Cisco IOS Content Filtering

Configuration Guide

What is Cisco IOS Content Filtering?

The Cisco IOS® Content Filtering feature using Trend Micro infrastructure provides a mechanism to allow, block, or simply log web (HTTP Universal Resource Locator [URL]) requests going through the router. The filtering is based on categories configured in Cisco IOS Software such as gaming, pornography, weapons, etc. You can either block or permit more than 50 available categories in Cisco IOS Software. Whereas these categories are to improve employee productivity, another set of categories is to protect the network and resources: Security categories protect from adware, malware, spyware, and phishing sites.

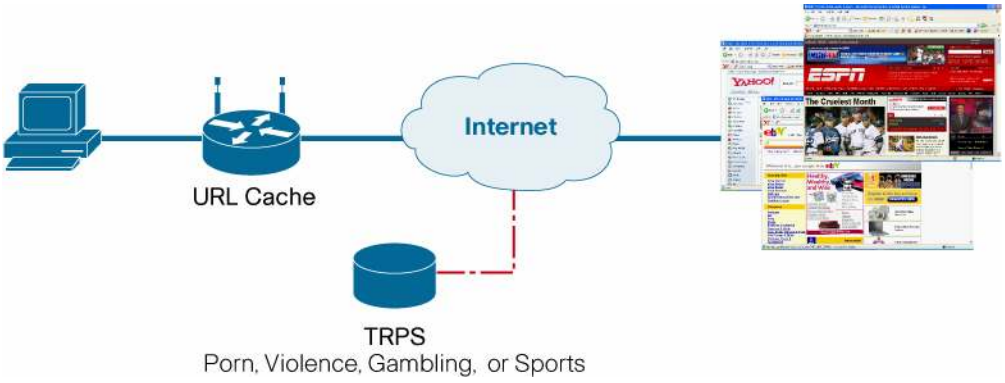
When a client makes a HTTP request, the information is sent to the Trend Router Provisioning Server (TRPS). The TRPS sends back category information about the HTTP request. For example: games.yahoo.com belongs to the Gaming category. If Gaming is denied in the Cisco IOS Software policy, the router disallows the request (Figure 1).

You can configure black and white lists locally in Cisco IOS Software to permit and deny URLs and domains. If the Trend Micro server is unreachable, the router defaults to local available black and white lists. Content Filtering also supports local black and white lists that you can configure to either permit or deny URLs and domains. Cisco IOS Software supports 100 black and 100 white lists.

In order to reduce the latency of the future HTTP transactions and thus improve your experience, the router caches the categorization information received from the TRPS and uses this information to verify policy, instead of sending the URL categorization request to the TRPS.

Management and configuration is through Cisco Configuration Professional 1.1

Figure 1. Cisco IOS Content Filtering



The feature operates in three modes based on whether the router can communicate with the TRPS:

- Local filtering mode: Content Filtering always first tries to match the requested URL with the local black and white lists. If a match is not found, Cisco IOS Software then consults the TRPS server to categorize the requested URL. If the Trend Micro server is unreachable, the software goes into an allow mode. Based on the **allow**-mode setting, Cisco IOS Software either allows or denies all URL requests that cannot be matched with the local filtering lists.
- Trend filtering mode: In this mode Cisco IOS Software can communicate with the TRPS server and receive categorization information. The software first checks all the local-based filtering rules (black and white lists). If a URL does not match any of the local filtering rules and Trend Micro communication is configured, Cisco IOS Software sends a categorization

lookup request to the TRPS and makes a decision based on the response received from the TRPS. If local filtering mode fails, the software falls into Trend filtering mode if the software can communicate with the TRPS and receive categorization information. Based on the policy set for URL category, URLF either allows, denies, or logs the response from the HTTP server. If no policy is set for the returned category, the default is to allow the response to be sent back to the HTTP client.

- Allow mode: If Cisco IOS Software is unable to communicate with TRPS or if Trend Micro communication is not configured, no HTTP requests are allowed to pass the router. If you turn on allow mode, HTTP requests can still pass the router, while also checking any local filtering rules (black and white lists). If the URL does not match any of the local filtering rules, the router decides to allow or block the HTTP request based on the action configured for allow mode. If the allow mode action is on, the HTTP request is allowed; otherwise the HTTP request is blocked. When both local and trend filtering modes fail, URLF goes into allow mode. If Allow Mode action is set to on, all URL requests are allowed; otherwise, all URL requests are denied.

Prerequisites

If you purchased a Cisco® integrated services router with Content Filtering, you would have received a product authorization key (PAK). Follow the link on www.cisco.com/go/license to register your router. You would have purchased a 1 year subscription license. In order to register your router, you must provide the router serial number and product ID (PID). After you register the router, follow the steps to configure Cisco IOS Content Filtering.

The Cisco IOS Advanced IP Services or Advanced Security image is required depending on the router model you have

Steps Required to Configure Cisco IOS Content Filtering

It is assumed that your Cisco IOS Content Filtering license is activated before you configure Cisco IOS Content Filtering on your router.

Step 1. Configure the router to be able to reach the Internet.

Step 2. Download a certificate from Cisco.com to enable communication with Trend Micro.

Step 3. Configure the router to communicate with Trend Micro.

Step 4. Configure Cisco IOS Content Filtering on the router.

Step 5. Configure show and monitoring commands.

The following sections describe each step and the specific commands. An example configuration is displayed following each command. Detailed information about the commands and options available are explained in the appendix.

Step 1: Configure Router to Be Able to Reach the Internet.

The first step is to ensure that the router has Internet connectivity. Please ensure that your router can reach the Internet and also note the WAN IP address of the router.

```
Router# show ip interface brief
Interface       IP-Address     OK?   Method  Status          Protocol
Ethernet0       64.10.40.5      YES   NVRAM   up              up
Ethernet1       unassigned      YES   unset          administratively
down    down
Loopback0   10.108.200.5   YES    NVRAM   up              up
Serial0          10.108.100.5   YES    NVRAM   up           up
Serial1          10.108.40.5     YES    NVRAM  up           up
Serial2          10.108.100.5   YES    manual  up           up
Serial3          unassigned       YES    unset        administratively
down    down
```

The router WAN IP address can be private as long as correct routing is configured and the router can get to the Internet.

Step 2: Download Certificate from Cisco.com.

To make use of Trend Micro's Content Filtering trial licenses or Trend Micro's Content Filtering paid subscription license from Cisco, you must configure a subordinate certificate on the router. The router uses this subordinate certificate to ensure that communication occurs with the appropriate Trend Micro servers.

Verify that your router clock has the correct time by issuing the following command:

```
Router# Show clock
```

If the system clock is not synchronized with the current time, change the time and date by issuing the following commands:

Note: The clock must be set to the current time for the feature to work.

```
Router(config)# clock set hh:mm:ss day month year
```

Example:

```
clock set 13:32:00 23 March 2007
```

The username and password are set to secure the router. The HTTP server needs to be configured so that the web server can connect to the router.

```
Router(config)# username url-eft privilege 15 secret lab
Router(config)# enable password lab
Router(config)# ip http server
```

When the system clock matches the actual time, download a certificate from Cisco.com. Please visit the following link: **http://www.cisco.com/warp/customer/707/trend-cert.html**

- Scroll down to the section “Installing a Certificate”.
- Enter the IP address of the router in the box provided and a certificate will be downloaded to the router (Figure 2). Note: The router should be able to reach the internet and the IP address to enter should be the router’s WAN IP address.

Figure 2. Installing the Certificate

Step 3: Configure Router to Communicate with Trend Micro.

The Trend Micro server clusters are located all over the world. The common domain name of the server is trps.trendmicro.com.

Issue a nslookup to determine the IP address of the TRPS in the DOS prompt of the PC connected to the Internet through the test router. Use this IP address in Cisco IOS Software. This IP address will be used to communicate with the TRPS.

```
C:\>nslookup trps.trendmicro.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Non-authoritative answer:
Name:    trps.trendmicro.com
Address:  216.99.133.100
```

Access your router through the command-line interface (CLI) and enter the following commands to set the Trend Micro parameters:

```
Router(config)# ip host trps.trendmicro.com 216.99.133.100
Router(config)#parameter-map type trend-global global-param-map
            server trps.trendmicro.com
            cache-size maximum-memory 256
            cache-entry-lifetime 1
```

At this point the router is configured to communicate with Trend Micro.

To verify that Trend registration is successful, issue the following show command:

```
Router#show ip trm subscription status
```

The output expected follows:

```
Package Name:  Security & Productivity
```

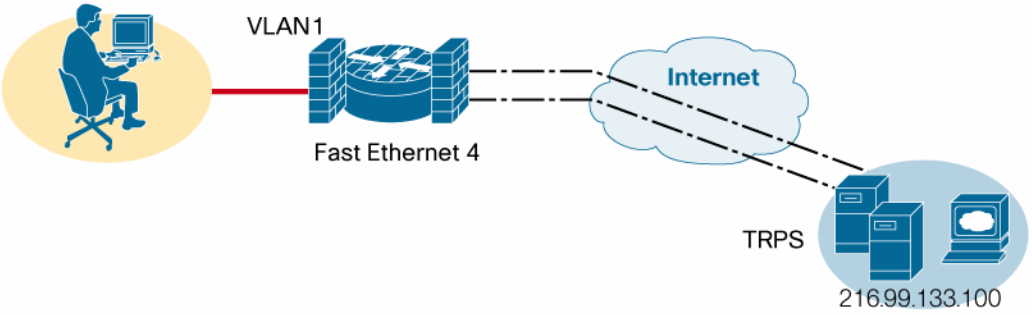
```
----------------------------------------
         Status:  Active
Expiration-Date:  Thu Jan  2 15:32:20 2020


   Package Name:  Anti-Malware
----------------------------------------
         Status:  Expired or Not Subscribed
Expiration-Date:  N/A
```

Note: If registration fails, try trm register in the router CLI to initiate registration again (Figure 3).

```
Router# trm register
```

Figure 3. Router Registration with TRPS



Step 4: Configure Cisco IOS Content Filtering on the Router.

The parameter-map type is used to specify per-policy parameters when Content Filtering is used. This parameter-map type **must** be specified to enable Content Filtering. Please type the following commands in the router CLI:

```
Router(config)#parameter-map type inspect global
Router(config)#parameter-map type urlfpolicy trend g1-trend-pm
 max-request 2147483647
 max-resp-pak 20000
 allow-mode on
 truncate hostname
 block-page message "group1: 10.10.10.0 is blocked by Trend."
```

You should use the class map as a traffic filter to segregate the traffic for which specific Layer 7 (including URL-filter) policies can be attached as child policies:

```
Router(config)#class-map type inspect match-all g1-http-class
match protocol http
Router(config)#class-map type inspect match-any tcp-class
match protocol tcp
```

This class-map type is used to configure a local filtering class. You can use it to configure the set of domains that can be allowed or blocked or the set of URL keywords that can be blocked. You

should configure the domains and the keywords using the urlf-glob parameter type prior to configuring this class. Type the following commands in the router CLI:

Note: The following commands are used to create local lists to permit or deny or local keywords that can be blocked in the URL. Keywords will be matched only with the URL (not including the domain), and not the content.

```
Router(config)# class-map type urlfilter match-any untrusted-domain-class
match  server-domain urlf-glob untrusted-domain-param
Router(config)#class-map type urlfilter match-any trusted-domain-class
match  server-domain urlf-glob trusted-domain-param
Router(config)# class-map type urlfilter match-any keyword-class
match  url-keyword urlf-glob keyword-param
```

This class-map type is used to configure categories and reputation of a URL that needs to be blocked or logged.

```
Router(config)#class-map type urlfilter trend match-any drop-category
match url category Adult-Mature-Content
match url category Pornography
match url category Gambling
match url category Nudity
match url category Gay-Lesbian
match url category Violence-hate-racism
match url category Personals-Dating
```

The policy-map type is used to configure a urlfilter policy. Under this policy map you can configure one parameter map and multiple class maps. Based on the parameter-map type configured, some of the class-map types may or not may not be allowed. When the class maps are configured under the policy, you can configure one or more actions under the class map to indicate what sort of action needs to be taken when a URL matches that class map.

```
Router(config)#policy-map type inspect urlfilter g1-trend-policy
parameter type urlfpolicy trend g1-trend-pm
class type urlfilter trend drop-category
reset
Router(config)#policy-map type inspect icmp_permit
class type inspect icmp_permit
pass
```

```
class class-default
drop
Router(config)#policy-map type inspect trend-global-policy
class type inspect g1-http-class
inspect global
service-policy urlfilter g1-trend-policy
class type inspect tcp-class
inspect global
class class-default
pass
```

The following commands create targets to which the URL filtering policy is applied. These targets are logical security zones and can be applied to the interface. You can add interfaces to these zones.

```
Router(config)#zone security zone_in
zone security zone_out
zone-pair security zp_out source zone_out destination zone_in
service-policy type inspect icmp_permit
zone-pair security zp_in source zone_in destination zone_out
service-policy type inspect trend-global-policy
```

Apply the policy and traffic direction to the WAN interface:

```
interface FastEthernet4
no ip dhcp client request tftp-server-address
ip address dhcp client-id FastEthernet4
ip nat outside
ip virtual-reassembly
zone-member security zone_out
duplex auto
speed auto
```

Apply the policy and traffic direction to the private interface:

```
interface Vlan1
ip address 192.168.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly
zone-member security zone_in
```

Additional commands to complete the configuration follow:

```
ip http server
no ip http secure-server
ip nat inside source list nat_acl interface FastEthernet4 overload
!
```

```
ip access-list extended nat_acl
permit ip 192.168.1.0 0.0.0.255 any
!
access-list 110 permit udp any any
access-list 110 deny tcp any any
access-list 110 permit ip any any
!
control-plane
!
line con 0
no modem enable
line aux 0
line vty 0 4
password lab
login
```

At this point, your router is ready to start testing Cisco IOS Content Filtering with Trend Micro.

Step 5: Configure Monitoring and Show Commands

In the router CLI turn on debug to see the working of the feature:

```
Router# debug ip urlfilter detail
Router# term mon
```

Turn debug off by typing **undebug all** in the router CLI.

Exec commands are the commands that provide some information about the feature, such as the statistics, status, etc.:

- **show ip trm subscription status:** This command displays the subscription status of the device. If the device is already registered with TRPS, the cached subscription status information is displayed. Otherwise a message is displayed indicating that the device is not registered yet.
- **show ip trm config:** This command displays the servers that are configured as TRPS.
- **show policy-map type inspect zone-pair [<zone-pair name>] sessions:** This command displays information about the connections being inspected by the firewall. If the zone-pair name is not specified, then information about all the zone pairs is displayed.
- **show policy-map type inspect zone-pair [<zone-pair name>] urlfilter cache [detail]:** This command displays information about the cache. Without the detail option the cache entries are not printed out. When the detail option is used, each cache entry is displayed. Because the URL can be quite long, only a few bytes of the URL are displayed.

The complete configuration follows:

```
fw21-871a#sh run
Building configuration...
Current configuration : 6264 bytes
!
```

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname fw21-871a
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone MST -8
clock summer-time MDT recurring
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool client
import all
network 192.168.1.0 255.255.255.0
domain-name cisco.com
netbios-name-server 171.68.235.228 171.69.2.87
dns-server 171.68.226.120 171.70.168.183
default-router 192.168.1.2
update arp
!
!
vlan ifdescr detail
!
multilink bundle-name authenticated
parameter-map type inspect global
parameter-map type urlfpolicy trend g1-trend-pm
max-request 2147483647
max-resp-pak 20000
allow-mode on
truncate hostname
block-page message "group1: 192.168.1.0 is blocked trendily."
!
parameter-map type urlf-glob trusted-domain-param
 pattern www.cisco.com
 pattern *.yahoo.com
 pattern www.110.cam*
 pattern 209.131.36.158
!
parameter-map type urlf-glob untrusted-domain-param
 pattern www.weapons.com
```

```
 pattern www.sex.com
 pattern *.sun.com
 pattern *.nbc.com
!
parameter-map type trend-global global-param-map
server trps.trendmicro.com
cache-size maximum-memory 128
cache-entry-lifetime 1
!
crypto pki trustpoint NetworkSolutions_CA
revocation-check none
!
!
crypto pki certificate chain NetworkSolutions_CA
certificate ca 10E776E8A65A6E377E050306D43C25EA
308204A6 3082038E A0030201 02021010 E776E8A6 5A6E377E 050306D4
3C25EA30
0D06092A 864886F7 0D010105 05003081 97310B30 09060355 04061302
5553310B
<EDITED FOR BREWITY>
quit
!
!
archive
log config
!
!
!
class-map type urlfilter match-any untrusted-domain-class
 match  server-domain urlf-glob untrusted-domain-param
class-map type urlfilter match-any trusted-domain-class
 match  server-domain urlf-glob trusted-domain-param
class-map type inspect match-all g1-http-class
match protocol http
class-map type inspect match-any tcp-class
match protocol tcp
class-map type urlfilter trend match-any drop-category
match url category Adult-Mature-Content
match url category Pornography
match url category Gambling
match url category Nudity
match url category Gay-Lesbian
match url category Violence-hate-racism
match url category Personals-Dating
class-map type inspect match-all icmp_permit
match access-group 110
!
!
policy-map type inspect urlfilter g1-trend-policy
parameter type urlfpolicy trend g1-trend-pm
```

```
class type urlfilter trusted-domain-class
  log
  allow
 class type urlfilter untrusted-domain-class
  log
  reset
class type urlfilter trend drop-category
reset
policy-map type inspect icmp_permit
class type inspect icmp_permit
pass
class class-default
drop
policy-map type inspect trend-global-policy
class type inspect g1-http-class
inspect global
service-policy urlfilter g1-trend-policy
class type inspect tcp-class
inspect global
class class-default
pass
!
zone security zone_in
zone security zone_out
zone-pair security zp_out source zone_out destination zone_in
service-policy type inspect icmp_permit
zone-pair security zp_in source zone_in destination zone_out
service-policy type inspect trend-global-policy
!

interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
no ip dhcp client request tftp-server-address
ip address dhcp client-id FastEthernet4
ip nat outside
ip virtual-reassembly
zone-member security zone_out
duplex auto
speed auto
!
interface Dot11Radio0
no ip address
```

```
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0
36.0 48.0 54.0
station-role root
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly
zone-member security zone_in
!
ip route 0.0.0.0 0.0.0.0 FastEthernet4
!
!
ip http server
no ip http secure-server
ip nat inside source list nat_acl interface FastEthernet4 overload
!
ip access-list extended nat_acl
permit ip 192.168.1.0 0.0.0.255 any
!
access-list 110 permit udp any any
access-list 110 deny tcp any any
access-list 110 permit ip any any
!
control-plane
!
!
line con 0
no modem enable
line aux 0
line vty 0 4
password lab
login
!
scheduler max-task-time 5000
!
webvpn cef
end
```

Another Sample Configuration

The following is a sample configuration with annotated text. The configuration can be copied as is to the router after the router is put in configuration mode by using the **config t** command.

```
! port map to indicate FW that all 8080 connections are http
connections
ip port-map http port 8080
```

```
! Trend global parameter-map to specify the TRPS server and cache-
sizes
parameter-map type trend-global hello
   server trps1.trendmicro.com
   cache-size maximum-memory 300

! Trend Policy parameter map for group-1.
!   If server is down allow the HTTP connections
parameter-map type urlfpolicy trend trend-g1-param
   allow-mode on
   block-page message “You are prohibited from accessing this web-
page”

! Trend Policy parameter map for group-2.
!   If the server is down block the HTTP connections
parameter-map type urlfpolicy trend trend-g2-params
   block-page message “Restricted access. Please contact your
administrator”

! Trend class map for group-1
!   Just match bad reputation sites
class-map type urlfilter trend trend-g1-c
   match url reputation ADWARE
   match url reputation SPYWARE
   match url reputation HACKING
   match url reputation DIALER
   match url reputation DISEASE-VECTOR
   match url reputation PASSWORD-CRACKING_APPLICATIONS
   match url reputation PHISHING
   match url reputation VIURS-ACCOMPLICE

! Trend class map for group-2
!   Match on bad reputation sites and on Adult, Pornography sites
class-map type urlfilter trend trend-g2-c
   match url reputation ADWARE
   match url reputation SPYWARE
   match url reputation HACKING
   match url reputation DIALER
   match url reputation DISEASE-VECTOR
   match url reputation PASSWORD-CRACKING_APPLICATIONS
   match url reputation PHISHING
   match url reputation VIURS-ACCOMPLICE
   match url category Adult-Mature-Content
   match url category Nudity
   match url category Pornography


! Local filtering class to allow certain domains
parameter-map type urlf-glob p-domains
   pattern “www.cisco.com”
```

```
   pattern “www.trend.com”

class-map type urlfilter p-domains
   match server-domain urlf-glob p-domains

! Local filtering class to deny certain domains
parameter-map type urlf-glob d-domains
   pattern “*.sex.com”
   pattern “www.playboy.com”

class-map type urlfilter d-domains
   match server-domain urlf-glob d-domains

! Urlfilter Policy map for group one.
!  Don’t block any of the domains locally
policy-map type inspect urlfilter g1-pol
   parameter type urlfpolicy trend trend-g1-param
   class type urlfilter p-domains
      allow
   class type urlfilter trend trend-g1-c
      reset

! Url filter policy map for group-2
!   Block the deny domains locally
policy-map type inspect urlfilter g2-pol
   parameter type urlfpolicy trend trend-g2-param
   class type urlfilter p-domains
      allow
   class type urlfilter d-domains
      log
      allow
   class type urlfilter trend trend-g1-c
      reset

! First level class to prevent Trend based url filtering for websites
that are local to the enterprise
! The first deny line is to make the http connections going to the
proxy to not match this class
ip access-list extended 101
   deny tcp any host 192.168.1.10 eq 8080
    permit tcp any 192.168.0.0 0.0.255.255 eq 80 8080
    permit tcp any 10.0.0.0 0.255.255.255 eq 80 8080

class-map type inspect no-urlf-c
   match access-group 101

! First level class map to support url-filtering for group one
ip access-list extended 102
   permit tcp 192.168.0.0 0.0.255.255 any
```

```
class-map type inspect urlf-g1-c
   match protocol http
   match access-group 102

! First level class map to support url-filtering for group two
class-map type inspect urlf-g1-c
   match protocol http


! First level class map to allow ICMP from protected network to
outside
class-map type inspect icmp-c
   match protocol icmp

! First level policy map that brings everything together
! Always configure the class with most restrictions first
policy-map type inspect fw-pol
   class type inspect icmp
      inspect

   class type inspect no-urlf-c
      inspect

   class type inspect urlf-g2-c
      inspect
      service-policy urlfilter g2-pol
   class type inspect urlf-g1-c
      inspect
      service-policy urlfilter g1-pol

!  Create targets to which the FW policy is applied
zone security z1
zone security z2
zone-pair security z1z2 source z1 destination z2
   service-policy type inspect fw-pol

! inside interface
interface FastEthernet 0/0
   ip address 1.1.1.1 255.255.0.0
   zone-member security z1

!outside interface
interface FastEthernet 1/0
   ip address 169.1.0.1 255.255.0.0
   zone-member security z2
```

Step 6: Alerts and Syslog Messages

Alert messages are syslogs that have an additional amount of user controlled visibility. Alerts can be can be controlled on a global basis using parameter map configuration.

Possible alert messages and their meanings:

- %URLF-5-LEAVE_ALLOW_MODE: Connection to an URL filter server is made, or subscription for URLF service is renewed. The router is returning from ALLOW MODE.
- %URLF-3-ENTER_ALLOW_MODE: Received registration error in URLF response, the router is entering allow mode.
- "%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?"

  This message is displayed when the URL in a look-up request is too long; any URL longer than 3K will be dropped.
- "%URLF-4-MAX_REQ: The number of pending request exceeds the maximum limit <1000>"

  This message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

These syslog messages are under per-class granular control via the log action associated with the matching Trend class.

Example:

```
policy-map type inspect urlfilter trend-policy
class type urlfilter untrusted-domain-class
log
```

- "%URLF-6-SITE_ALLOWED: Client 10.0.0.2:12543 accessed server 10.76.82.21:8080" This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged because the IP address of the request is found in the cache, so parsing the request and extracting the URL is a waste of time.
- "%URLF-4-SITE-BLOCKED: Access denied for the site `www.sports.com'; client 10.54.192.6:34557 server 172.24.50.12:80" This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.
- "%URLF-6-URL_ALLOWED: Access allowed for URL http://www.n2h2.com/; client 10.54.192.6:54123 server 192.168.0.1:80" This message is logged for each URL request that is allowed by a UFS. It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and logged.
- "%URLF-6-URL_BLOCKED: Access denied URL http://www.google.com; client 10.54.192.6:54678 server 172.19.14.2:80" This message is logged for each URL request that is blocked by a UFS. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

Syslog messages under no additional granular control and their meanings:

- %FW_TRM-5-SUB_ACTIVE: Subscription for 'Security and Productivity Package' is currently Active

- %FW_TRM-5-SUB_PRE_EXPIRATION: Subscription for 'Security and Productivity Package' is to expire in 15 Days. Expiration Date Wed Dec 31 16:00:00 1969
- %FW_TRM-4-SUB_GRACE_PERIOD: Subscription for 'Security and Productivity Package' is in Grace Period. Expiration Date Wed Dec 31 16:00:00 1969
- %FW_TRM-3-SUB_EXPIRED: Subscription for 'Security and Productivity Package' has Expired. Expiration Date Wed Dec 31 16:00:00 1969
- %FW_TRM-3-TRPS_ERROR: TRPS indicated Authentication Failure Error. All Subscriptions will be disabled

Appendix: Detailed Explanation of Configuration Commands

Configuration Commands

Configuration commands are the commands that you can enter after the router CLI is put in the configuration mode by using the **config terminal** command. All these commands can potentially affect router operation. When you change the configuration, you must save it using the **write** command for the changes to be effective after a reboot.

parameter-map type trend-global <name>

This command is used to configure the global parameters associated with TRPS-based URL Filtering. Only one such parameter map can exist on the router. The <name> can be any string. The following are the sub-mode commands that are available under this parameter map:

- **alert <on|off>:** This command enables or disables the alerts. The default is On. If the alerts are on, the firewall logs certain events to the syslog server.
- **cache-entry-lifetime <time in hours>:** This command allows you to specify the time for which a cached entry is valid. A cache entry is removed from the cache when either the cache-entry lifetime for that entry expires or when the cache is full and more room needs to be made for the subsequent entries. The default value without this command is 24 hours.
- **cache-size maximum-memory <Kilo Bytes>:** This command specifies the maximum amount of memory to be used by the URL cache. Based on the available memory on the router, it is not always guaranteed that the amount specified by this command will be available for caching. The default value if this command if not specified is 250 KB.
- **Server <server name of IP address> [https-port <portnum>] [http-port <portnum>] [retrans <count>] [timeout <seconds>]:** You can use this command to specify the TRPS server name and the HTTP and HTTPS ports of the server. Also, the retrans value specifies the number of times to retry if a response is not received prior to declaring the server as down. The timeout specifies the amount of time to wait prior to retransmitting a request. The default values follow:
  - Server: trps1-bldr.cisco.com (This server will be changed later.)
  - HTTP port: 80
  - HTTPS port: 443
  - Retransmission count: 3
  - Timeout: 60 seconds

If the trend-global parameter-map type is not configured, then the default values indicated are used if TRPS-based URL filtering is enabled.

Parameter-Map Command: parameter-map type urlfpolicy trend <name>

The parameter-map type is used to specify per-policy parameters when TRPS-based URL filtering is used. This parameter-map type must be specified to enable TRPS-based URL filtering. The following are various sub-mode commands available under this parameter-map type:

- **allow-mode <on|off>:** This command specifies what needs to be done if a URL does not match any of the local filtering rules and the firewall cannot receive categorization information for the external server. If the value is **On**, the URL is let through; otherwise it is blocked. The default value for this value is **Off**.
- Block-page {[message <string>] | [redirect-url <url>]}: Use this command to customize the information displayed when a URL is blocked by the firewall. The default for this value [[ok? otherwise pls put another noun]] is a preconfigured string, which simply indicates that the user is not authorized to access the URL.
- Max-request <value>: This command specifies the maximum number of outstanding categorization requests on a per-target per-policy basis. Here the target is a zone pair on which the firewall is configured and the policy is the URL-filter policy. The default value is 1000.
- Max-resp-pak <value>: This command specifies the number of web responses that should be held, on a per-target per-policy basis, when waiting for a categorization response from TRPS. The default value is 200.
- Truncate <hostname>: This command indicates what needs to be sent to the TRPS server when the total URL length, excluding the length of script parameters, exceeds the maximum allowed by TRPS. If you configure this command, then only up to the domain name is sent to TRPS. If this command is not configured and the URL length exceeds the maximum, then the request is blocked. The default is to block a page whose URL length exceeds the maximum.

parameter-map type urlfpolicy local <name>

The parameter-map type is used to specify per-policy based parameters when no server-based filtering is used (that is, only local filtering is enabled). This parameter-map type is optional, and default values are used if it is not specified. The following are various sub-mode commands available under this parameter-map type:

- alert <on/off>: This command enables or disables the alerts. The default is On. If the alerts are on, the firewall logs certain events to the syslog server.
- allow-mode <on|off>: This command specifies what needs to be done if a URL does not match any of the local filtering rules and the firewall cannot receive categorization information for the external server. If the value is On, the URL is let through; otherwise it is blocked. The default value for this value is Off.

- Block-page {[message <string>] | [redirect-url <url>]}: Use this command to customize the information displayed when a URL is blocked by the firewall. The default for this value is a preconfigured string, which simply indicates that the user is not authorized to access the URL.

parameter-map type urlf-glob <name>

Use this parameter-map type to specify the list of domains or URL keywords that should be allowed or blocked by the firewall. It supports only one subcommand (pattern < urlf glob expressions>) to indicate one glob expression. You can specify the same command multiple times to specify a list of urlf-glob expressions.

- pattern

class-map type urlfilter <name>

This class-map type is used to configure a local filtering class. You can use it to configure the set of domains that can be allowed or blocked or the set of URL keywords that can be blocked. The domains and the keywords must have been configured using the urlf-glob parameter type prior to configuring this class. The following are the match commands available under this class-map type:

- **match server-domain urlf-glob <urlf-glob parameter-map name>:** Use this command to indicate a set of domains to be matched.
- **match url-keyword urlf-glob <urlf-glob parameter-map name>:** Use this command to indicate a set of keywords that should be matched.

class-map type urlfilter trend <name>

Use this class-map type to configure categories and reputation of a URL that needs be blocked or logged. The following are the match commands available under this class-map type:

- **match url category <category>:** Use this command to indicate the URL category that should be matched. You can use multiple match commands within a single class map.
- **match url reputation <reputation>:** Use this command to indicate the URL reputation that should be matched. You can use multiple match commands within a single class map.

  You can use a combination of url-reputation and url-categorization [[should those be URL?]] within a single class map.

policy-map type inspect urlfilter <name>

Use this policy-map type to configure a urlfilter [[is that ok?]] policy. Under this policy map you can configure one parameter map and multiple class maps. Based on the parameter-map type configured, some of the class-map types may or not may not be allowed. After the class maps are configured under the policy, you can configure one or more actions under the class map to indicate what sort of action needs to be taken when a URL matches that class map.

- **parameter type urlfpolicy {local | trend} <name>:** Use this command to specify what kind of url filtering—either local or server (TRPS)-based URL filtering—will be allowed by the URLF policy. If the parameter is not configured, the policy allows only local filtering.

Note: In addition to a parameter map, you must configure class maps for the actual filtering to happen. If no class maps are configured in a urlf policy, all the URLs are handled based on the allow-mode action.

- **Class type urlfilter [trend] <name>:** This command specifies what kind of class needs to be matched under an urlfilter policy.

The following are the actions that are supported under a class of a policy:

- log: This action indicates that a portion of the URL that matched the class should be logged to a syslog server. This action is available for all types of class maps.
- Reset: This action indicates that the HTTP request should be blocked when the URL matches the classes. This action is available for all types of class maps.
- Allow: This action indicates that the HTTP request should **not** be blocked. This action is allowed for all local filtering classes. This action is not allowed for trend class map; that is, class map of type "**urlfilter trend**".

class-map type inspect <name>

Use this class map as a traffic filter to segregate the traffic for which specific Layer 7 (including URL filtering) policies can be attached as child policies. **As of today, the inspect class map needs to have a match protocol HTTP statement to be able to attach the Urlfilter [[pls address that expression; you have urlf, URLF, Urlfilter (as here), url-filtering, etc. please use just one expression for this and fix globally]] policy as the child policy.**

policy-map type inspect <name>

This policy map is the top-level policy map needed to enable URL filtering. This policy map enables the firewall, and inside this policy map you can configure a URL filtering policy. Under this policy map, you must configure the class of type **inspect**, specify the **inspect** action to enable firewalling, and then configure **service-policy urlfilter <urlfilter policy name>** to enable content filtering.

Note: You will also notice urlfilter action, but do not use that because that is the traditional way of configuring URL Filtering, which is obsolete.

ip port-map http port tcp <value> list <acl>

Use this command to tell the firewall what IP address or port numbers should be treated as HTTP connections. For example:

- **Ip port-map http port tcp** 8080 tells the firewall that all TCP connections to port 8080 should be treated as HTTP connections.
- **ip port-map http port tcp 1500 list 101** tells the firewall that all TCP connections to port 1500 of the servers specified in access control list (ACL) 101 should be treated as HTTP connections.

Note: Unless explicitly disabled, the **no** command treats the connection to port 80 as an HTTP connection.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C89-492776-01 10/10