smoothwall®

The Web You Want

Bandwidth Shaping

Bandwidth Installation and Administration Guide

Smoothwall® Bandwidth, Installation and Administration Guide, December 2014

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Bandwidth.

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Bandwidth contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada: United Kingdom: All other countries:	1 800 959 3760 0870 1 999 500 +44 870 1 999 500
Fax	USA and Canada: United Kingdom: All other countries:	1 888 899 9164 0870 1 991 399 +44 870 1 991 399

Contents

About This Guide

Smoothwall Bandwidth is a licensed feature of your Smoothwall System.

This supplement provides guidance for installing and managing Bandwidth. For a detailed description of all other features of your Smoothwall System, refer to your *Smoothwall System Administration Guide*.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Bandwidth.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System
- An overall understanding of networking concepts

Organization and Use

This guide is made up of the following chapters and appendices:

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Bandwidth Shaping
Cross-references and references to other guides	Italics	See *Chapter 1, Introducing Bandwidth* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`
Smoothwall System	This may be one of: • Advanced Firewall • Unified Threat Management • Network Guardian • Secure Web Gateway • WAM-Edge depending on the license purchased	

This guide is written in such a way as to be printed on both sides of the paper.

Related Documentation

The following guides provide additional information relating to the Smoothwall System:

- *Smoothwall System's Administration Guide*, which describes how to configure your Smoothwall System
- *Smoothwall System's Operations Guide*, which describes how to use your Smoothwall System
- *Smoothwall System's User Portal Guide*, which describes how to use the user portal feature
- http://www.smoothwall.net/support contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introducing Bandwidth

This chapter introduces the Bandwidth shaping feature of your Smoothwall System, including:

Note: Bandwidth is a licenced feature. For more information, contact your Smoothwall representative.

About Bandwidth Shaping

Bandwidth shaping is a licenced feature of your Smoothwall System. Bandwidth allows you to shape the traffic throughput of specified external or bridged interfaces. It provides you with the ability to create multi-tiered, application-aware, bandwidth shaping policies.

Bandwidth provides the following features:

- The ability to create classes of service that guarantee bandwidth allocation to a specific IP address, or groups of IP addresses
- The ability to create classes of service that restrict available bandwidth for a specific IP address, or groups or IP addresses
- The ability to create classes of service that offer a “best efforts” bandwidth allocation
- The ability to guarantee a minimum bandwidth allocation available for specific applications
- The ability to restrict specific applications to a maximum bandwidth allocation
- The ability to equally reduce the quality of service within a class of service group

Note: Traffic to and from the Smoothwall System’s administration user interface, and SSH traffic to the Smoothwall System, is not limited, as an error in configuration may prevent access.

However, the following limitations apply:

- Only traffic using external, or bridged ports can be shaped.
- Bandwidth does not block applications from accessing the internet. For a detailed description of how to block applications, refer to your *Smoothwall System's Administration Guide*.
- Traffic that is redirected through Guardian is not classified as originating from the client, but from your Smoothwall System instead.

Note: Traffic shaping configured in the Guardian add-on module may overlap with configuration in Bandwidth. In such cases, both configuration rules are applied, however, the smallest limit always overrides the latter. For example, if Guardian has a policy to limit "news" traffic to two megabits per second, but Bandwidth limits all HTTP traffic to only one megabit per second, only the Bandwidth limit is applied.

About Application Classification

It should be noted that not all applications are classified perfectly. This particularly applies to protocols which are designed to avoid detection, such as BitTorrent, or some peer-to-peer protocols. In some cases, such traffic may be classified as `Unknown`.

Typically, such protocols use more bandwidth. To guarantee that the protocols are restricted, you can create a policy which restricts the amount of available bandwidth for unknown traffic, and add exceptions for allowed protocols. However, it should be noted that the majority of connections are initially classified as `Unknown` until several packets are sent. A policy which blocks those protocols, rather than restricts them, may be more practical.

Note: Encrypted, secure packets may be classified as SSL traffic where another application group does not exist. However, it should be noted that there are some protocols that were not originally encrypted, but may have been upgraded using SSL, so may be classified as such now. Also, there are some protocols which use SSL as part of their protocol specification, in which case, these may classified correctly.

For a detailed description of those classifications available in the Bandwidth module, see *Appendix A:Application Groups* on page 29.

Use Case Examples

The following are example scenarios where Bandwidth can be implemented.

A Hotel Guest Network

Network services can be tailored for each type of guest service at the hotel:

- A basic hotel internet service which provides enough bandwidth for general web browsing and email traffic. This may be a free service.
- A premium hotel internet service which provides additional bandwidth for online gaming, messaging services such as Skype™, and video streaming.

- Conference facilities can be assigned a guaranteed slice of bandwidth for video conferencing, VoIP, file transfer applications, and collaboration tools.

A Corporate Network

Business critical applications can be given priority over other applications. This can be further customized for each department, for example:

- Helpdesk staff are assigned a policy which gives priority to remote access applications, such as VPN, VNC, and TeamViewer™, followed by VoIP calls and email traffic. General web browsing is given the lowest priority.
- The Marketing department's policy prioritizes collaboration tools, such as Lotus Notes™ and WebEx Messenger™, and email traffic as equally important. General web browsing is given the lowest priority.
- A default policy for all other staff prioritizes email traffic over general web browsing.

A School Network

Bring your own device (BYOD) services can be limited to a specific bandwidth share per user, with access to some applications restricted to the point where they are virtually unusable.

- Video streaming services, such as YouTube, are severely restricted for all devices, including BYOD. Within dormitories however, access is allowed but capped.
- Messaging services, such as Skype, are allowed unlimited bandwidth within dormitories.
- Online gaming services are restricted for all devices, including BYOD, from all subnets.

2 Installing Bandwidth

This chapter describes how to install Bandwidth, including:

Prerequisites

Bandwidth is a licenced module that you add to your Smoothwall System. Before adding the module, you must ensure your Smoothwall System has the latest updates installed.

To update your Smoothwall System, do the following:

1. Log into your Smoothwall System, and browse to **System > Maintenance > Updates**.
2. Click **Refresh updates list** to ensure your Smoothwall System is up to date.

   Any updates not installed will appear in the **Available updates** panel.
3. Click **Download updates**.

   New updates not installed will appear in the **Pending updates** panel.
4. Click **Install updates**.

For a detailed description of how to schedule an update installation, refer to your *Smoothwall System's Administration Guide*.

Installing Bandwidth

You install Bandwidth through your Smoothwall System's user interface.

You do this as follows:

1. Log into your Smoothwall System, and browse to **System > Maintenance > Modules**.
2. Click **Refresh module list** if you do not see **Bandwidth** in the **Available modules** panel.

3. Select **Bandwidth**, and click **Install**.

Once installation has completed, you must reboot your Smoothwall System.

You do this as follows:

1. Browse to System > Maintenance > Shutdown.
2. Select **Immediately**, and click **Reboot**.
3. Once the reboot has finished, click the Smoothwall logo, and log back in.

Upgrading from SmoothTraffic

You cannot install and run SmoothTraffic at the same time as Bandwidth. Also, you cannot migrate configuration from a SmoothTraffic-licensed Smoothwall System to a Bandwidth-licensed Smoothwall System. You must configure Bandwidth separately.

3 Configuring Bandwidth

This chapter describes how to configure the Bandwidth module, including:

Tip: The order of configuration listed above is not fixed, it is a cyclical configuration procedure, depending on your operational needs. Additionally, Bandwidth is installed with pre-defined shaping policies that can be used without additional configuration. To configure additional policies, or adjust the pre-defined ones, see *Creating Bandwidth Shaping Policies* on page 13.

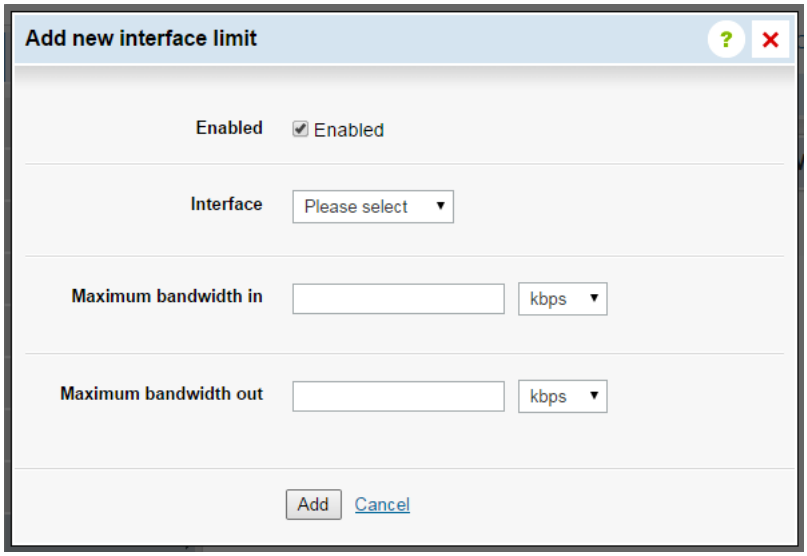
Configuring Bandwidth Interfaces

You must configure the available bandwidth for incoming and outgoing traffic, for each interface on your Smoothwall System that you want to shape. It is recommended that you configure slightly less than the expected maximum throughput of that interface to be certain of avoiding packet queues. Typically, this would be 95% of the expected maximum.

The following procedure assumes you have configured your Smoothwall System to either process external traffic, or as a bridge. For a detailed description of how to do either, refer to your *Smoothwall System's Administration Guide*.

You configure the interfaces to be shaped as follows:

1. From your Smoothwall System, browse to **Bandwidth > Control > Interfaces**.
2. Click **Add new interface limit**.



3. Ensure **Enabled** is selected.
4. From the **Interface** drop down list, select the relevant external interface.
5. Configure the appropriate amount of incoming and outgoing bandwidth for this interface.

   You can choose to configure the bandwidth as kilobits per second (**kbps**), or megabits per second (**Mbps**).
6. Click **Add**.

By default, all classes, including the **All traffic** class (see *Creating Bandwidth Classes* on page 10) will be assigned to the new interface, with the following pre-defined:

- **Use interface limits** (as defined in *step 5.*) for **Maximum bandwidth in**, and **Maximum bandwidth out**
- **Dynamic** share type — see *About Bandwidth Share Types* on page 12

To change this, click **Edit**. For a detailed description of how to share available bandwidth between classes, see *Allocating Bandwidth to Classes* on page 11.

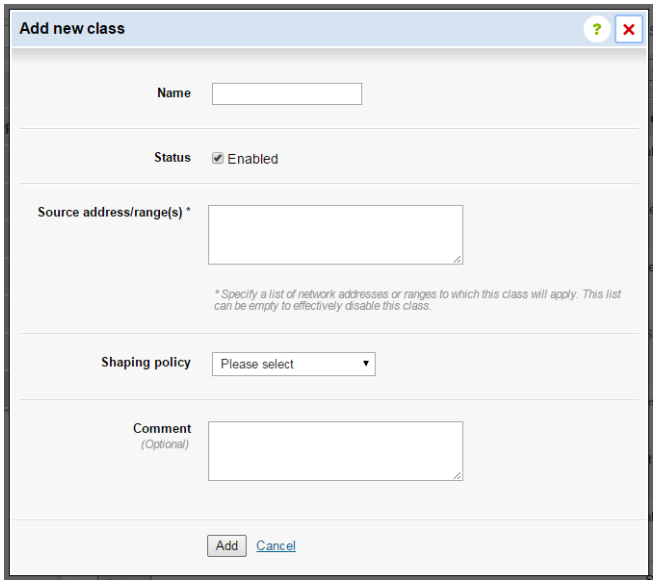
Creating Bandwidth Classes

A class is a group of users, defined by IP address. All users within the group receive the same quality of bandwidth service, as defined by the shaping policy.

The Bandwidth module comes with an **All traffic** class pre-defined. This is a “catch-all” class for traffic originating from an IP address not assigned to a existing class. The **Default** shaping policy is applied. For more information about shaping policies, see *Creating Bandwidth Shaping Policies* on page 13.

To create more classes, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Classes**.
2. Click **Add new class**.



3. Configure the following:
   - **Name** — Configure a meaningful name for this class.
   - **Status** — Leave this as enabled if this class is to be used immediately. Cancel the selection if this class is not to be used.
   - **Source address/range(s)** — List the IP addresses, and ranges that belong to this class. Leaving this box blank also disables this class.
   - **Shaping policy** — From the drop down list, choose the relevant policy.

Tip: You can leave this option blank if there isn't an appropriate policy configured, and add one at a later stage — see *Creating Bandwidth Shaping Policies* on page 13.

   - **Comment** — If required, add an optional comment about this class.
4. Click **Add**.

Allocating Bandwidth to Classes

Newly configured classes are automatically assigned a bandwidth limit for each interface configured on the **Interfaces** page. However, each class will be allocated the maximum bandwidth in and out (**Use interface limits**), with a share type of **Dynamic**.

About Bandwidth Share Types

Each bandwidth class can be given one of three different share types:

- **Dynamic** — This is a "best efforts" bandwidth share. A dynamic share is allocated a maximum slice of available bandwidth, however, the total allocated can exceed the maximum available bandwidth. If there is an excessive demand on bandwidth in total for the interface, the quality of service will be reduced for all in proportion to their allocation. If you have more than one bandwidth class with a Dynamic share type, the total bandwidth allocated to all classes can also exceed the maximum throughput for the interface.

  Use the dynamic sharing type to allow classes to use more bandwidth when it is spare, but share fairly when it is in demand.

  Typical use for a dynamic sharing type would be in a non-critical business or customer environment, such as a hotel lobby, school classrooms, or a company department that does not require guaranteed bandwidth services.

- **Guaranteed** — A guaranteed share is allocated a maximum amount of bandwidth which is guaranteed to the class, and which is not impacted by the performance of any other bandwidth sharing type. You cannot guarantee more than the total bandwidth available. If an allocated class does not use up its share, the remainder is temporarily available to use by other classes which have not reached their limit, but is immediately available should the allocated class require it.

  Use the guaranteed share type to protect important traffic in the event of excessive demand from other classes.

  Typical use for a guaranteed sharing type would be a hotel conference room, or a school classroom or company department running video training.

- **Per user** — Each IP address allocated to a class using a Per user bandwidth sharing type, is assigned a maximum bandwidth allocation. The total allocated may be more than the interface's maximum throughput if all IP addresses were in use at the same time. If there is excessive demand on bandwidth in total for that interface, the available bandwidth for each user is proportionally reduced.

  Use the per user share type to ensure users receive a fair share of bandwidth, unaffected by the usage of other users in the same class.

  Typical use for a per user sharing type would be for networks where users are not running critical applications, such as for individual guests at hotels. Bring your own device (BYOD) services are also supported through this policy.

Allocating Bandwidth

Note: You can assign a higher allocation to a dynamic, or per user policy, than is configured as the maximum for the shaped interface. This can express the relative importance of classes that are allowed to use the full bandwidth limit. If one class is allocated 200% of the bandwidth to use, and another 100%, both can use up the whole interface bandwidth individually. However, when both are in use at the same time, bandwidth is allocated using a 2:1 ratio.

To allocate bandwidth to classes, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Interfaces**.
2. From the **Interfaces** panel, click the expand arrow for the relevant interface to display the **Bandwidth shares** table.

All configured classes will be listed.

3. Highlight the relevant class, and click **Edit**.
4. Configure the following:
   - **Maximum bandwidth in** — You can choose to leave this allocation as **Use interface limits**, or allocate a slice of incoming, available bandwidth in kilobits per second (**kbps**) or megabits per second (**Mbps**)
   - **Maximum bandwidth out**— You can choose to leave this allocation as **Use interface limits**, or allocate a slice of outgoing, available bandwidth in kilobits per second (**kbps**) or megabits per second (**Mbps**)
   - **Type** — From the drop-down list, choose whether this allocation is **Dynamic**, **Guaranteed**, or **Per user**. For more information, see *About Bandwidth Share Types* on page 12.
5. Click **Save changes**.

Tip: Very small allocations are unreliable. Around 20 kilobits per second is a practical allocation.

Creating Bandwidth Shaping Policies

Shaping policies determine the bandwidth allocated to a number of applications. Each shaping policy is allocated a maximum incoming and outgoing bandwidth level, and a number of applications to share that allocation.

You can assign a shaping policy to more than one Bandwidth class.

About Application Weighting

You can use a weighting system to provide a level of preferred access to network bandwidth, for different applications. For example:

- Hotels artificially restricting video services over a free WiFi connection to encourage customers to use the premium service
- Businesses prioritizing VoIP traffic over video streaming

Applications, and application groups, can be given relative weights on a defined scale. When there is contention for bandwidth within a class, relative weighting is used to proportionately allocate bandwidth for the specified applications. A single application's weighting is calculated as a proportion of the total weighting for all applications, or application groups, for that shaping policy. The total share for a class does not depend upon which applications are in use.

Bandwidth shaping rules are applied before application weighting. Weighting is only used as a fairness measure when traffic exceeds the available bandwidth for that class.

About Application Caps

In addition to using an application weighting, you can also configure a cap on the bandwidth available for each application or application group. This can be used to provide an absolute restriction on particular services.

About Pre-Defined Shaping Policies

Bandwidth comes with the following pre-defined policies:

- **Business** — The Business policy defines bandwidth application slices and caps for the following services relevant for a corporate environment:
  - All Collaboration services, such as, SharePoint and WebEx
  - All Mail services, such as Exchange and POP3
  - Remote access services, such as remote desktop connections, and VPN/Tunneling services, such as OpenVPN

  This configuration gives priority to home working services. If there is excessive demand, Collaboration services receive half the allocation of Remote Access services, and Mail services receive half again. The Mail services slice is smaller as email packets tend to be small and non-interactive. All other services receive the same priority as home working services.
- **Control video streaming** — This policy defines bandwidth application slices and caps for the following services typically relevant for a video streaming environment:
  - Google Videos™, Hulu, NetFlix, RTMP, SHOUTcast

  This configuration gives priority to all other traffic. If there is excessive demand on bandwidth, named video streaming services will receive one tenth of the available bandwidth compared to all others.
- **Default** — This is the “catch-all” policy for those services that are not allocated to another bandwidth shaping policy. All traffic is treated fairly.
- **Limit file sharing** — This policy defines bandwidth application slices and caps for services relevant for peer-to-peer file sharing:
  - All File Transfer services, such as DropBox™

  This configuration gives priority to all other traffic. File transfer services will receive one tenth of the available bandwidth compared to all others, but are capped at 32 kilobits per second.
- **Slow video streaming** — This policy defines bandwidth application slices and caps for the following services typically relevant for a video streaming environment:
  - Google Video™ (including YouTube™), Hulu, NetFlix, RTMP, SHOUTcast

  This configuration caps available bandwidth for the specified services so that they are slow all the time.
- **Video conference** — This policy reserves up to 90% of allocated bandwidth for video conferencing. Desktop sharing is also included in this policy. The following services are defined:
  - All Collaboration services
  - All Messaging services
  - All Remote Access services
  - FaceTime, Google Video (including YouTube), H.225, H.245, H.323, Paltalk Video, PalTalk Voice, RTCP, RTMP, RTP, RTSP, SIP, Skype

  This configuration gives priority to all listed above.
- **Voice over IP** — This policy defines bandwidth application slices and caps for the following VoIP protocols:
  - FaceTime, H.225, H.245, H.323, MagicJack, Paltalk Voice, RTCP, RTP, RTSP, SIP, Skype, T-Mobile, Vonage

If there is excessive demand on bandwidth, this configuration provides a dedicated slice of bandwidth to specified services to avoid VoIP latency.

The pre-defined policies listed above are defined according to function, and can be altered to suit your own operational needs. However, you can create policies based on a single application, single application group, or a mixture of the above to suit a particular subnet. For example, a school may choose to create a policy which lists all individual applications that need to have restricted bandwidth which accessed from a classroom, and an additional policy that has less restrictive bandwidth for the same applications when accessed from a recreational area. For more information, see *Assigning Application Slices* on page 15.

Creating Shaping Policies

To create additional shaping policies, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Shaping policies**.
2. Click **Add new policy**.
3. Configure the following:
   - **Name** — Enter a meaningful name for the policy.
   - **Comment** — Enter an optional comment for this policy. You can view each policy's comments by clicking **Show comments** in the **Shaping policies** table.
4. Click **Add**.

Assigning Application Slices

Shaping policies determine the amount of bandwidth that *may* be used by specified applications. Additionally, you can prioritize bandwidth for specific applications, or application groups. You do this by slicing up the allocated bandwidth, according to the relative importance of the application. You can also apply an additional cap to the amount of bandwidth used by that application.

Before configuring application slices, it may be useful to the consider the following:

- By configuring an application slice, you are saying that you want to control traffic from specified applications, and application groups.
- Applications not specified are not prevented from using bandwidth. The amount of bandwidth is relative to previously specified applications.
- **Relative weight** refers to the relative importance of that application, or application group, specified as an integer between `1` and `100`. It may be useful to configure the first application of that slice with a **Relative weight** of `10`, then base other applications and weights around that. For example, if you configure a second slice with a weight of `20`, you are saying that applications from slice two will receive two times as much bandwidth than those in slice one.

These slices are only used as a prioritization method when available bandwidth for that class is nearing capacity.

To add an application slice to a Bandwidth shaping policy, do the following:

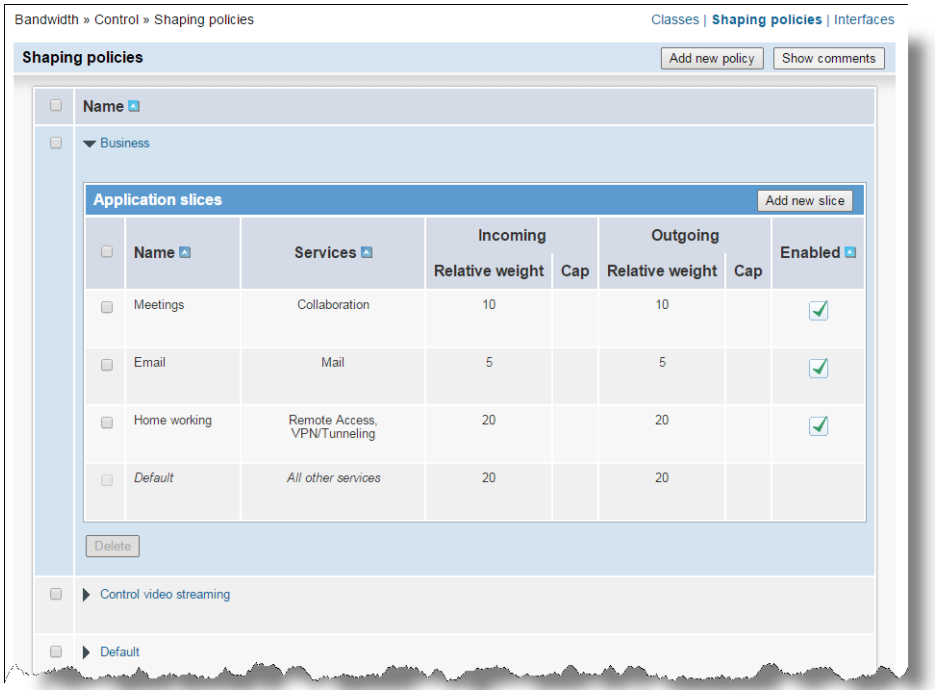
1. From the **Shaping policies** table, click the expand arrow to display the **Application slices** table.
2. Click **Add new slice**.

3. Configure the following:
   - **Status** — Leave this checked unless the application slice is not going to be used.
   - **Name** — Configure a meaningful name for this application slice.
   - **Services** — Select those relevant services for this application slice. Note that you can select the category name to select all services for that category, rather than selecting each one individually.
   - **Incoming relative weight** — Configure an incoming bandwidth ratio as an integer between `1` and `100`.
   - **Incoming cap** — Configure an optional cap for the amount of incoming bandwidth used. This is either in kilobits per second (**kbps**) or megabits per second (**Mbps**).
   - **Outgoing relative weight** — Configure an outgoing bandwidth ratio as an integer between `1` and `100`.
   - **Outgoing cap** — Configure an optional cap for the amount of outgoing bandwidth used. This is either in kilobits per second (**kbps**) or megabits per second (**Mbps**).
   - **Comment** — Configure an optional comment for this application slice.

     An additional button, **Show comments**, will be displayed in the **Application slices** table if any comments are configured. Clicking this will display configured comments under the application slice name.
4. Click **Add**.

Example Application Slice

For example, a class is assigned the pre-defined **Business** shaping policy:



This class is given a **Dynamic** sharing type, with 2 megabits per second of incoming, and 2 megabits per second of outgoing bandwidth. The **Business** shaping policy slices up the 2 megabits per second of bandwidth as follows:

- Traffic from **Collaboration**, **Mail**, **Remote Access**, and **VPN/Tunneling** applications are more important than all other traffic originating from IP addresses assigned to that class.
- If traffic for all four application groups was detected originating from IP addresses assigned to the class, bandwidth would be shared as follows:
  - **Collaboration** applications would receive two times more bandwidth than **Mail** applications (10 being two times more than 5).
  - **Remote Access** and **VPN/Tunnelling** services will receive two times more bandwidth than **Collaboration** applications, and four times more bandwidth than **Mail** applications.
  - All other traffic would receive a similar share of bandwidth as **Remote Access** and **VPN/Tunnelling** services.

If traffic matching only one application slice is present, this would use up the full 2 megabits per second allocation as needed.

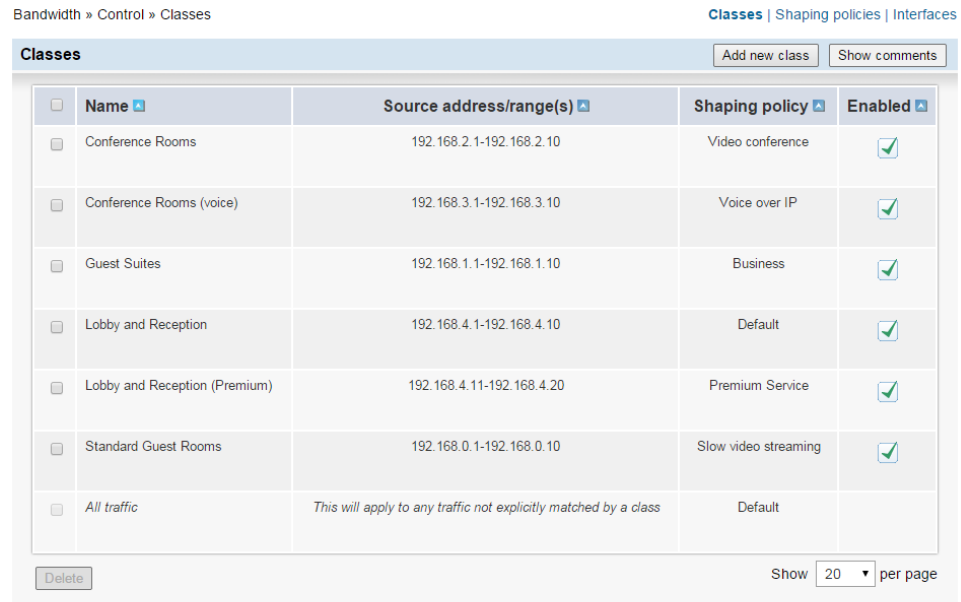
Example Bandwidth Shaping Configuration

The following example is based upon a hotel offering an internet service to guest bedrooms, conference rooms with separate subnets for video conferencing, and VoIP traffic, and public areas such as the lobby.

A single external interface is configured to be shaped, with a total of 5 megabits per second incoming and outgoing bandwidth.

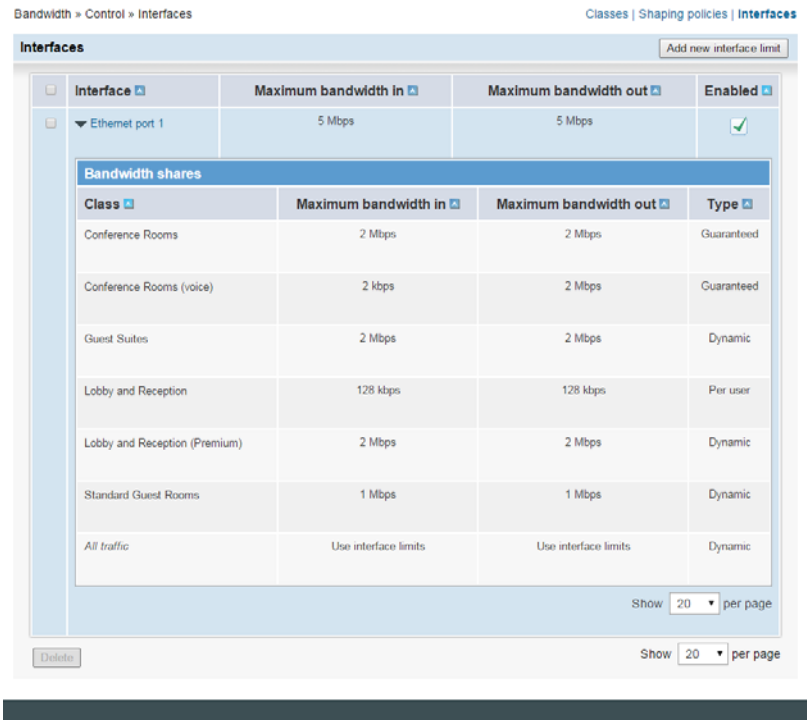
The **Default** shaping policy has been given a cap of 128 kilobits per second for both incoming and outgoing traffic. An additional shaping policy has been added, **Premium Service**. Similar to the **Default** shaping policy, this policy is not for an specific service or application. It is capped at 2 megabits per second for both incoming and outgoing traffic.

The following classes are setup:



- Conference Rooms — The **Video conference** shaping policy is applied to those IP addresses specified in the Conference Rooms class. Applications that are listed in the **Video conference** policy (see *Creating Bandwidth Shaping Policies* on page 13) are shaped if there is excessive demand on bandwidth.
- Conference Rooms (voice) — The **Voice over IP** shaping policy is applied to those IP addresses specified in the Conference Rooms (voice). Applications that are listed in the **Voice over IP** policy (see *Creating Bandwidth Shaping Policies* on page 13) are shaped if there is excessive demand on bandwidth.
- Guest Suites — The **Business** shaping policy is applied to those IP addresses specified in the Guest Suites class. Applications that are listed in the **Business** policy (see *Creating Bandwidth Shaping Policies* on page 13) are shaped if there is excessive demand on bandwidth.
- Lobby and Reception — This class uses the **Default** shaping policy. This has deliberately been set to a low level of bandwidth, to restrict users from using excess bandwidth in public areas.
- Lobby and Reception (Premium) — This class uses the **Premium** shaping policy. This allows a greater share of the bandwidth, without restricting it to any particular service. This is to encourage users in public areas to upgrade to the premium service.
- Standard Guest Rooms — The only traffic that is shaped from guest rooms is video streaming, using the **Slow video streaming** policy. This is to encourage users to use the hotel's own film and video service.

The above classes are allocated the following bandwidth:



- Both conference room types are allocated a guaranteed slice of 2 megabits per second for incoming and outgoing traffic. Note that two conference room classes could be combined as their bandwidth allocations are the same.
- Guest suites have a dynamic allocation of 2 megabits per second.
- Users in the lobby and reception area are allocated 128 kilobits per second each, unless they upgrade to the Premium Service.
- Standard guest rooms have a dynamic allocation of 1 megabit per second.

4 Managing Bandwidth

This chapter describes how to manage Bandwidth, including:

Managing Bandwidth Interfaces

From time to time, you may need to edit or remove those interfaces configured for Bandwidth shaping.

Editing Bandwidth Interfaces

To edit an existing Bandwidth interface, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Interfaces**.
2. Highlight the relevant interface within the Interfaces table, and click **Edit**.
3. Edit the configuration as required. For a detailed description of each setting, see *Configuring Bandwidth Interfaces* on page 9.
4. Click **Save changes**.

Note: It is recommended you reconfigure the bandwidth share for each class assigned to the interface if the maximum incoming or outgoing bandwidth has been adjusted for that interface.

Deleting Bandwidth Interfaces

Typically, you would not need to remove interfaces configured for shaping. However, it should be noted that removing a shaped interface does not remove associated classes from the Bandwidth configuration as they are available to all shaped interfaces.

Note: The following procedure does not remove the interface from your Smoothwall System, just from the bandwidth shaping configuration.

To delete a existing Bandwidth interface, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Interfaces**.
2. Highlight the relevant class within the **Interfaces** table, and click **Delete**.

Managing Bandwidth Classes

You can edit or remove Bandwidth classes as required. Any updates made, will automatically be reflected on the **Bandwidth > Control > Interfaces** page.

Editing Classes

To edit an existing Bandwidth class, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Classes**.
2. Highlight the relevant class within the **Classes** table, and click **Edit**.
3. Edit the configuration as required. For a detailed description of each setting, see *Creating Bandwidth Classes* on page 10.
4. Click **Save changes**.

Changes to the class **Name** will automatically be reflected in the **Bandwidth > Control > Interfaces** page.

Deleting Classes

To delete a existing Bandwidth class, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Classes**.
2. Highlight the relevant class within the **Classes** table, and click **Delete**.
3. Confirm the deletion when prompted.

Deleted classes will automatically be reflected in the **Bandwidth > Control > Interfaces** page.

Managing Shaping Policies

You can edit or remove shaping policies as required.

Tip: It is recommended that you do not delete unused shaping policies as they may be of use at a later date. They can be left in the **Shaping policies** table without affecting other policies.

Editing Shaping Policies

To edit an existing policy, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Shaping policies**.
2. Highlight the relevant policy within the **Shaping policies** table, and click **Edit**.
3. Edit the configuration as required. For a detailed description of each setting, see *Creating Bandwidth Shaping Policies* on page 13.
4. Click **Save changes**.

Deleting Shaping Policies

To delete a existing policy, do the following:

1. From your Smoothwall System, browse to **Bandwidth > Control > Shaping policies**.
2. Highlight the relevant policy within the **Shaping policy** table, and click **Delete**.
3. Confirm the deletion when prompted.

Managing Classes Through the User Portal

Smoothwall System's user portal allows you to manage certain operations through a simplified user interface.

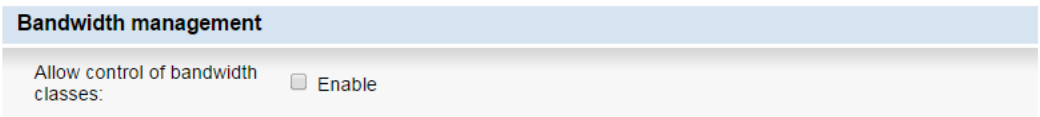
From the user portal, you can enable or disable Bandwidth classes. No other Bandwidth operations are provided through the user portal.

The following assumes you have configured a number of user portals in your Smoothwall System.

To add class management to a user portal, do the following:

1. From your Smoothwall System, browse to **Services > User portal > Portal**.
2. From the **Portals** panel, select the relevant portal from the drop-down list and click **Select**.

   The portal name will appear in the **Name** box on the right.
3. Scroll down to the **Bandwidth management** panel.



4. Select **Allow control of bandwidth classes**.
5. Scroll down to the bottom of the page, and click **Save**.

For a detailed description of how to configure all operations for the user portal, refer to your *Smoothwall System's Operations Guide*.

For a detailed description of how to use the user portal, refer to the *Smoothwall System's User Portal Guide*.

Monitoring Bandwidth Usage

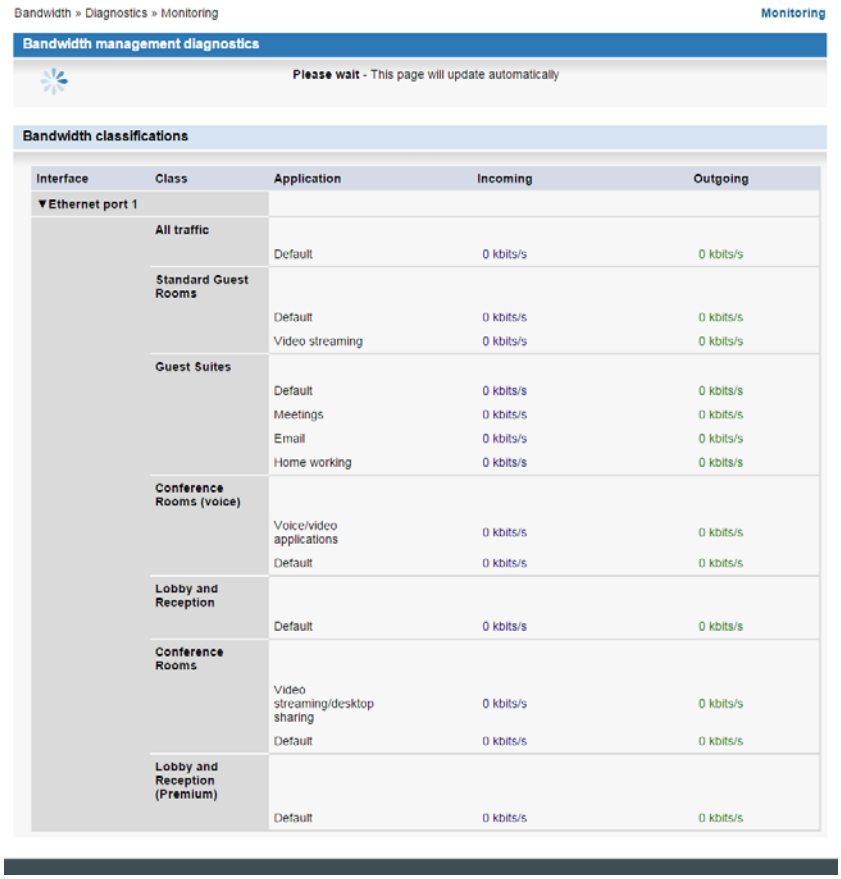
You can monitor the throughput in each application, for each slice, for incoming and outgoing bandwidth. Throughput is continuously monitored, and the page refreshed constantly.

Each interface configured under **Bandwidth > Control > Interfaces** is listed, followed by the classes, and associated applications.

Irrespective of your configuration, all throughput is displayed in kilobits per second.

To view bandwidth throughput, do the following:

- From your Smoothwall System, browse to **Bandwidth > Diagnostics > Monitoring**.



5 Reporting and Alerting

This chapter describes how to use the Bandwidth reporting and alert functions, including:

About the Bandwidth Report

The **Application Bandwidth Statistics** report provides details of the bandwidth used by application groups, including:

- Measurements of the incoming and outgoing bandwidth
- Measurements of the bandwidth used by individual IP addresses
- Measurements of the bandwidth used by individual applications
- Measurements of bandwidth across external interfaces, and, or, bridges
- Drill down through the report from application bandwidth into IP address bandwidth, and vice versa

  Note that drill down options are not available through the Bandwidth user portal.
- Application classification into groups, and bandwidth measurements of these groups. For a list of those applications and application groups, see *Appendix A:Application Groups* on page 29

Note: A Layer 7 licence (deep packet inspection) is required to run this report fully. Without this licence, limited information is displayed. For more information about obtaining a Layer 7 licence, refer to your Smoothwall representative.

Generating the Report

To generate the Application Bandwidth Statistics report, do the following:

1. From your Smoothwall System, browse to **Logs and reports > Reports > Reports**.
2. At the top of the page, set the **Start** and **End** dates for the report.
3. Open the **Firewall and Networking** folder.
4. Scroll down to the **Application Bandwidth Statistics** panel.
5. Click the **Advanced** button to expand the advanced reporting features.
6. From the **Data flow direction to highlight** drop down menu, choose the data direction to report on. Valid values are: **incoming**, **outgoing**.

   Note that you cannot report both incoming and outgoing data at the same time.
7. From the **Interface** drop down menu, choose the interface to report on.

   For a detailed description of how to set up Bandwidth interfaces, see *Chapter 16, Working with Interfaces* on page 267.
8. Click **Run report**.

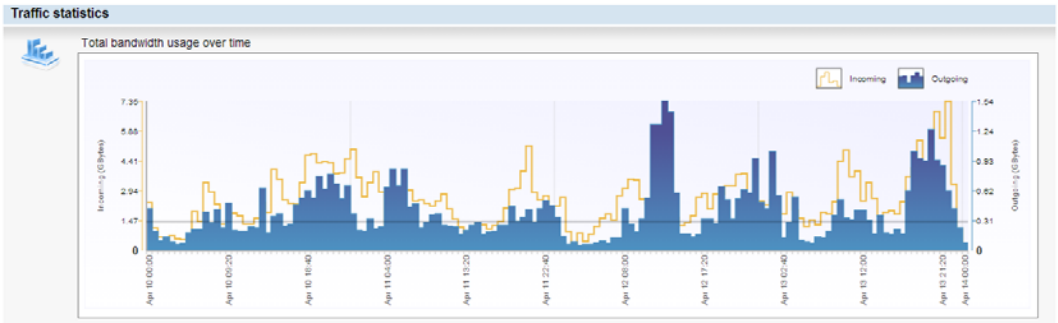
   Bandwidth generates the report to the screen.

For more information about your Smoothwall System's reporting functions, including other reports available, refer to your *Smoothwall System's Operations Guide*.

About the Generated Report

The generated Application Bandwidth Statistics report is broken down into the following sections:

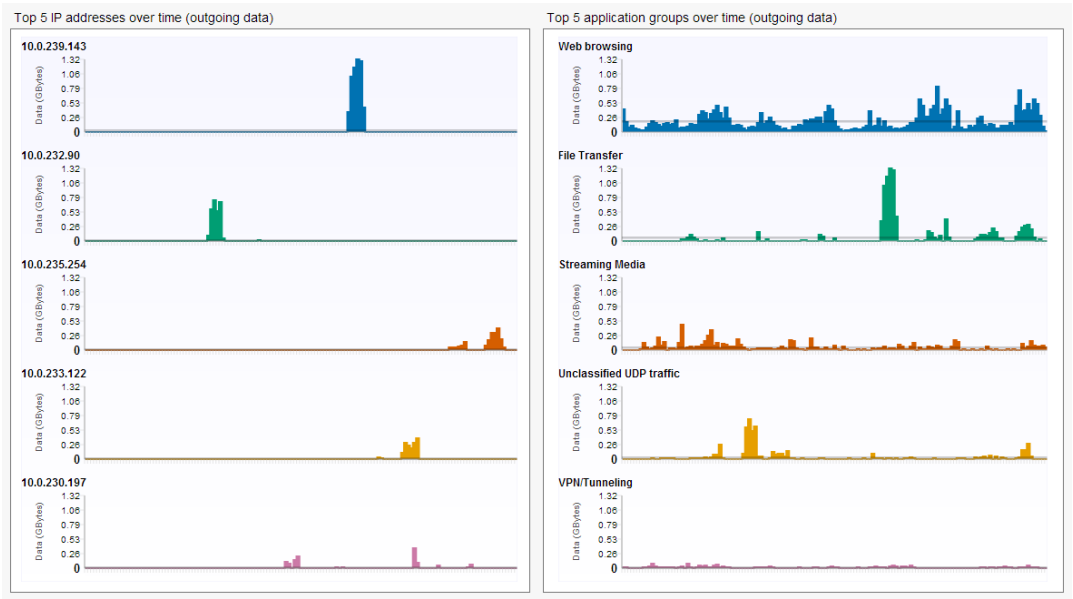
- **Traffic statistics** — Shows the incoming and outgoing bandwidth as a graph, over the specified date range, for example:



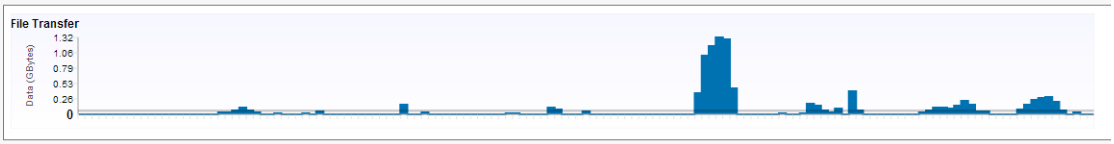
Note: This is the only graph that shows incoming and outgoing bandwidth together.

- **Top 5 IP addresses over time** — Shows the bandwidth used, as a graph, for each of the top five IP address. Incoming or outgoing data is shown, dependant on the traffic direction chosen when running the report.

- Top 5 application groups over time — Shows the bandwidth used, as a graph, for each of the top five application groups. Incoming or outgoing data is shown, dependant on the traffic direction chosen when running the report.



You can also drill down through the graphs to show a further break down of either the IP addresses that accessed the application groups, or the application groups accessed by the IP address. The following example is a break down of the File Transfer application group from the image above:



Top 8 application protocols for application group 'File Transfer' (outgoing data)

Application protocol	Total bytes	Average bytes
Dropbox	6.92G	49.21M
BitTorrent	3.04G	21.63M
iCloud	173.42M	1.2M
BITS	33.03M	234.91K
eDonkey	17.11M	121.65K
Winny	3.64M	25.91K
CIFS	2.29M	16.25K
FTP	99.87K	710

Top 5 IP addresses for application group 'File Transfer' (outgoing data)

IP address	Total bytes	Average bytes
10.0.239.143	5.61G	39.89M
10.0.235.254	1.48G	10.49M
10.0.230.20	653.63M	4.54M
10.0.230.197	594.69M	4.13M
Other IP addresses (Less than 5% of total traffic each)	1.88G	13.38M

Note that as you drill down through the report, the **Traffic statistics** graph is always displayed at the top.

About Alerts

Alerts are generated when certain trigger conditions are met. Trigger conditions can be individual events, for example, an administrator login failure, or a series of events occurring over a particular time period, for example, a sustained high level of traffic over a five minute period.

The following sections assumes you have configured your Smoothwall System alerts. For a detailed description of how to do this, refer to your *Smoothwall System's Operations Guide*.

About the Bandwidth Monitor Alert

The Bandwidth Monitor alert continuously monitors for activity. Alerts are triggered whenever the traffic flow for an external interface, or bridge, exceeds configured thresholds.

The Bandwidth Monitor alert is disabled upon installation.

To enable and configure the alert, do the following:

1. From your Smoothwall System, browse to **Logs and reports > Alerts > Alert settings**.
2. Scroll down to the **Bandwidth Monitor** panel.
3. Configure the following:
   - **Incoming** — Select this to enable incoming bandwidth monitoring
   - **Outgoing** — Select this to enable outgoing bandwidth monitoring

Note: Each alert you configure can only monitor traffic in a single direction. However, you can configure multiple Bandwidth Monitor alerts to enable you monitor all traffic.

- **Traffic for** — From the drop-down list, select to monitor the bandwidth used for:

Traffic Option	Description
Total	For all interfaces configured on your Smoothwall System
Any IP	Any IP address going through your Smoothwall System
Single application	A single, specified application. An additional drop down list will appear for you to specify the application.
Single application group	A single, specified application group. An additional drop list will appear for you to specify the application group.

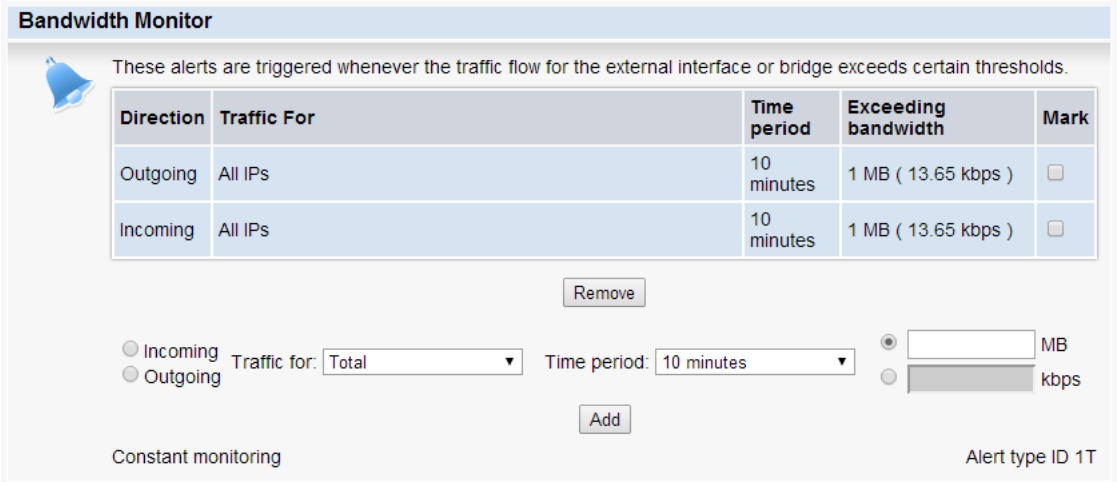
- **Time period** — From the drop-down list, select the required time period to monitor bandwidth for
- **MB** — The maximum amount of data usage, in megabytes, permitted before the alert is triggered.
- **kbps** — The average data transfer rate, in kilobits per second, permitted before the alert is triggered.

Note: The Smoothwall System will calculate the bandwidth used to two decimal places.

4. Click **Add**.

   The alert will be added to the table at the top of the panel.

Example Bandwidth Monitor Alert



The example above shows two configured alerts.

An outgoing alert is triggered if the total outgoing bandwidth consumed by any IP address on the network exceeds one megabyte in ten minutes. Similarly, an incoming alert is triggered for total incoming bandwidth consumed in the same time frame.

Removing Bandwidth Monitor Alerts

To delete an alert, do the following:

1. From your Smoothwall System, browse to **Logs and reports > Alerts > Alert settings**.
2. Scroll down to the **Bandwidth Monitor** panel.
3. Mark the relevant alert to delete.
4. Click **Remove**.

Appendix A: Application Groups

This appendix lists the available application groups for Bandwidth, including:

Application Groups

Application groups are classified as follows

Application Group	Applications
Databases	• Microsoft SQL • MySQL • PostgreSQL
File Transfer	• FTP
Infrastructure	• DHCP • DNS • ICMP • IGMP • Internet printing (IPP) • LDAP • Microsoft • NTP • RPC/SMB/CIFS • SNMP • Sun RPC/NFS
Mail	• IMAP • POP • SMTP
Messaging	• IRC
News	• NNTP

Application Group	Applications
Proxies	• SOCK proxy • Web proxy
Remote Access	• Remote Desktop • SSH • Telnet • VNC
Streaming Media	• SIP (VoIP)
VPN/Tunneling	• IPsec tunneling • IPv6 tunneling
Web browsing	• HTTP • HTTPS (unencryoted)

Deep Packet Inspection Application Groups

If deep packet inspection (DPI) is licensed for your Smoothwall System, the following additional application groups are also defined:

Application Group	Applications
Collaboration	• Citrix • Citrix GoToMyPC • GoToMeeting • Groupwise • HL7 • Lotus Notes • Lync • Meeting Maker • Microsoft ActiveSync • NetMeeting • SAP • SharePoint • WebEx
Databases	• BLIDM • CLDAP • dBase • INGRES-NET • LDAP • MaxDB • Mini SQL • MS SQL • Oracle • RIS • SVN • Sybase SQL • TDS

Application Group	Applications	
File Transfer	• ACR-NEMA • AFP • Akamai Netsession • Apple Update • AppleJuice • Ares • Astraweb • auditd • AVG • Avira • BitDefender • BitTorrent • BITS • BlazeFS • CFDPTKT • CIFS • Clubbox • Commvault • DirectConnect • Dropbox • eDonkey • Eset • FASP • F-Prot • Freenet • Giganews • Gnutella • GPFS • Google Talk File Transfer • HiveStor • iCloud • iMesh • Kaspersky • Manolito • McAfee	• MC-FTP • McIDAS • MUTE-net • NateOn File • NFA • NFS • NNTP • NovaBACKUP • OFTP • OFTPS • Paltalk File Transfer • Panda • Pando • PDbox • PDbox P2P • PFTP • Qik Upload • SBNTBCST • SFTP • Share P2P • Shareman • Skype File Transfer • SuperNews • TFTP • Usenet • Vegaa • WebDAV • WinMX • Winny • Windows Update • Xunlei • Yahoo Msg File Transfer • ZanNet
Games	• Battle.net • Quake Live	• Steam • XBox
Mail	• Exchange • gmail • InfoStore • Microsoft Mail API • Microsoft Mail Transfer Agent • Microsoft RFR • MS IMAP	• NI Mail • PCMAIL • POP2 • POP3 • Store Admin • SMTP • System Attendant

Application Group	Applications	
Messaging	• 050Plus • Aliwangwan • AIM • APNS • BaiduHi • C2DM • CISCOUC • CISUCAUD • CISUCVID • DeNA Comm • eBuddy • eBuddy XMS • Fring • Google Hangouts • Google Helpouts • Google Talk • iCall • ICQ • ISCHAT • Kakao • Kakao Audio • LINE	• Line2 • Meebo • MMS • MSMQ • MSNP • NateOn • NateOn Phone • Nokia Message • OSCAR • Paltalk • Pinger • QQ • Skype Video • Skype Voice • Snapchat • Tango • Viber • WeChat • XMPP • YiXin • Yahoo Messenger

Application Group	Applications
Networking	• Active Directory • Apple ARP • Apple • AppleShare • AppleTalk • BGMP • BGP • BJNP • Cableport AX • Cisco DRP • Cisco FNATIVE • Cisco GDP • Cisco SYSMAINT • Cisoc TNATIVE • Clearcase • DASP • DCAP • DCCP • DCE/RPC • DHCP • DHCPv6 • Diameter • DNS • FIX • GPRS Tunneling Protocol Control • GPRS Tunneling Protocol Prime • GPRS Tunneling Protocol User • FINTA • HDAP • HTTP • Ident • IGMP • ISAKMP • Java RMI • Kerberos • LLMNR • MDNS • MFTP • Microsoft Spooler Subsystem • MobileIP • MortgageWare • MUMPS • NDS Auth • Netware • NSS • NSSTP • NetBIOS Datagram Distribution Service • NetBIOS Name Service • NetBIOS Session Service • NTP • OCS • OCSP • ODMR • OSPF • PIM • PKIX Timestamp • PPP Discovery • PPP Session • Printer • PTP • RADIUS • RADIUS-ACCT • RAP • RPC2PMAP • RSVP • Rsync • SCCM • SCCP • SCTP • SEND • SSDP • SSL • STUN • Sun RPC • SVRLOC • TACACS • Teredo • Timbuktu • WCCP • WebSocket • Whois • Wyse TCX • XNS

Application Group	Applications	
Network Monitoring	• Chargen • Daytime • Discard • Echo • Finger • ICMP • ICMPv6 • Naverisk	• SMUX • SNMP • Syslog • Systat • Tivoli • Tripwire • UMA • Zabbix
Proxies	• Avocent • Freegate • Hopster • Jondo	• Privax • SOCKS • Tor • Ultrasurf
Remote Access	• Citrix CGP • Citrix ICA • Citrix IMA • Citrix Licensing • Citrix RTMPL • Citrix SLG • Citrix WANScaler • ERPC • GOM Remote • HP VMM	• KWDB • LogMeIn • PCoIP • RDP • SCCM Remote Control • ShowMyPC • Sophos RED • TeamViewer

Application Group	Applications	
Streaming Media	• Adobe Flash • FaceTime • Fring A/V • Google Talk Audio • Google Talk Video • Google Video • H.225 • H.245 • H.248 • H.323 • Hulu • Instagram Video • iTunes • Kugou • Lync Audio • Lync Media • Lync Video • MagicJack • Nate Video • NetFlix • Paltalk Video • Paltalk Voice • Pandora • PPTV • QIK • QIK Chat	• QIK Video • QuickTime • RTCP • RTMP • RTP • RTSP • RTSPS • SHOUTcast • Silverlight • Sina Video • SIP • Skype • Sopcast • Spotify • Secure RTCP • SRTP • STRP Audio • SRTP Video • T-Mobile • UltraViolet • Vonage • WhatsApp • Windows Media • Yahoo Messenger Audio • Yahoo Messenger Video
VPN/Tunneling	• AH • CyberGhost • DynGate • ESP • GRE • Hamachi • Hotspot Shield • IPComp	• IPIP • IPsec • L2TP • OpenVPN • PPTP • RSVP Tunnel • SecurityKISS • VPNReactor

Index


smoothwall®
The Web You Want