Cisco Videoscape Distribution Suite Transparent Caching Manager User Guide

Release 5.6.1
August 2015

Cisco Systems, Inc.
www.cisco.com

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface vii

Document Conventions vii

Terminology viii

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1 **Getting Started** 1-1

Logging Into VDS TC Manager 1-1

VDS TC Manager Elements 1-5

Monitoring the System Status 1-6

Viewing Graphs 1-7

Viewing Data for a Specific Time Frame 1-8

Closing VDS TC Manager 1-10

CHAPTER 2 **Status Menu** 2-1

Dashboard 2-1

Hardware View 2-3

Logical View 2-7

Cluster Status 2-8

Cache Engines 2-10

Management Server 2-13

Memory Utilization 2-15

CPU Utilization 2-16

Storage 2-17

CHAPTER 3 **Statistics Menu** 3-1

Interfaces 3-1

Total Data 3-2

Management Server (mg) 3-2

Cache Engine (ce "#") 3-3

TCP Connections 3-6

Downstream 3-6

Upstream 3-7

Downstream Handling 3-8
Asymmetric Connections 3-9
Unknown Direction 3-10
Loop Detected 3-11
Bandwidth 3-12
Total Downstream 3-13
In Downstream 3-14
Cache Out 3-15
In-Out 3-16
Bytes Hit Ratio 3-17
Cache Productivity 3-17
Percentile 3-18
Total Upstream 3-19
In Upstream 3-20
HTTP Services 3-21
Total Downstream 3-22
In Downstream 3-22
Cache Out 3-23
Bytes Hit Ratio 3-24
Cache Content 3-25
Cache Size 3-26
Cache Files 3-26
Top HTTP URLs 3-27
Top P2P Hashes 3-28
Storage 3-29
Volume Usage 3-30
Requests 3-31
Block Size 3-32
Read Percentage 3-33
iSCSI Network 3-34
Bandwidth 3-35
QoE 3-36
HTTP Clear vs. Cache 3-36
P2P Clear vs. Cache 3-37
IP Statistics 3-38

CHAPTER 4 **Configuration Menu** 4-1
Cluster Configuration 4-1
Exporting the Configuration File 4-2

Using the Policy Manager 4-3
Rules 4-4
Editing Rules 4-5
Adding Rules and Subrules 4-6
Deleting Rules 4-8
Configuration Section 4-8
Export 4-9
Import 4-9
Version History 4-10
Current Configuration 4-10
Categories 4-11
Editing Categories 4-12
Adding Categories 4-14
Policies 4-17
Editing Policies 4-18
Adding Policies 4-19
Timeplans 4-21
Editing Timeplans 4-22
Adding Daily Timeplans 4-23
Adding Weekly Timeplans 4-24
Adding Monthly Timeplans 4-25
Adding Yearly Timeplans 4-26
HTTP Services 4-27
Editing HTTP Services Groups 4-28
Adding an HTTP Services Group 4-30
Publish the Configuration 4-30
The License Manager 4-31
Generating a License Request 4-32
Installing a New License 4-32
License Enforcement 4-33
License Enforcement Functionality 4-33
License Measurements and Warnings 4-33
Exceeded License 4-34
License Enforcement 4-34
Licensed Forwarding Example in VDS TC Manager 4-34
Settings 4-35
General 4-35
Changing or Resetting Passwords 4-36

CHAPTER 5 **Maintenance Menu** 5-1

Upload Files 5-1

Logs 5-2

Graphs 5-4

Cache Lists 5-5

Export Cache List 5-5

Export Black List 5-6

UI Log 5-7

APPENDIX A **Basic Policy Example** A-1

Basic Policy Management Example A-1

Preface

Revised: August 2015, OL-28017-05

Cisco Videoscape Distribution Suite (VDS) Transparent Caching (TC) Manager is a web monitoring application that you can use for both integrated appliance and cluster installations. Using graphs and statistics, the intuitive user-friendly interface of Cisco VDS TC Manager enables you to monitor your VDS-TC Transparent Caching HTTP and P2P aching performance. Cisco VDS TC Manager provides an immediate presentation of the system overall operational performance, logical and cache statuses, and information regarding configuration, storage, and interface.

The *Cisco Videoscape Distribution Suite Transparent Caching Manager User Guide* provides information on how to use the VDS TC Manager for both cluster and integrated appliance installations.

This preface describes terminology that is used throughout this guide and demonstrates the styles and conventions used in this guide. This preface contains:

- Document Conventions
- Terminology
- Obtaining Documentation and Submitting a Service Request

Document Conventions

Table 1 describes the conventions used in the this guide.

Table 1 Conventions Used

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Choosing a menu item in paragraphs	**Option > Network Preferences**
Choosing a menu item in tables	Option > Network Preferences

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Terminology

Table 2 describes terms and concepts that apply to VDS TC Cache Manager.

Table 2 VDS TC Cache Manager Terminology

Term	Description
bytes hit ratio	The number of bytes of cached out traffic divided by the total number of bytes of traffic, whether it was cached or not. For example, a 60% bytes hit ratio means that 60% of the overall bandwidth came from the cache and 40% came from the world.
cache in	A connection where the object requested by a subscriber does not exist in the cache (which creates a “miss”), and the requested incoming data from the world is stored in the cache.
cache out	A connection where the object requested by a subscriber exists in the cache (which creates a “hit”), and the request is served from the cache as outgoing traffic to the subscriber.
cache productivity	The total cached out traffic divided by the total cached in traffic. This information is available for all protocols.
clear	The status of a subscriber request when the requested file segment does not exist in the cache. Subsequently, this object is either cached in or forwarded.
CMDB miss	The status of a subscriber request when the requested file segment does not exist in the cache due to an unexpected deletion or corruption.
data	A connection where P2P or HTTP file segments are transferred.
data non-data ratio	The ratio of data to non-data. The average data non-data ratio is between 1% and 10%.
downstream	Objects transmitted from the world to the subscriber. Also called W2I.
forward	The process of forwarding an object directly to its requesting subscriber without caching it. This is applied to an object that does not yet exist in the cache. At this stage, it is only listed in the cache, according to the predefined license rules of the platform (*see* verify), and will only be cached upon future request.
hit	The status of an ISP subscriber request when the requested file segment exists in cache. Subsequently, this object is cached out.
hit miss ratio	The number of hits divided by the number of misses.
I2W	Upstream data flowing from the ISP to the world.

Table 2 VDS TC Cache Manager Terminology (continued)

Term	Description
incoming	Downstream and upstream objects transmitted from the redirector into the cache server. Each incoming object is either cached in, cached out, forwarded, or blocked.
non-data	A connection through which P2P clients communicate with each other but do not transfer P2P file segments. For example, P2P clients may communicate the details of the file segments and the uploader queue number, but do not transfer the file segments.
outgoing	Downstream and upstream objects transmitted out from the redirector. Each outgoing object was either cached in, cached out, or forwarded.
request hit ratio	The first time a new session arrives in the cache, it is labeled as cache out, cache in, or forward. The request hit ratio represents the number of cache out sessions divided by the number non-cache out sessions. That is, the request hit ratio measures the percentage of requests delivered from cache versus the world.
upstream	Objects transmitted from the subscriber to the world. Also called I2W.
verify	A predefined set of license dependent rules that determine the caching parameters of an object.
world	The World Wide Web (WWW).
W2I	Downstream data flowing from the world to the subscriber.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Getting Started

This chapter describes how to get started with the Cisco VDS TC Manager.

Note To get started with the Cisco VDS TC Manager, you need the IP address of the VDS TC management server, and the VDS TC Manager username and password that were provided by Cisco at installation.

This chapter contains the following sections:

- Logging Into VDS TC Manager
- VDS TC Manager Elements
- Monitoring the System Status
- Viewing Data for a Specific Time Frame
- Closing VDS TC Manager

Logging Into VDS TC Manager

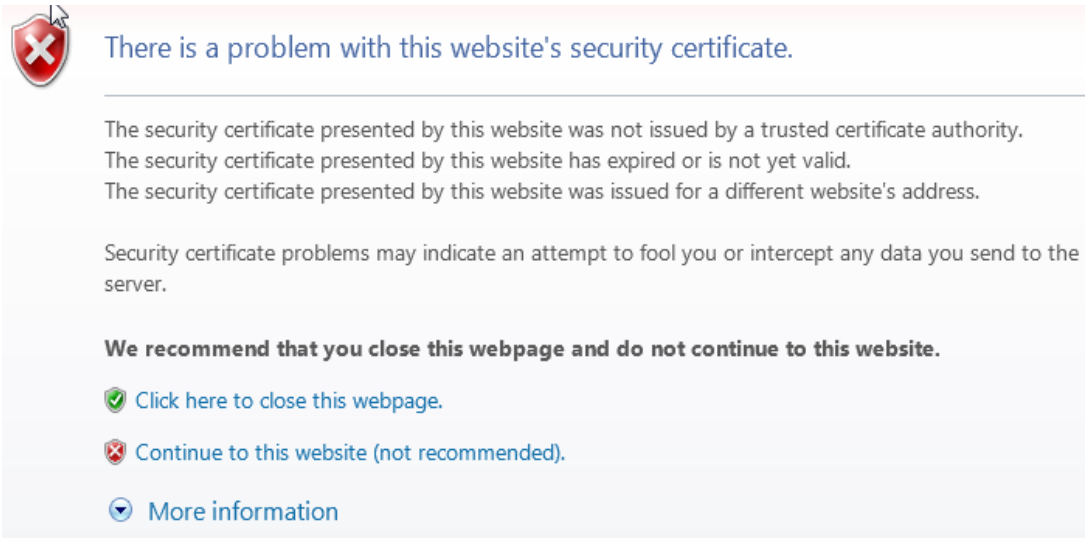
Follow these steps to log into the VDS TC Manager:

Step 1 In a web browser, such as Internet Explorer or Firefox, enter **https://***IP_address*, where *IP_address* is the IPv4 address of the VDS TC management server or enter **https://[***IP_address***]**, where *IP_address* is the IPv6 address of the VDS TC management server.

Note Notice the brackets ([]) around the IPv6 address.

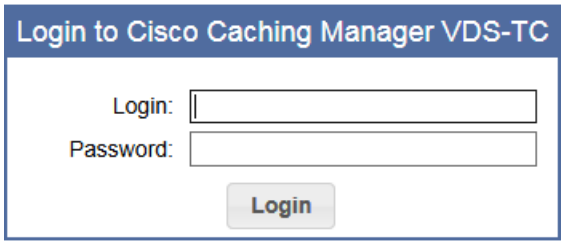
Step 2 A Security Alert window appears.The Security Alert window will vary depending on the web browser that you use. Figure 1-1 shows an example of the Internet Explorer Security Window.

Figure 1-1 Security Alert Window



Step 3 Click **Continue to this website**. An authentication dialog box appears. Figure 1-2 shows an example of an authentication dialog box for Internet Explorer.

Figure 1-2 Authentication Dialog Box for Internet Explorer



Step 4 There are two levels of users for VDS TC Manager; one level of users has full privileges and the other level has read-only privileges. Enter a user name and password that is appropriate for the level of privilege that you need.

Note Please contact your Cisco account system engineer if you need a list of user names and default passwords. It is recommended that you modify the default passwords.

Please contact your Cisco account system engineer if you need the procedure for changing the default passwords.

Step 5 The VDS TC Manager window appears.

Figure 1-3 VDS TC Manager Integrated Appliance Window

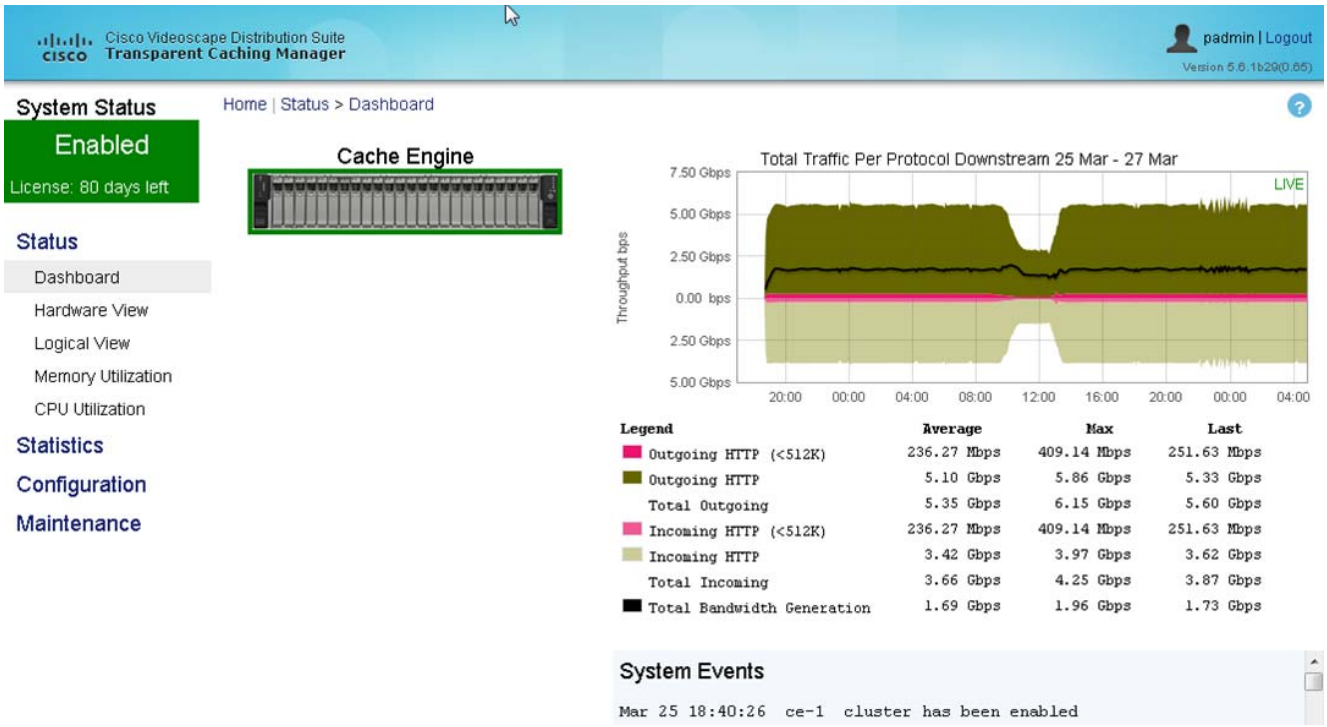


Figure 1-4 VDS TC Manager Blade Server Cluster Window

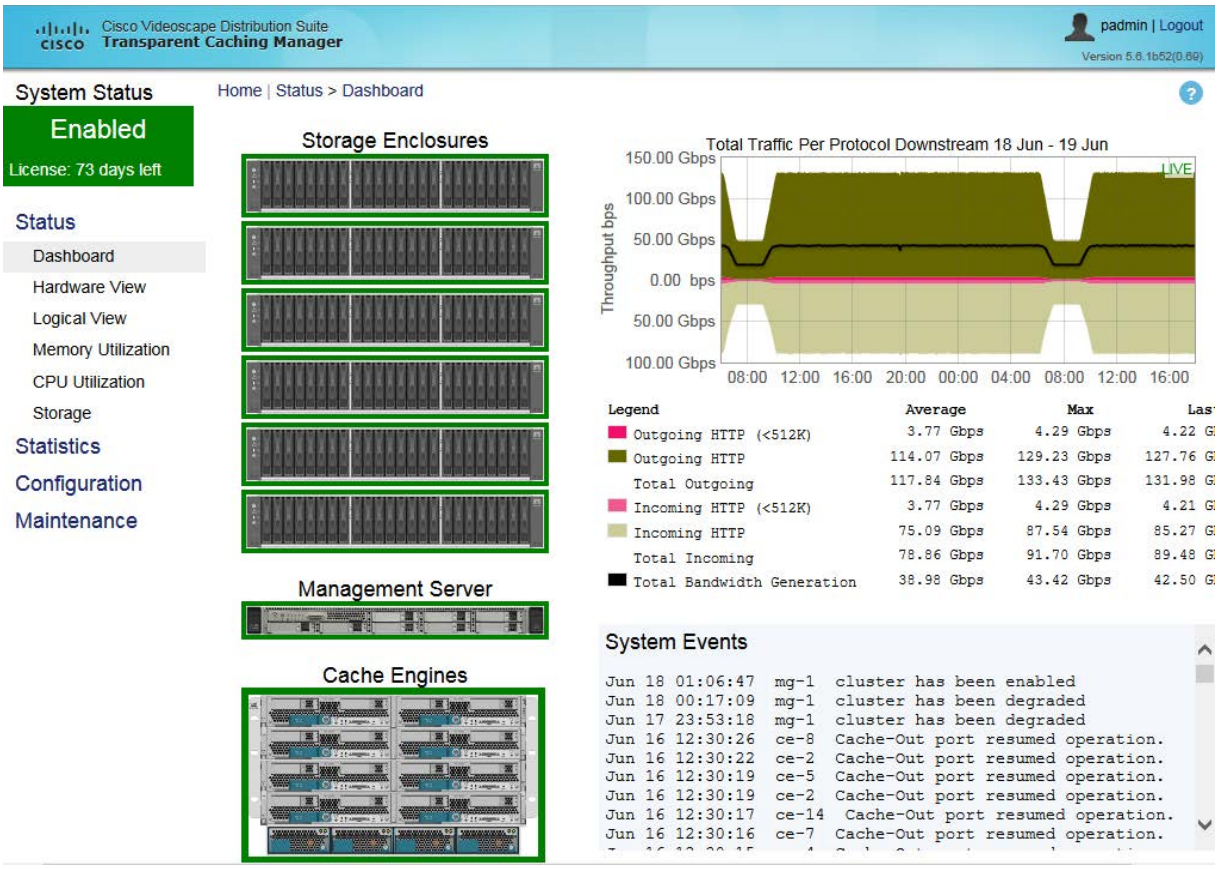
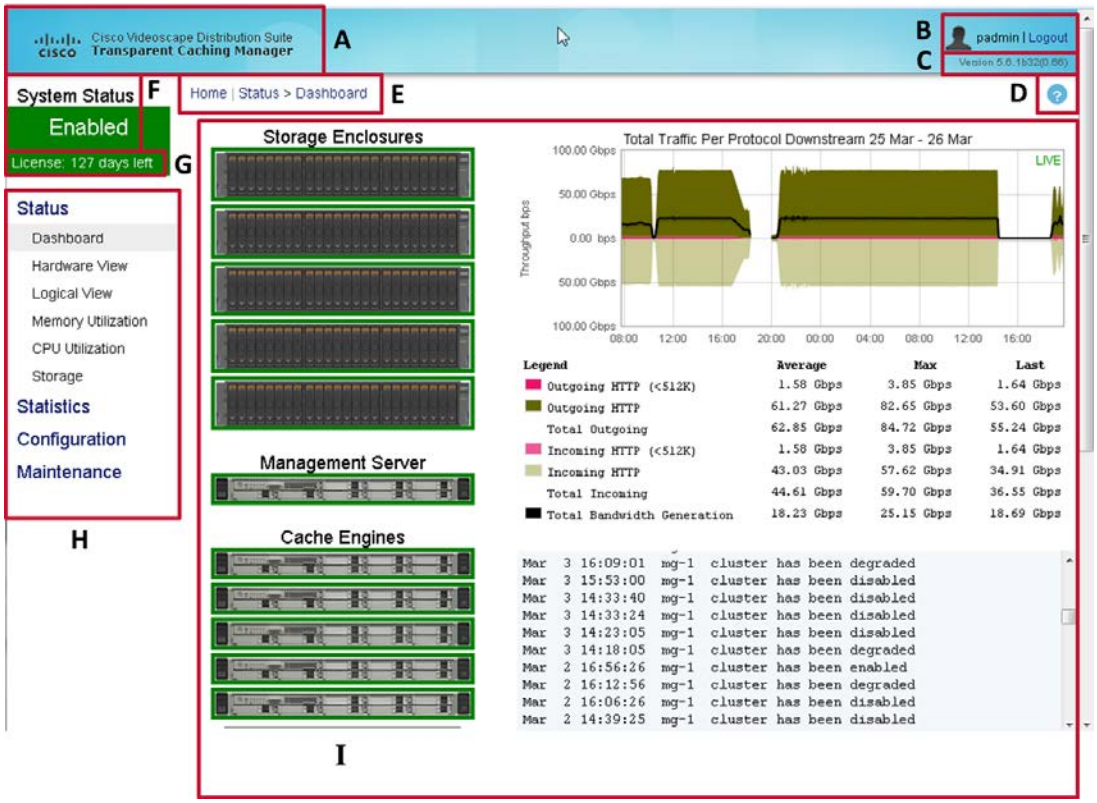


Figure 1-5 VDS TC Manager C-Series Cluster Window



VDS TC Manager Elements

Use the letters denoted in Figure 1-5 as a guide for the Cisco VDS TC Manager elements.The VDS TC Manager includes the following elements:

- **(A) Product Name:** The name of the product (Cisco VDS TC Manager).
- **(B) User/Logout:** Displays the user name and allows you to logout and switch users.

Note Clicking **Logout** allows the user to log in as a different user from the log in window.

- **(C) Version Number:** Displays the version number of the product.
- **(D) Help:** Clicking the question mark opens the help file.
- **(E) Links:** This section displays the path of the current page with associating links for each one of the menus across the path. By clicking the **Home** link, the dashboard page opens.
- **(F) System Status:** This indicates the system status: Enabled, R-Degraded, Degraded, and Disabled.
- **(G) License:** Displays the amount of days before your license expires.

Note The License Health field only appears if you have an evaluation version license.

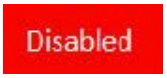
- **(H) Cisco VDS TC Manager Pane (Navigation):** Provides indicators and navigational menus.
- **(I) Working area:** The information that is displayed in this area depends on what menu you choose. This information may include component status, file information, and performance graphs and charts.

Monitoring the System Status

The System Status indicator monitors your platform system status. Using colors, this indicator shows the global status of the entire system: cache engines and storage controllers. The system status is automatically updated upon a system state change.

The system status is displayed in the upper left corner of the Cisco VDS TC Manager pane. One of five possible colors and statuses are displayed, as described in the System Status table.

Table 1-1 System Status

Status	Color	Description
	Green	All of the following system components are working as expected: • **System Status is Up:** All cache engine servers are enabled. • **Storage Status:** Storage is operational • **Cache Server:** Service is up and running. • **Storage:** All storage controllers are up and running.
	Yellow	**The status is redundancy degrading:** The redundant server is not “up”. **Note** This status is valid only when N+1 feature is configured.
	Orange	**The status is degraded:** If less then “N” Cache Engines are active, or if one or more of the controllers are down, its status is downgraded to a degraded status.
	Red	The disabled status is engaged when all cache engines are “down” or if the license is expired.

Viewing Graphs

Figure 1-6 Graph Enhancements

VDS TC Manager includes the following interactive graph enhancements for version 5.6.1:

- **Hovering:** By hovering over a specific value point in the line, that numerical value appears to the right of the Focal Point Legend.
- **Dragging:** By dragging the time line right or left, you can adjust the specific time for viewing a numerical value.
- **Zooming:** Using the icons located above the graph allows the user to zoom-in or zoom-out.
- **Show All/Hide All/Hide Filtered/Show Filtered:** By using the check boxes in the Focal Point Legends section you can show or filter specific items in the graph. To show all of the items in the graph, click the **Legend** check box. To filter all of the items from the graph, uncheck the **Legend** check box.
- **Export:** Click the **Export** button and the Graph Export window appears. In this window, click **Download** to save the graph as a file.

Note When a graph contains several lines that cannot be aggregated to a graph (for example Status > CPU Utilization, Statistics > Bandwidth > BHR, or HTTP Services > BHR), the graph displays only the top five lines based on the maximum value of each line.

Note To enable these interactive graph features, choose **Configuration > Settings** and click **Enable**. To disable the interactive graph features, click **Disable**.

Viewing Data for a Specific Time Frame

Many of the VDS TC Manager windows enable you to choose a preferred time frame for which to display information. These windows include:

- All windows under the Statistics > Interfaces menu
- All windows under the Statistics > TCP Connections menu
- All windows under the Statistics > Bandwidth menu, except Percentile
- All windows under the Statistics > HTTP Services menu
- The Cache Size and Cache Files windows under Cache Content
- The Statistics > Storage window except Volume Usage
- The HTTP Clear vs. Cache window and the P2P Clear vs. Cache window under the QoE menu

You can view information for the following time frames:

- Day
- Week
- Month
- Year

Choosing Day or Week requires an additional time frame selection using the date navigation buttons.

Figure 1-7 Date Navigation Buttons

Table 1-2 describes the Date Navigation buttons.

Table 1-2 Date Navigation Buttons

Button	Description
Day	Displays data from the previous 24 hours
Week	Displays data from the previous 7 days.
Month	Displays data from the previous 30 days.
Year	Displays data from the previous 12 months.

Table 1-2 Date Navigation Buttons (continued)

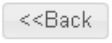
Button	Description
	• **In day mode:** When you click this button in Day mode, the graph displays data from the first 36 housrs that VDS TC started capturing data. • **In week mode:** When you click this button in Week mode, the graph displays data from the first 9 days that VDS TC started capturing data. • **In month mode:** When you click this button in Week mode, the graph displays data from the first 35 days that VDS TC started capturing data.
	• **In day mode:** When you click this button in Day mode, the graph displays data for the 36 hours, relative to the currently selected day. • **In week mode:** When you click this button in Week mode, the graph displays data for the 9 days, relative to the currently selected week. • **In month mode:** When you click this button in Month mode, the graph displays data for the previous 35 days, relative to the currently selected week.
	Displays the data for the date you select. When you click this button, a calendar opens. From this calendar you can click the date for which you want to view data. This option not available for month or year. **Note:** You cannot click future dates.

Table 1-2 Date Navigation Buttons (continued)

Button	Description
Forward>>	• **In day mode:** When you click this button in Day mode, the graph displays data for the next 36 hours, relative to the currently selected day. • **In week mode:** When you click this button in Week mode, the graph displays data for the next 9 days, relative to the currently selected week. • **In month mode:** When you click this button in Month mode, the graph displays data for the next 35 days, relative to the currently selected week. **Note:** This button does nothing if the selected date is the current date.
>>>	• **In day mode:** When you click this button in Day mode, the graph displays data for the most recent 36 hours. • **In week mode:** When you click this button in Week mode, the graph displays data for the most recent 9 days. • **In month mode:** When you click this button in Month mode, the graph displays data for the most recent 35 days. **Note:** This button does nothing if the selected date is the current day.

Note You can choose any week within the past 52 weeks.

Closing VDS TC Manager

To close the VDS TC Manager, click **Logout** in the upper-right hand corner and close your web browser.

Note For security reasons, you should always logout of VDS TC Manager before closing the web browser window.

Status Menu

This chapter describes how to view information regarding your platform, focusing on status details. Information is presented in a designated set of menus.

The Status menu contains the following choices:

- **Dashboard:** This option displays information about the status of your daily events, caching downstream, and the devices using color indicators applied to component figures
- **Hardware View:** Displays information about the status of the platform hardware, including ports, using color indicators to indicate the status of the platform components.
- **Logical View:** Displays information about the VDS-TC configuration, including status, version, average CPU utilization, and memory usage for the cluster, cache engines, and the management server, where applicable.
- **Memory Utilization:** Displays information about the memory utilization.
- **CPU Utilization:** Displays information about the CPU server utilization.
- **Storage:** Displays status information for the storage controllers. This tab is available only in VDS-TC Cluster configurations.

This chapter contains the following sections:

- Dashboard
- Hardware View
- Logical View
- Memory Utilization
- CPU Utilization
- Storage

Dashboard

To view an overall status of your Cisco VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **Dashboard**. The Dashboard window opens, displaying the default Dashboard Status window.

Figure 2-1 Dashboard Window–Appliance Configuration

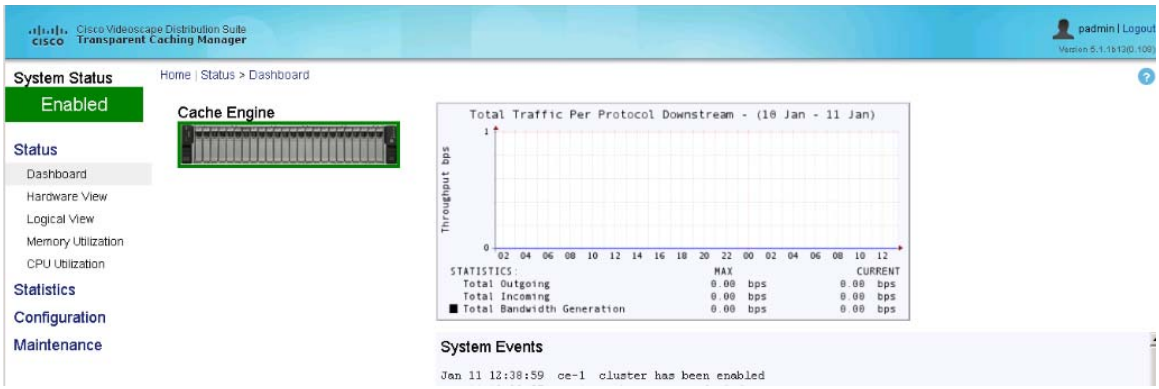
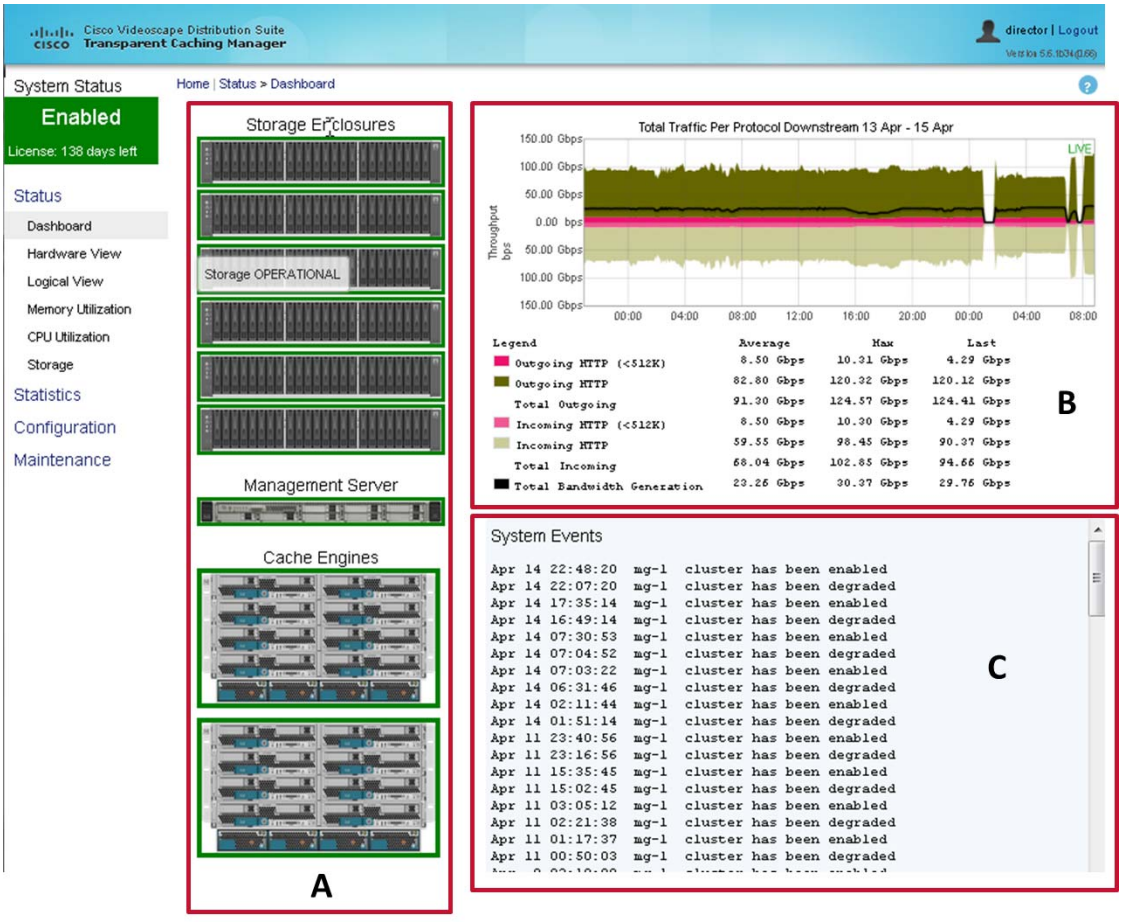


Figure 2-2 Dashboard Window–Cluster View



The Dashboard page enables you to monitor the following:

- **(A) Dashboard Hardware:** This section displays the platform figures and uses color to show the status of those figures.

- **(B) Total Traffic per Protocol Downstream Graph:** This section displays the total incoming, outgoing, and cache out traffic and the per protocol incoming and outgoing traffic for downstream traffic.
- **(C) System Events:** The system events section displays the last 100 events messages.

Hardware View

The Hardware view displays up to three different platforms (storage enclosures, cache engines, and management server) depending on the system configuration.

To view the hardware status of your Cisco VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **Hardware View**.

The Hardware View Status window opens and the color highlighting each component indicates its performance status as explained below.

Figure 2-3 Hardware View Window–Blade Server Cluster View

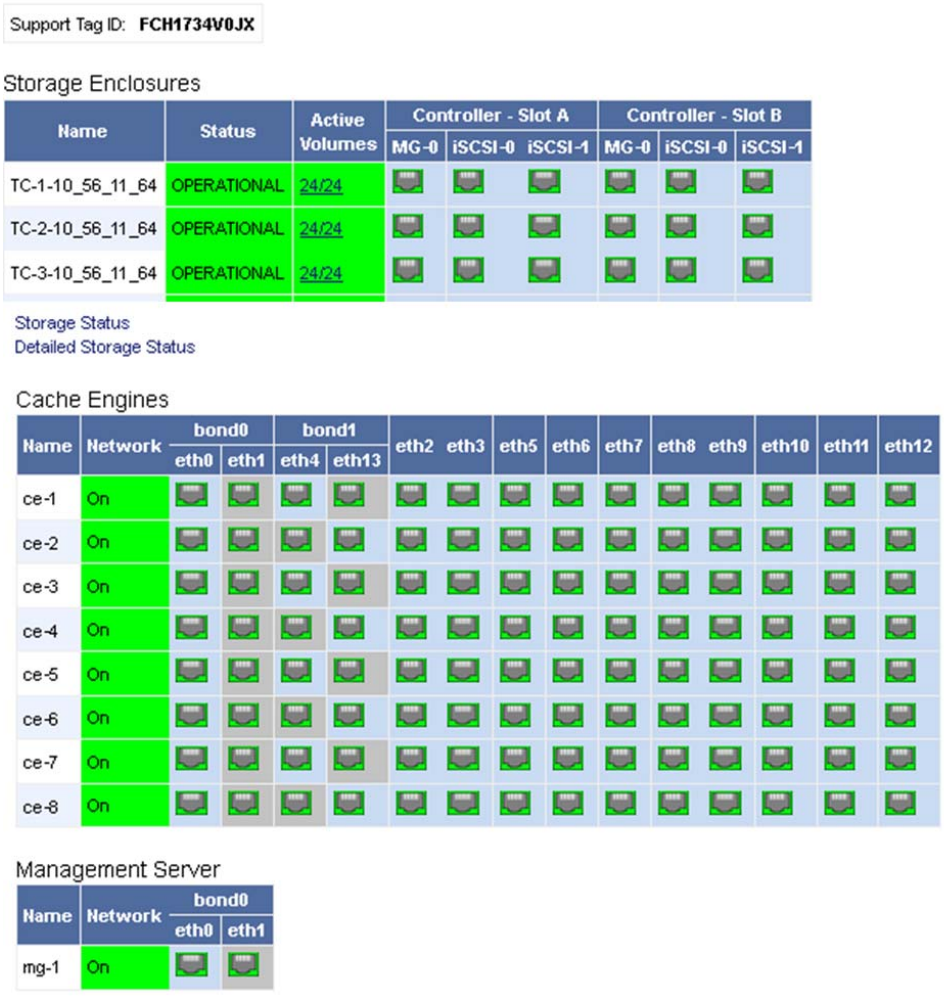
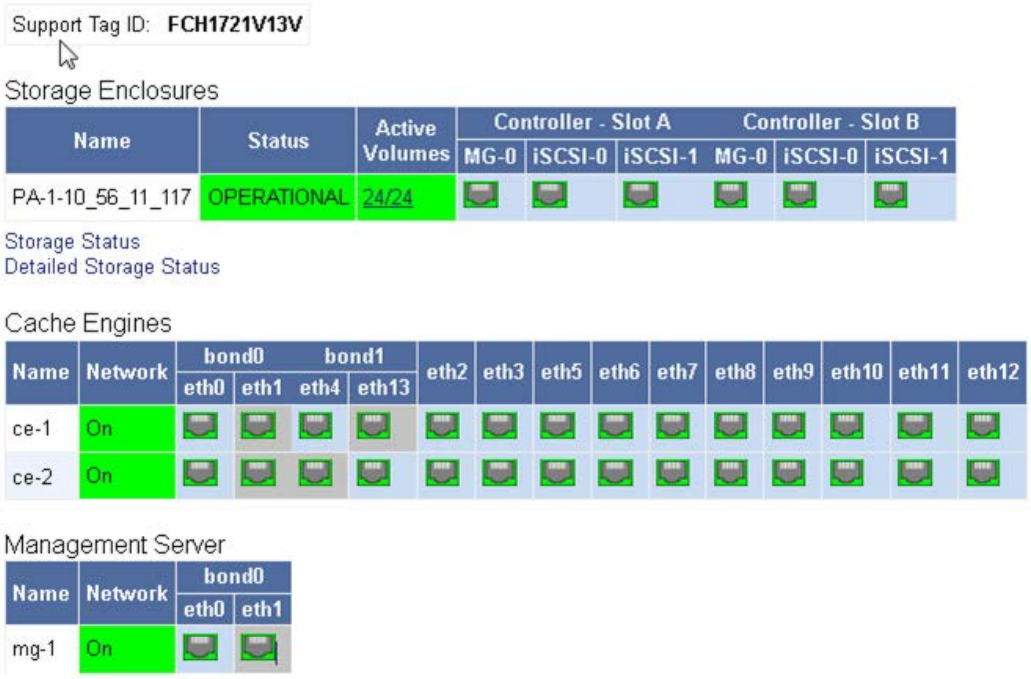


Figure 2-4 Hardware View Window–C-Series Cluster View



The Hardware View window displays the following information:

- **Support Tag ID:** This section displays the Management Server ID number, which is used as a reference whenever technical support is needed.
- **Storage Enclosures:** Table 2-1describes the information that is displayed in the Storage Enclosures section.
- **Storage Status:** This link, which is located below the Storage Enclosures area, allows you to view a brief summary of the storage status and operational information taken from the controllers.
- **Detailed Storage Status:** This link, which is located below the Storage Enclosures area, allows you to view the detailed status of each storage device. It also displays the operational state of the controllers.
- **Cache Engines:** Table 2-2 describes the information that is displayed in the Cache Engines section.
- **Management Server:** Table 2-3 describes the information that is displayed in the Management Server section.

Table 2-1 Storage Enclosures Information

Field	Description
Name	Displays the ID designation.
Status	The Status indicator monitors the storage status. Using colors, this indicator shows the status of the storages. • Green indicates an operational status • Red indicates a fault status.
Active Volumes	Displays the active storage volume per storage enclosure. Click these links to display the Volume Usage window.
Controller Slot A and Controller Slot B	Displays the following icons, detailing if the controller ports are active or inactive. **Note** Hover over an icon to display a tool tip that displays the link status. • Green indicates an active port. • Red indicates an inactive port.

Table 2-2 Cache Engines Information

Field	Description
Name	Displays the ID designation.

Table 2-2 Cache Engines Information (continued)

Field	Description
Network	This field monitors the network connectivity status between the management server and the cache engine. Using colors, this indicator shows the status of the network.
Interfaces	When using bonding, the background color of the port icon informs the user whether the port is in Standby or Active mode. iSCSI networks use bonding when network redundancy is configured. • Active Mode: Blue background • Standby Mode: Gray background The following icons indicate whether the interface ports are active: • Green indicates an active port. • Red indicates an inactive port. **Note** By hovering over an icon, a tool tip is displayed that describes the link status. **Note** Clicking an icon opens a link to the Interface graph (including VLAN, if available).

Table 2-3 Management Server Information

Field	Description
Name	Displays the ID designation.

Table 2-3 Management Server Information (continued)

Field	Description
Network	The Status indicator monitors the network status. Using colors, this indicator shows the status of the network.
Interfaces	When using bonding, the background color of the port icon informs the user whether the port is in Standby or Active mode. Management networks use bonding when network redundancy is configured. • Active Mode: Blue background • Standby Mode: Gray background The following icons indicate if the interface ports are active or not. • Green indicates an active port. • Red indicates an inactive port. **Note** By hovering over an icon, a tool tip is displayed that describes the link status. **Note** Clicking an icon opens a link to the Interface graph (including VLAN, if available).

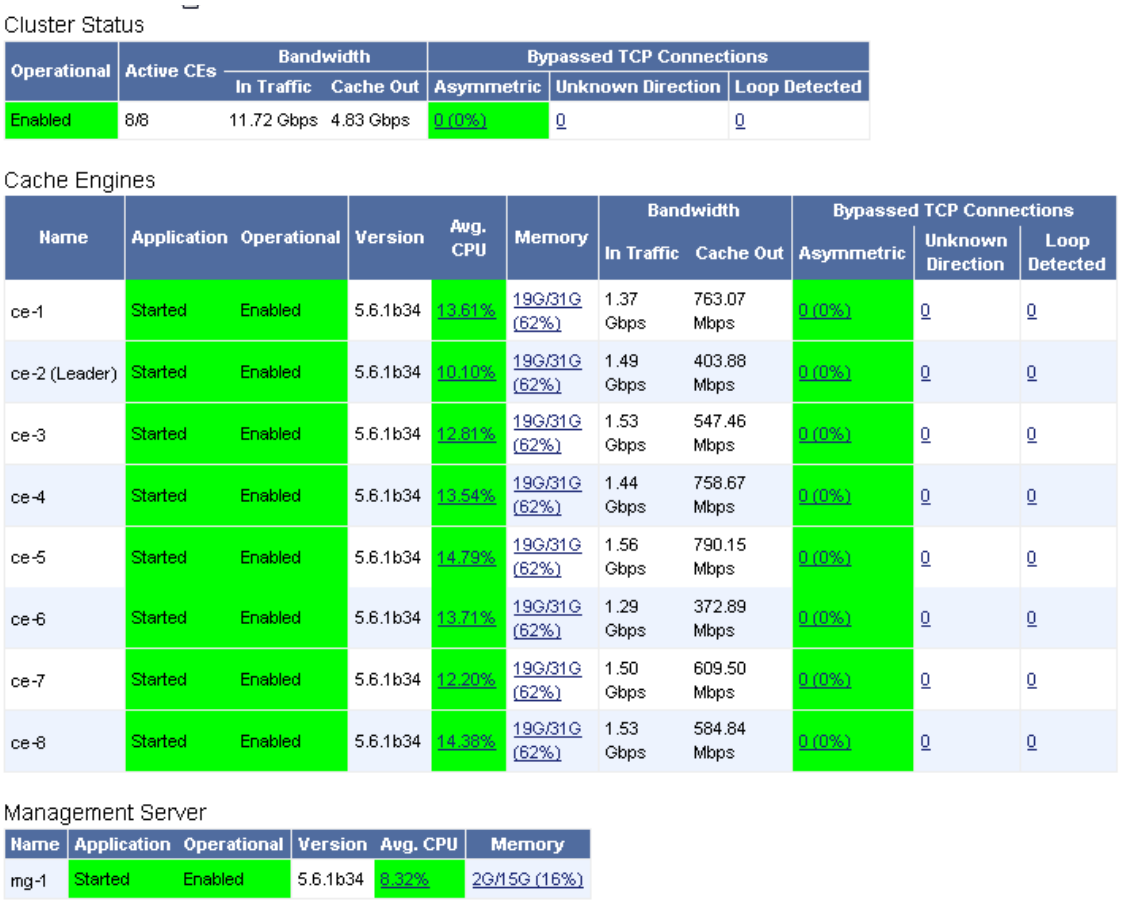
Logical View

To open the Logical View window of your VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **Logical View**.

From the Logical View window you can monitor the following information:

- **Cluster Status:** Displays the aggregate status of all cache engines in the cluster.
- **Cache Engines:** Displays the individual status of each of the cache engines including information about the traffic, memory, and CPU.
- **Management Server:** Displays status information about the application, operational, and performance status of the Management Server.

Figure 2-5 Logical View Window–Cluster View



Cluster Status

Operational	Active CEs	Bandwidth		Bypassed TCP Connections		
		In Traffic	Cache Out	Asymmetric	Unknown Direction	Loop Detected
Enabled	8/8	11.72 Gbps	4.83 Gbps	0 (0%)	0	0

Cache Engines

Name	Application	Operational	Version	Avg. CPU	Memory	Bandwidth		Bypassed TCP Connections		
						In Traffic	Cache Out	Asymmetric	Unknown Direction	Loop Detected
ce-1	Started	Enabled	5.6.1b34	13.61%	19G/31G (62%)	1.37 Gbps	763.07 Mbps	0 (0%)	0	0
ce-2 (Leader)	Started	Enabled	5.6.1b34	10.10%	19G/31G (62%)	1.49 Gbps	403.88 Mbps	0 (0%)	0	0
ce-3	Started	Enabled	5.6.1b34	12.81%	19G/31G (62%)	1.53 Gbps	547.46 Mbps	0 (0%)	0	0
ce-4	Started	Enabled	5.6.1b34	13.54%	19G/31G (62%)	1.44 Gbps	758.67 Mbps	0 (0%)	0	0
ce-5	Started	Enabled	5.6.1b34	14.79%	19G/31G (62%)	1.56 Gbps	790.15 Mbps	0 (0%)	0	0
ce-6	Started	Enabled	5.6.1b34	13.71%	19G/31G (62%)	1.29 Gbps	372.89 Mbps	0 (0%)	0	0
ce-7	Started	Enabled	5.6.1b34	12.20%	19G/31G (62%)	1.50 Gbps	609.50 Mbps	0 (0%)	0	0
ce-8	Started	Enabled	5.6.1b34	14.38%	19G/31G (62%)	1.53 Gbps	584.84 Mbps	0 (0%)	0	0

Management Server

Name	Application	Operational	Version	Avg. CPU	Memory
mg-1	Started	Enabled	5.6.1b34	8.32%	2G/15G (16%)

Cluster Status

Table 2-4 describes the information that is available in the Cluster Status section of the Logical View window.

Table 2-4 Cluster Status Information

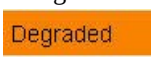
Column	Description
Operational	The status indicator monitors whether the cache engines are operational or not. • Green indicates that all the Cache Engines in the Cluster are up and running and that the Cache Engines are operational. • Yellow indicates R-Degraded (redundancy degrading), which indicates that the redundant server is not “up”. **Note** This status is valid only when N+1 feature is configured. • Orange indicates a degraded cluster. If less then “N” cache engines are active or, if one or more of the controllers are down, the status is downgraded to a degraded status.  • Red indicates that all Cache Engines are down.
Active CEs	This displays the number of active cache engines over the total number of cache engines.
Standby Cache Engines	This displays the hot standby servers over the total number of standby servers (in N+1, it is always 1). This status is valid only when the N+1 is configured.

Table 2-4 Cluster Status Information

Column	Description
Bandwidth	Displays the In Traffic and Cache Out traffic in bits per seconds (bps).
Bypassed TCP Connections	Displays the Asymmetric, Unknown Direction, and Loop Detected connections. These connections are forwarded and cannot be cached. • **Asymmetric:** Only one direction of a connection is transferred to the system. • **Unknown Direction Connections:** Connection from client to server where the server is in the upstream. • **Loop Detected:** The same packet is received from Tx and Rx. By clicking the links, the TCP Connections page is displayed.

Cache Engines

Table 2-5 describes the information that is available in the Cache Engines section of the Logical View window.

Table 2-5 Cache Engines Information

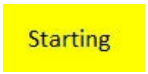
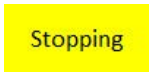
Column	Description
Name	Displays the ID of the Cache Engines.
Application	The Status indicator monitors the application status. Using colors, this indicator shows the status of the application. • Yellow can indicate three different status: Starting, Stopping, or Stopped. Check the status that is displayed.   • Green indicates the application process has started. • Gray indicates the application process is not applicable (N/A). • Red indicates the application process is unavailable.

Table 2-5 Cache Engines Information (continued)

Column	Description
Operational	The Operation status indicator monitors the operational status. Using colors, this indicator shows the status of the system. • Green indicates that the system is enabled. • Light Green indicates that the cache engine is in Hot Standby mode. • Red indicates that the system is disabled. • Gray indicates that the system is not available.
Standby	The Standby status it is available on n+1 only. • Green indicates the cache engine in active mode. • Light Green indicates n+1 is in Standby mode. • Yellow indicates when the operational status is disabled or when the application status has not “started”.
Version	Displays the version.
Average CPU	Displays the average of all CPU core usage of a server measured in percentage. By clicking the link, the CPU Utilization page is displayed.
Memory	Displays the average memory usage measured in percentage. By clicking the link, the Memory Utilization page is displayed.

Table 2-5 Cache Engines Information (continued)

Column	Description
Bandwidth	Displays the In Traffic and Cache Out traffic in bits per seconds (bps).
Bypassed TCP Connections	Displays the Asymmetric, Unknown Direction, and Loop Detected connections. These connections are forwarded and cannot be cached. • **Asymmetric:** Only one direction of a connection is transferred to the system. • **Unknown Direction:** A connection from client to server where the server is in the upstream. • **Loop Detected:** The same packet is received from Tx and Rx. By clicking the links, the TCP Connections page is displayed.

Management Server

Table 2-6 describes the information that is available in the Management Server section of the Logical View window.

Table 2-6 Management Server Information

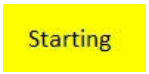
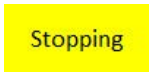
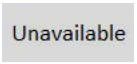
Column	Description
Name	Displays the ID of the Management Server.
Application	The application status indicator monitors the application status. Using colors, this indicator shows the status of the application. • Yellow can indicate three different status: Starting, Stopping, or Stopped. Check the status that is displayed.   • Green indicates the application process has started. • Gray indicates the process is unavailable. 
Operational	The Operation status indicator monitors the operational status. Using colors, this indicator shows the status of the system. • Green indicates that the system is enabled. • Red indicates that the system is disabled. • Gray indicates that the system is not available.
Version	Displays the version.

Table 2-6 Management Server Information (continued)

Column	Description
Average CPU	Displays the average CPU usage measured in percentage. By clicking the link, the CPU Utilization page is displayed.
Memory	Displays the average memory usage measured in percentage. By clicking the link, the Memory Utilization page is displayed.

Memory Utilization

To open the Memory Utilization graph of your VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **Memory Utilization**.

The Memory Utilization graph displays information for all of the management servers or cache engines. The All tab displays the Memory Utilization across the management server and all cache engines (where applicable). The Memory Utilization page also has tabs that display the memory utilization of each individual component.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 2-6 Memory Utilization Window–All

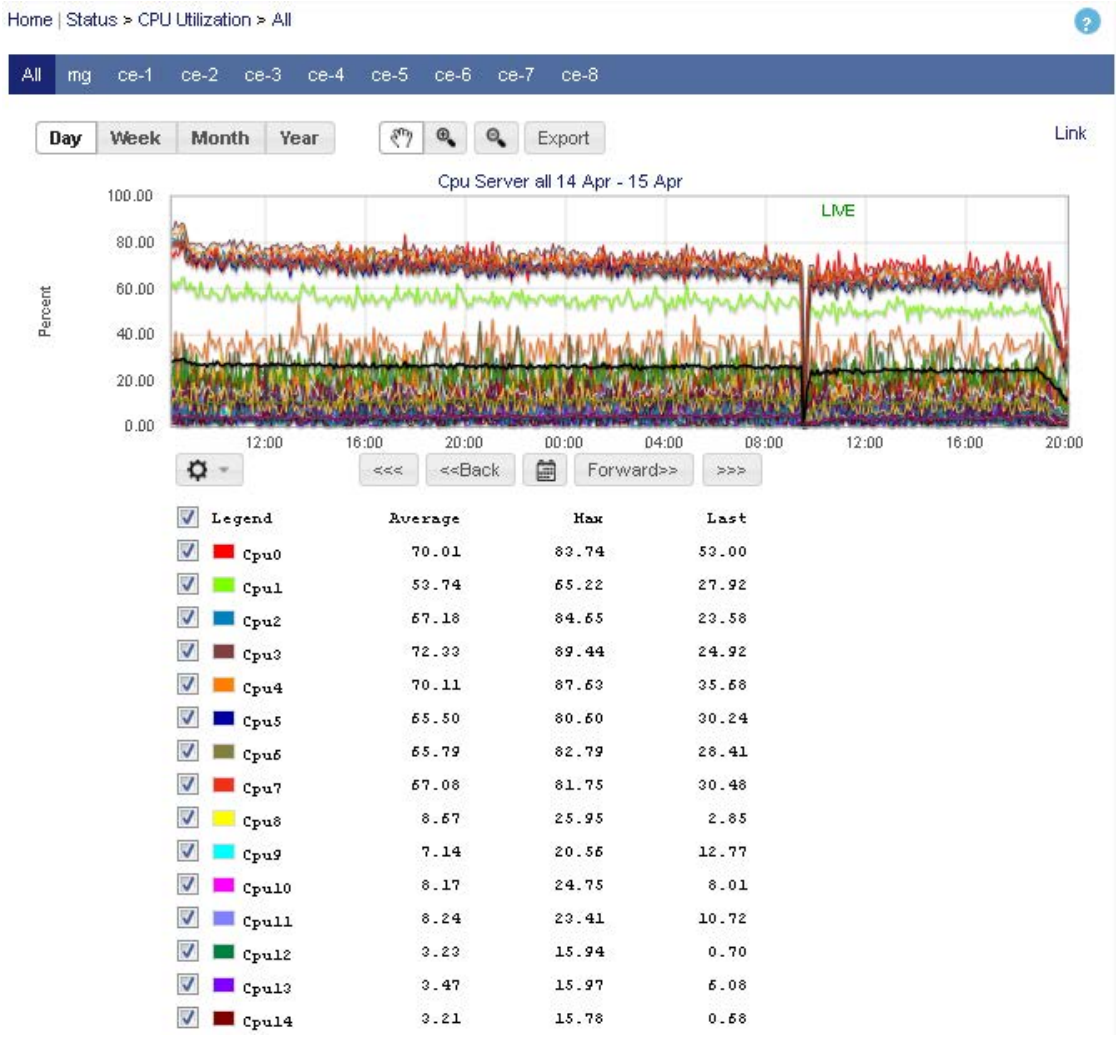
CPU Utilization

To open the CPU Utilization graph of your VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **CPU Utilization**.

The CPU Utilization graph displays information for all of the management servers or cache engines. The All tab displays the CPU Utilization across the management server and all cache engines (where applicable). The CPU Utilization page also has tabs that display the CPU utilization of each individual component.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 2-7 CPU Utilization Window–All



Storage

To open the Storage Status window of your VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window under the Status menu, choose **Storage**.

Note The Storage menu is available only in a VDS TC Cluster installation.

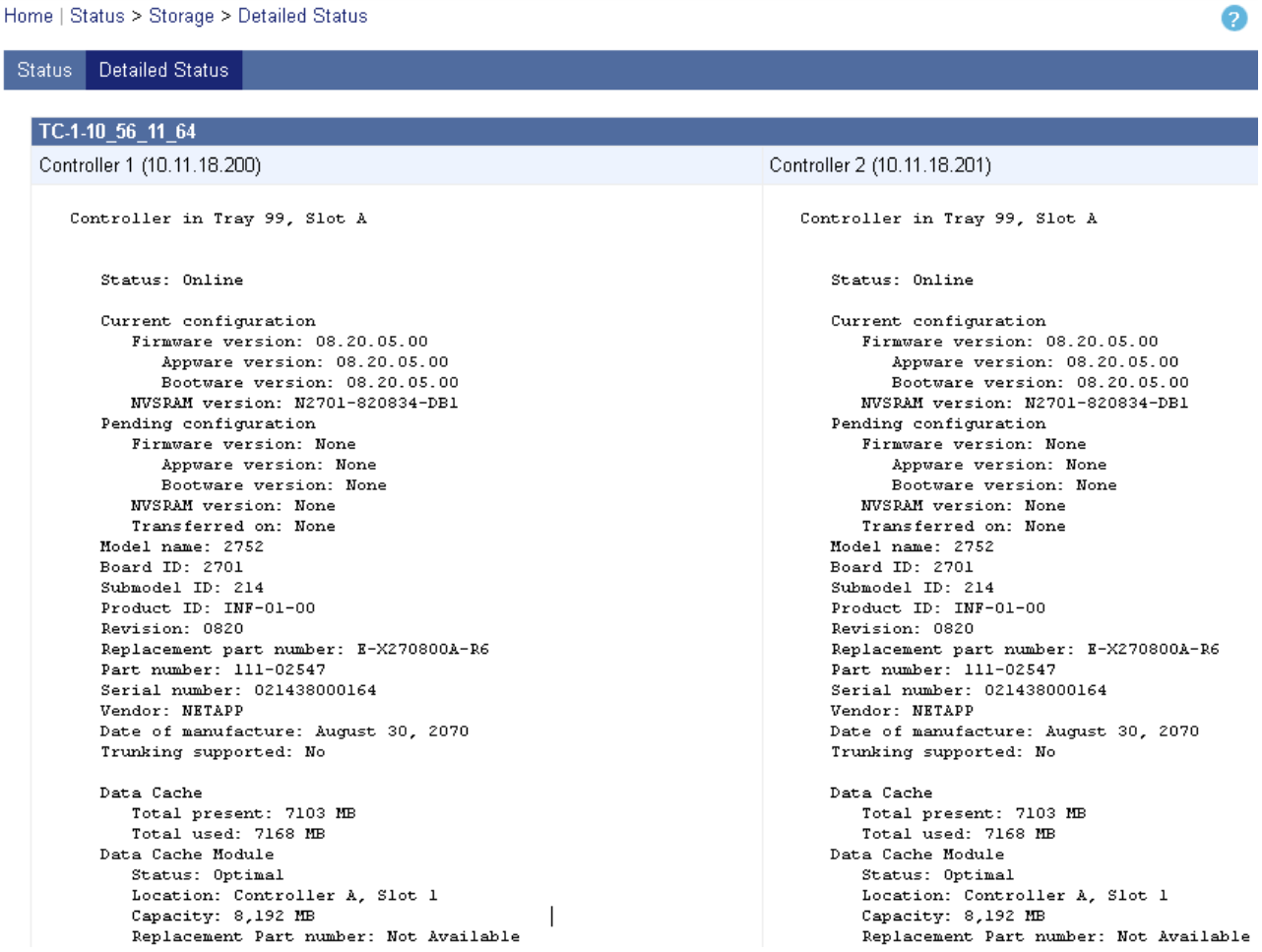
The Storage window displays the status of the storage devices per controller.The storage window is divided into two tabs:

- **Status:** The Status tab displays a synopsis of the storage status.
- **Detailed Status:** The Detailed Status tab displays a detailed expanded view of the storage status.

Figure 2-8 Storage Window–Status Tab

To view the detailed status information of the storage devices, including the operational state of each controller, click the **Detailed Status** tab.

Figure 2-9 Storage Window–Detailed Status Tab



Statistics Menu

This chapter describes how to view statistical information regarding your platform, focusing on the statistical details.

The Statistics menu contains the following choices:

- **Interfaces:** Displays interface information in graph format.
- **TCP Connections:** Displays information about the incoming and outgoing traffic of the cache server and additional operational parameters.
- **Bandwidth:** Displays graphs of total incoming and outgoing traffic, and bandwidth generation distributed by protocols.
- **HTTP Services:** The HTTP Services window displays statistics on the total HTTP traffic distributed by service.
- **Cache Content:** The Cache Content window displays general hash information by protocol, such as cache size and the number of cached files.
- **Storage:** Displays storage information and storage status.
- **QoE**: Displays clear vs. cache data statistics for HTTP and P2P traffic as well as statistics IP addresses served by the VDS TC system.

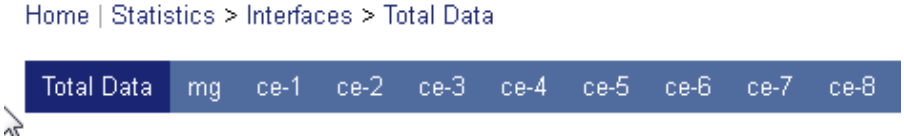
This chapter contains the following sections:

Interfaces

To display interface information in graph format, from the Statistics menu, choose **Interfaces**. The Interfaces > Total Data window opens, displaying the Total Data graph.

The Interfaces window also contains tabs to view interface information for the Management Server and all of the cache engines, including physical interface, bond interface, and VLAN interfaces details as described in eth2 and eth3 information.

Figure 3-1 Interface Tabs



Total Data

The Total Data graph displays an aggregated graph that includes all of the data traffic collected from all of the cache engines.

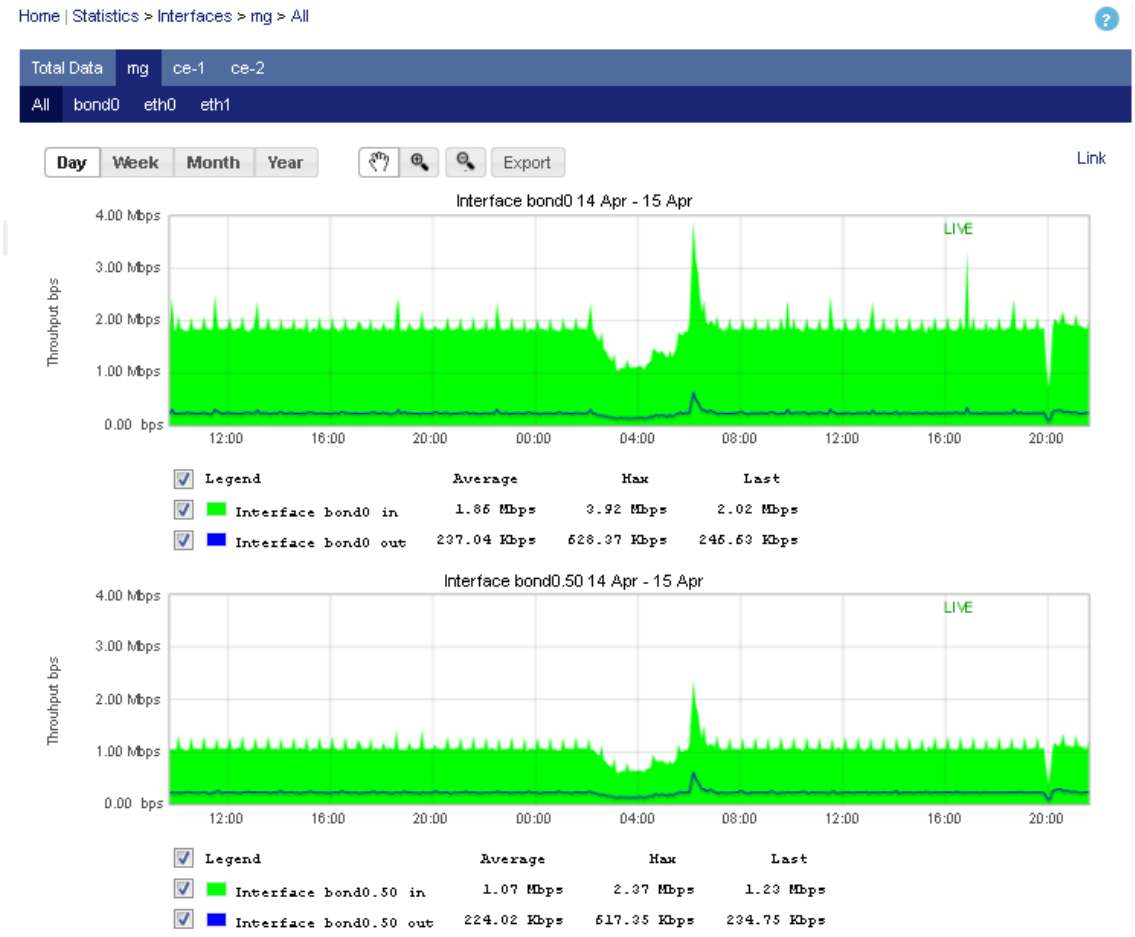
Figure 3-2 Interfaces–Total Data

Management Server (mg)

The mg tab displays information for all of the bond interfaces and the physical interfaces in graphs. The mg tab contains the following subtabs:

- **All:** Displays all the virtual and physical interfaces on the management server. This is the default subtab that displays when you click the mg tab.
- **bond:** This is a virtual interface which is assigned to a group of physical interfaces. This allows you to have link redundancy between the physical interfaces.
- **eth "x":** This is a physical (ethernet) interface.

Figure 3-3 Interfaces Window–mg Tab All



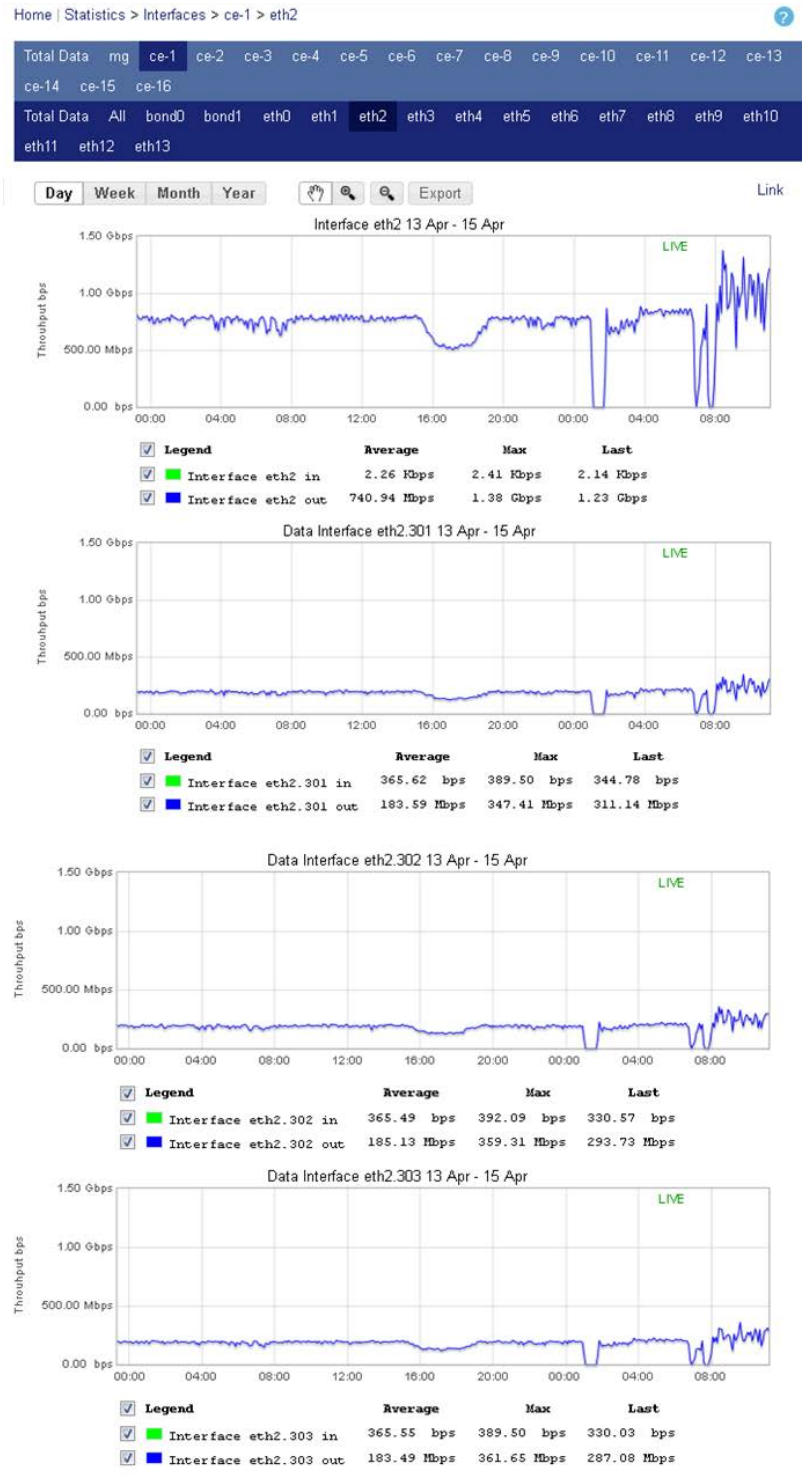
Cache Engine (ce “#”)

When you click the tab for one of the cache engines (for example ce-1), the following subtabs are available:

- **Total Data:** If you click one of the cache engine tabs, the total data subtab displays the total aggregated graph of the collected data traffic from the chosen cache engine. This is the default subtab that displays when you click a cache engine tab.
- **All:** Displays all the virtual and physical interfaces on the cache engine.
- **bond”#”:** This is the link redundancy of the Cache Server.

Figure 3-4 Interfaces–Cache Engine Tab Total Data

Figure 3-5 Interfaces–Cache Engine Tab eth 2 data



TCP Connections

To display statistics on TCP connections that pass through the VDS TC system, from the Statistics menu choose **TCP Connections**. The tabs available from the TCP Connections menu display the TCP Connections statistics of each one of the supported protocols.

The following tabs are available from the Statistics > TCP Connections menu:

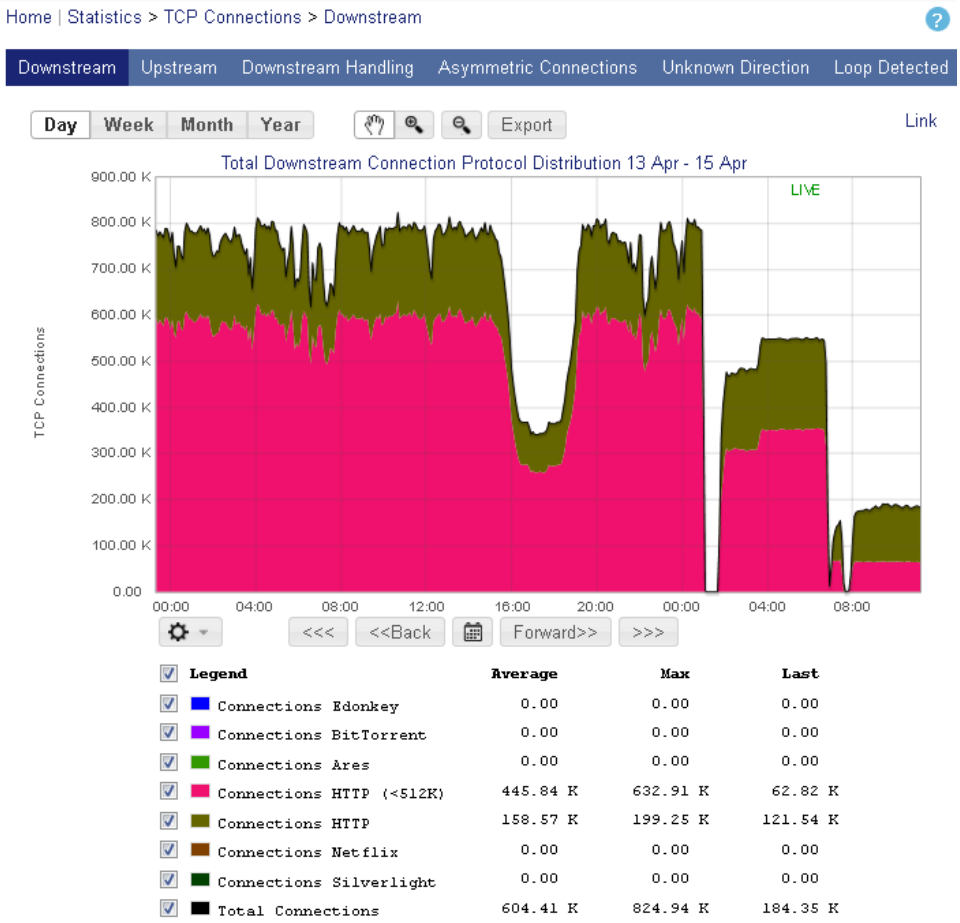
- **Downstream:** This tab displays the downstream distribution within the TCP connections. See the Downstream section.
- **Upstream:** This tab displays the upstream distribution within the TCP connections. See the Upstream section.
- **Downstream Handling:** This tab displays the downstream handling within the TCP connections. See the Downstream Handling section.
- **Asymmetric Connections:** This tab displays the number of asymmetric connections within the TCP connections. See the Asymmetric Connections section.
- **Unknown Direction:** This tab displays the number of unknown direction connections within the TCP connections. See the Unknown Direction section.
- **Loop Detected:** This tab displays the number of loop detected connections within the TCP connections. See the Loop Detected section.

Downstream

The Downstream tab displays the downstream distribution within the TCP connections.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-6 TCP Connections–Downstream Tab

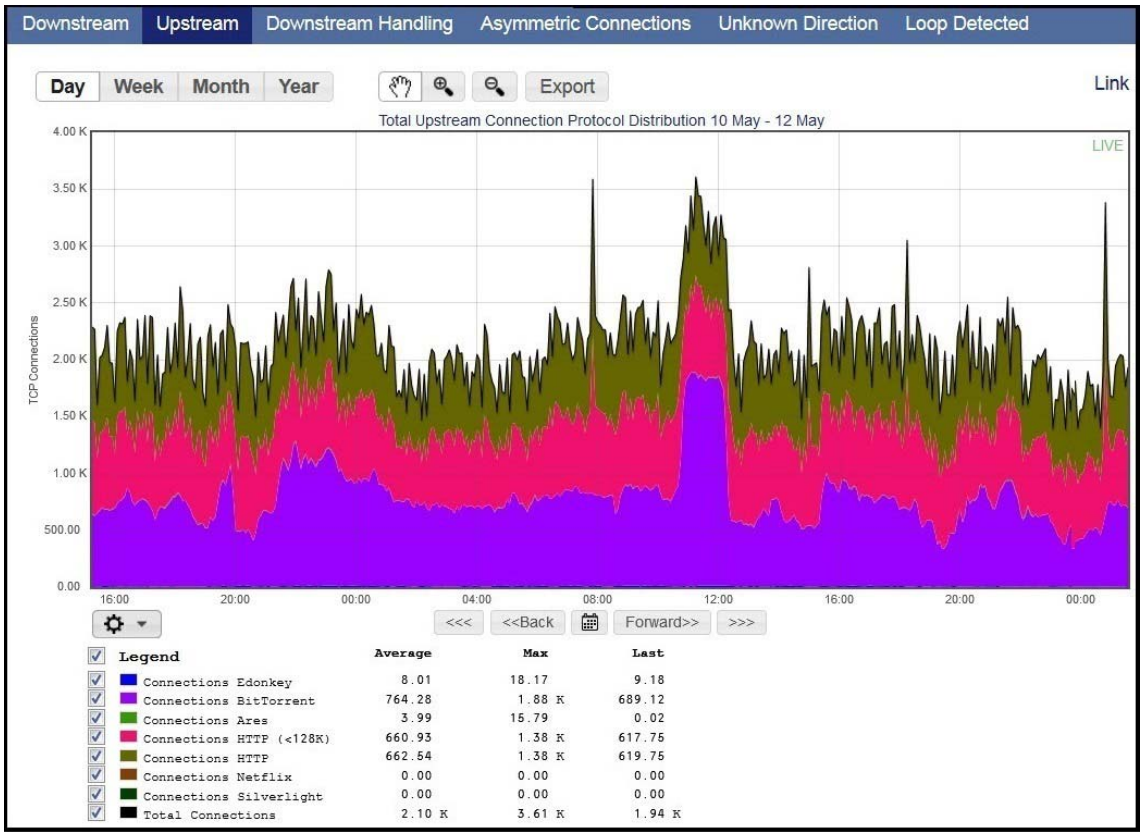


Upstream

The Upstream tab displays the concurrent TCP connections established from downstream to upstream. These connections will not be cached in.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-7 TCP Connections–Upstream Tab

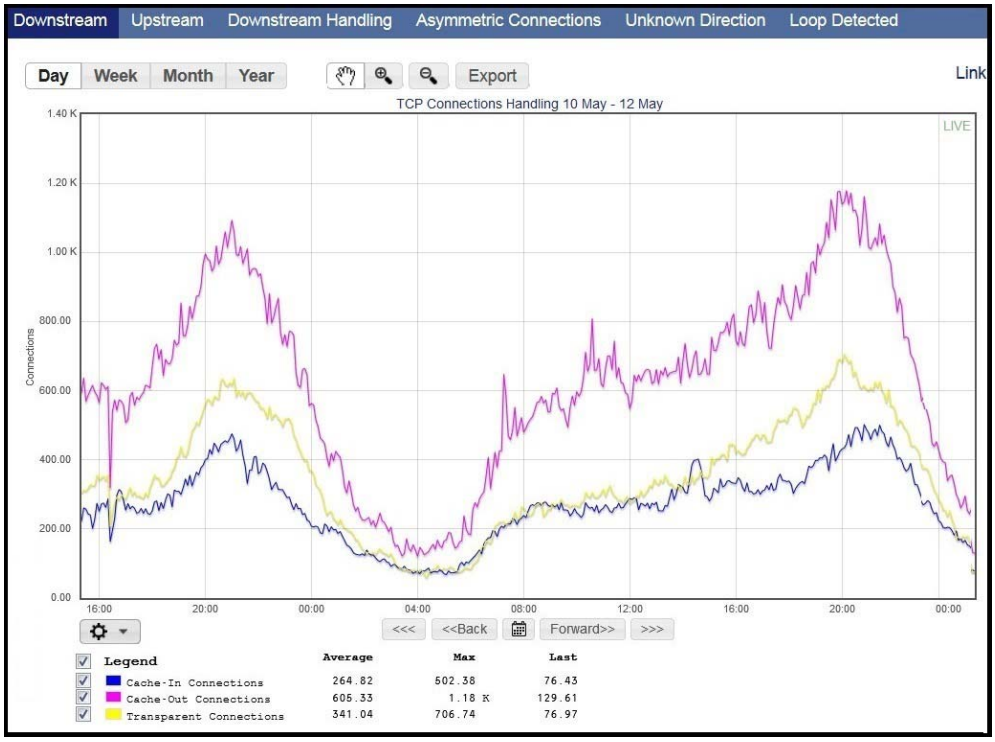


Downstream Handling

The Downstream Handling tab displays how the Cisco VDS TC Manager handles the downstream connections, whether the connection data is cache-in, cache-out, or transparency forwarded.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-8 TCP Connections–Downstream Handling Tab



Asymmetric Connections

The Asymmetric Connections tab displays the connections in which only one direction (Tx or Rx) is forwarded through a specific Cache Engine. These connections are bypassed through the system but can not be cached-in or cached-out.

The Asymmetric Connections tab contains the following subtabs:

- **All:** The All tab displays the total asymmetric TCP connections of all the cache engines. This is the default subtab that displays when you click the Asymmetric Connections tab.
- **ce "#":** This displays the total asymmetric TCP connections for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-9 TCP Connections–Asymmetric Connections Tab

Unknown Direction

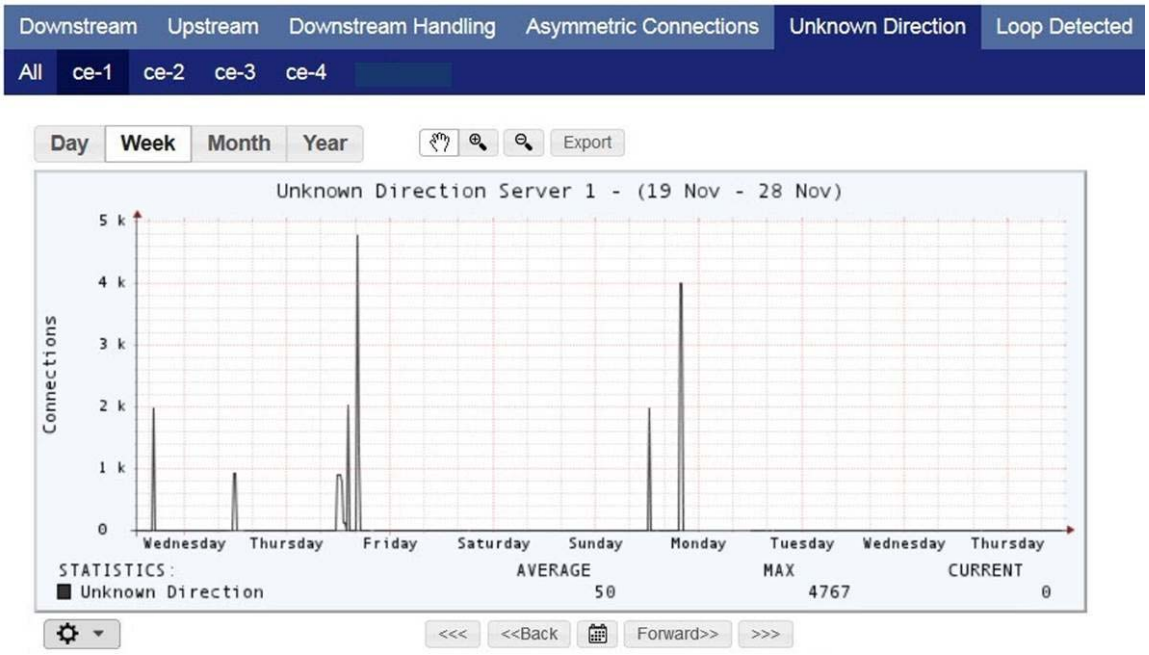
The Unknown Direction tab displays the connections established from the network (world) to the ISP subscribers. This can happen only in bounce mode, where the subscriber network is configured. These connections are bypassed through the system but cannot be cached-in or cached-out.

The Unknown Direction tab contains the following subtabs:

- **All:** The All tab displays the total number of unknown direction TCP connections of all the cache engines. This is the default subtab that displays when you click the Unknown Direction tab.
- **ce "#":** This displays the total unknown direction TCP connections for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-10 TCP Connections–Unknown Direction Tab



Loop Detected

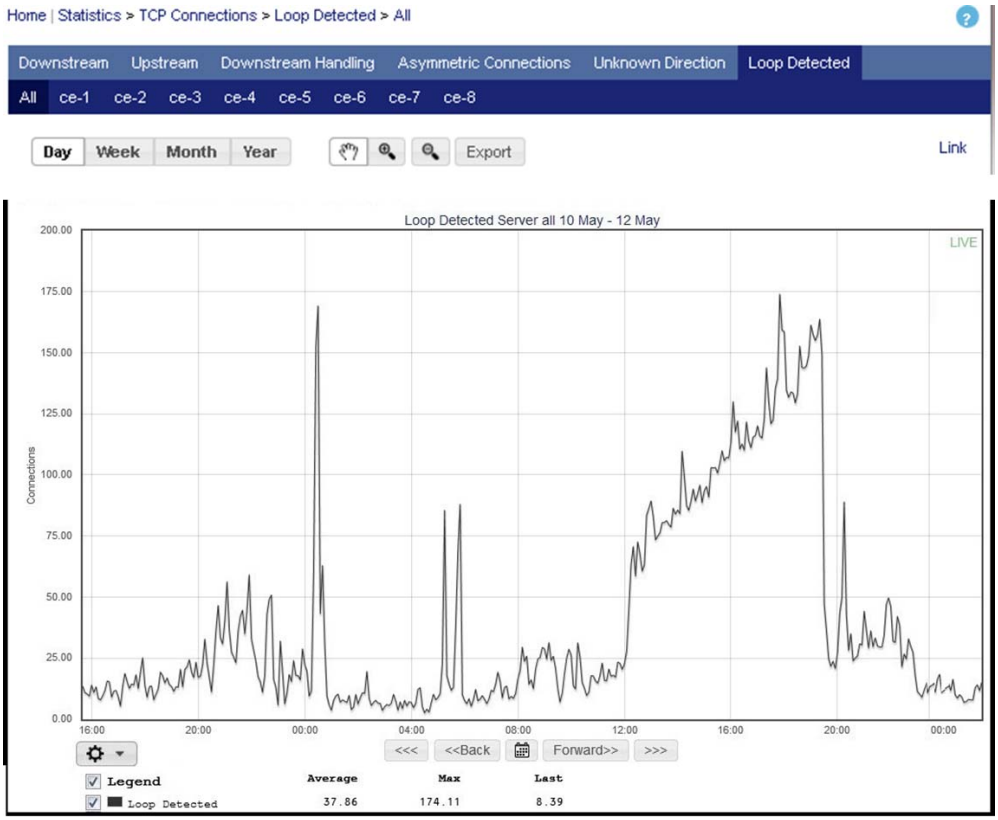
The Loop Detected tab displays the TCP connections for which their packets are duplicated and received on both Tx and Rx. These connections are bypassed through the system but cannot be cached-in or cached-out.

The Loop Detected tab contains the following subtabs:

- **All:** The All tab displays the total number of loop detected TCP connections of all the cache engines. This is the default subtab that displays when you click the Loop Detected tab.
- **ce "#":** This displays the total loop detected TCP connections for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-11 TCP Connections–Loop Detected Tab



Bandwidth

To display the bandwidth statistics of each of the supported protocols, from the Statistics menu, choose **Bandwidth**.

The following tabs are available from the Statistics > Bandwidth menu:

- **Total Downstream:** This tab displays the total outgoing and incoming downstream traffic in bits per second (bps). See the Total Downstream section.
- **In Downstream:** This tab displays the incoming downstream traffic in bps. See the In Downstream section.
- **Cache Out:** This tab displays the cache out outgoing traffic in bps. See the Cache Out section.
- **In-Out:** This tab displays the total incoming and outgoing cache traffic on the upstream/downstream in bps. See the In-Out section.
- **Bytes Hit Ratio:** This tab displays the cache out outgoing traffic as a percentage. See the Bytes Hit Ratio section.
- **Cache Productivity:** This tab displays the cache protocol productivity as a percentage. See the Cache Productivity section.
- **Percentile:** This tab displays the Cache Out graph of a month together with a 95% percentile value of the months sample values. See the Percentile section.

- **Total Upstream:** This tab displays the total outgoing and incoming upstream traffic in bps. See the Total Upstream section.
- **In Upstream:** This tab displays the incoming upstream traffic in bps. See the In Upstream section.

Total Downstream

The Total Downstream tab displays the total downstream incoming, outgoing, and cache out traffic together with the per protocol incoming and outgoing traffic. The incoming traffic is displayed in the negative values and the outgoing traffic with the positive values.

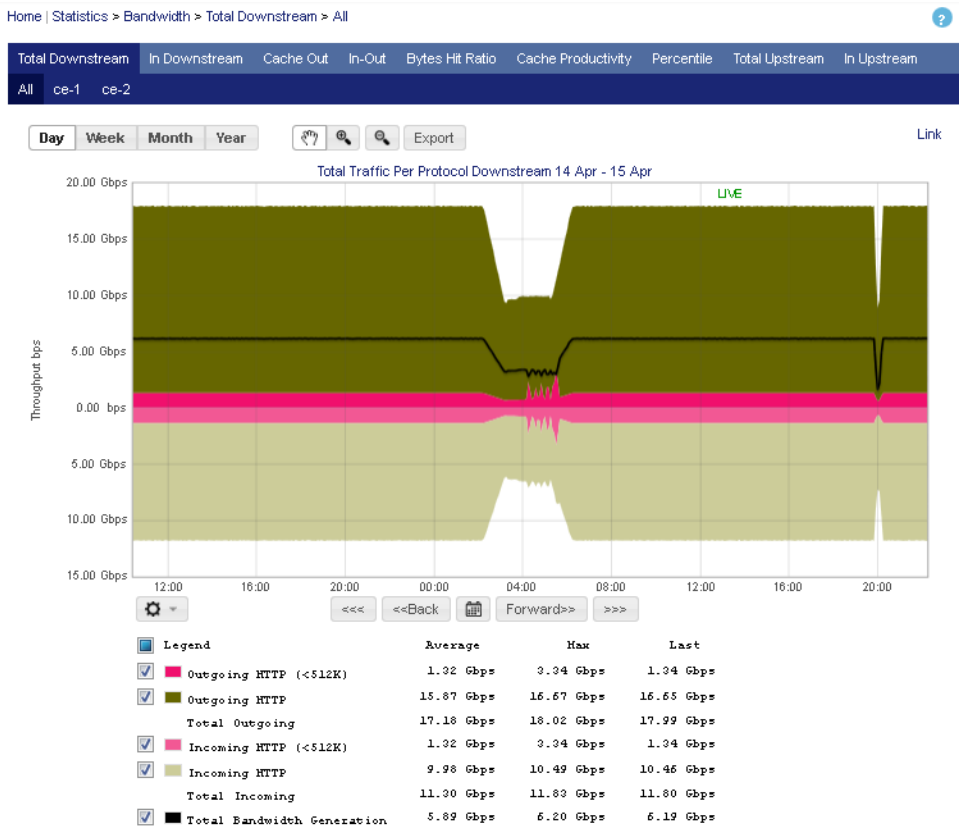
Only protocols that are above the minimum percentage are visible in the graph. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The Total Downstream tab contains the following subtabs:

- **All:** The All tab displays the total downstream traffic of all the cache engines. This is the default subtab that displays when you click the Total Downstream tab.
- **ce "#":** This displays the total downstream traffic for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-12 Bandwidth–Total Downstream Tab



In Downstream

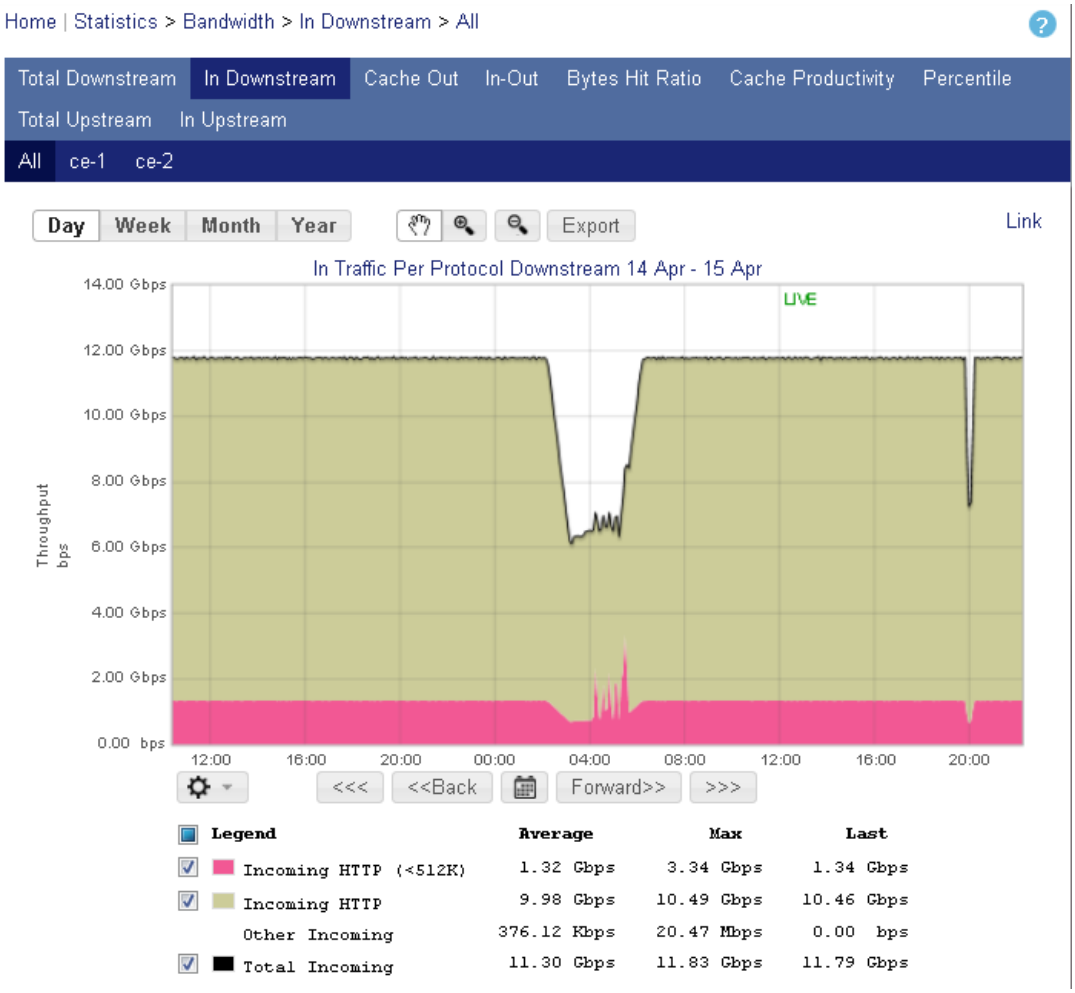
The In Downstream tab displays the total downstream incoming traffic, distributed by protocols. Only protocols that are above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The In Downstream tab contains the following subtabs:

- **All:** The All tab displays the total downstream incoming traffic of all the cache engines. This is the default subtab that displays when you click the In Downstream tab.
- **ce "#":** This displays the total downstream incoming traffic for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-13 Bandwidth–In Downstream



Cache Out

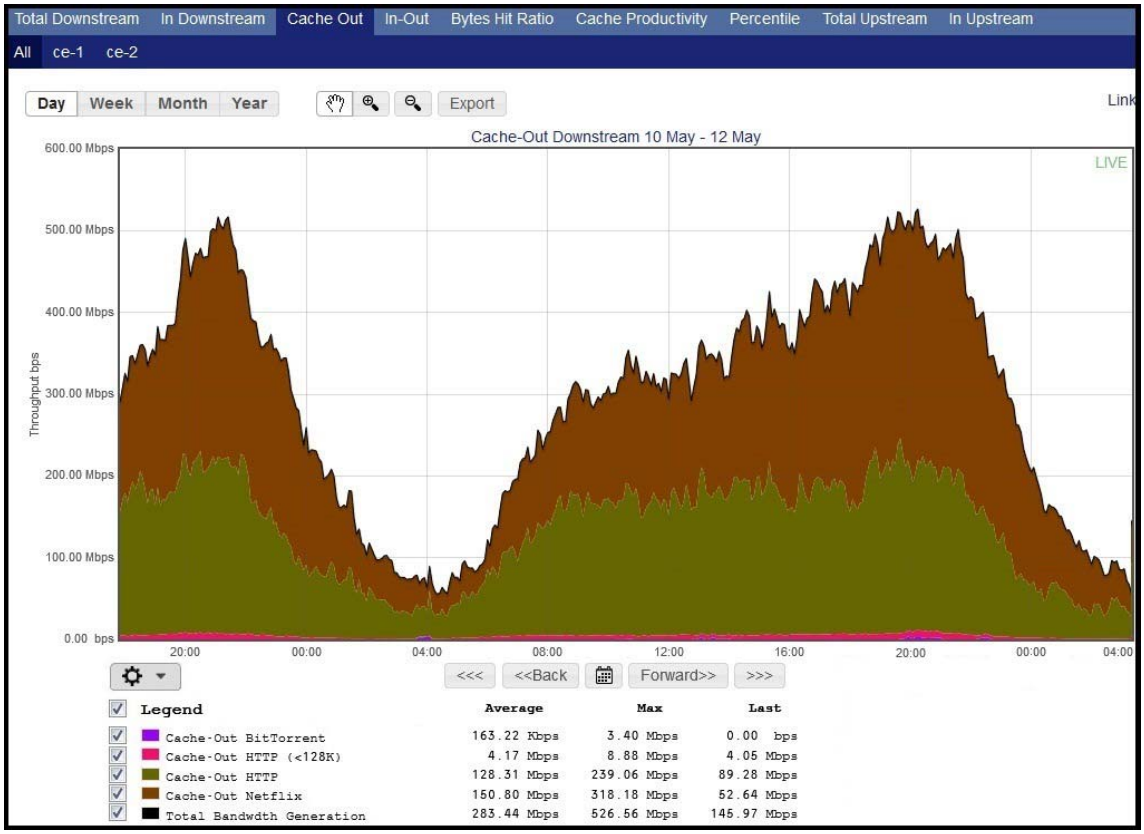
The Cache Out tab displays the total outgoing cache out traffic on the downstream, distributed by protocols. Only protocols that are above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The Cache Out tab contains the following subtabs:

- **All:** The All tab displays the total cache out traffic of all the cache engines. This is the default subtab that displays when you click the Cache Out tab.
- **ce "#":** This displays the total cache out traffic for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-14 Bandwidth–Cache Out



In-Out

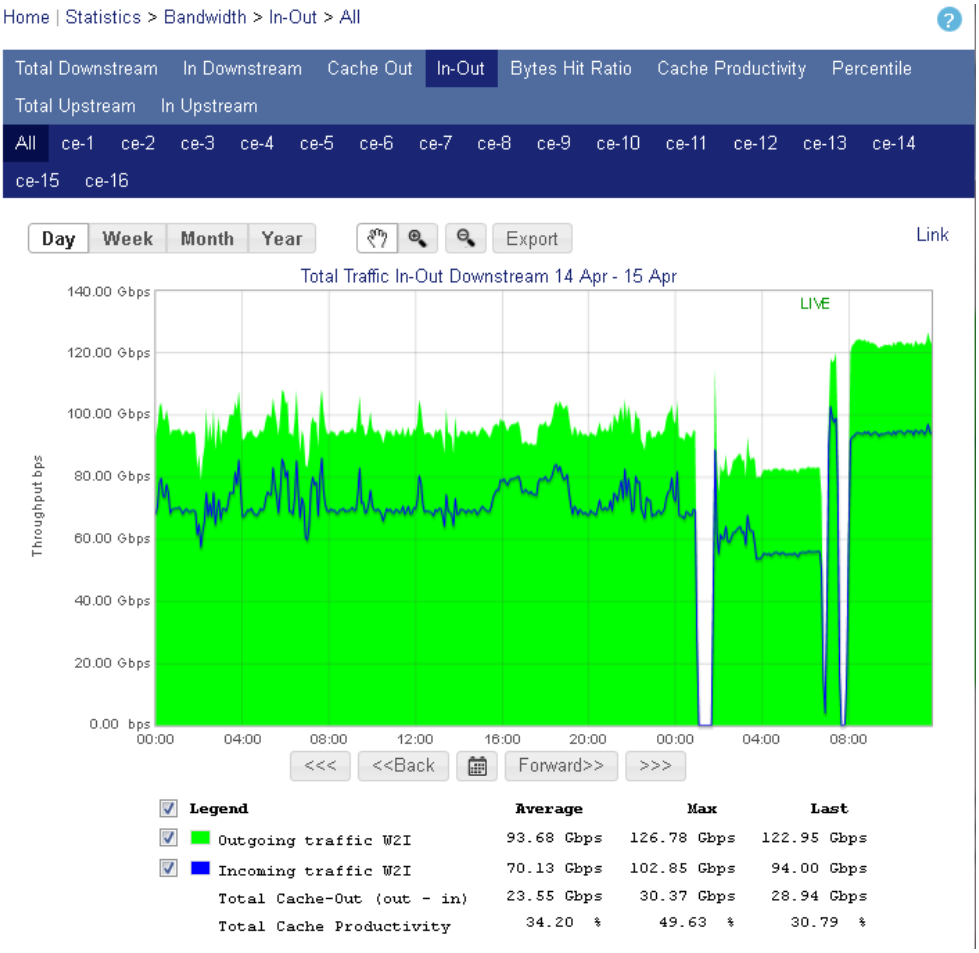
The In-Out tab displays the total incoming and outgoing cache traffic on the upstream/downstream, is distributed by protocols. Only protocols that are above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The In-Out tab contains the following subtabs:

- **All:** The All tab displays the total In-Out traffic for all of the cache engines.
- **ce "#":** This displays the In-Out traffic for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-15 Bandwidth–In-Out Tab



Bytes Hit Ratio

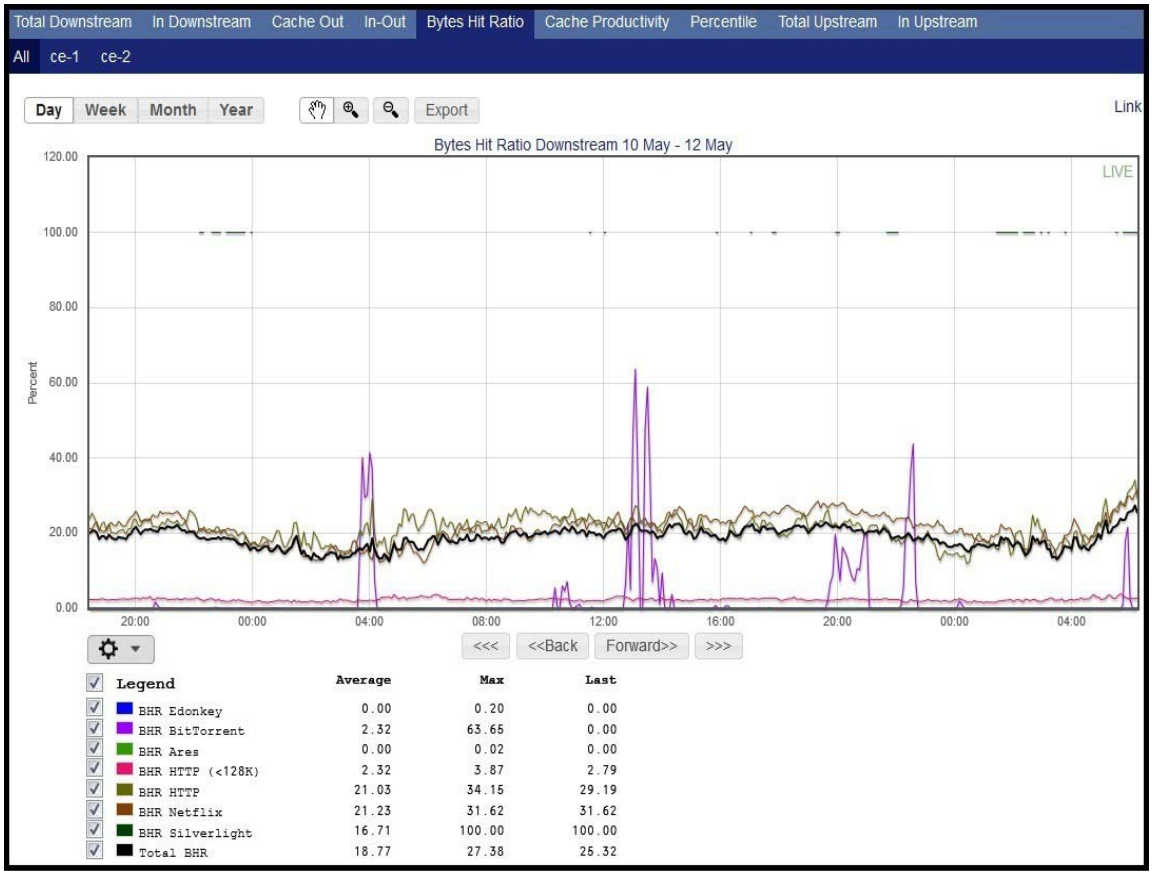
The Bytes Hit Ratio tab displays the Downstream Bytes Hit Ratio by dividing the downstream Cache Out by the total downstream outgoing traffic.

The Bytes Hit Ratio tab contains the following subtabs:

- **All:** The All tab displays the total downstream Bytes Hit Ratio of all the cache engines. This is the default subtab that displays when you click the Bytes Hit Ratio tab.
- **ce "#":** This displays the total downstream Bytes Hit Ratio for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-16 Bandwidth–Bytes Hit Ratio Tab

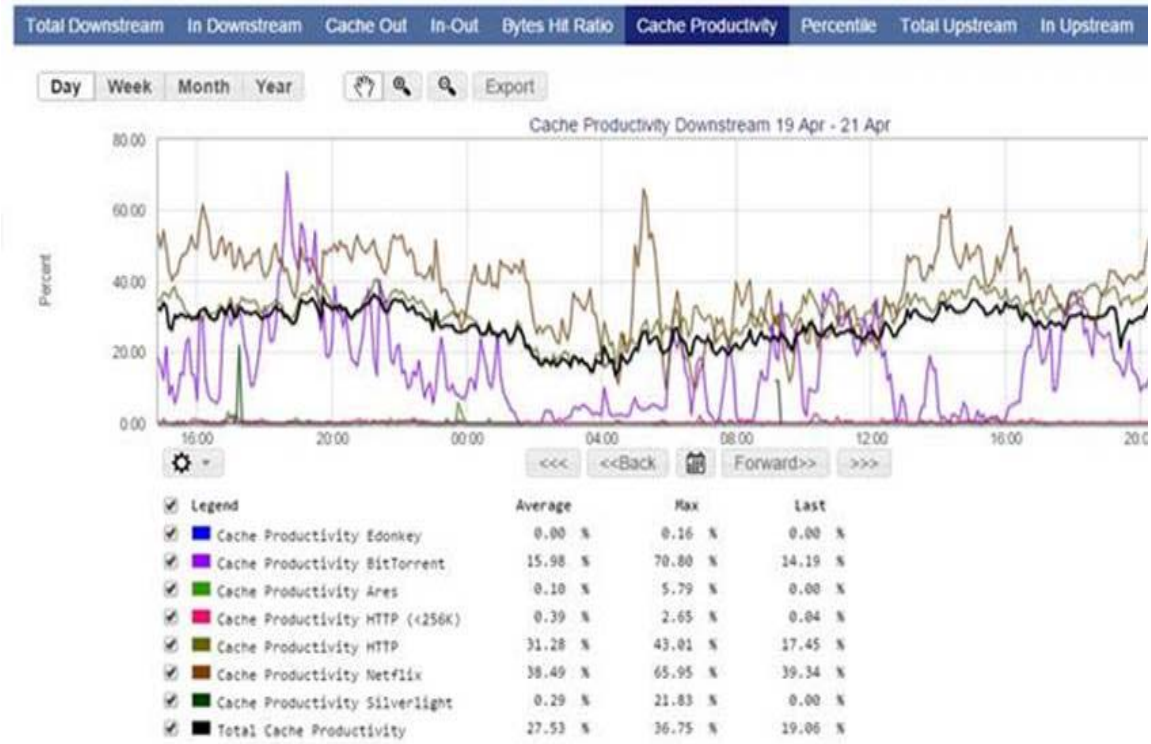


Cache Productivity

The Cache Productivity tab displays the Downstream Cache Productivity by dividing Cache Out traffic by Total Downstream Incoming traffic.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

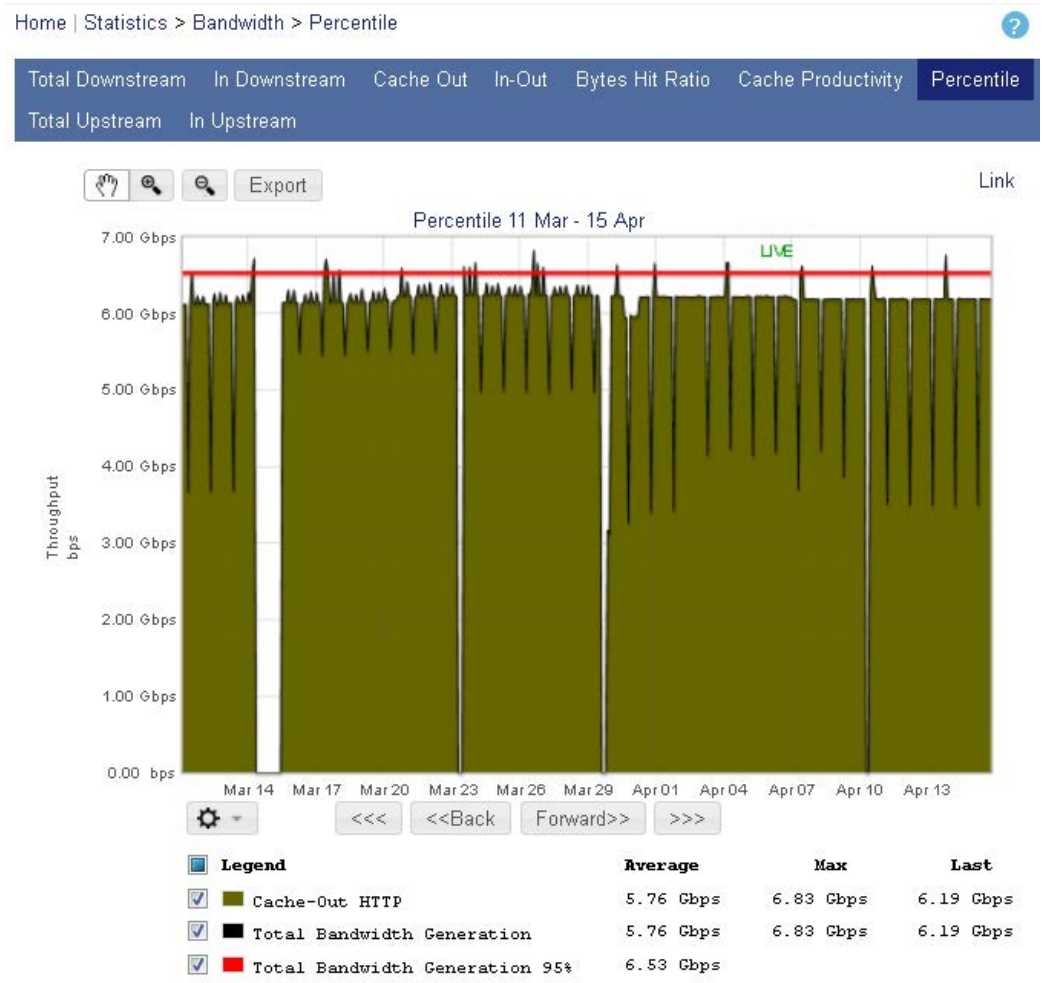
Figure 3-17 Bandwidth–Cache Productivity



Percentile

The Percentile tab displays the Cache Out graph of each month of the year from the beginning of the month until the end month or current date. The graph also displays another straight line that represents the 95% percentile samples value.

Figure 3-18 Bandwidth–Percentile Tab



Total Upstream

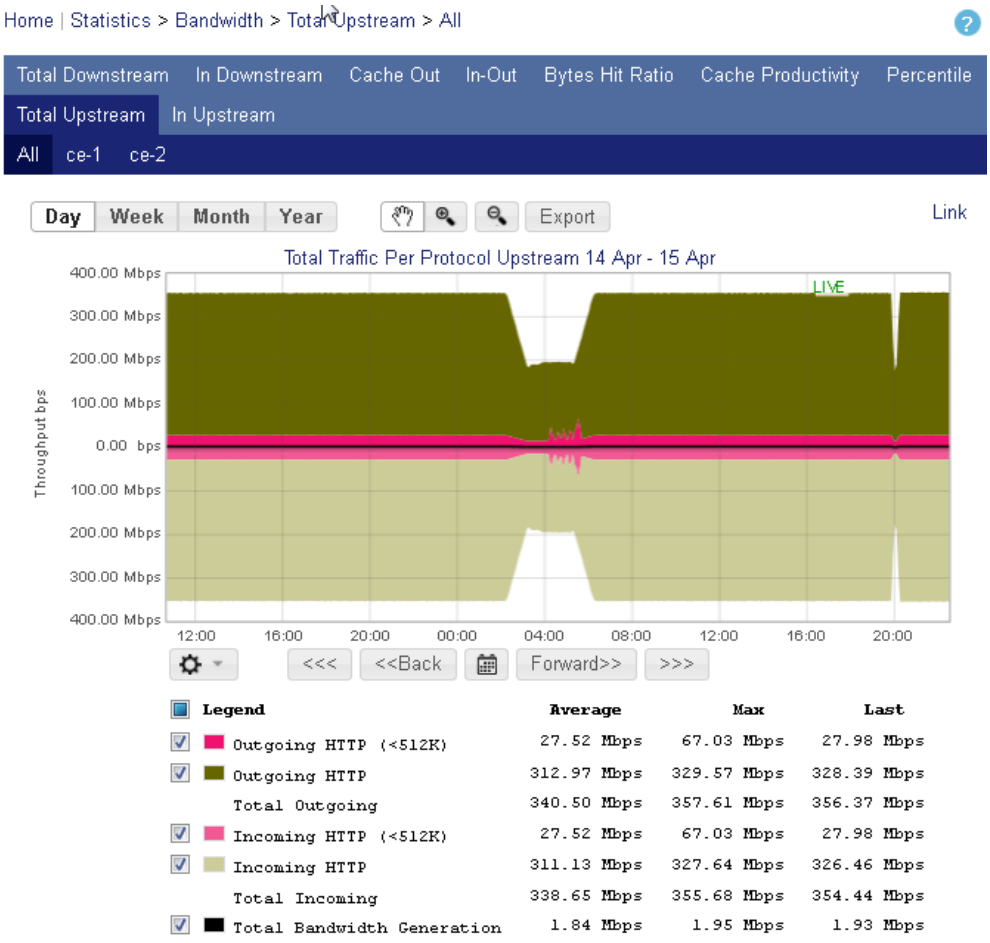
The Total Upstream tab displays the total upstream incoming and outgoing traffic together with the per protocol incoming and outgoing traffic. The incoming value is displayed in negative values and the outgoing value with positive values. Only protocols above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The Total Upstream tab contains the following subtabs:

- **All:** The All tab displays the total upstream protocol traffic distribution of all the cache engines. This is the default subtab that displays when you click the Total Upstream tab.
- **ce "#":** This displays each of the individual upstream protocol traffic distribution for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-19 Bandwidth–Total Upstream



In Upstream

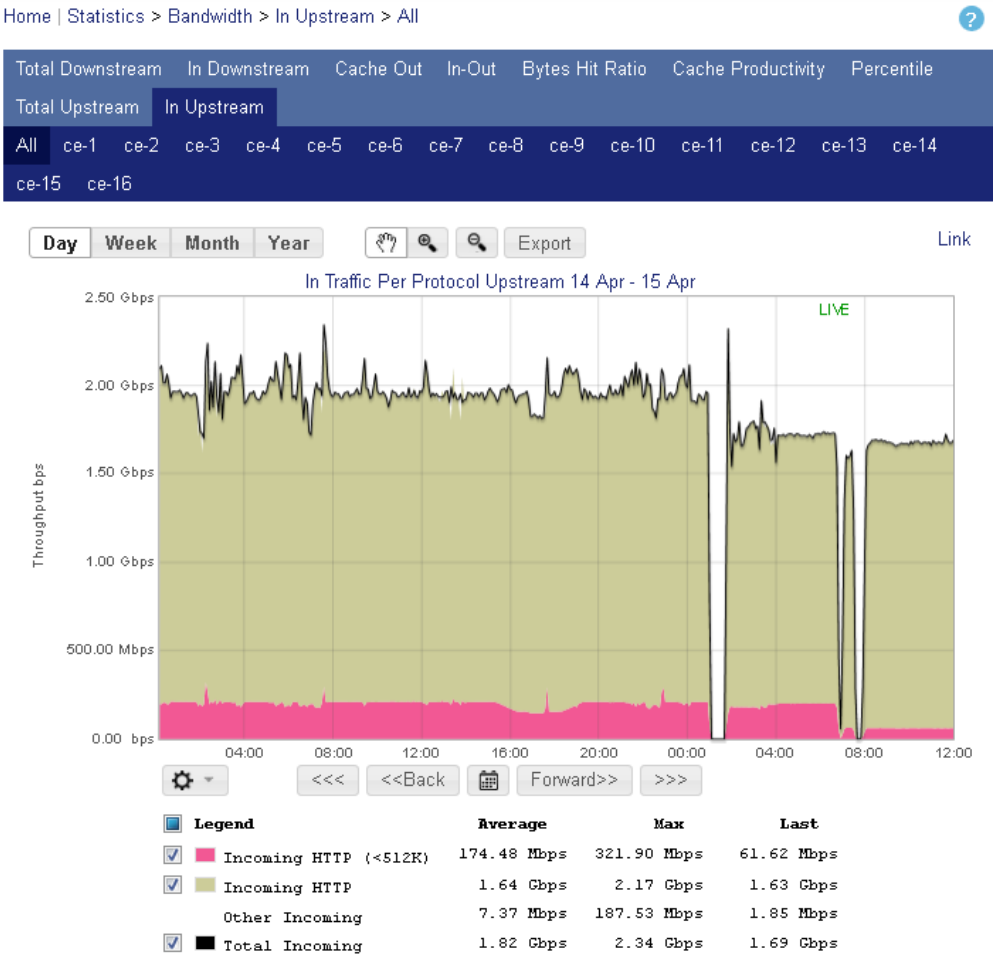
The In Upstream tab displays the incoming upstream protocol traffic capacity. You can see the total upstream incoming traffic, distributed by protocols. Only protocols above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

The In Upstream tab contains the following subtabs:

- **All:** The All tab displays the total incoming upstream protocol traffic capacity of all the cache engines. This is the default subtab that displays when you click the In Upstream tab.
- **ce "#":** This displays the incoming upstream protocol traffic capacity for one specific cache engine.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-20 Bandwidth–In Upstream



HTTP Services

To view statistics on the total HTTP traffic, distributed by service, from the Statistics menu choose **HTTP Services**. The service is a traffic category that is configured in the Policy Manager HTTP Service.

The following tabs are available from the Statistics > HTTP Service menu:

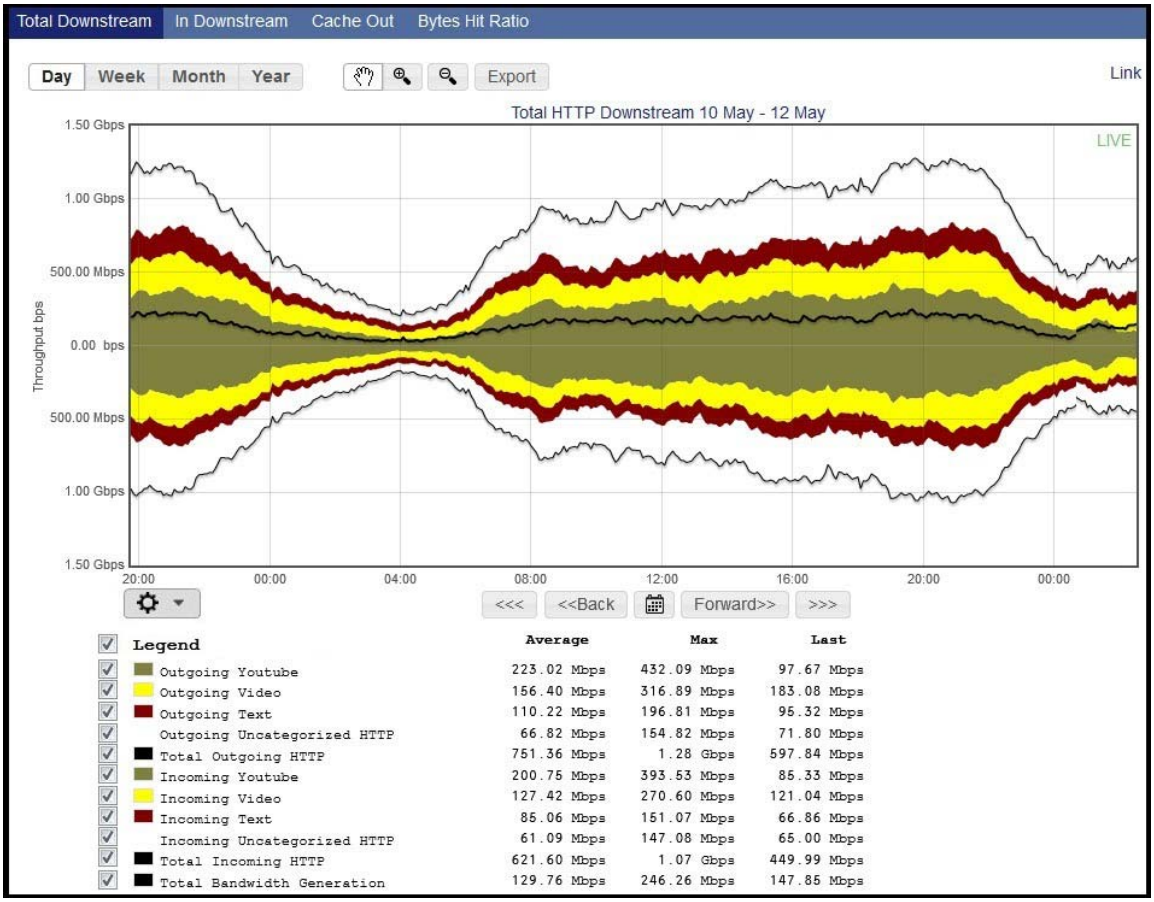
- **Total Downstream:** This tab displays the total HTTP downstream incoming, outgoing, and cache out traffic. See the Total Downstream section.
- **In Downstream:** This tab displays the HTTP incoming downstream traffic. See the In Downstream section.
- **Cache Out:** This tab displays the outgoing HTTP cache out traffic. See the Cache Out section.
- **Bytes Hit Ratio:** This tab displays the HTTP bytes hits ratio per service. See the Bytes Hit Ratio section.

Total Downstream

The Total HTTP Downstream tab displays the total HTTP downstream incoming, outgoing, and cache out traffic together with the per service incoming and outgoing traffic. The incoming traffic is displayed as the negative values and the outgoing traffic is displayed as the positive values. Only services that are above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-21 HTTP Services–Total Downstream Tab

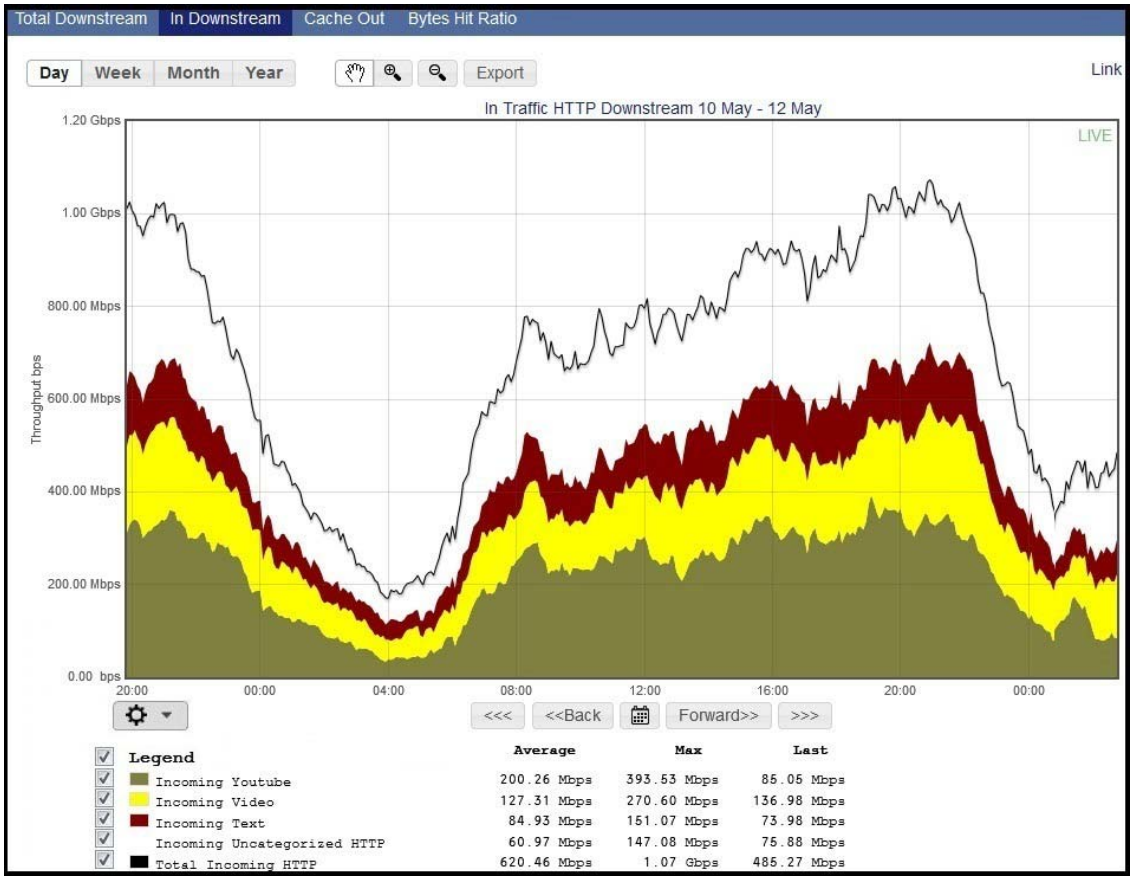


In Downstream

The Incoming Downstream tab displays the incoming HTTP downstream traffic, distributed by service. Only services that are above the minimum percentage are visible. You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-22 HTTP Services–In Downstream Tab

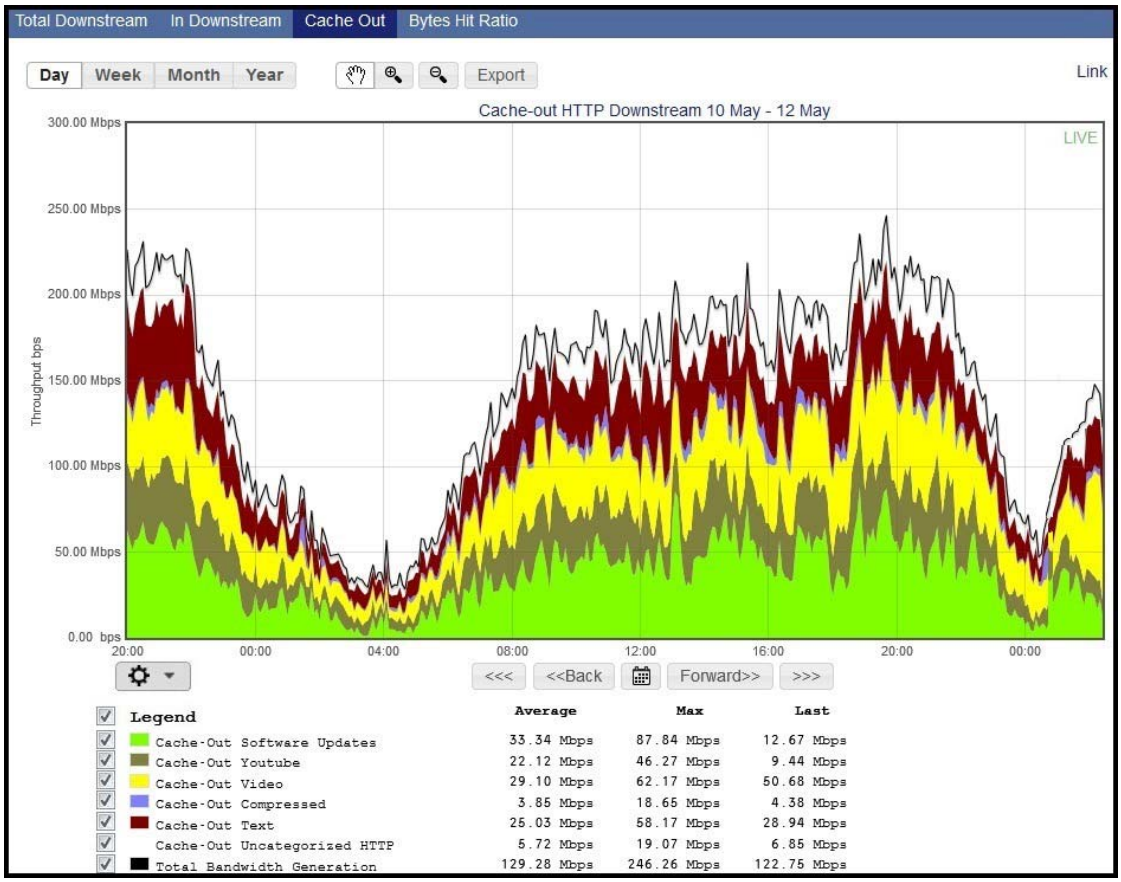


Cache Out

The Cache Out tab displays the total HTTP outgoing cache out traffic on the downstream, distributed by service. Only services that are above the minimum percentage are visible.You can configure the minimum percentage threshold by going to **Configuration > Settings > General**.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-23 HTTP Services–Cache Out Tab

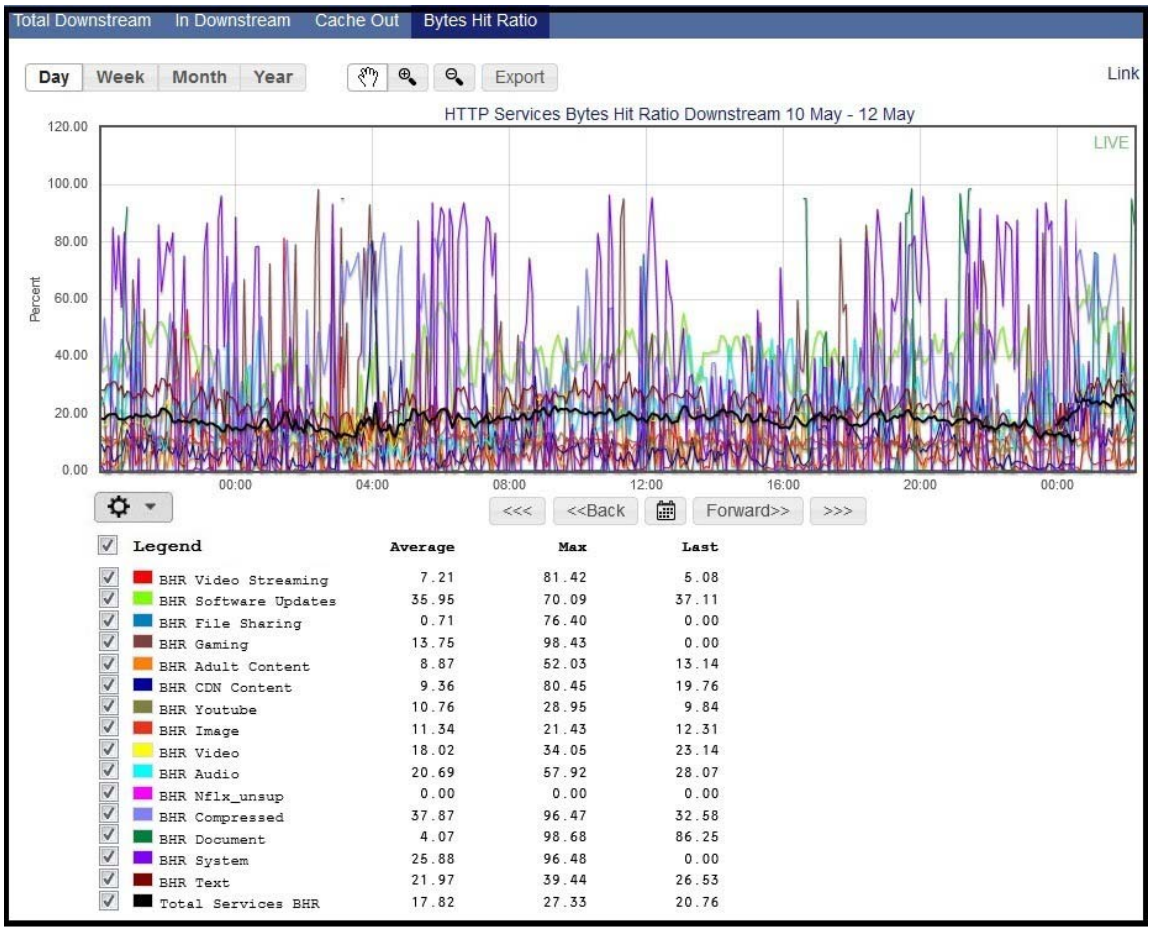


Bytes Hit Ratio

The Bytes Hit Ratio tab displays the HTTP Downstream Bytes Hit Ratio by dividing the downstream HTTP Cache Out traffic by downstream outgoing traffic. The Bytes Hit Ratio is determined by the Policy Manager.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-24 HTTP Services–Bytes Hit Ratio Tab



Cache Content

To display the content information cached in the storage, from the Statistics menu choose **Cache Content**.

The following tabs are available from the Statistics > Cache Content menu:

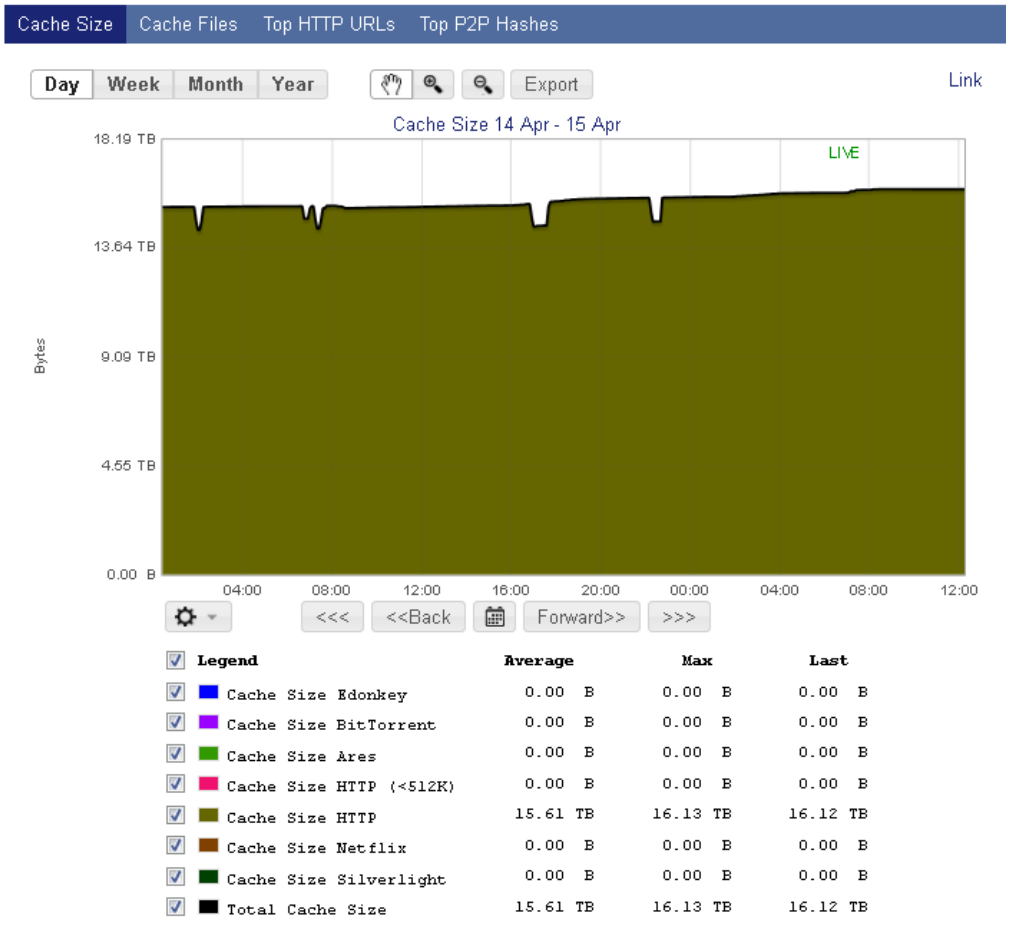
- **Cache Size:** This tab displays the total cache size, distributed by protocols. See the Cache Size section.
- **Cache Files:** This tab displays the general cache file information by protocol, such as cache size and the number of cached files. See the Cache Files section.
- **Top HTTP URLs:** This tab displays the top 100 URLs in the last hour. See the Top HTTP URLs section.
- **Top P2P Hashes:** This tab displays the top 100 P2P hashes. See the Top P2P Hashes section.

Cache Size

The Cache Size tab displays the total cache size distributed by protocol.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

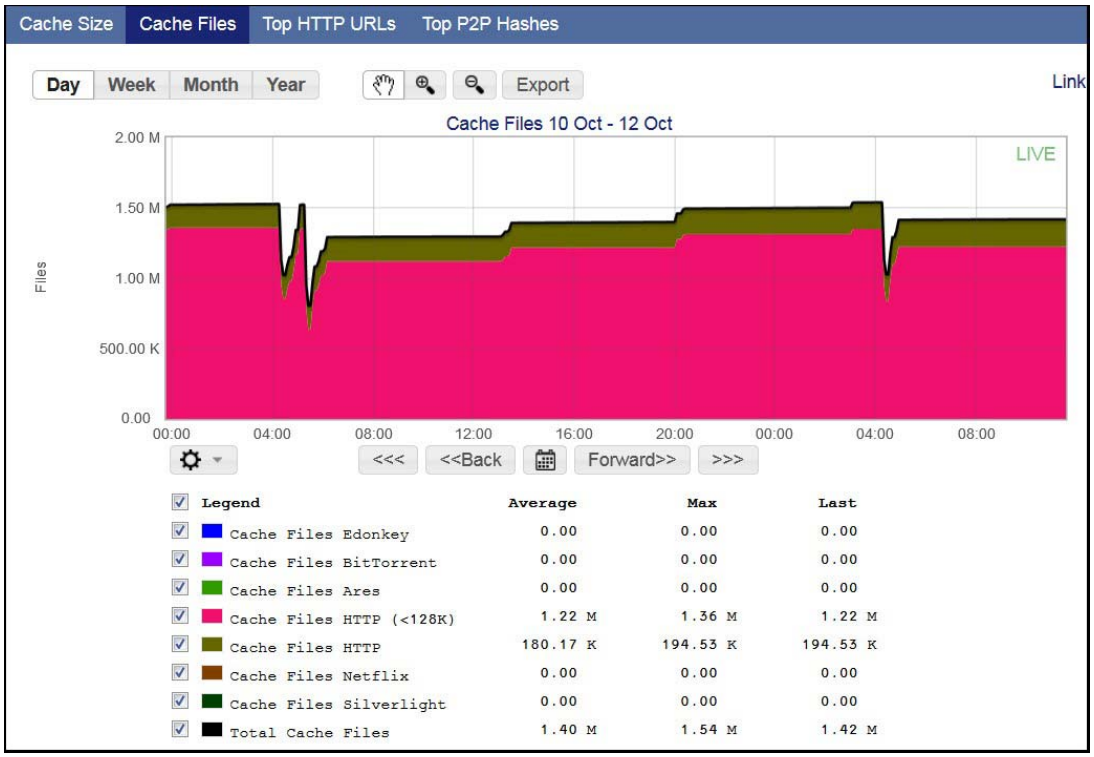
Figure 3-25 Cache Content–Cache Size Tab



Cache Files

The Cache Files tab displays the total number of files per protocol that are in the cache.

Figure 3-26 Cache Content–Cache Files Tab



Top HTTP URLs

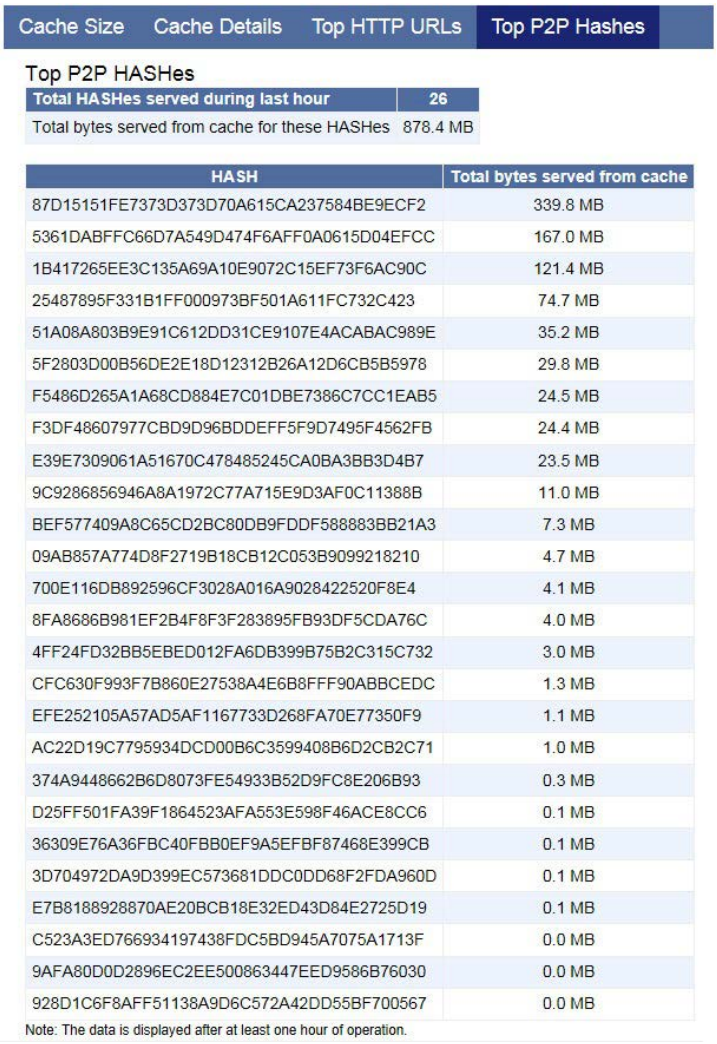
The Top HTTP URLs table displays information on the top 100 most popular URLs within the past hour.

Figure 3-27 Cache Content–Top HTTP URLs Tab

Top P2P Hashes

The Top P2P Hashes table displays information on the top 100 most popular P2P hashes that were served by the platform within the past hour.

Figure 3-28 Cache Content–Top P2P Hashes Tab



Cache Size | Cache Details | Top HTTP URLs | Top P2P Hashes

Top P2P HASHes

Total HASHes served during last hour	26
Total bytes served from cache for these HASHes	878.4 MB

HASH	Total bytes served from cache
87D15151FE7373D373D70A615CA237584BE9ECF2	339.8 MB
5361DABFFC66D7A549D474F6AFF0A0615D04EFCC	167.0 MB
1B417265EE3C135A69A10E9072C15EF73F6AC90C	121.4 MB
25487895F331B1FF000973BF501A611FC732C423	74.7 MB
51A08A803B9E91C612DD31CE9107E4ACABAC989E	35.2 MB
5F2803D00B56DE2E18D12312B26A12D6CB5B5978	29.8 MB
F5486D265A1A68CD884E7C01DBE7386C7CC1EAB5	24.5 MB
F3DF48607977CBD9D96BDDEFF5F9D7495F4562FB	24.4 MB
E39E7309061A51670C478485245CA0BA3BB3D4B7	23.5 MB
9C9286856946A8A1972C77A715E9D3AF0C11388B	11.0 MB
BEF577409A8C65CD2BC80DB9FDDF588883BB21A3	7.3 MB
09AB857A774D8F2719B18CB12C053B9099218210	4.7 MB
700E116DB892596CF3028A016A9028422520F8E4	4.1 MB
8FA8686B981EF2B4F8F3F283895FB93DF5CDA76C	4.0 MB
4FF24FD32BB5EBED012FA6DB399B75B2C315C732	3.0 MB
CFC630F993F7B860E27538A4E6B8FFF90ABBCEDC	1.3 MB
EFE252105A57AD5AF1167733D268FA70E77350F9	1.1 MB
AC22D19C7795934DCD00B6C3599408B6D2CB2C71	1.0 MB
374A9448662B6D8073FE54933B52D9FC8E206B93	0.3 MB
D25FF501FA39F1864523AFA553E598F46ACE8CC6	0.1 MB
36309E76A36FBC40FBB0EF9A5EFBF87468E399CB	0.1 MB
3D704972DA9D399EC573681DDC0DD68F2FDA960D	0.1 MB
E7B8188928870AE20BCB18E32ED43D84E2725D19	0.1 MB
C523A3ED766934197438FDC5BD945A7075A1713F	0.0 MB
9AFA80D0D2896EC2EE500863447EED9586B76030	0.0 MB
928D1C6F8AFF51138A9D6C572A42DD55BF700567	0.0 MB

Note: The data is displayed after at least one hour of operation.

Storage

To display storage information and operational information, from the Statistics menu choose **Storage**.

The following tabs are available from the Statistics > Storage menu:

- **Volume Usage:** This tab displays information on the remaining capacity of the storage hard disk. See the Volume Usage section.
- **Requests:** This tab displays statistics on the storage read and write requests. See the Requests section.
- **Block Size:** This tab displays statistics on the general storage read and write block sizes. See the Block Size section.
- **Read percentage (VDS TC Cluster only):** This tab displays the storage read write amounts. See the Read Percentage section.

- **iSCSI Network (VDS TC Cluster only):** This tab displays the capacity of incoming and outgoing traffic through the iSCSI network. See the iSCSI Network section.
- **Bandwidth (Appliance only):** This tab displays the capacity of the read and write data per second (time) in the local storage. See the Bandwidth section.

Volume Usage

The Volume Usage tab displays information about the Cache Content Storage (hard disks). When you click the Volume Usage tab, the Cache Content Storage table appears. Table X describes the information in this table.

Figure 3-29 Storage–Volume Usage Tab

Cache Content Storage

LUN	App Volume #	Size	Used	Avail	Usage %	Status
Storage Enclosure PA-1-10_56_11_117						
0	1	538G	424G	114G	78.81%	active
1	2	538G	419G	119G	77.88%	active
2	3	538G	417G	121G	77.51%	active
3	4	538G	417G	121G	77.51%	active
4	5	538G	414G	124G	76.95%	active
5	6	538G	415G	123G	77.14%	active
6	7	538G	413G	125G	76.77%	active
8	8	538G	414G	124G	76.95%	active
9	9	538G	411G	127G	76.39%	active
10	10	538G	411G	127G	76.39%	active
11	11	538G	412G	126G	76.58%	active
12	12	538G	412G	126G	76.58%	active
13	13	538G	416G	122G	77.32%	active
14	14	538G	413G	125G	76.77%	active
15	15	538G	412G	126G	76.58%	active
16	16	538G	409G	129G	76.02%	active

Table 3-1 Cache Content Storage Table

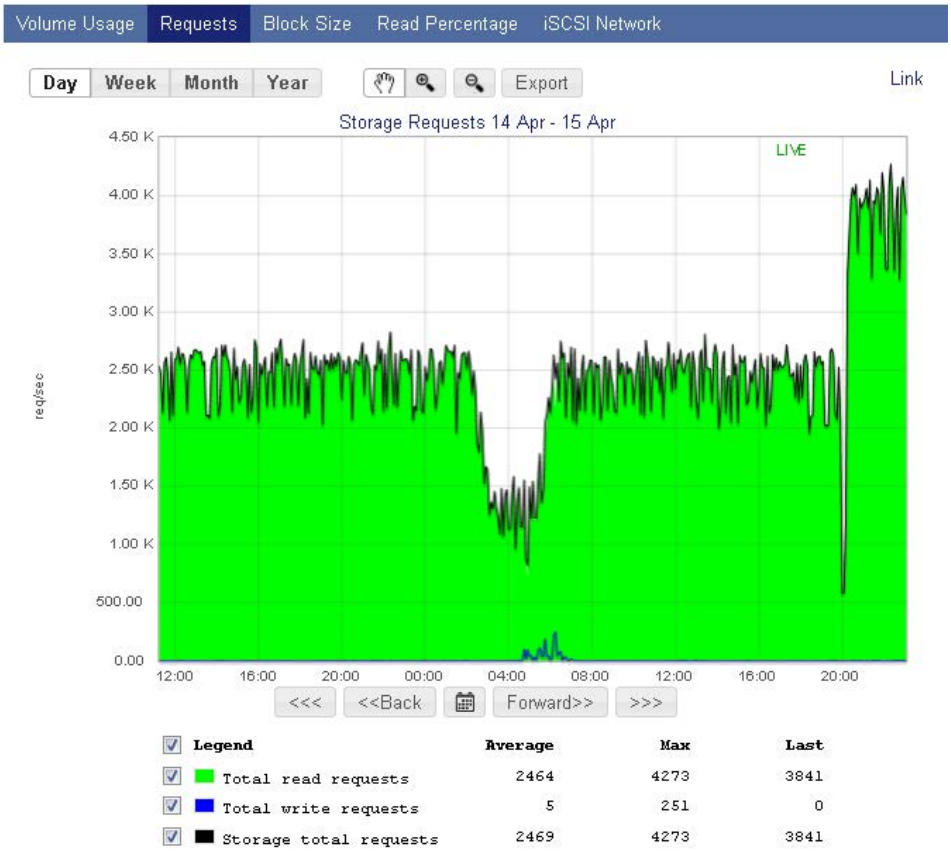
Column	Description
LUN	Displays the storage volume number of a specific storage enclosure. **Note** The enclosure name is displayed below the title bar (for example: as shown above - "Storage Enclosure PA-1"). This enclosure name only appears in Cluster configurations.
App Volume #	Displays the volume ID number in a specific storage enclosure.
Size	Displays the total volume disk size in gigabytes (GB).
Used	Displays the amount of used disk space in GB.
Avail	Displays the amount of available volume disk space in GB.
Usage %	Displays the percentage of used disk space. **Note** The background color is red in this column if the usage is above 97%.
Status	Displays the current status of the volume. • Green indicates active. active • Red indicates inactive. inactive

Requests

The Requests tab displays statistics on the storage read and write requests.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-30 Storage–Requests Tab

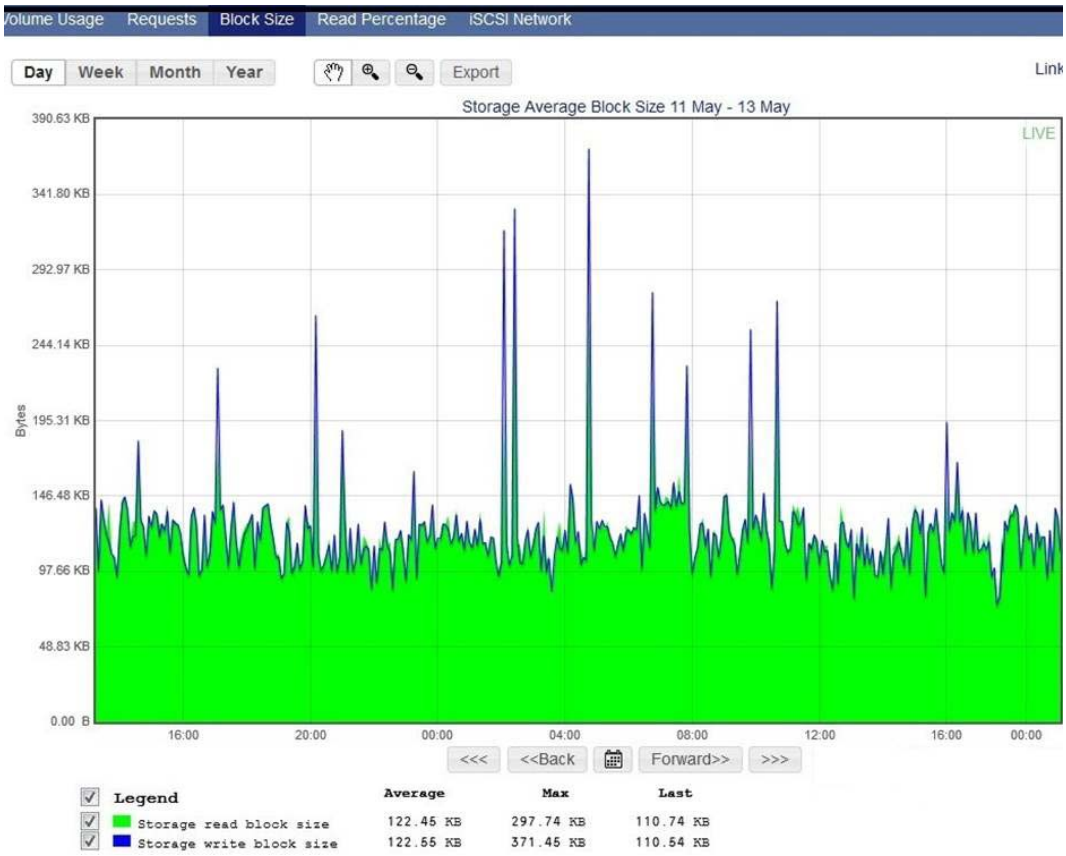


Block Size

The Block Size tab displays statistics on the storage read and write block sizes.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-31 Storage–Block Size Tab

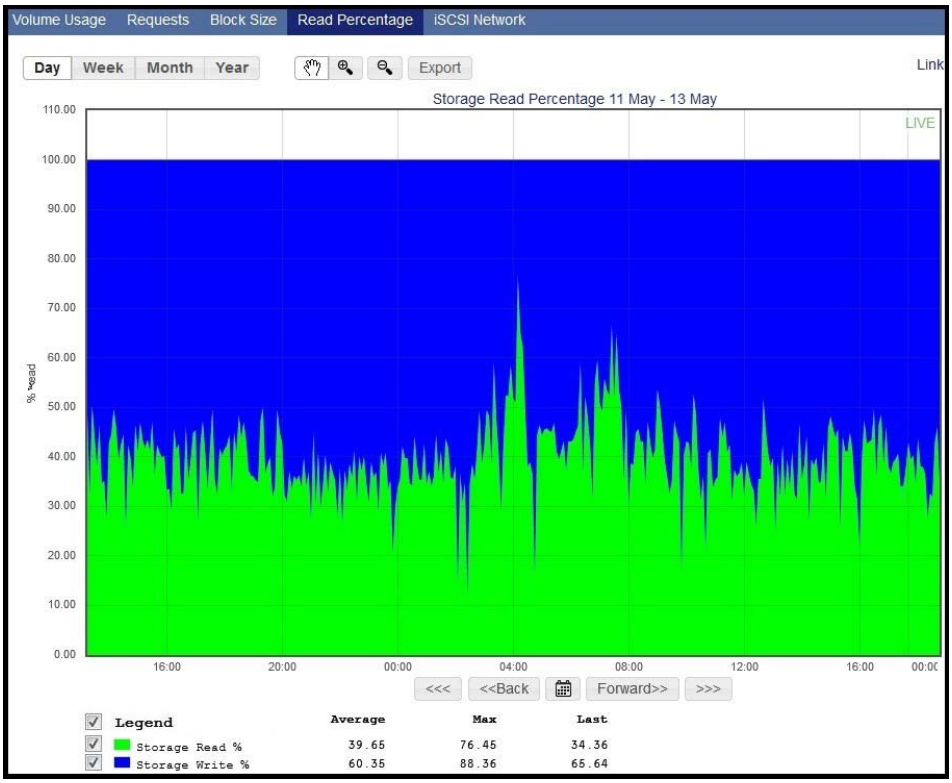


Read Percentage

The Read Percentage tab displays statistics on the storage read and write percentages from the total number of requests. (This tab is only available in Cluster Systems).

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-32 Storage–Read Percentage Tab (Cluster Only)

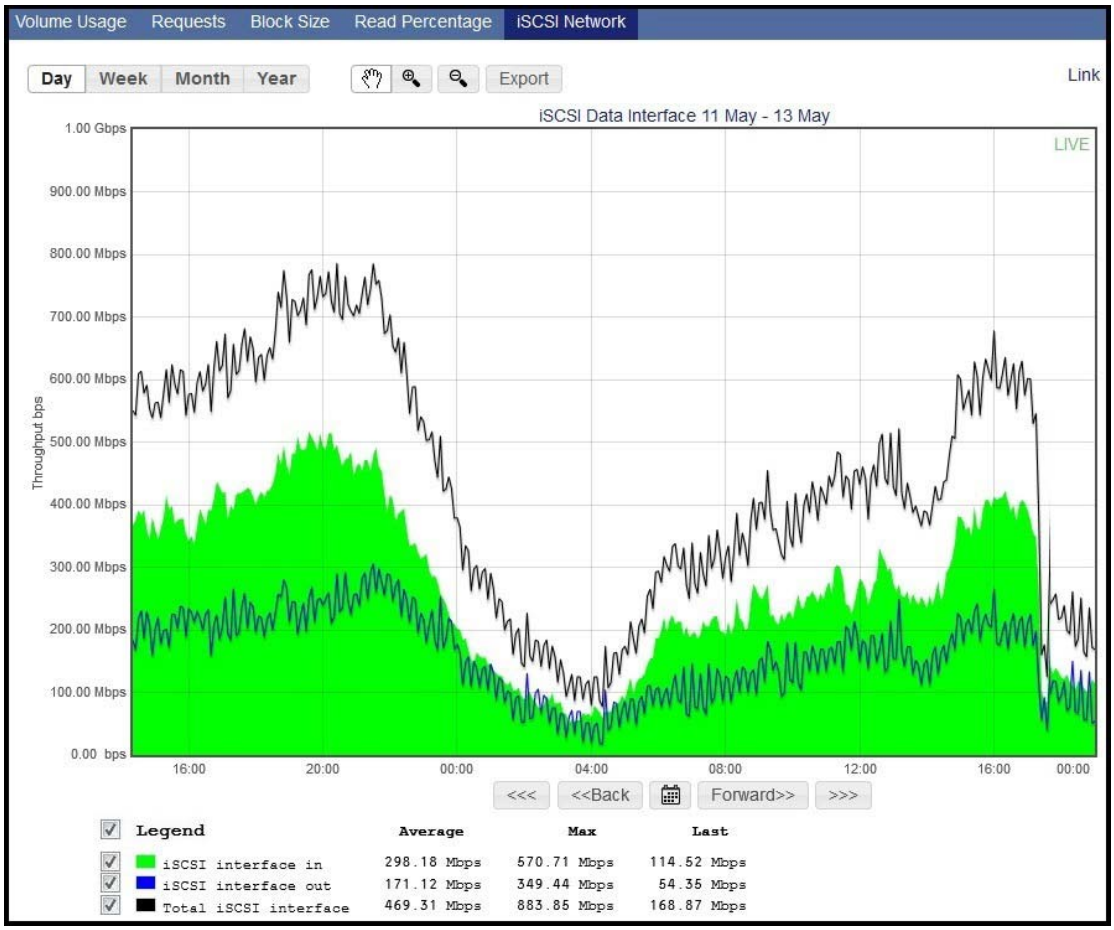


iSCSI Network

The iSCSI Network tab displays statistics from the total read (Rx) and total write (Tx) capacity, from all cache engines to the storage system through the iSCSI network. (This tab is only available in Cluster systems).

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-33 Storage–iSCSI Tab (Cluster Only)

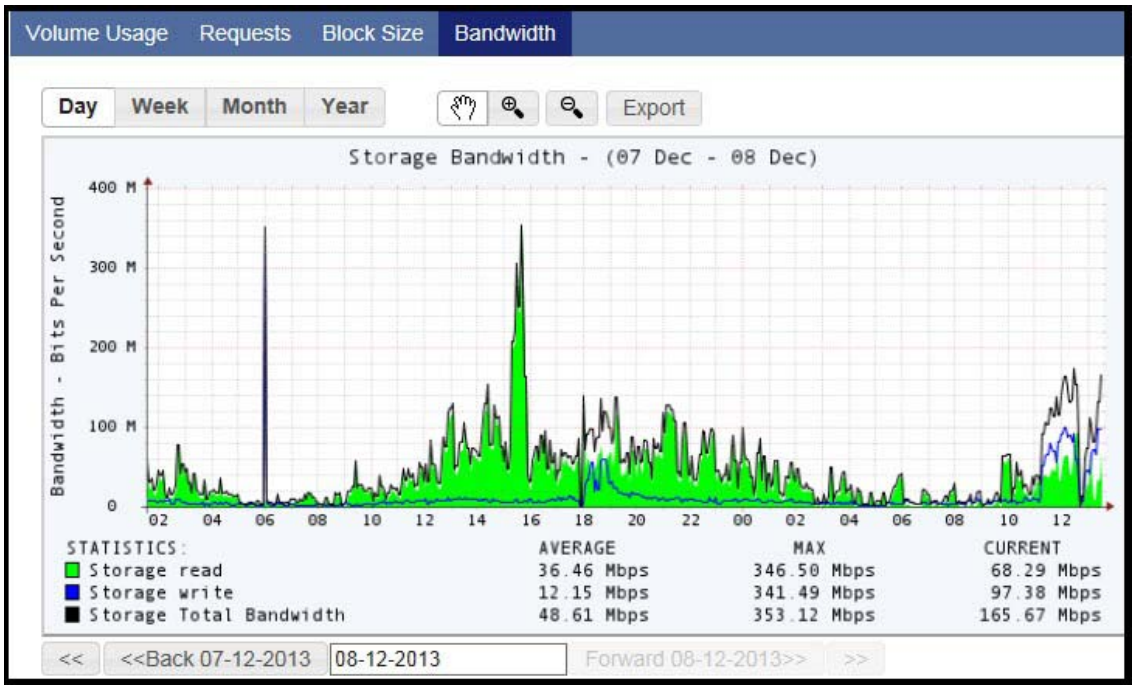


Bandwidth

The Bandwidth tab displays statistics on bandwidth storage read, storage write, and total bandwidth storage. (This tab is only available in Appliance Configuration).

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-34 Storage–Bandwidth Tab (Appliance Only)



QoE

To view information about the quality of experience (QoE) that the Cisco VDS TC Manager provides, from the Statistics menu choose **QoE**.

The following tabs are available from the Statistics > QoE menu:

- **HTTP Clear vs. Cache:** This tab displays a comparison between the clear and cached HTTP per user. See the HTTP Clear vs. Cache section.
- **P2P Clear vs. Cache:** This tab displays a comparison between clear and cached P2P bandwidth per user. See the P2P Clear vs. Cache section.
- **IP Statistics:** This tab displays information about IP addresses that were served by the VDS TC platform. See the IP Statistics section.

HTTP Clear vs. Cache

The HTTP Clear vs. Cache Service graph is the default window that appears when you choose QoE. This graph displays a comparison between the clear and cached HTTP traffic measurements.

The green line in the graph indicates the ratio between the measured HTTP traffic flowing through the platform and the number of active HTTP users sending out from the platform. The blue line indicates the ratio between the cached HTTP traffic and the number of active cache out users for the platform.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

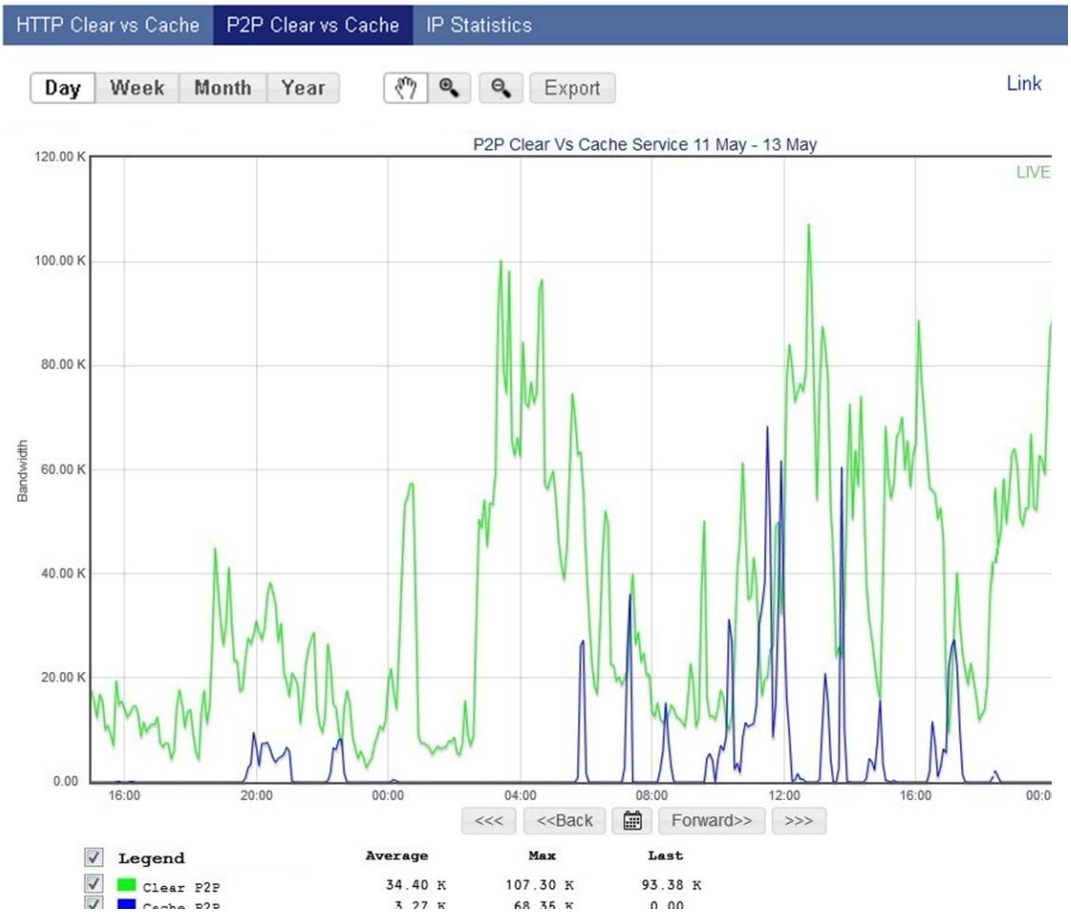
Figure 3-35 QoE–HTTP Clear vs. Cache Tab

P2P Clear vs. Cache

The P2P Clear vs. Cache Service graph displays a comparison between clear and cached HTTP bandwidth per user. The green line in the graph indicates the ratio between the measured P2P traffic flowing through the platform and the number of active P2P users for the platform. The blue line indicates the ratio between the cached P2P traffic sending out from the platform and the number of active P2P cache out users for the platform.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-36 QoE–P2P Clear vs. Cache Tab

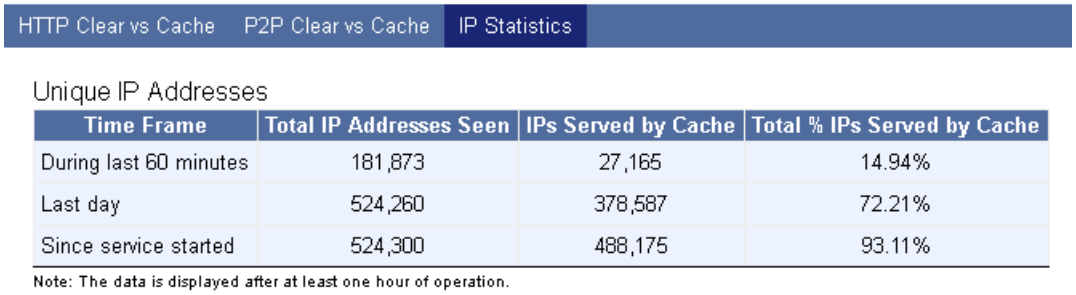


IP Statistics

The IP Statistics table displays information about IP addresses (users) that were served by the platform, including the total number of IP addresses (users) that were passed through the system, the number of IP addresses (users) that were served by the system (received cache out traffic), and their ratio.

Note You can change the time frame for which you want to display information by clicking Day, Week, Month, or Year. See the "Viewing Data for a Specific Time Frame" section in Chapter 1, "Getting Started".

Figure 3-37 QoE–IP Statistics Tab



Configuration Menu

This chapter describes how to view general information regarding your configuration, focusing on configuration details. Information is presented in a designated set of tabs. This Menu includes the Policy Manager. You use the Policy Manager to configure rules that you apply to categories.

Note To access the Configuration menu, you must be logged into VDS TC Manager with a user that has these privileges. Contact your Cisco account system engineer if you need this information.

The Configuration menu contains the following choices:

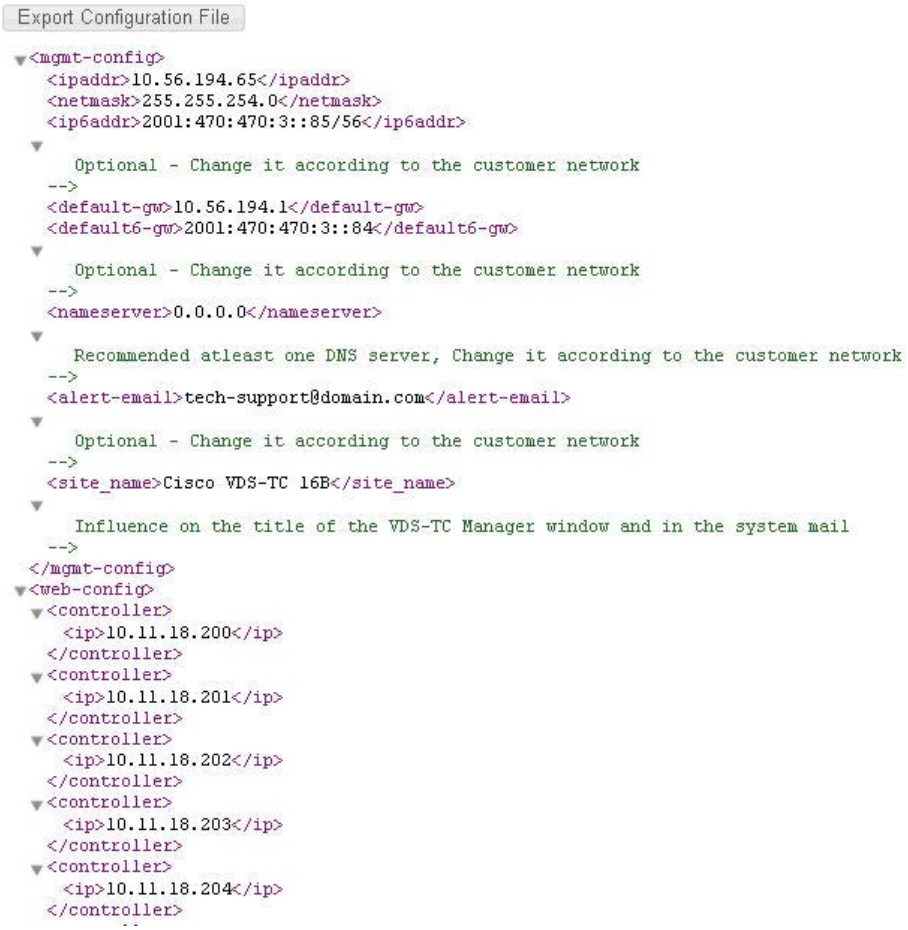
- **Cluster Configuration:** Displays information about the status of your configuration. You can export the configuration file to your system for future use (such as, using it as a reference to change the configuration). See the Cluster Configuration section.
- **Policy Manager:** This option enables you to view, configure, and set the policies for the system. See the Using the Policy Manager section.
- **License Manager:** This option displays the License file in read-only format. From this window you can generate a license request and install a new license. See the The License Manager section.
- **Settings:** This option enables you to change general settings for the system and reset the enable password. See the Settings section.

Cluster Configuration

To view the configuration of your Cisco VDS TC platform, in the left menu bar of the Cisco VDS TC Manager window choose **Configuration > Cluster Configuration**. The Cluster Configuration window opens, displaying the Configuration file in read-only format.

Note For details on configuring the platform, see the “Cisco Videoscape Distribution Suite Transparent Caching Software Configuration Guide.”

Figure 4-1 Configuration–Cluster Configuration Window

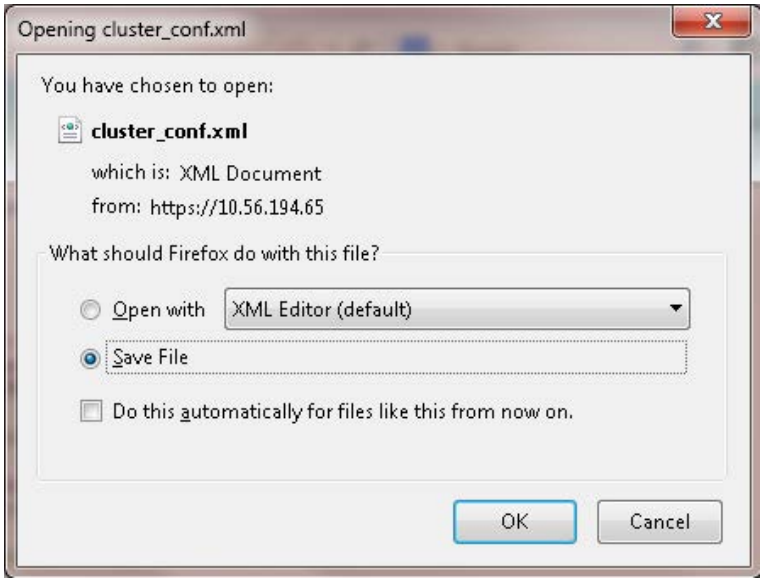


Exporting the Configuration File

From the Cluster Configuration window you can export the configuration file to an XML file. Follow these steps to export the configuration file:

Step 1 From the left navigation pane, choose **Configuration > Cluster Configuration**. The Cluster Configuration window appears.

Step 2 Click the **Export Configuration File**. The Export Configuration popup window appears.



Step 3 Click the **Save File** option. The File Save dialog box appears.

Step 4 In the File name text box either accept the default name of cluster_conf or enter a new name for the file.

Step 5 Click **Save**. The configuration file is exported.

Using the Policy Manager

The Policy Manager is a web-based tool that is included with the Cisco VDS TC Manager software that enables you to configure rules that you apply to categories. To use the Policy Manager choose **Configuration > Policy Manager**.

Note To create or edit policies using Policy Manager, you must be logged into VDS TC Manager with a user that has these privileges. If you do not have this information, contact your Cisco representative.

The Policy Manager window contains the following tabs:

- **Rules:** This tab displays the rules, with each line representing a separate rule. It includes the following information about each rule.
  - Rule ID number
  - Rule Info, including the name and category
  - Timeplans
  - Policies
  - Whether the rule is active

  From this tab you can add, edit, or delete a rule. You can also change the order of the rules.
- **Categories:** Categories are used to help organize subjects into common functions, types, or a field of use. From the Category tab you can add, delete, or edit a category.

- **Policies:** The Policies tab displays information about the global policies and any user created policies, including the name of the policy and what type of policy it is. From the Policy tab you can add, delete, or edit a policy. There are three types of policies that you can create: Admission, Bandwidth Limit, or DSCP.
- **Timeplans:** This tab displays each timeplan, including its name and the type of timeplan that it is. From this tab you can add, delete, or edit a timeplan.
- **HTTP Services:** The HTTP Services option enables you to group specific subject categories together. The HTP Services tab displays the exiting groups and enables you to add, delete, or edit a group.

Note For changes that you make to the rules, categories, policies, timeplans, and HTTP Services groups to take effect, you must publish these changes. *See* the Publish the Configuration section.

Rules

Creating rules can be very complex. To reduce the complexity, you should group categories with common properties and parameters together into one group (where applicable).

The Rules tab displays all of the rules together in a scrollable format. Each rule is displayed in a single row.

This section covers the following subjects:

- Editing Rules
- Adding Rules and Subrules
- Deleting Rules

Note Long rule names are shown in a truncated form and whole names are shown in a “hint”.

Note Each configuration uses a special default rule. This rule defines policies that are applied by default.

Follow these steps to access the list of rules:

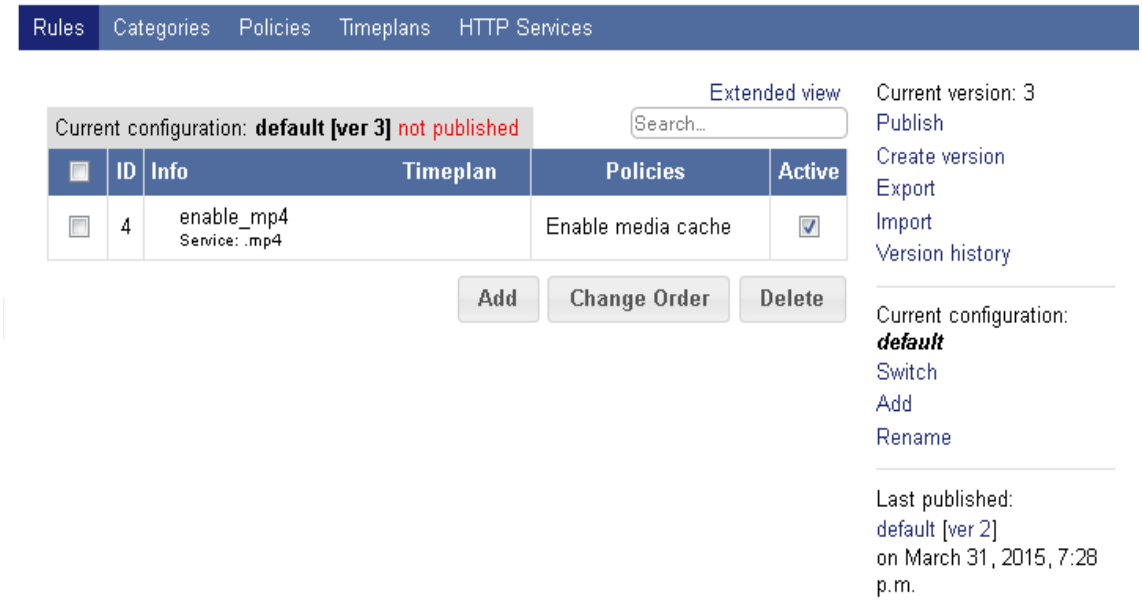
Step 1 In the Cisco VDS TC Manager window choose **Configuration > Policy Manager**.

Step 2 The Rules list and current configuration version appears. The rules appear in the middle pane and include the following information:

- **Check box:** A check box in the row indicates that you can edit the rule.
- **ID:** An identifying number that applies to the CDR.
- **Info:** A simple description of the rule.
- **Timeplan:** A preset plan of when the rules take affect.
- **Policies:** A list of policies that are applied to the rule.
- **Active:** If this check box is checked, the rule is enabled. You can enable or disable the rule from this column.

The right pane displays information about the current version and current configuration.

Figure 4-2 Policy Manager, Rules Tab



When defining a Rule, the category definition can include more than one category type. If the category definition includes more than one category type, the rule matching of traffic includes asserting one or more of the criteria of each category type, and containing *all* of the category types that are defined within the rule.

For example, assume a rule has the following categories configured:

- The application is.ascx OR .asmx OR .asp.
- The services is video.facebook OR megavideo OR Sourceforge.net.

The rule is considered matched if the traffic is either for the .ascx OR .asmx OR .asp application AND the service is either video.facebook OR megavideo OR Sourceforge.net.

Editing Rules

Follow these steps to edit a rule:

Step 1 Open the Edit Rule dialog box. You can open this dialog box in two ways:

- Right-click a rule and choose **Edit** from the pop-up menu.
- Click anywhere on the rule that you want to edit.

The Edit Rule dialog box appears.

Figure 4-3 Edit Rule Dialog Box

Step 2 Complete the fields in the Edit Rule dialog box:

- To manage the categories, do the following as needed:
  - To add a new category, from the Add Category drop-down list choose a new category.
  - To remove an existing category, click the **X** at the end of the category.
  - To remove an entry in an existing category, click the **X** at the end of the entry.
- To manage the policies do the following as needed:
  - To add a new policy, from the Add Policy drop-down list choose a new policy.
  - To remove an existing policy, click the **X** at the end of the policy.
- To manage the timeplans, do the following as needed:
  - To add a new timeplan, from the Add Timeplan drop-down list choose a new timeplan if desired.
  - To remove an existing timeplan, click the **X** at the end of the timeplan.

Step 3 Click **OK** to save the changes.

Step 4 After you make changes to rules, for those changes to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Rules and Subrules

A subrule enables you to add a criteria within a rule. Follow these steps to add a rule or subrule:

Step 1 To start adding a rule or subrule, do one of the following:

- To add a subrule, right-click the rule under which the subrule should be added and choose **Add subrule**.
- To add a rule, do one of the following:
  - Right-click a rule and choose either **Add before** or **Add after** depending on where the rule should be placed in the list.
  - Click **Add** at the bottom of the rules list.

Figure 4-4 Adding a Rule or Subrule

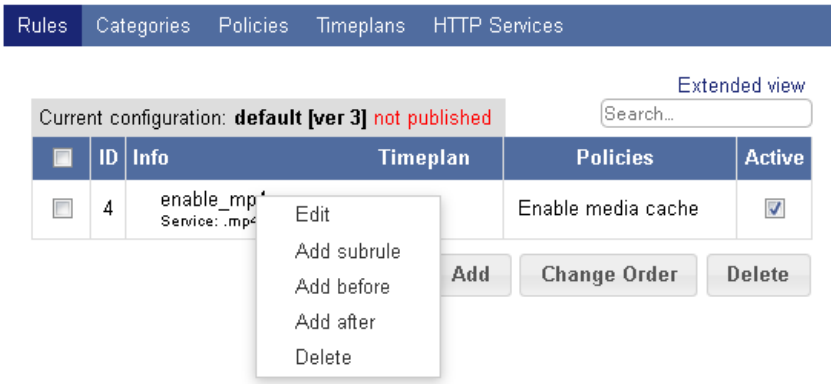
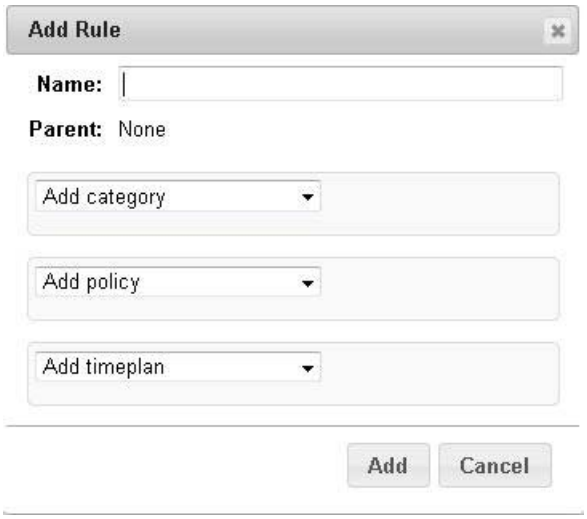


Figure 4-5 Add Rule Dialog Box



Step 2 In the Add Rule dialog box that appears, in the Name field enter a name for the rule.

Step 3 From the Add Category drop-down list do one of the following:

- Choose **Application** and then choose an option from the Application dialog box.
- Choose **Service** and then choose an option from the Service dialog box.
- Choose **Device** and then choose an option from the Device dialog box.

- Choose **Subscriber** and then choose an option from the Subscriber dialog box.
- Choose **Network** and then choose an option from the Network dialog box.

Step 4 From the Add Policy drop-down list, choose one or more of the listed policies.

Step 5 From the Add Timeplan drop-down list, choose one or more timeplans.

Step 6 Click **Add** in the Add Rule dialog box to add the new rule.

Step 7 After you add a rule, for that rule to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Deleting Rules

To delete a rule, do one of the following:

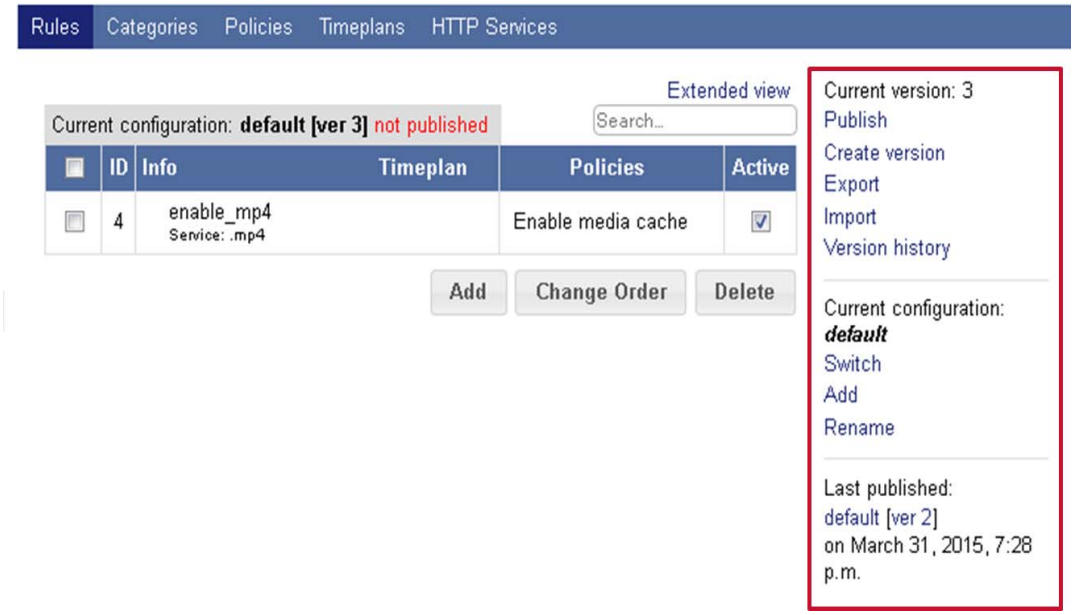
- Check the check box in the first column of the rule that you want to delete and click **Delete**.
- Right-click the rule you want to delete and choose **Delete** from the pop-up menu.

Configuration Section

On the right pane of the Rules tab, the following configuration options are available:

- **Current Version:** Displays the current configuration version.
- **Publish:** Click this link to publish the configuration.
- **Create Version:** Click this link to save any updates or new versions to the configuration.
- **Export:** Click this link to export the configuration. Configurations are saved in XML format (*.xml). You can back up the XML files to a remote server using TFTP.
- **Import:** Click this link to import a configuration from a zip archive file that contains XML files. To choose how to resolve conflicts between the current configuration and the configuration that you are importing, click the **Keep Existing**, **Replace Existing**, or **Create Copies** radio button.
- **Version History:** Click this link to display the version list and the date it was created.
- **Current Configuration:** This section displays the name of the current configuration. If more than one configuration is available, you can choose the current configuration to use from the drop-down list. The following options appear under Current Configuration:
  - **Switch:** Enables you to switch between configurations.
  - **Add:** Enables you to add a configuration to the configuration list.
  - **Rename:** Allows you to rename the configuration using the Edit Configuration dialog box.
- **Last published default:** Displays the last published configuration.

Figure 4-6 Configuration Section



Export

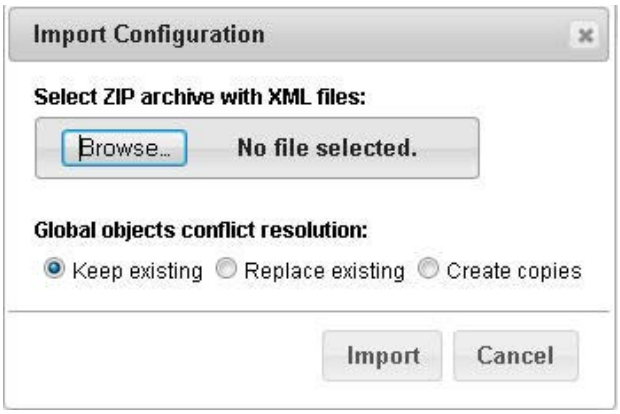
By clicking the Export option, you can open the file to view it or save it to a file. Configurations are saved in text format (*.xml) and can be backed up on remote servers via TFTP.

See the Exporting the Configuration File section for more information.

Import

By clicking the Import link in the Configuration pane, you can import a configuration by selecting a zip archive with XML files using a Browse button. You can utilize conflict resolution by selecting either **Keep Existing**, **Replace Existing**, or **Create Copies**.

Figure 4-7 Configuration–Import



Version History

By clicking the Version History link, you can view the configuration version list and the date the versions were created.

Note You can open a previous configuration, but you cannot publish it or edit it because it was previously published.

Figure 4-8 Configuration–Version History

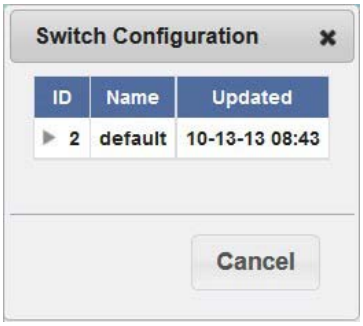
Current Configuration

Switch

To switch the current configuration, from the Current Configuration section click the **Switch** link. The Switch Configuration dialog box appears. Click the configuration to which you want to switch.

Figure 4-9 Switch Configuration

e



Add

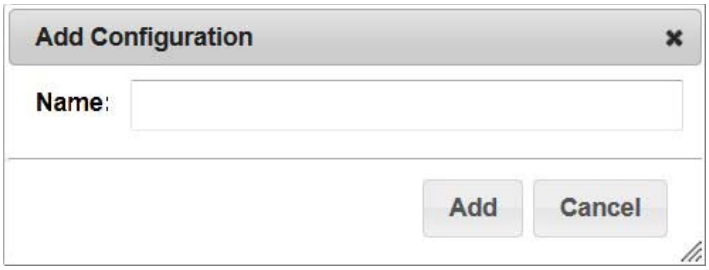
Follow these steps to add a new configuration to the configuration list:

Step 1 From the Current Configuration section click the **Add** link. The Add Configuration window appears.

Step 2 In the Name field, enter the name of a configuration to add.

Step 3 Click **Add**.

Figure 4-10 Add a Configuration



Categories

From the Policy Manager you can manage the categories. Follow these steps to manage categories:

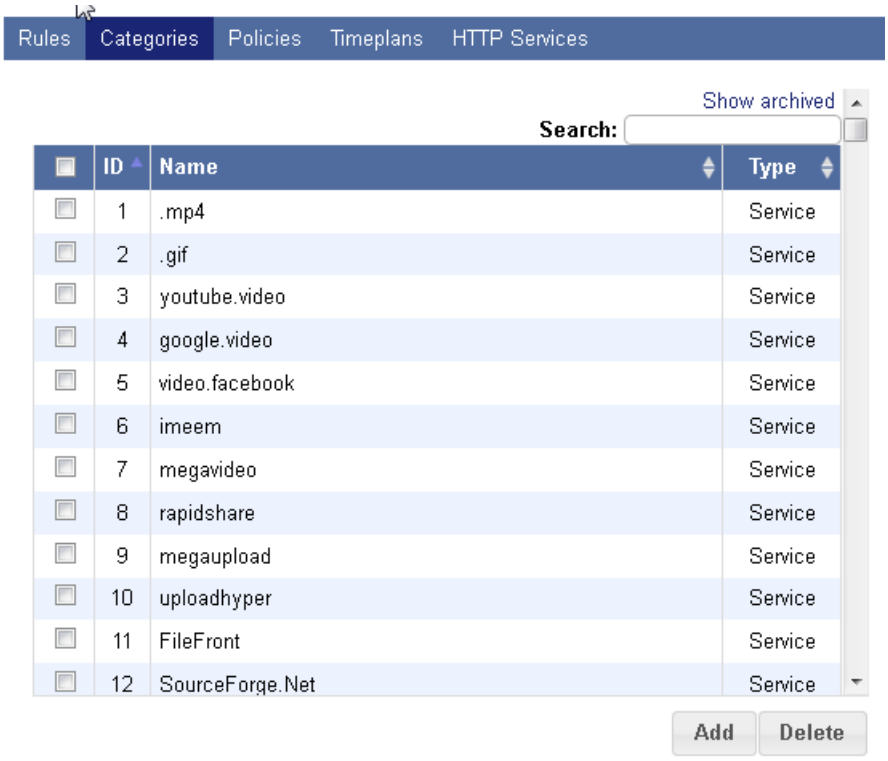
Step 1 In the Cisco VDS TC Manager window choose **Configuration > Policy Manager**.

Step 2 Click the **Categories** tab. The list of categories appears in the work area.

The list of categories contains the following columns:

- **Check box:** A check box in the row indicates that you can edit the category
- **ID:** An identifying number that applies to the CDR
- **Name:** The name of the category
- **Type:** The class of the category

Figure 4-11 Categories Tab



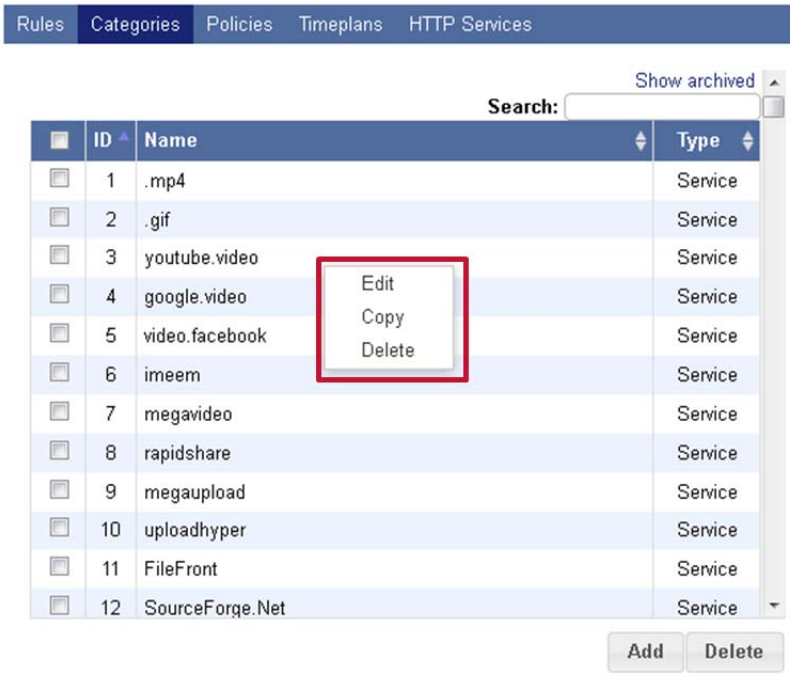
Editing Categories

Follow these steps to edit a category:

Step 1 Open the Edit Category dialog box. You can open this dialog box in two ways:

- Right-click a category and chose **Edit** from the pop-up menu.
- Click anywhere on the category that you want to edit.

Figure 4-12 Edit Category



Note When you right-click a category you can edit the category or you can copy the category. When you copy a category, you are adding a category with the parameters of the copied category. When you right-click a category you can also delete the category.

The Edit Category dialog box appears.

Figure 4-13 Edit Category Dialog Box

Step 2 From the Edit Category dialog box, edit the following fields as needed:

- **Name:** Enter a new name if desired.

- **Condition Section:** You can add or delete multiple conditions. To add additional conditions for the same type of parameter, enter a new value and click the **Plus (+)** icon at the end of the input field. To add a condition for a different type of parameter, click the **Switch to Advanced** button. You can match or exclude traffic based on the following parameters:
  - Domain
  - Referrer
  - URI
  - Protocol
  - User Agent
  - Subscriber IP Network
  - Service IP Network

Step 3 After you have finished making changes, click **OK** to save the changes.

Step 4 After you make changes to categories, for those changes to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Categories

Follow these steps to add a new category:

Step 1 Click **Add** at the bottom of the categories list. The Add Category dialog box appears.

Figure 4-14 Add Category

Step 2 In the Name field enter a name for the category.

Step 3 From the Type drop-down list, choose one of the following types:

- Application
  - Application: Match domains
  - Application: Exclude domains
  - Application: Match referrers
  - Application: Exclude Referrers
  - Application: Match URIs
  - Application: Exclude URIs
  - Application: Match protocols
  - Application: Exclude protocols

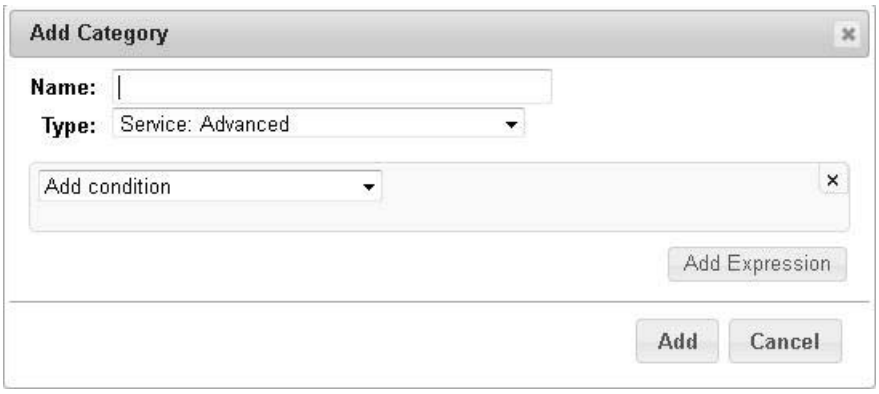
  - Application: Advanced
- Service
  - Service: Match domains
  - Service: Exclude domains
  - Service: Match referrers
  - Service: Exclude referrers
  - Service: Match URIs
  - Service: Exclude URIs
  - Service: Match protocols
  - Service: Exclude protocols
  - Service: Advanced
- Device
  - Device: Match user agents
  - Device: Exclude user agents
- Subscriber
  - Subscriber: Match user IP networks
  - Subscriber: Exclude user IP networks
- Network
  - Network: Match service IP networks
  - Network: Exclude service IP networks

Step 4 After you choose a type, a field appears in which you can enter a value to match or exclude (depending on the type that you selected) or choose a value from a list, depending on the type that you selected. For example, if you choose the type Application: Match domains you would enter domains to match. If you choose the type Application: Match protocols you would choose a protocol from a list.

Step 5 If you choose Application: Advanced or Service: Advanced as the type, the Add Condition drop-down list appears in the Add Category dialog box. You can add multiple conditions by clicking **Add Expression** and you can remove a condition by clicking the **X**. You can match or exclude traffic based on the following parameters:

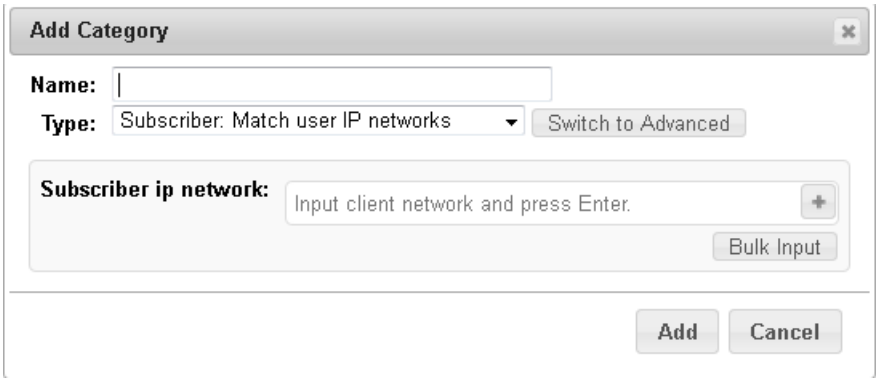
  - Domain
  - Referrer
  - URI
  - Protocol
  - User Agent
  - Subscriber IP Network
  - Service IP Network

Figure 4-15 Add Condition



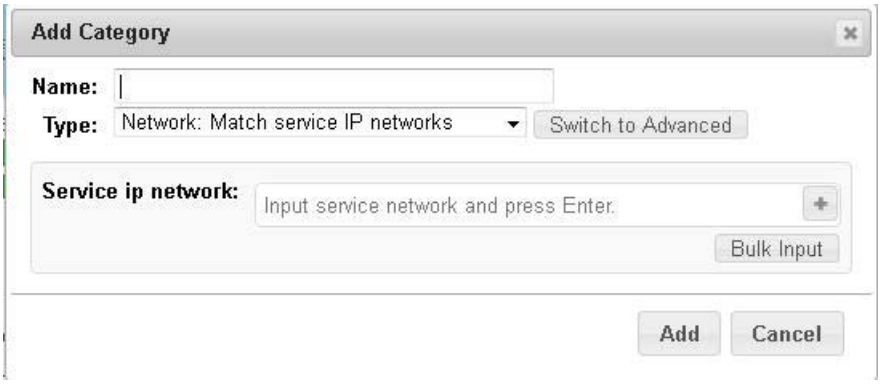
a. If you choose Subscriber: Match user IP networks or Subscriber: Exclude user IP networks from the Type drop-down list, enter a subscriber IP network in the text box to match or exclude.

Figure 4-16 Add Subscriber



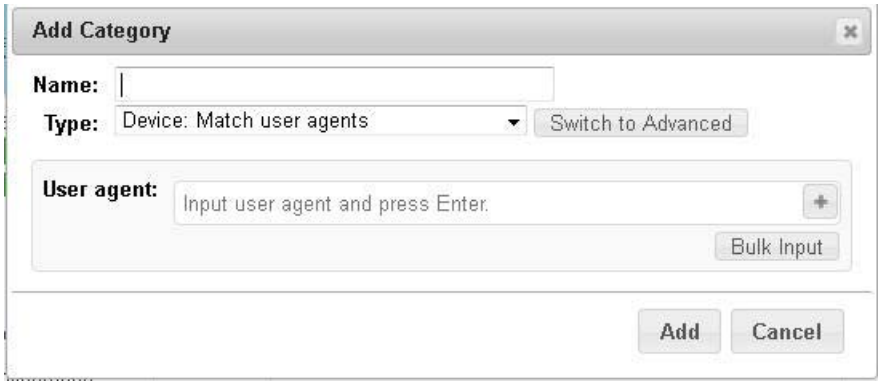
b. If you choose Network: Match service IP networks or Network: Exclude service IP networks from the Type drop-down list, enter a service IP network in the text box to match or exclude.

Figure 4-17 Add Network



c. f you choose Device: Match user agents or Device: Exclude user agents from the Type drop-down list, enter a user agent in the text box to match or exclude.

Figure 4-18 Add Device



Step 6 Click **Add** to add the category.

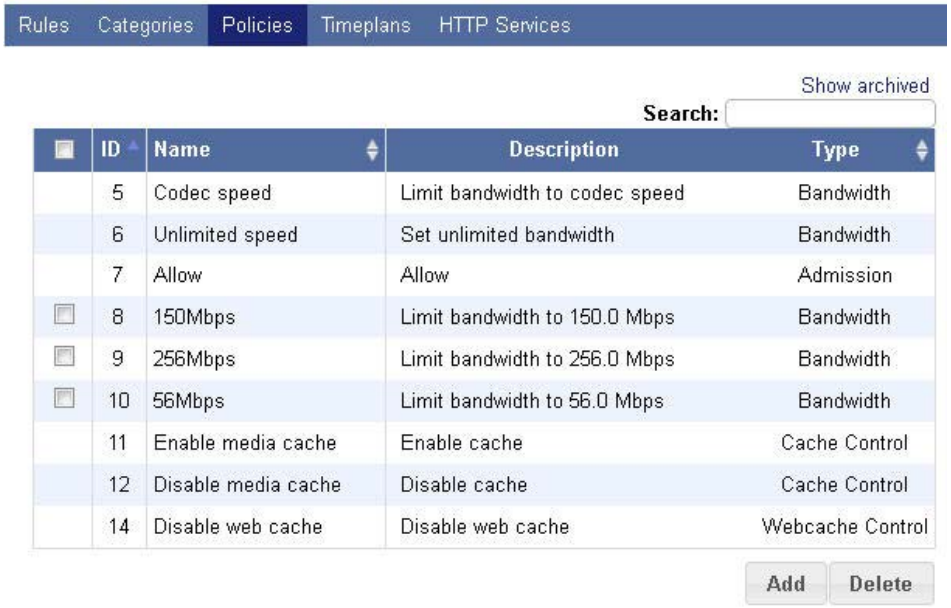
Step 7 After you add a category, for that category to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Policies

The policy configuration is a list of rules that you can apply to one or more categories.

All *explicitly* created policies are global and are not connected to any specific configuration. If you change a global policy, it is changed in all of the configuration versions. Global policies display when you click the Policies tab. All *implicitly* created policies are connected to their rules. Implicit policies are not shown in the policies list and are deleted with the rules.

Figure 4-19 Policy Manager, Policies Tab



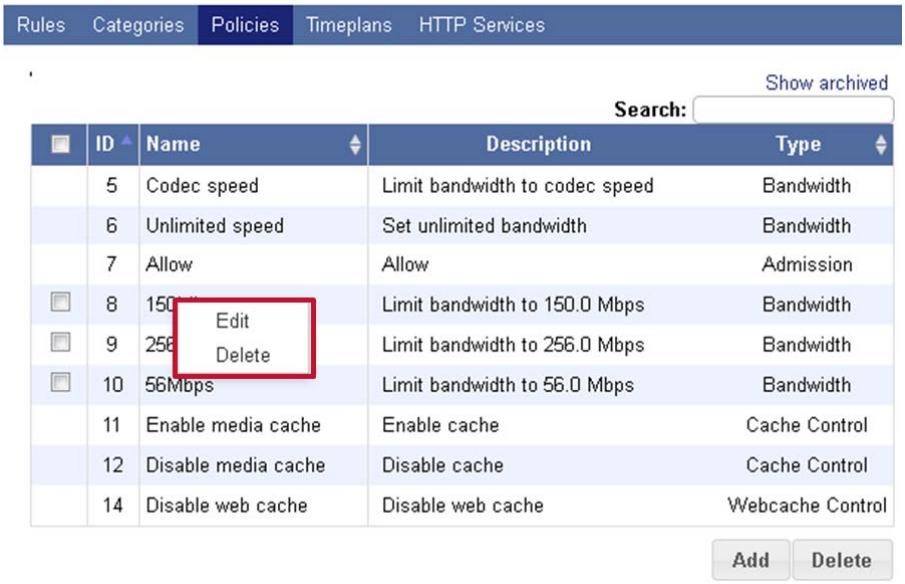
Editing Policies

Follow these steps to edit a policy:

Step 1 Open the Edit Policy dialog box. You can open this dialog box in two ways:

- Right-click a category and chose **Edit** from the pop-up menu.
- Click anywhere on the policy that you want to edit.

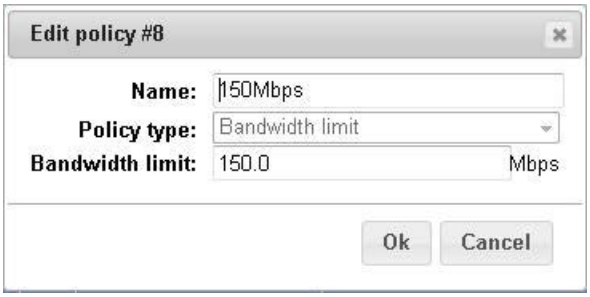
Figure 4-20 Edit Policy



Note When you right-click a policy you can edit the policy or you can delete the policy.

The Edit Policy dialog box appears.

Figure 4-21 Edit Policy Dialog Box



Step 2 From the Edit Policy dialog box, edit the following fields as needed:

- **Name:** Enter a new name if desired.
- **Bandwidth:** Enter a new bandwidth in the bandwidth field if desired.

Step 3 Click **OK** to save the changes.

Step 4 After you make changes to policies, for those changes to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Policies

Follow these steps to add a policy:

Step 1 Click the **Add** button at the bottom of the policies list.

Step 2 In the Name field, enter a policy name.

Step 3 In the Policy Type drop-down list, choose one of the following policy types:

- Bandwidth Limit
- Admission
- DSCP

a. If you choose Bandwidth Limit for the policy type, enter a bandwidth in the Bandwidth Limit field.

Figure 4-22 Bandwidth Policy

b. If you choose Admission for the policy type, from the Action drop-down list choose either Redirect or Block.

– If you choose Redirect, enter the URI to which you want users to be forwarded.

Figure 4-23 Admission Policy, Redirect Action

– If you choose Block, choose the error code that you want returned to the user. An example of an error code is “404: Page not found”.

Figure 4-24 Admission Policy, Block Action

c. If you choose DSCP for the policy type, from the Mode drop-down list choose one of the following:

- Preserve: Maintains the present packet DSCP mark
- Overwrite: Rewrites a new DSCP mark with the value you enter in the DSCP field
- Bitwise OR: Adds the DSCP mark you enter in the DSCP field to the present mark

Figure 4-25 DSCP Policy

Step 4 Click **Add** to add the policy.

Step 5 After you add a policy, for that policy to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Timeplans

Timeplans allow you to create schedules that activate a rule at certain times. From the Timeplans tab you can create, edit, or delete a timeplan.

Follow these steps to manage timeplans:

Step 1 In the Cisco VDS TC Manager window choose **Configuration > Policy Manager**.

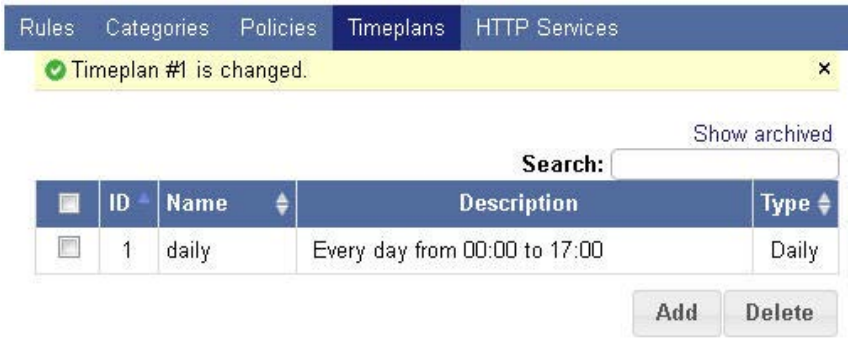
Step 2 Click the **Timeplans** tab. The list of timeplans appears in the work area.

The list of timeplans contains the following columns:

- **Check box:** A check box in the row indicates that you can edit the timeplan.
- **ID:** An identifying number

- **Name:** The name of the timeplan
- **Description:** A brief description of the timeplan
- **Type:** The type of timeplan. A timeplan can be one of the following types:
  - **Daily:** Enables the user to add several time ranges.
  - **Weekly:** Enables the user to add several weekdays with daily parameters.
  - **Monthly:** Enables the user to add several months and days with daily parameters.
  - **Yearly:** Enables the user to add several months and monthly parameters.

Figure 4-26 Timeplans Tab



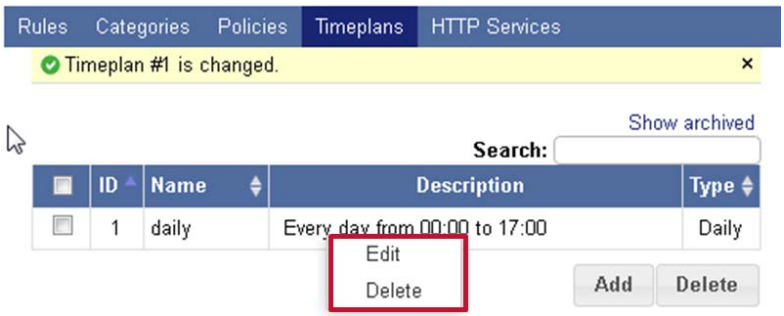
Editing Timeplans

Follow these steps to edit a timeplan:

Step 1 Open the Edit Timeplan dialog box. You can open this dialog box in two ways:

- Right-click a timeplan and chose **Edit** from the pop-up menu.
- Click anywhere on the timeplan that you want to edit.

Figure 4-27 Edit Timeplan



Note When you right-click a timeplan you can edit the timeplan or you can delete the timeplan.

The Edit Timeplan dialog box appears.

Figure 4-28 Edit Timeplan Dialog Box

Step 2 From the Edit Timeplan dialog box, edit the following fields as needed:

- **Name:** Enter a new name if desired.
- **Time:** From the Time fields choose a starting time and an ending time.

Note You cannot change the Recurrence type when you edit the timeplan.

Step 3 Click **OK** to save the changes.

Step 4 After you make changes to timeplans, for those changes to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Daily Timeplans

Follow these steps to add a timeplan that recurs daily:

Step 1 From the Timeplans tab, click **Add** at the bottom of the timeplans list. The Add Timeplans dialog box appears.

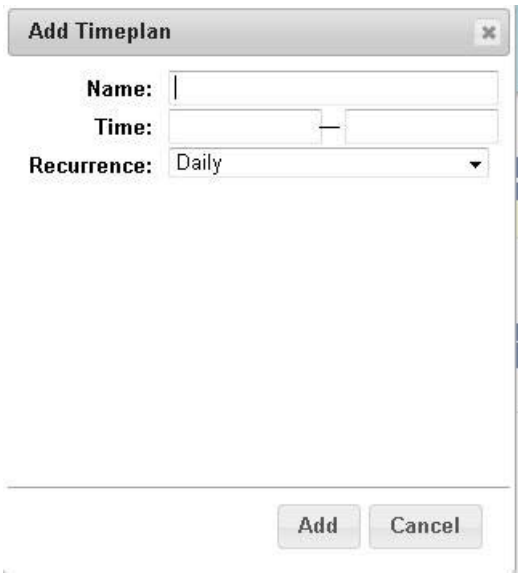
Step 2 In the Name field, enter a name.

Step 3 In the first box in the Time field, choose a start time. In the second box in the Time field, choose an end time.

Step 4 In the Recurrence field, make sure **Daily** is selected. This is the default recurrence type.

Step 5 Click **Add** to add the timeplan.

Figure 4-29 Add Daily Timeplan



Step 6 After you add a timeplan, for that timeplan to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Weekly Timeplans

Follow these steps to add a timeplan that has a recurrence of weekly:

Step 1 From the Timeplans tab, click **Add** at the bottom of the timeplans list. The Add Timeplans dialog box appears.

Step 2 In the Name field, enter a name.

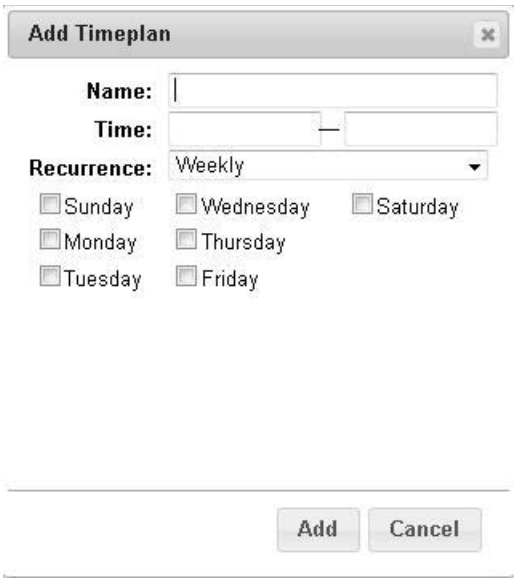
Step 3 In the first box in the Time field, choose a start time. In the second box in the Time field, choose an end time.

Step 4 In the Recurrence field, choose **Weekly**.

Step 5 Check the check boxes for the days of the week that you want to add to the timeplan.

Step 6 Click **Add** to add the timeplan.

Figure 4-30 Add Weekly Timeplan



Step 7 After you add a timeplan, for that timeplan to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Monthly Timeplans

Follow these steps to add a timeplan that has a recurrence of monthly:

Step 1 From the Timeplans tab, click **Add** at the bottom of the timeplans list. The Add Timeplans dialog box appears.

Step 2 In the Name field, enter a name.

Step 3 In the first box in the Time field, choose a start time. In the second box in the Time field, choose an end time.

Step 4 In the Recurrence field, choose **Monthly**.

Step 5 From the Day drop-down list choose the day that you want for the timeplan.

Step 6 Click **Add** to add the timeplan.

Figure 4-31 Add Monthly Timeplan

Step 7 After you add a timeplan, for that timeplan to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding Yearly Timeplans

Follow these steps to add a timeplan that has a recurrence of yearly:

Step 1 From the Timeplans tab, click **Add** at the bottom of the timeplans list. The Add Timeplans dialog box appears.

Step 2 In the Name field, enter a name.

Step 3 In the first box in the Time field, choose a start time. In the second box in the Time field, choose an end time.

Step 4 In the Recurrence field, choose **Yearly**.

Step 5 Check the check boxes for the months that you would like to include in the timeplan.

Step 6 Click **Add** to add the timeplan.

Figure 4-32 Add Yearly Timeplan

Step 7 After you add a timeplan, for that timeplan to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

HTTP Services

The HTTP Services option enable you to group HTTP Service specific subject categories together. From the HTTP Services tab you can add, delete, or edit HTTP Services groups. The HTTP Services tab is divided into four columns:

- **Check box:** A check box in the row indicates that you can edit the group.
- **ID:** An identifying number
- **Name:** The name of the HTTP group

Figure 4-33 HTTP Services Tab

Editing HTTP Services Groups

Follow these steps to edit an HTTP Services group:

Step 1 Open the Edit HTTP Service dialog box. You can open this dialog box in two ways:

- Right-click an HTTP Services group and choose **Edit** from the pop-up menu.
- Click anywhere on the HTTP Services group that you want to edit.

Figure 4-34 Editing an HTTP Services Group

Note When you right-click a group you can edit the group, add a group before or after an existing group, or you can delete the group.

The Edit HTTP Service dialog box appears.

Figure 4-35 Edit HTTP Service Dialog Box

Step 2 From the Edit HTTP Service dialog box, edit the following fields as needed:

- **Name:** Enter a new name if desired.
- **Categories Field:** If you want to delete one of the services, click the **X** for the service. To add a service, click within the Services field and choose an available service.

Step 3 Click **OK** to finish editing the group.

Step 4 After you make changes to HTTP Services groups, for those changes to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Adding an HTTP Services Group

Follow these steps to add an HTTP Services group:

Note The HTTP Service tab only allows the service category to be entered.

Note Remember to adjust your action order by your priority. For example, if you entered Gaming last, and Video Streaming is first, but you need Gaming to be first in priority, you must use the action arrows to move the Gaming to first priority.

Step 1 Click **Add** at the bottom of the group list. The Add HTTP Service dialog box appears.

Figure 4-36 Add HTTP Service

Step 2 In the Name field, enter a name for the group.

Step 3 Click within the Services field and choose an available service. Continue to add services as needed.

Step 4 Click **OK** to finishing adding the group.

Step 5 After you add a HTTP Services group, for that group to take effect on the system, you must publish the changes. To publish the changes, *see* the Publish the Configuration section.

Publish the Configuration

For changes that you make to the rules, categories, policies, timeplans, and HTTP Services groups to take effect, you must publish these changes. To publish the changes follow these steps:

Step 1 Click the **Rules** tab.

Step 2 In the right-hand side of the window, click **Publish**.

Step 3 After the policy is successfully published to the system, the message "Configuration is Published" displays at the top of the Rules window.

Note If you have multiple changes to make to the policies on the VDS TC system, wait to publish the changes until you have finished all of the changes.

The License Manager

The License Manager is used to view the current license and to install a new license if needed.

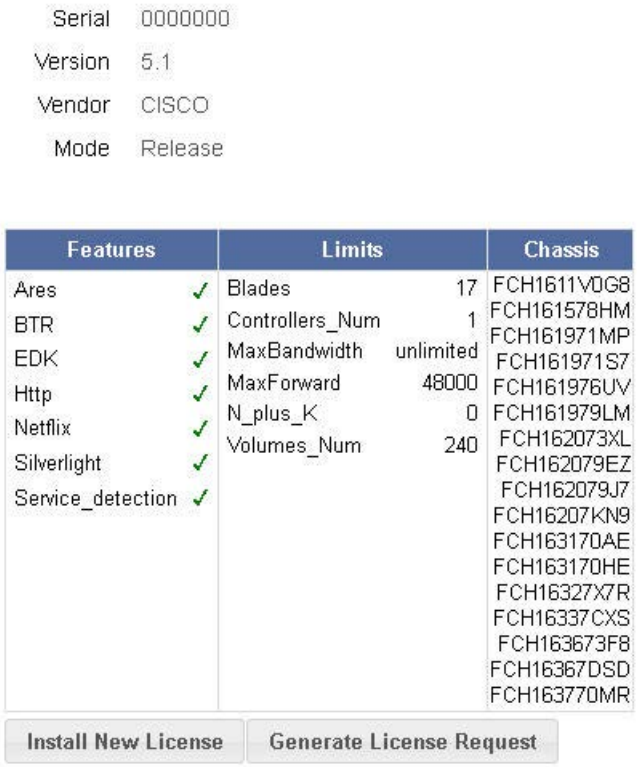
Follow these steps to open the License Manager:

Step 1 In the Cisco VDS TC Manager window choose **Configuration > License Manager**.

The License Manager window displays the following information:

- The heading displays the serial number, version, license mode, and start and end dates for the license if it is an evaluation license.
- The Features column lists the features that are included with the license.
- The Limits column displays the limits of the license.
- The Chassis column displays the chassis number. For a cluster configuration this column shows the chassis number for each chassis.

Figure 4-37 License Manager Window



Generating a License Request

Follow these steps to generate a new license request:

Step 1 From the License Manager window click the **Generate License Request** button. The Open license-request dialog window appears.

Step 2 Click **Save File** and then **OK** to save the file request.

Step 3 Enter a name and location of the file to save. You must send this file to Cisco support to receive a license file.

Note You must request a new license if you are upgrading from any previous version of VDS TC to VDS TC 5.6.1. You also must request a new license if you are upgrading the capacity of your VDS TC installation.

Installing a New License

Follow these steps to install a new license:

Step 1 From the License Manager window click the **Install New License** button. The Install New License dialog box appears.

Step 2 From the Install New License dialog box click **Browse** and navigate to the license file that you want to install.

Step 3 After the file is displayed in the Select License field, click **Install**.

Figure 4-38 Install New License Dialog Box

License Enforcement

Cisco VDS TC is a licensed application. The amount of traffic that Cisco VDS TC can process depends on the value that is specified in the license file that you install on the VDS TC Cluster or Integrated Appliance installation. This license is typically referred to as a Forwarding license.

The total number of Gigabits per second (Gbps) that are directed to the Cisco VDS TC application for processing is determined by the Forwarding license. This MaxForward license setting covers all downstream and upstream traffic; from the network to the subscribers (downstream [DS]) and from the subscribers to the network (upstream [US]).

The amount of cache generated traffic (Cache Out) that is sent to the subscribers is added to the forwarding license and is limited by the Cluster or the Integrated Appliance specification. For example, if a single cache engine can forward X Gbps and serve up to Y Gbps of cache generated traffic, the cache engine will be able to serve X+Y Gbps.

License Enforcement Functionality

The Cisco VDS TC application uses the License mechanism to determine how much forwarding capacity there is to process subscriber requests. The processing of requests include operations such as verify, cache-in, and cache-out. Once the licensed Forwarding capacity is exceeded, these operations are not performed for the traffic that exceeds the Forwarding capacity.

License Measurements and Warnings

During operation, the VDS TC platform (standalone or cluster) monitors how much traffic is directed to each cache engine. The forwarded traffic is measured as an average over two hours, taking into account only 90% of the samples, so that traffic spikes can be accommodated.

When the forwarded traffic reaches 90% of what is allowed by the forwarding license, the following warning message is sent to the log and is displayed on VDS TC Manager GUI in the System Events section of the Status > Dashboard, once a day for each cache engine:

```
ce-1 license forwarding almost exceeded
```

In addition, the cache engine will generate an SNMP trap for this critical alarm once per day. No license enforcement actions are taken by the Cisco VDS-TC application at this point.

Exceeded License

The first time that the traffic that is redirected to the Cisco VDS TC solution reaches 120% of what the Forwarding license allows, the system starts a 30 day count down. The platform will also send a one-time message to the log and display the message on VDS-TC Manager GUI in System Events section of the Status > Dashboard, once for each cache engine.

```
ce-10 license forwarding exceeded
```

In addition, the cache engine generates an SNMP trap for this critical alarm once per day. No license enforcement actions are taken by the Cisco VDS TC Application at this stage.

License Enforcement

When the 30 day countdown ends, the platform generates the following one-time message to the log and Cisco VDS TC Manager GUI, for each cache engine:

```
ce-1 license forwarding enforcement started
```

In addition, the cache engine will generate an SNMP trap for this critical alarm once per day. Every time the measured traffic goes above 120% of the licensed Forwarding traffic, the platform will enforce the license on all traffic above the “MaxForward” value.

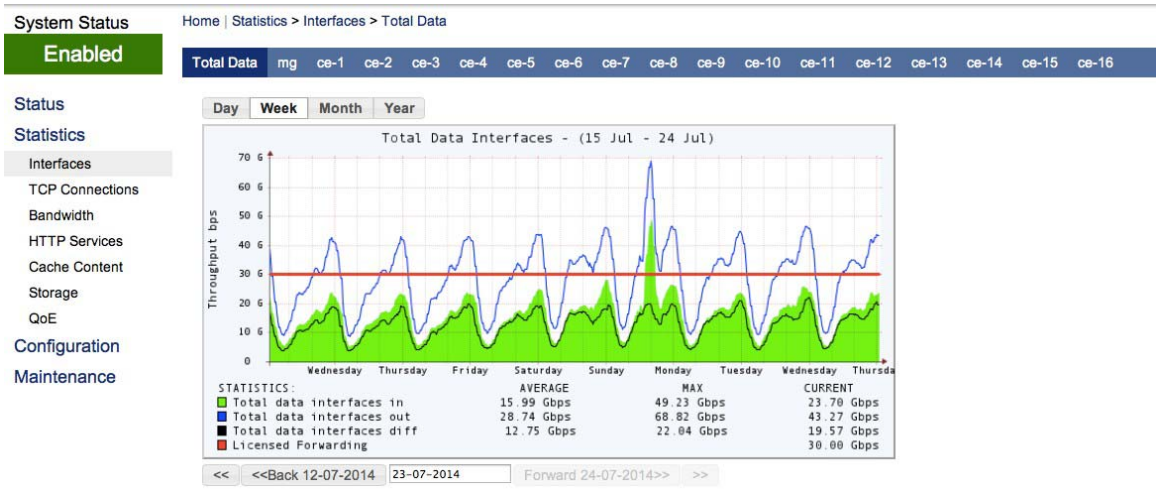
When the Forwarding license enforcement begins, all traffic that goes above the “MaxForward” limit of the Forwarding license is forwarded only and is *not* processed by the cache. In other words, this traffic will not be analyzed for popular content, will not be cached-in, and will not generate cache out.

Licensed Forwarding Example in VDS TC Manager

In the following example, which shows a weekly total data interface view, the platform displays the total data on all interfaces with a red line that shows up after the forwarded traffic license is exceeded for the first time.

When license enforcement occurs, all the traffic that is above the red line is forwarded and is not used to generate cache content.

Figure 4-39 License Enforcement Shown on Total Data Graph

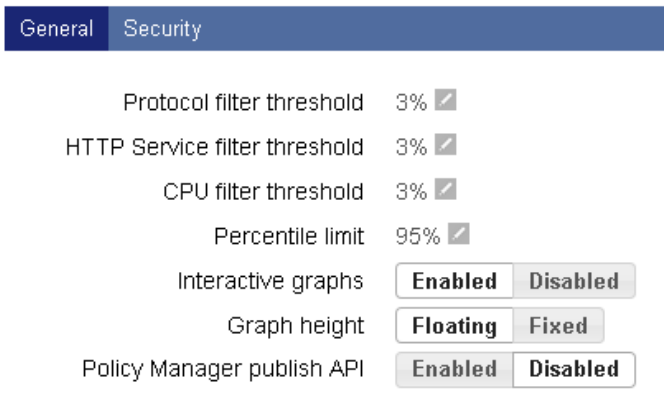


Settings

The Settings window enables you to change thresholds and change or reset the Admin password and the Enable password. Follow these steps to access the Settings window:

Step 1 In the Cisco VDS TC Manager window choose **Configuration > Settings**.

Figure 4-40 Settings Window



General

The General tab allows the user to change the following thresholds:

- **Protocol filter threshold:** The protocols displayed on the Bandwidth graphs are filtered using this threshold. If the MAX AVG outgoing traffic for the protocol for a displayed period is less than the threshold (of total outgoing traffic), the protocol is not shown.
- **HTTP Service filter threshold:** The protocols displayed on the HTTP Service graphs are filtered using this threshold. If the MAX AVG outgoing traffic for the HTTP Services for a displayed period is less than the threshold (of total outgoing traffic), the protocol is not shown.
- **CPU filter threshold:** The protocols displayed on the CPU Utilization graphs are filtered using this threshold. If the MAX AVG CPU traffic for a CPU graph is displayed for a period is less than the threshold, the protocol is not shown.
- **Percentile limit:** This is the Cache Out percentile of the Statistics > Bandwidth > Percentile graph.

To change any of the thresholds, click the pencil icon of the threshold and enter a new value.

From the General tab you can also configure the following:

- **Interactive Graphs:** Click **Enabled** to use interactive graphs or click **Disabled** to disable the interactive graphs feature.
- **Graph height:** The height of the graph can be displayed by either a fixed position or a floating position by clicking the appropriate button.
- **Policy Manager publish API:** This is the Cache Out percentile of the Statistics > Bandwidth > Percentile graph.

Changing or Resetting Passwords

Follow these steps to change the Enable password:

Step 1 Choose **Configuration > Settings** and click the **Security** tab.

Step 2 In the Security window next to Enable Password, click the pencil icon. If the password is still the default, the word *default* will appear before the icon.

Step 3 In the Enable password text box that appears, enter the new password.

Step 4 In the Repeat text box, re-enter the new password.

Step 5 Click the check mark button to save the changes.

Figure 4-41 Changing Passwords

Maintenance Menu

This chapter describes how to use the options that are available from the Maintenance menu.

Note To access the Maintenance menu, you must be logged into VDS TC Manager with a user that has these privileges. Contact your Cisco account system engineer if you need this information.

The following choices are available from the Maintenance menu:

- **Upload Files:** From this window you can upload a file to the TFTP directory on the server for Cisco VDS TC Manager operations. See the Upload Files section.
- **Logs:** From this window you can generate and export the system logs for a specific period of time. See the Logs section.
- **Graphs:** From this window you can generate and export all Cisco VDS TC Manager statistics graphs of the last day, last week, and last month. See the Graphs section.
- **Cache Lists:** This window enables you to export the Cached List report. See the Cache Lists section.
- **UI Log:** This window displays the log of processes that are executing in the background of VDS TC Manager. See the UI Log section.

Upload Files

The Upload Files page enables you to upload a file to the /tftpboot directory on the server for use with CLI operations. For more information about the CLI, see the “Cisco Videoscape Distribution Suite Transparent Caching Software Configuration Guide”.

Follow these steps to upload a file to the /tftpboot directory:

Step 1 In the Cisco VDS TC Manager window choose **Maintenance** > **Upload Files**.

Step 2 In the menu bar on the left, click **Upload Files**. The Upload File window appears.

Figure 5-1 Upload Files Window

Step 3 Click **Browse** and choose the file that you want to upload. Wait as the action completes.

Step 4 Click **Upload File**. The file is uploaded to the server.

Logs

The Logs window enables you to export the system logs for a specific period of time. If the system is a Cluster, it will export the logs from all servers within that Cluster system, including the Management Server.

Follow these steps to export the system logs:

Step 1 In the Cisco VDS TC Manager window choose **Maintenance > Logs**. The Logs window appears

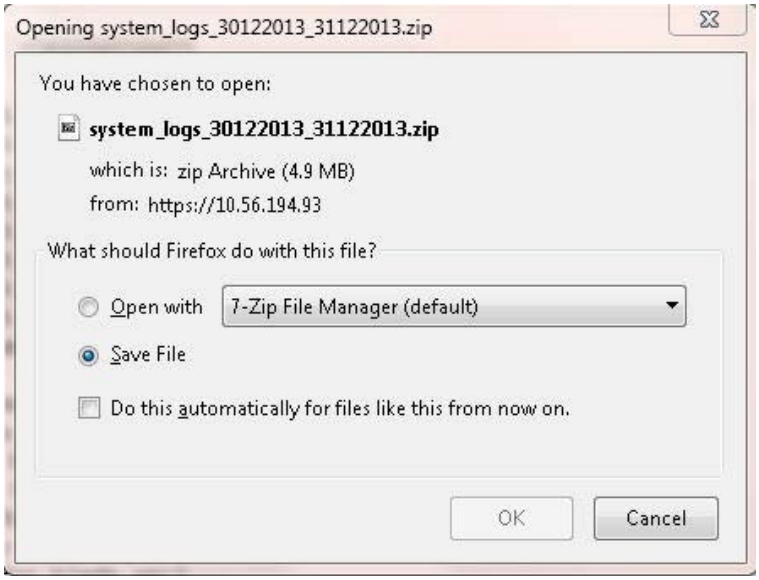
Step 2 In the From: field, enter a starting date and in the To: field enter an ending date.

Step 3 Click Export Logs. You will see the log file being processed.

Figure 5-2 Log File Processing

Step 4 After the log file is generated, the Export Logs file popup window appears.

Figure 5-3 Export Log Dialog



Step 5 Choose to **Open** or **Save** the file. If you choose to save the file, enter the location and file name in the File Save dialog box.

Step 6 Click **OK**.

Graphs

The Graphs window enables you to generate and export the graphs of the traffic information. The Graphs window enables you to save the graphs locally, which can then be exported to all Cisco VDS TC Manager statistics graphs of the last day, last week, and last month. The exported zip file will create subfolders for each type of statistics group that correspond to the GUI statistics menu items. You can access these folders by clicking the down arrow located at the top right of the location bar of the Internet Browser. The graphs are saved in png format (*.png).

Follow these steps to export the graphs:

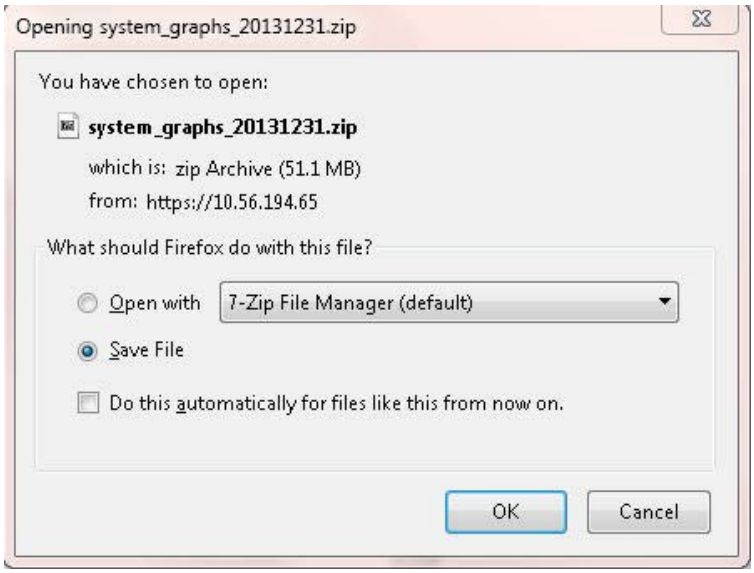
Step 1 In the Cisco VDS TC Manager window choose **Maintenance > Graphs**. The Graphs window appears.

Step 2 Click **Export Graphs**. You will see the graph file being processed.

Figure 5-4 Graphs being processed

Step 3 After the graph file is generated, the Export Graphs file popup window appears.

Figure 5-5 Export Graphs Dialog



Step 4 Choose to **Open** or **Save** the file. If you choose to save the file, enter the location and file name in the File Save dialog box.

Step 5 Click **OK**.

Cache Lists

From the Cache Lists window you can export the cached hash list and the cache black list.

Export Cache List

The Cached List window enables you export the cached hashes list. A cached hashes report lists the hash ID, protocol, size (in bytes), and age (in days) of the hashes that are cached. You can modify this list only using the CLI. For more information about the CLI, see the "Cisco Videoscape Distribution Suite Transparent Caching Software Configuration Guide."

Follow these steps to export the cache list:

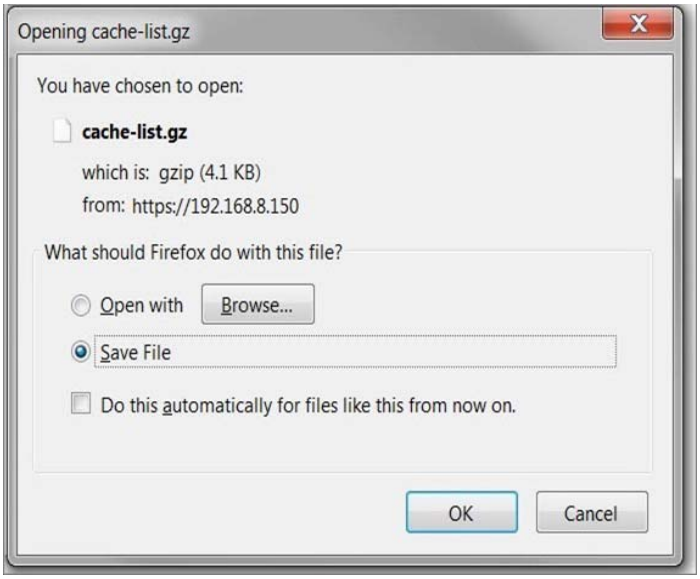
Step 1 In the Cisco VDS TC Manager window choose **Maintenance** > **Cache Lists**.

Step 2 Click the **Export Cache List** button.

Figure 5-6 Cache Lists Window

Step 3 After the cache list file is generated, the Export Cache List popup window appears.

Figure 5-7 Export Cache List Dialog



Step 4 Choose to **Open** or **Save** the file. If you choose to save the file, enter the location and file name in the File Save dialog box.

Step 5 Click **OK**.

Export Black List

The Export Black List button enables you to generate and export the Cache Black List (media objects). The Cache Black List allows you to save the lists locally, which can be accessed by clicking the down arrow located at the top right of the location bar of the Internet Browser.

Follow these steps to export the black list:

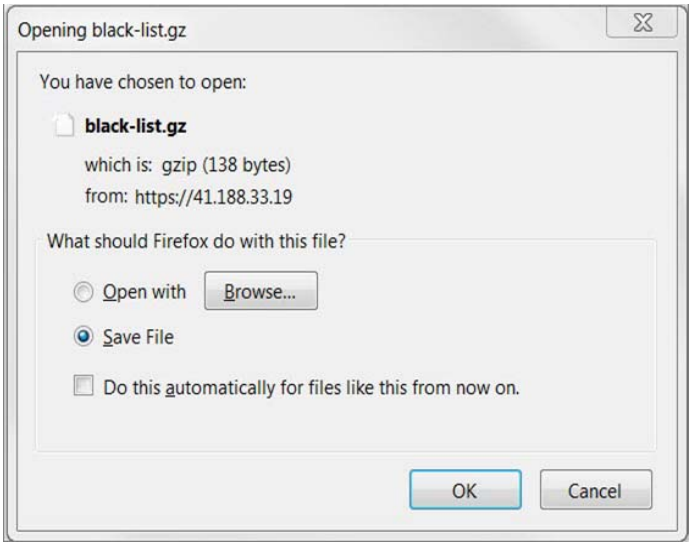
Step 1 In the Cisco VDS TC Manager window choose **Maintenance** > **Cache Lists**.

Step 2 Click the **Export Black List** button.

Figure 5-8 Cache Lists Window

Step 3 After the black list file is generated, the Export Black List popup window appears.

Figure 5-9 Export Black List Dialog



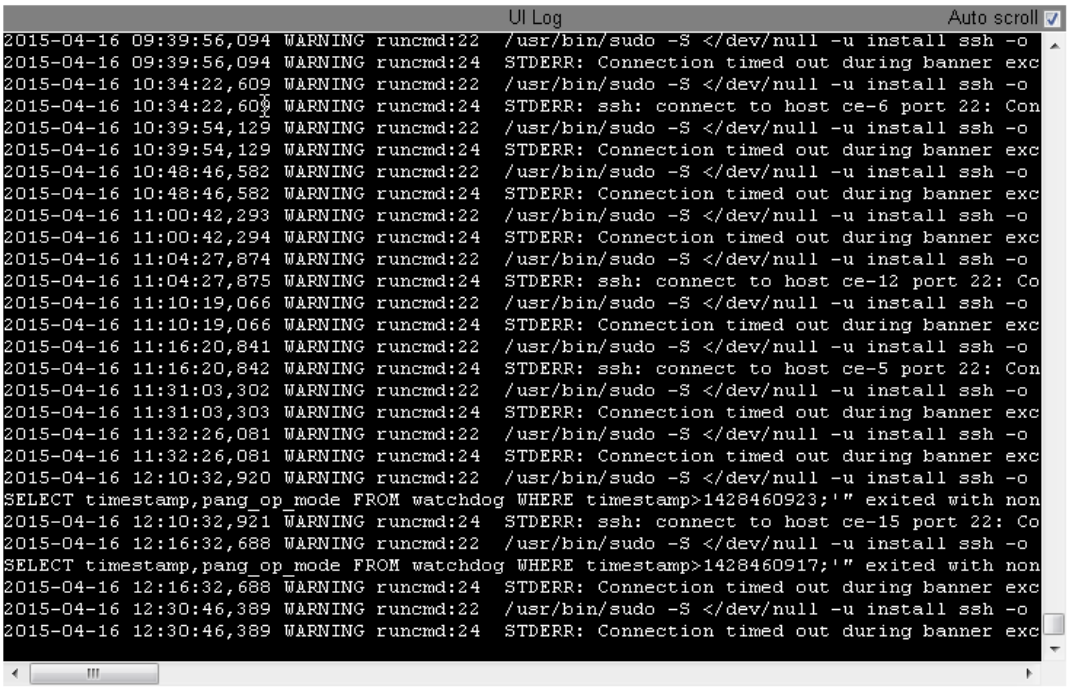
Step 4 Choose to **Open** or **Save** the file. If you choose to save the file, enter the location and file name in the File Save dialog box.

Step 5 Click **OK**.

UI Log

The UI Log option allows you to view all of the generated log messages that are generated in the background. Using this log can help you analyze graphs problems on the system.

Figure 5-10 UI Log



Basic Policy Example

Revised: August 2015, OL-28017-05

Basic Policy Management Example

This appendix provides an example of how to set up a policy within the Cisco VDS TC Manager environment.

Follow these steps to create a basic policy using VDS TC Manager:

Step 1 Log into VDS TC Manager with a user that has privileges to create and modify polices, such as director. If you are already logged into VDS TC Manager, you can switch users if needed, to log in with a user with the necessary privileges. To switch users, click **Logout** in the upper right-hand corner of the VDS TC Manager window and then log back in as a different user.

Step 2 If you are not already in the Policy Manager window, from the VDS TC Manager home page choose **Configuration > Policy Manager**.

Step 3 Click the **Categories** tab to open the Categories window.

Step 4 Click **Add** to add a new category. The Add Category dialog box appears. In this example you will create a category that refers to Internet Connection Sharing platforms.

Step 5 In the Name field, enter a name to help you identify this category. The example uses ICS-IS.

Step 6 From the Type drop-down list choose **Network** and ensure the **Match** radio button is selected.

Step 7 In the Input service network text box enter the IP address that you would like to match. In this example, the IP address is 112.0.71.11.

Step 8 Click the **Plus** (+) button to add the IP address.

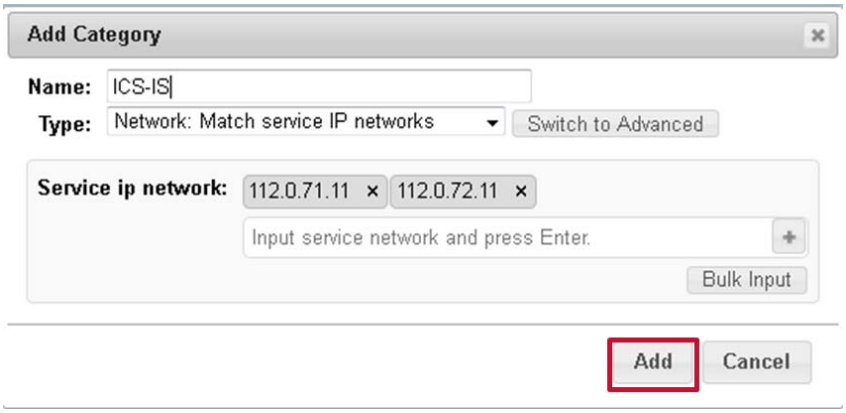
Figure A-1 Add Category Dialog Box

Step 9 If you would like to add another IP address to match, enter it in the new blank Input service network text box and click the **Plus** (+) button when you are done. In this example, the IP address 112.0.72.11 is also added.

Step 10 Repeat Step 9 until you have added all of the IP addresses.

Step 11 When you are finished adding the criteria, click **Add**.

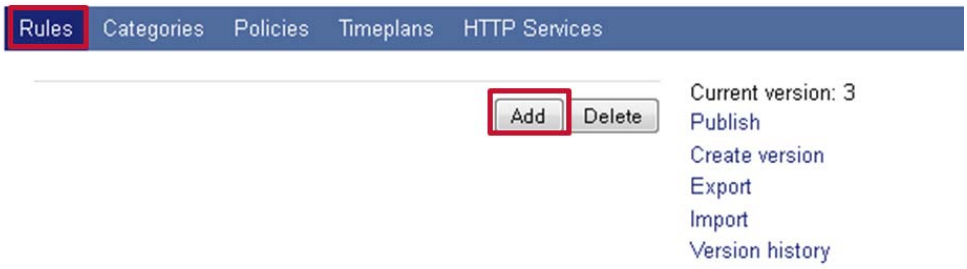
Figure A-2 Add Category



Step 12 You will now create a rule that references the ICS-IS category that you just created. This rule will prevent any caching of content that arrives from the IP addresses referenced in this category.

Step 13 Click the **Rules** tab to go to the Rules window and click the **Add** button.

Figure A-3 Rules Tab

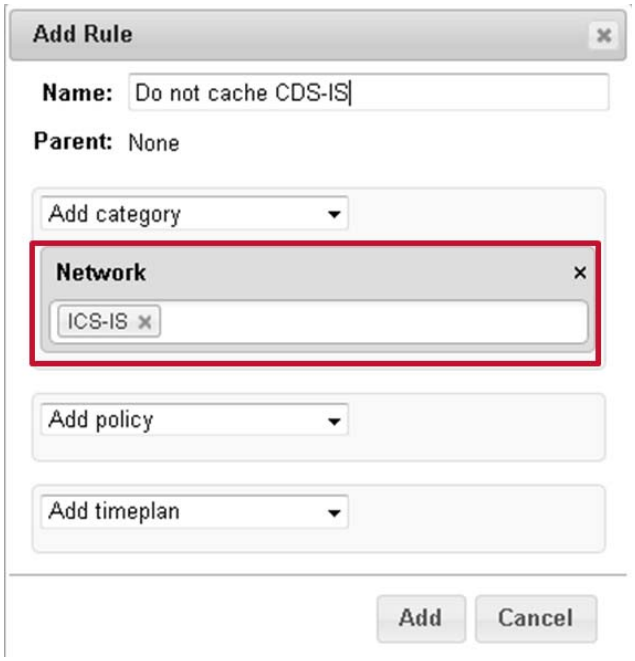


Step 14 The Add Rule dialog box appears. In the Name field, enter a name to help you identify the rule. The example uses “Do not cache CDS-IS”.

Step 15 From the Add Category drop-down list choose **Network**. You choose Network because that is the type of category that the ICS-IS category is.

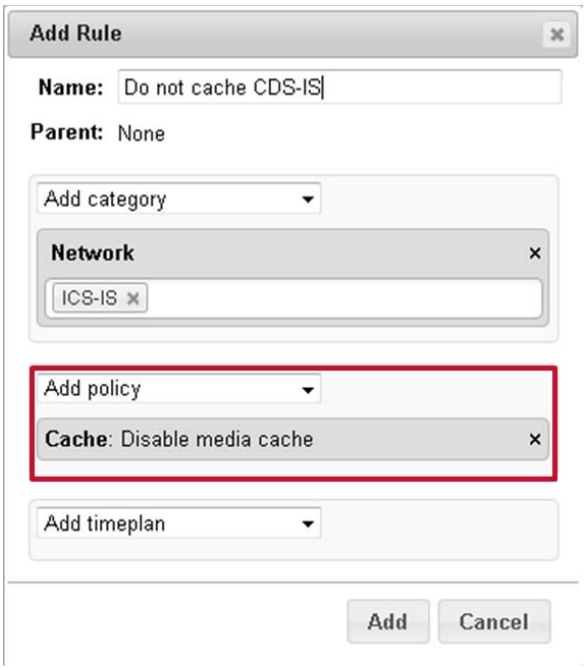
Step 16 From the Network field that appears, choose the category that you want, ICS-IS in this example.

Figure A-4 Rule Category



Step 17 From the Add Policy drop-down list choose **Cache > Disable Media Cache**.

Figure A-5



Step 18 Leave the Timeplan field empty, which will allow the rule to work all the time, and click **Add** to finish adding the rule.

Step 19 The rule is now in the system.

Step 20 To be able to use the newly created rule on the system, you must publish this policy into the production platform. To publish the policy, ensure the Rules tab is still selected and on the right-hand side of the window click **Publish**. After the policy is successfully published to the system, the message "Configuration is Published" displays at the top of the Rules window.

Figure A-6 Publish the Configuration