Secure Web

Bandwidth Management
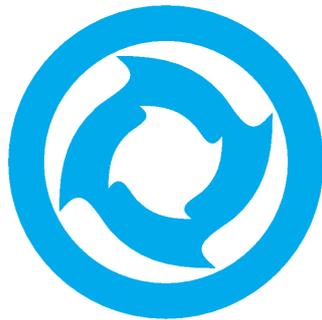
cyan

NETWORK SECURITY

Table of Contents

List of Figures

1. Introduction

1.1. About this Manual

This manual explains the Bandwidth Management module. It describes how to set up and operate a Secure Web installation with bandwidth management.

This manual is to be used with a CYAN Secure Web appliance with version 2.1.5 and above.

1.1.1. Document Conventions

	Indicates a potentially risky situation, leaving the appliance in an unusable state.
	Indicates a potentially risky situation, causing misfunction of the solutions.
	Indicates information that is substantial for successfully configuring and using the product.
	Provides helpful information for the process of configuring and using the product.
	Provides additional information about typical scenarios and best practices.

2. Bandwidth Management

2.1. Overview

Bandwidth Management for Secure Web gives the administrator possibilities to limit or scale certain traffic on the Secure Web Proxy.

The implementation of this feature is based on a tree of traffic profiles, each of them representing a certain down-/upstream bandwidth. Profiles are arranged in a tree, allowing each profile to grab unused traffic bandwidth from their parent in case their own contingent has been used up.

This system allows flexible assignments of network bandwidth and avoids underused bandwidth, which may happen if reserved bandwidth is not in use.

Bandwidth Profiles are then assigned to specific user Profiles and, to allow more detailed control over traffic, may be assigned to specific URL categories, Applications and Target Hosts.

> Please note that in cluster environments with load balancing in place, bandwidth management will be applied on a per-machine basis and not as a cluster-wide limitation of traffic.

2.2. Configuration overview

2.2.1. Bandwidth Profiles

Bandwidth Profiles define the down-/upstream limitations that may be used later to assign traffic through user Profiles. The configuration is layed out in a tree and can be found in *Services/Proxy Settings/Bandwidth Management* tab.
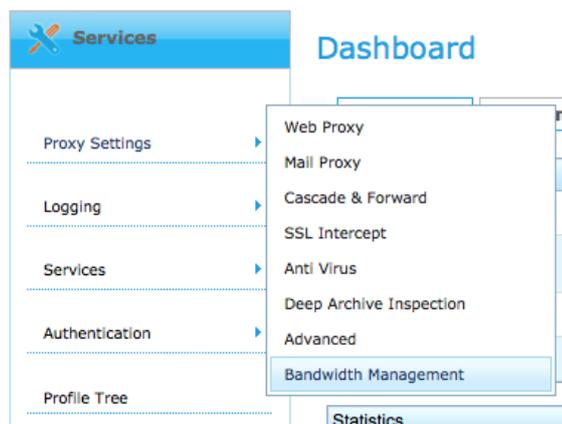

Figure 2.1. Navigation to Bandwidth Profile tree

The tree defines the available Bandwidth Profiles for later assignments through Profiles. Every tree node represent one Bandwidth Profile and defines down-/upstream limitations. The *Downstream* and *Upstream* columns show the available down- and upstream bandwidth for this Bandwidth Profile as well as bandwidth available from their parents. Through inheritance, all profiles may use their parent profiles bandwidth in case their own bandwidth has been used up. This avoids underused bandwidth that may be available on the network, but nobody using it.

Downstream is traffic coming from a web server back to the client. This may be a download, video stream or any kind of traffic from third-party applications that deliver content to the client.

Upstream is traffic being sent from the client to the web server. This may be a file upload, WebDAV uploads or any kind of traffic that is sent from your client to a server. The columns *Downstream* and *Upstream* show the Profile limitations (left value) as well as traffic bandwidth that is available from parent profiles (right value).

Figure 2.2. Example of a Bandwidth Profile tree

In the example configuration above, there are three Bandwidth Profiles defined:

- **Generic Traffic** defines the root of the bandwidth tree with a down- and upstream bandwidth of 4096 KB/s. All traffic assigned to this bucket will be limited to 4096 KB/s both up- and downstream.

- **Business Critical** is a child of *Generic Traffic* and allocates 4096 KB/s both up- and downstream for business critical traffic. If this traffic is used up, the profile will be allowed to use its parent profile *Generic Traffic* which adds another 4096 KB/s. Thus, the available traffic bandwidth for this Profile is a minimum of 4096 KB/s and up to 8192 KB/s depending on the utilization of the parent Profile.

- **Streams** is another child of *Generic Traffic* and allocates 2048 KB/s both up- and downstream for Audio/Video streams. Since this Profile is also a child of *Generic Traffic*, it may use up to another 4096 KB/s from *Generic Traffic* as well.

As a result, traffic assigned to Profile *Streams* has a minimum assigned bandwidth of 2048 KB/s and *Business Critical* 4096 KB/s. Generic Traffic, which is limited to 4096 KB/s is lower priority and has to share its bandwidth with its childs. At most, traffic assigned to *Generic Traffic* will be allowed to utilize 4096 KB/s. It may be less though, if either *Business Critical* or *Streams* utilize more than their assigned bandwidth.

2.2.2. Profile Settings

Assignment of traffic to specific Bandwidth Profiles is done through Profile Settings. This allows bandwidth management on a per user, group and IP basis through the well known Profile Management of Secure Web.

Figure 2.3. Profile Management general settings

- **Bandwidth Management** controls if bandwidth management should be performed for this profile at all.

- **Default Bandwidth Profile** defines the Bandwidth Profile to use if no other decision based on Category, Application or Target Host can be made.

- **Evaluation order** controls in which order assignment of traffic should be made (from top to bottom). Evaluation will be performed as long as no Bandwith Profile has been found assigned for specific traffic on a first-hit basis.

Assignment of traffic to a specific Bandwidth Profile can be made through various means. The order of evaluation, as defined above, controls in which order the information for a request is processed and a Bandwidth Profile assigned for traffic.

Figure 2.4. Profile Management Category settings

Every request passing the Secure Web Proxy engine is assigned a Category. Bandwith Profiles may be assigned to every Category, allowing Bandwidth Management on a per category basis.

Figure 2.5. Profile Management User-Defined Categories

Also user-defined categories can be the source of Bandwith Profile assignments. They have preceedence over general categories.

Figure 2.6. Profile Management Applications settings

Bandwidth Profiles can be assigned to Application Groups or specific Application Types. Application Types have preceedence over Groups, allowing fine-grined control for specific content.

Figure 2.7. Profile Management Target Hosts settings

For user-specific Bandwidth Profile assignments based on target hosts, a list of these can be configured and Bandwidth Profiles assigned. The entries can be in any of Full Match, Wildcard Match or Regular Expression and follow the same semantics as found in other lists used throughout the Web Admin Interface.

2.3. Sample scenario

In this sample we implements simple bandwidth management ruleset with fixed bandwidth allocations. All traffic going through the Secure Web Proxy engine is assigned to a Bandwidth Profile. There is shared traffic implemented to avoid underused available bandwidth.

Figure 2.8. Bandwidth Management sample

We define three Bandwidth Profiles *Business Critical*, *Streams* and *Web*. A root Bandwidth Profile *Root* is defined for shared bandwidth across the other profiles. The companies internet backbone is set up with synchronous bandwidth of 20 MB/s (20240 KB/s), but only as much as 15 MB/s may be used for web traffic.

The idea is to allocate all traffic to one of these Bandwidth Profiles:

• *Business Critical* is allocated to Categories and Applications critical for the business. It is important for the business that traffic to these sites have highest priority and bandwidth available. For business critical applications, there is 8 MB/s allocated and an additional 1 MB/s of shared traffic.

• *Streams* is allocated to Audio/Video Category and Application. Employees are allowed to watch video streams, but should not overstress the available Internet bandwidth with it. For streams, there is 2 MB/s allocated and an additional 1 MB/s of shared traffic.

• *Web* is allocated for generic web traffic and set up as a default traffic class for anything else. For generic web traffic, there is 4 MB/s allocated an an additional 1 MB/s of shared traffic.

The available bandwidth of 15 MB/s is now completely distributed across the three child profiles (8 MB/s + 2 MB/s + 4 MB/s). 1 MB/s is shared through the parent profile and available for all three Bandwidth Profiles if needed.

Profiles are set up to inherit Bandwidth Management from the top profile, which happens to be the default setting when adding a new child profile. The top profile is set up as following:

Figure 2.9. Bandwidth Management sample

Bandwidth Management is enable in the top Profile. The *Default Bandwidth Profile* is set to *Web*. All traffic that is not assigned to any other Bandwidth Profile by means of Category, Application or Target Host is assigned to this traffic class. The *Evaluation Order* is changed to have *Target Host* as primary source (business critical sites are put in there), then *Application* and last *Category*.

Figure 2.10. Bandwidth Management sample

Primary source for traffic bandwidth assignments is through Target Hosts. We've identified a Microsoft SharePoint host, Exchange and the companies websites as the most critical environments and assign the *Business Critical* Bandwidth Profile.

Figure 2.11. Bandwidth Management sample

Secondary source is the Application. All Audio/Video and Adobe Flash Applications are assigned the *Streams* Bandwidth Profile.

Figure 2.12. Bandwidth Management sample

Last source to assig a Bandwidth Profile is based on the Category. Important business categories are assigned the *Business Critical* Bandwidth Profile. Some traffic that is classified as Music/ Radio Broadcast is assigned the *Streams* profile.

All reamining traffic that is not intified by any of these means is classified as generic web traffic and put into the *Web* Bandwidth Profile.

This model can be used to implement maximum bandwidth utilization for certain traffic based on Category, Application or Target Host. It favors business critical traffic by assigning most of the available bandwidth to it, leaving the rest shared across unrelevant applications like Audio/Video streams and generic web traffic.

Appendix A. Contact data

A.1. How to contact our sales department

Tel.:   +43 (1) 33933-0

Email: sales@cyan-networks.com

A.2. How to contact our support department

Tel.:   +43 (1) 33933-333

Email: support@cyan-networks.com

A.2.1. Getting Support

In case you should have any technical problems, or questions and would like to get support from our team, we kindly ask you to provide us with the following information:

• Description of your question or problem

• The version information of the product:

  • The version information of Secure Web can be found after logging into the Web Admin Interface in the top part of the screen:

Figure A.1. Version information of the Secure Web

  • The version information of the Reporting System can be found after login in the top part of the screen of the Web Admin Interface:

Figure A.2. Version information of the Reporting System

  • All the information contained in the screen found in menu *Services / Services / Overview*

• In the case authentication is activated, provide us with the method in place (via Windows Agent, via Linux Agent, etc.)

• The deployment method of the Appliance (Out-of-line, In-Line, DMZ)

• The operation mode of the Appliance (dedicated mode, transparent mode)

- Information about the environment (proxy cascades that are used, firewalls and gateways involved in the infrastructure that are of relevance to the Appliance)

The appliance interface provides the possibility to create a support package that includes the configuration and log files of the system. This package can help us to track down the issue easier and faster. Please attach this package to your e-mail.

In order to create a support pack, navigate to menu *Appliances / Maintenance / Support* and click on the *Download* button. You may select the files you want to provide to our support team and then download a package, which we kindly ask you to send to our support email address.

A support packages will be created with the following information included in the archive:

| Secure Web log files	✓
Secure Web configuration database	✓
System log files	✓
System info	✓
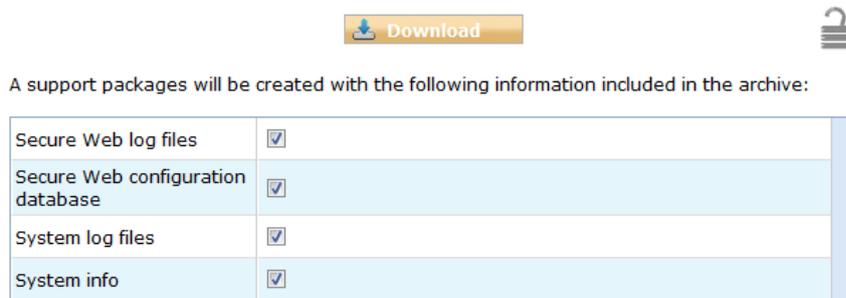
Figure A.3. Support Package

Further documentation about the product as well as technical white papers that describe certain use cases can be found in our documentation repository on our homepage:

http://www.cyan-networks.com/documentation