, the **term** statement is configured as *3*.

3. Configure the **url-list** statement and specify the name of a URL list to be included as a matching condition.

   A URL matching any hostname and any request-URI inside the same term is considered a match for that term.

4. Configure the **url** statement and specify an integer between 1 and 32,767.

   This integer uniquely identifies a particular URL definition within a term. In the following example, the url statement is configured as a **from** clause inside a term called *3* and inside a **url-rule** called *rule3*.

5. Configure the **host** statement and specify the hostnames to match.

   A URL matching any hostname and any request URI inside the same term is considered a match for that term. If you specify multiple hostnames in the match condition, the matching is performed as a logical OR. If the hostnames match any of the hostnames specified in the rule, it is considered a match.

6. Configure the **request-uri** statement and specify the request URIs to match.

   A URL matching any hostname and any request URI inside a term is considered a match for that term. If you specify multiple request URIs in the match condition, the matching is performed as a logical OR. If the request URIs match any of the request URIs specified in the rule, it is considered a match.

7. Specify the action to be performed on the HTTP requests that match the criteria.

   You can discard, accept, reset, log, and count the HTTP requests.

   NOTE: **You can specify the rule to perform multiple actions on HTTP requests; however, only a predefined combination of actions is allowed. See "HTTP Content Management Overview" on page 1 for more information about the predefined combination of actions.**

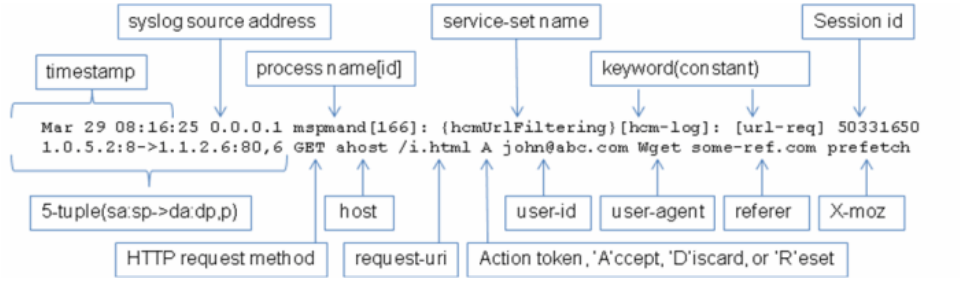
8. Configure the **log-request** statement and specify the HTTP request context (or header) to be included or excluded from URL request logs.

The following table lists the set of valid HTTP request contexts, their default settings, the order where they appear in the log message, and the maximum size of the field before it gets truncated.

HTTP Request Contexts	Default Settings	Order	Maximum Length
“session-id”	default: included	1	NA
“5-tuple”	default: included	2	NA
“request-method”	default: included	3	NA
“host”	default: included	4	64 characters
“request-uri”	default: included	5	100 characters
“action-code”	default: included	6	NA
“user-id”	default: not included	7	79 characters
“user-agent”	default: not included	8	100 characters
“referrer”	default: not included	9	100 characters
“x-moz”	default: not included	10	40 characters

The following figure displays the URL log message for HTTP request.

Figure 1: URL Log Message for HTTP Request



9. Configure the **log-response** statement and specify an HTTP response context (or header) to be included or excluded from URL response logs.

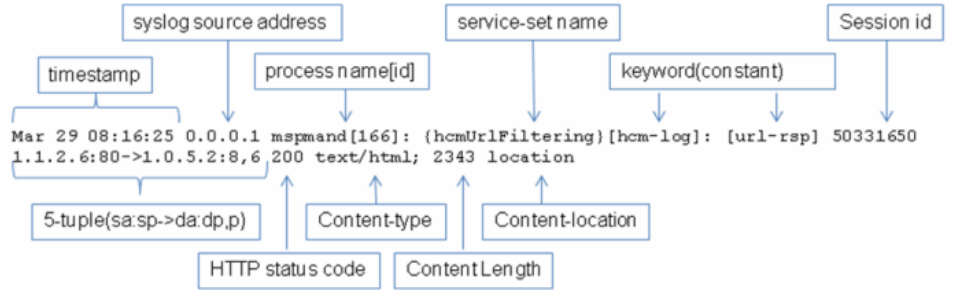
   The following table lists the set of valid HTTP response contexts and their default settings.

HTTP Response Contexts	Default Settings	Order	Maximum Length1
“session-id”	default: included	1	NA
“5-tuple”	default: included	2	NA
“status-code”	default: included	3	NA

HTTP Response Contexts	Default Settings	Order	Maximum Length1
“content-type”	default: not included	4	100 characters
“content-length”	default: not included	5	16-bit quantity
“location”	default: not included	6	100 characters

The following figure displays the URL log message for HTTP response.

Figure 2: URL Log Message for HTTP Response



NOTE: If both <**http-req-content**> and <**http-rsp-content**> are not specified, then log-request and log-response actions log default contexts. An attempt to include a context that is already included by default or exclude a context that is already excluded by default is flagged as an error while you are committing the configuration.

10. If you want to configure a rule set with multiple rules, configure the **url-rule-set** statement and specify the name for the rule set. A rule set is a collection of rules ordered in the sequence in which they are entered. Rule sets are evaluated in the order in which they are configured in a service set.
11. Configure the **service-set** statement to create a service set for the URL filtering rules and rule sets that you have created. See “Configuring HTTP Content Management Service Sets” on page 15 for more information.

NOTE: Specify the rules and the terms within the rules carefully to ensure desired actions for a matched HTTP request. If an HTTP request matches more than one rule or term, the action applied on the HTTP request is nondeterministic and may be any of the actions associated with the rules and terms within the rules.

Configuring HTTP URL Filtering Rule sets

```
services {
  http-manager {
    url-rule rule3 {
      term 3{
        from {
```

```
            url-list list 1;
            url 100 {
              host <hostname>;
              host "other.specific.domain.name.org";
              host "other.specific*";
              host “*”;
              request-uri <page-name>;
              request-uri "/another-page/ex9/page”;
              request-uri "/another-page*”;
              request-uri “*”;
            }
          }
          then {
            accept;
            count;
            log-request;
            log-request {
              include “request-method”;
              exclude “user-id”;
            }
            log-response;
            log-response {
              include “status-code”;
              exclude “content-length”;
            }
          }
          count;
        }
        }
      }
    }
    url-rule-set urlruleset1 {
      rule rule3;
      rule rule6;
    }
    }
}
```

Related Documentation

- Configuring the HTTP Content Management Package on the Router on page 3
- Configuring HTTP Tagging on page 6
- Configuring HTTP Error-redirect on page 9
- HTTP Content Management Overview on page 1
- Configuring HTTP Content Management Service Sets on page 15
- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Configuring HTTP Content Management Service Sets

Before you start configuring HTTP Content Management service sets, ensure that you have configured the rules and rule sets that you want to include in the service sets. See "Configuring HTTP Tagging" on page 6, "Configuring HTTP Error-redirect" on page 9, and "Configuring HTTP URL Filtering and Logging" on page 11 for more information about how to configure rule sets.

To configure HTTP Content Management service sets:

1. Configure the **service-set** statement at the **services** hierarchy level to specify a name for the service set.
2. Configure the **extension-service http-manager** statement and specify the HCM tag rules and rule sets.

   You should specify at least one tag rule and one tag rule set for the configuration to be valid; otherwise, the configuration is rejected. You cannot specify error-redirect or URL filtering rules and rule sets in this statement.
3. Configure the **extension-service http-packet-manager** statement and specify the HCM error-redirect rules, rule sets, and HCM URL filtering rules and rule sets.

   You should specify at least one error-redirect rule, one error-redirect rule set, one URL filtering rule , and one URL filtering rule set for the configuration to be valid; otherwise, the configuration is rejected. You cannot specify HCM tag rules and rule sets in this statement.
4. Configure the **service-order** statement to specify the order in which the service set is used for HTTP Content Management for both forward and reverse flows.

Configuring HTTP Content Management Service Sets

```
services {
  service-set http-manager-all-in-one {
    interface-service {
      service-interface ms-5/1/0;
    }
    extension-service http-manager {
      hcm-tag-rules tag-sub-id-radius;
    }
    extension-service http-packet-manager {
      hcm-redirect-rules redirect404;
      hcm-url-rules logAll;
    }
    service-order {
      forward-flow [ junos-ptsp http-manager http-packet-manager ];
      reverse-flow [ junos-ptsp http-manager http-packet-manager ];
    }
  }
}
```

Related Documentation

- Configuring HTTP Tagging on page 6
- Configuring HTTP Error-redirect on page 9

- Configuring HTTP URL Filtering and Logging on page 11
- HTTP Content Management Overview on page 1
- Viewing and Clearing HTTP Content Management Rule Statistics on page 17

Viewing and Clearing HTTP Content Management Rule Statistics

You can view the statistics for an HCM rule only if you have specified the count action in the rule. To verify the HTTP rule statistics, from operational mode, enter the **show services http-manager statistics <rule-type> <rule-name>** command.

The statistics displayed for a rule is the sum of all the instances of that rule. If you use the rule in multiple service sets, the statistics displayed will be the sum of statistics of the rule in all service sets.

Enter the **show services http-manager statistics hcm-tag-rule <tag-rule-name>** to view the current statistics for an HTTP tag rule.

```
user@router> show services http-manager statistics hcm-tag-rule <tag-rule-name>
Interface: ms-3/0/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
Interface: ms-3/1/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
```

Enter the **clear services http-manager statistics hcm-tag-rule <tag-rule-name>** command to clear the statistics for all instances of the specified HTTP tag rule.

Enter the **show services http-manager statistics hcm-redirect-rule <redirect-rule-name>** to view the current statistics for an HTTP redirect rule.

```
user@router> show services http-manager statistics hcm-redirect-rule
<redirect-rule-name>
Interface: ms-3/0/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
Interface: ms-3/1/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
```

Enter the **clear services http-manager statistics hcm-redirect-rule <redirect-rule-name>** command to clear the statistics for all instances of the specified HTTP redirect rule.

Enter the **show services http-manager statistics hcm-url-rule <url-rule-name>** to view the current statistics for an HTTP URL rule.

```
user@router> show services http-manager statistics hcm-url-rule <url-rule-name>
Interface: ms-3/0/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
Interface: ms-3/1/0
Term id                          Hits
1                                  10
22                                100
333                              1000
4444                            10000
55555                          100000
6                          4292967296
```

Enter the **clear services http-manager statistics hcm-url-rule <url-rule-name>** command to clear the statistics for all instances of the specified HTTP URL rule.

Related Documentation

- Configuring the HTTP Content Management Package on the Router on page 3
- Configuring HTTP Tagging on page 6
- Configuring HTTP Error-redirect on page 9
- Configuring HTTP URL Filtering and Logging on page 11
- HTTP Content Management Overview on page 1
- Configuring HTTP Content Management Service Sets on page 15