smoothwall®

The Web You Want

Unified Threat Management

SmoothTraffic – Administrator's Guide

Smoothwall® SmoothTraffic, Administrator's Guide, March 2013

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

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.

SmoothTraffic 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

Chapter 1
Introducing SmoothTraffic

In this chapter:

- An introduction to SmoothTraffic, Smoothwall's add-on module for bandwidth management.

About SmoothTraffic

SmoothTraffic provides your Smoothwall System with a powerful set of bandwidth management controls. Network administrators can use these controls to determine how bandwidth should be allocated amongst the various types of traffic competing to use a congested Internet connection. Here are a few examples:

- **Office web browsing**

  In a normal office environment, interactive services such as web browsing should receive a higher priority than background traffic such as FTP file transfers and email downloads. This ensures that web browsing is fast and responsive, and that big file transfers do not consume vast amounts of bandwidth.

- **Web hosting**

  In a web hosting environment, HTTP requests and responses should receive a higher priority than other traffic. This ensures good server response times, while other (less critical) traffic can be allocated a small (but fair) amount of any spare bandwidth. For multiple web servers, it might be appropriate to partition the available bandwidth, thus preventing any one server consuming a disproportionately large share.

- **Discouraging misuse**

  The use of unauthorized software, such as P2P or file sharing clients, can be discouraged by enforcing a go-slow policy for all unknown traffic types. This ensures that acceptable network traffic such as HTTP and email are given priority, while all other traffic (including port-adaptive P2P software) is forced to run at a practically unusable speed. SmoothTraffic can also identify specific p2p protocols and assign different priorities. For example, all BitTorrent activity can be set to low priority, and statistics registered for it.

  There are many more ways that SmoothTraffic can be used to manage network traffic. This manual provides extended examples for a number of typical bandwidth management requirements, in addition to explaining how to configure rules for more specialized situations.

Configuration Overview

Configuring SmoothTraffic consists of the following steps:

- Select a traffic management scheme and calibrate the bandwidth settings, see *Chapter 4, Configuring SmoothTraffic* on page 9
- Create rules to priorities network protocols and services and, optionally, selectively apply rules to specific IP addresses and networks, see *Chapter 5, Creating and Managing Traffic Rules* on page 15
- Start SmoothTraffic, see *Chapter 4, Stopping and Starting SmoothTraffic* on page 10.

Who should read this guide?

System administrators maintaining and deploying SmoothTraffic should read this guide.

Note: We strongly recommend that everyone working with Smoothwall products attend Smoothwall training. For information on our current training courses, see http://smoothwall.net/support/training/

Other Documentation and User Information

Your Smoothwall System comes with the following guides.

Smoothwall Installation and Setup Guide contains complete information on installing and configuring your Smoothwall System initially.

Smoothwall Administrator's Guide is a guide to working with your Smoothwall System.

Smoothwall module guides explain how to use Smoothwall add-on modules with your Smoothwall System.

http://smoothwall.net/support/ contains support, self-help and training information as well as product updates.

Support

All Smoothwall products include unlimited email and telephone support for 30 days from the date of purchase of the software licence. Useful support resources are:

- Email: support@smoothwall.net
- Web site: www.smoothwall.net/support
- Sales department: +44-(0)870-1-999-500

Chapter 2
Installing SmoothTraffic

In this chapter:

- How to install SmoothTraffic.

Before Installing

You install SmoothTraffic by adding it to your existing Smoothwall System. For information on working with Smoothwall products, see the Administrator's Guide delivered with your product.

Before installing SmoothTraffic:

1 Start a web browser, browse to your Smoothwall System, authenticate yourself and navigate to **System > Maintenance > Updates** page.

2 Click **Refresh updates list** to check that you have all the latest updates installed on your Smoothwall System.

3 If there are any updates available, download and install them. See your *Smoothwall System Administrator's Guide* if you need more information.

Installing SmoothTraffic

After checking that you have the latest updates installed, you are ready to install SmoothTraffic.

To install SmoothTraffic:

1 Navigate to the **System > Maintenance > Modules** page.

2 In the **Available modules** list, select **SmoothTraffic** and click **Install**. Your Smoothwall System installs SmoothTraffic.

3 Navigate to the **System > Maintenance > Shutdown** page.

4 Select **Immediately** and click **Reboot**.

5 When your Smoothwall System has rebooted, authenticate yourself and log on. You are now ready to begin prioritizing network traffic for improved bandwidth usage. Some initial configuration steps are:

- Calibrating SmoothTraffic according to the various internal and external interface speeds.
- Choosing the traffic scheme settings.

For further information, see *Chapter 3, About Bandwidth Management* on page 5 and *Chapter 4, Configuring SmoothTraffic* on page 9.

Installing SmoothTraffic

Chapter 3
About Bandwidth Management

In this chapter:

- How SmoothTraffic's bandwidth management controls can be used to dramatically improve traffic flowing over computer networks.

Network Communication Protocols

Network communication protocols are the standards that define how messages are structured and communicated over a computer network. Each message flowing through a network consumes an amount of bandwidth, and this section explains how the most commonly used network protocols affect bandwidth consumption.

Internet Protocol

Internet Protocol (IP) is used to determine how data is structured and communicated over a computer network. IP arranges messages into small blocks of data known as 'packets', which can then be individually forwarded on to an intended recipient.

IP does not guarantee that individual data packets will reach their destinations. Neither does IP ensure that packets are processed quickly or in any particular order. These characteristics make IP extremely flexible – it simply concentrates on routing packets to their destination as efficiently as possible.

The simplicity of IP means that it can be used with communications technologies of vastly differing speeds and capabilities. IP makes it possible for a supercomputer with a Gbit/ second connection to communicate with a legacy computer using a 32 Kbit/second modem.

Transmission Control Protocol

The nature of IP means that packets can arrive at their destination via different routes and out of sequence. Some packets might even have been corrupted or lost along the way. Transmission Control Protocol (TCP) is used in conjunction with IP to guarantee delivery of data and ensure that packets are reassembled in the correct order. This is achieved using two mechanisms:

- TCP headers – TCP data packets are prefixed by a TCP header that contains information about the source, destination and sequence number of the data. The recipient system uses the header information to reassemble the message correctly.
- ACK packets – TCP ensures that the receiving computer acknowledges the sender by returning ACK packets. If the sender does not receive an ACK packet within a reasonable time period, the packets are presumed to be lost and then resent.

TCP Transmission Windows

If every data packet received by a computer generated a corresponding ACK packet, the volume of network traffic would be significantly larger than the size of the useful messages being transmitted! This additional traffic would slow network communication down, and waste valuable bandwidth.

To alleviate such wastage, TCP uses the concept of transmission windows. In this mode, only a single ACK packet is required to acknowledge receipt of several packets transmitted during the same time frame. When a network connection is initially formed between two computers, the transmission window is set to a small size. This is because the speed of the network connections between each system cannot be guaranteed – they might be on the same local network using Gigabit ethernet, or they may be separated by 20 or more different network segments and a dialup modem link. TCP determines the speed of a connection by monitoring how quickly ACK packets are returned by the recipient. When ACK packets are received quickly, the window size is increased to allow more packets to be sent before the next ACK packet is required.

Larger window sizes will be used when the connection is fast and nearly error free, such as when using gigabit ethernet over a local network. If the quality of a connection deteriorates, large numbers of packets will require retransmission. This will be met by a reduction in the number of successfully returned ACK packets, causing the transmission window to be reduced accordingly.

This powerful mechanism adapts rapidly to its environment, always sending as many data packets and as few ACK packets as is efficiently possible. As a result, transmission speeds are dramatically increased – providing there are few errors and only occasionally retransmissions.

Other types of Internet traffic such as UDP do not use TCP's transmission window mechanism. Such traffic is still regulated by packet dropping, but the rate of packet retransmission (if required at all) is the responsibility of the applications involved. Some applications that work well on a LAN perform poorly in the higher packet loss environment of the Internet. Traffic management can improve the performance of such applications by controlling greedy TCP sessions, thereby allowing non-TCP data a greater chance of survival.

Internet Traffic Dynamics

Of course, the Internet is not all gigabit ethernet, and sooner or later a greedy TCP session will overload some part of the Internet and the offending packets will either be delayed or dropped. IP has the right to discard such packets, and this happens all the time.

Unacknowledged packets cause a TCP session to reduce the size of its transmission window, and the sender retransmits packets at a rate more appropriate to the speed and quality of the connection. Such rate slowing may be due to some temporary congestion.

TCP is always pushing its luck by constantly trying to raise the size of its transmission window. If the restriction is only temporary, the transmission rate will be slowed for only a few seconds, before scaling back to a higher rate. Thus the normal state for the Internet is one in which lots of packets are being dropped. This may seem wasteful, but it should be considered as a necessary overhead in order to get all the users of the Internet transmitting data at a maximum but appropriate rate.

Packets are normally dropped at the slowest point in the route between two communicating network devices. Bandwidth management is all about taking active control of network traffic, and deciding which packets get passed through quickly and which get delayed or even dropped. Dropping a moderate number of packets will not cause data errors; it will cause the sender to reduce its transmission rate.

It is possible that just a single, large file download over a fast and reliable Internet connection could consume all of the available bandwidth. Anybody trying to use the connection after the download has started will experience poor response times because their packets are being delayed (or possibly even dropped) due to the mass of file download packets.

SmoothTraffic applies temporary blocking rules to throttle back particular types of traffic and selectively reduce transmission windows. These rules can be configured to ensure a fairer distribution of bandwidth, by prioritizing traffic according to protocol, service, source or destination.

Managing Bandwidth Effectively

In the previous section, we explained how the TCP protocol is designed so that its transmission rate adapts to the current network conditions.

Using an analogy, we will now demonstrate how active controlling your network traffic is better than letting some arbitrary part of the Internet regulate TCP.

The Sports Stadium Analogy

Consider a crowd of people trying to enter a stadium. Without a means of regulating the influx of people, chaos would soon develop. A free for all crush would probably mean that the biggest and strongest push their way through; not necessarily the people that the stadium owners wanted to enter first, such as VIP guests. Another problem arises when people are jammed together in a crush – movement is very slow.

Allowing a crush to develop means it takes longer for everyone to enter the stadium. Having a number of different entrances with turnstiles and stewards enables the stadium to regulate the flow of people entering it. VIPs can use their own priority entrance, and the general crowd is allowed to enter at a controlled rate through a number of other entrances and turnstiles.

However, there are still potential problems to consider. If the stewards let people in too fast a crush may develop inside the stadium. If this occurs, the turnstile queues will be held up by the crush, and the stewards will no longer be in control of entry rate. Conversely, if the stewards slow the entry rate too much, not everybody will enter the stadium in time. The queue will still be under control, but the result is still not desirable.

The best solution is to manage the queue in such a way that the entry rate is just fast enough to avoid uncontrolled congestion developing inside the stadium.

All of these principles can be applied to packets leaving a local network for the Internet. It is important that packets are sent at a rate just below the rate at which the service provider's equipment (which is the next stage on the route through the Internet) is willing to accept them. Failure to do this means that the Internet Service Provider (ISP) will be managing the bandwidth – i.e. arbitrarily deciding which packets are sent, delayed or dropped.

If the ISP delays or drops your packets, it will not be possible to priorities your own traffic. For this reason is important that you are realistic about the actual speed of your Internet connection. If SmoothTraffic believes the connection to be faster than it is, it will not be able to control your network traffic. By configuring SmoothTraffic with the actual connection speed, it will be able to send packets out at an appropriate rate – just 2% less than the actual speed will yield excellent results. If SmoothTraffic is not working as expected, reducing the configured connection speed is often all that needs to be done.

Controlling P2P

There are a vast number of Peer-to-Peer (P2P) file sharing protocols in existence, and it can be difficult to block such traffic from passing through a firewall. Many P2P protocols are port adaptive – i.e. they attempt to use any ports that they can open. This allows many P2P protocols to evade traditional firewalling techniques.

SmoothTraffic can eliminate the threat posed by such traffic by setting a default go-slow policy for any traffic for which rules have not been specifically configured. While the P2P client software on the

user's PC will be able to connect to a P2P server, the software will assume that it is connected to a very slow line – the user's P2P download speed will be so slow they will almost certainly give up!

Note: For some P2P protocols, you can write rules to match the traffic and handle it as fast or slow as required.

This approach allows all normal authorized communication to run quickly, while unauthorized usage like P2P will run very slowly. In contrast, blocking all unknown communication may prevent unforeseen (and sometimes) valid communication from taking place. For example, it would be more desirable for software that registers itself using a non-standard port to be allowed to communicate (albeit slowly) than not at all.

Network administrators can monitor unapproved use of bandwidth by logging all packets that have not passed one of the configured rules. However, large scale packet logging can rapidly consume disk space, and in some circumstances reduce general system performance. It is advisable to enable logging for short periods of time, in order to capture a 'snapshot' of unclassified traffic activity. Such logs can then be used as a basis for creating new traffic rules – repeating this process will improve bandwidth management and the usefulness of the logging facility.

Chapter 4

Configuring SmoothTraffic

In this chapter:

- How to configure SmoothTraffic to manage bandwidth on your network.

Accessing SmoothTraffic

Note: Currently, it is not possible to deploy intrusion prevention policies and run SmoothTraffic at the same time. This limitation will be removed as soon as possible. Contact your Smoothwall representative if you need more information.

To access SmoothTraffic:

1 On your Smoothwall System, browse to the **Networking > Traffic > Control** page.

The following pages are available:

Page	Description
Control	Used to manage SmoothTraffic and apply global settings. For more information, see *Stopping and Starting SmoothTraffic* on page 10.
Ports	Used to create rules which identify and categorize network traffic based on the traffic's destination port. For more information, see *Chapter 5, Creating a Port Traffic Rule* on page 15.
Diffserv	Used to create rules which SmoothTraffic can interpret and use to either assign a new diffserv mark, or assign traffic containing a specific diffserv mark to a specific tag as defined by the active traffic scheme. For more information, see *Chapter 5, Creating Diffserv Traffic Rules* on page 18.
Peer-to-peer	Used to create rules which SmoothTraffic can interpret and use to manage peer to peer traffic, such as BitTorrent or Kazaa. For more information, see *Chapter 5, Creating a Peer-to-Peer Traffic Rule* on page 19.
Address	Used to create address rules for selectively applying rules to specific IP addresses and networks. For more information, see *Chapter 5, Creating an Address Rule* on page 21.
Groups	Used to apply rules that match all traffic coming from those users' addresses. For more information, see *Chapter 5, Applying Traffic Rules to Groups* on page 22.

Stopping and Starting SmoothTraffic

SmoothTraffic can be configured to start automatically following a system boot.

- To enable automatic starting: select **Start Traffic sub-system automatically** and click **Save**.
- To manually restart or stop SmoothTraffic: click **Restart** or **Stop**.
- To re-display the current status of SmoothTraffic: click **Refresh**.

Selecting a Traffic Scheme

A scheme is a pre-defined list of bandwidth allocation rules that can be applied to different types of network traffic.

SmoothTraffic contains a number of built-in traffic schemes that are listed in the Available schemes region of the Networking > Traffic > Control page.

Each scheme contains rules that describe how network traffic can be prioritized. Such rules typically consist of a minimum bandwidth, and a ceiling. Some schemes may contain special rules – for example, schemes that allow bandwidth to be partitioned into one or more separate channels.

Scheme Information

All traffic schemes are self-describing, and are explained in detail by opening the Scheme Information page.

To launch the scheme information page.

1 On the **Networking > Traffic > Control** page, in the Available schemes area, click the name of the scheme you wish to view.

Most schemes have two built-in rules that cannot be modified:

Built-in rule	Description
Small packets get high priority	This rule is primarily intended to ensure that acknowledgement (ACK) packets get transmitted without delay, thereby avoiding what is known as ACK starvation. This typically occurs on Asymmetric Digital Subscriber Line (ADSL) connections where the upstream ACKs (i.e. ACK packets being returned towards the ISP/ Internet) are not being transmitted fast enough, with the result that the remote computer sending the data will reduces its TCP window size and thus its data transmission rate. This can happen despite the fact that the faster downstream channel of the ADSL circuit might not be fully loaded, and could actually accept a faster data rate. This rule will only affect small packets that have not been prioritized by virtue of another configured traffic rule. For example, if priority rules have been configured for FTP traffic, any small FTP packets will be prioritized according to that rule, not the built-in Small packets get high priority rule. However, if no such priority rule has been configured for FTP, the built-in Small packets get high priority rule will be applied to small FTP packets.
smoothadmin and webcache	These rules ensure that it is always possible to remotely manage SmoothTraffic no matter how busy the Internet connection might be. A small amount of bandwidth will be guaranteed for SSH and HTTPS traffic to the Smoothwall System.

Creating a traffic scheme is a complex process that requires detailed knowledge of the underlying characteristics of network communication. For this reason, it is not possible to create new traffic schemes within SmoothTraffic. However, the range of traffic schemes that are included with SmoothTraffic are flexible enough to adapt to almost all bandwidth management requirements. In special circumstances, it may be possible for Smoothwall to produce a specialized traffic scheme. Please contact the Smoothwall support team if you wish to discuss this.

Deciding which Scheme to Use

An overview of each traffic scheme provided with SmoothTraffic is given below.

Scheme	Description
Default	This scheme should be suitable for most applications and is the recommended choice for most network scenarios. The set of rules it contains are designed for a mixed range of network traffic with high priority, normal priority, low priority and slow traffic priority categories.
Cascade	This scheme is designed for networks with just a few users sharing a connection. It can be used to guarantee high priority (or bandwidth intensive) traffic a large amount of bandwidth (88% guaranteed with a maximum of 98% if there is spare capacity). Any spare capacity is cascaded down to three normal priority tags, each guaranteed 1% of bandwidth (with a maximum of 98% if there is any spare capacity). If there is any capacity remaining at this point, two lower priority tags, low and slow, will be allocated some bandwidth.
Multiway	This scheme is used to divide bandwidth into an equal number of high priority slices. Normal traffic can be classified as low, normal or slow priority. The optional scheme parameter is used to specify the number of slices.

Scheme	Description
Split	This scheme is used to divide bandwidth into two or more partitions. The optional scheme parameter is used to specify the number of partitions. Each partition replicates the traffic priority categories of the Default scheme. Unused bandwidth in any partition cannot be shared by the other partition. The scheme parameter can either be a simple number in which case there will be that many equal splits or a sequence of numbers separated by commas, e.g. 50,23,23. This scheme could be used where an Internet connection is to be shared by two sets of users (or servers) and each needs an equal share of the available bandwidth to be permanently allocated.
VPN_special	This scheme has some built-in rules that use diffserv mark AF12 to mark all traffic coming down a VPN to classify it as normal priority on an interface where the default for other traffic is low. Also, any traffic marked with an AF11 or an EF will be classified as high priority, and AF13 is classified as low. It is up to the user to identify what traffic needs to be high priority, e.g. VOIP. Ensure that any traffic assigned as high priority should not take more than 20% of the total bandwidth as this is the amount that is guaranteed for such traffic. If you are not sure that the bandwidth use will be within this limit then normal would be a better choice as normal traffic has more of the bandwidth allocated to it.

Setting the Scheme

The Available schemes area on the Networking > Traffic > Control page is used to set the traffic scheme.

To set the traffic scheme:

1 On the **Networking > Traffic > Control** page, choose the scheme from the **Current scheme** drop-down list.

2 Enter an optional parameter to modify the behavior of the scheme. See *Scheme Information* on page 10 for more information.

3 Select which of the scheme's rule will be applied to unassigned traffic. This is largely dependent on the traffic shaping effect you are trying to achieve. For example, you may wish to specifically allow normal bandwidth or higher to all traffic types and slow down unauthorized use of bandwidth. In this case, a slow or low priority setting should be selected from this drop-down list.

4 To enable logging of all unassigned traffic, select **Log unassigned traffic**.

5 Click **Save**.

Calibrating Bandwidth

In order to apply bandwidth management controls, it is important that SmoothTraffic knows accurate speeds for each of SmoothTraffic's internal and external network connections.

External connections such as ADSL provide asymmetric connectivity, i.e. different upstream and downstream bandwidth capacities. For this reason, administrators must specify both the upload and download speeds for SmoothTraffic's default external connection.

Consult your Internet Service Provider about what method they recommend for testing the bandwidth of your Internet connection. ADSL, in particular, varies in speed depending on the number of other users sharing the line.

Note: If an interface is left without setting the bandwidth, that interface will be ignored by SmoothTraffic. SmoothTraffic cannot start if no interfaces at all are configured.

To calibrate SmoothTraffic's bandwidth settings:

1 On the **Networking > Traffic > Control** page, choose the downstream bandwidth for each external connection from the appropriate **Download** drop-down list. To enter a user defined speed, choose the User defined option and enter a rate using the adjacent **User defined** field and drop-down list controls.

2 Choose the upstream bandwidth for each external connection (including VPN where applicable) from the appropriate **Upload** drop-down list. To enter a user defined speed, choose the User defined option and enter a rate using the adjacent **User defined** field and drop-down list controls.

3 Choose the bandwidth for all other internal connections using the **Upload & download** drop-down list. To enter a user defined speed, choose the **User defined** option and enter a rate using the adjacent User defined field and drop-down list controls.

4 Click **Save**.

Managing Traffic on Internal Interfaces

SmoothTraffic can manage traffic between internal interfaces. As internal interfaces typically run at much higher speeds, up to gigabit, traffic management is done rather differently to gain the performance needed.

What must be understood first is that if speeds approaching the underlying Ethernet speed are required, then traffic management at the IP level, as SmoothTraffic does, is not effective. The reason for this is as the load on Ethernet increases, the Ethernet level congestion control features start to become noticeable. This means that SmoothTraffic is no longer the slowest component so control has, to some extent, been lost.

This is not as bad as it sounds as the situation degrades to all traffic getting an equal share of the bandwidth. This means that if there is constant low, normal and high class traffic across Ethernet, each will be able to transfer data at roughly the same rate. When under SmoothTraffic control, the high class would be able to transfer more than the normal, which in turn will be able to transfer more than the low.

The speed that you have to set the internal interface to enable full SmoothTraffic control is about 60Mbit/s for 100mbit Ethernet and about 500 Mbit/s for gigabit Ethernet. Exact figures vary depending on hardware, network loading, etc. If you just state that the internal interfaces are 100Mbit, or 1Gbit etc. then the three normal traffic classes of normal, high, and low become equivalent to each other if used on internal interfaces.

What does remain useful, however, is the slow class. This could be useful if you have services on the DMZ that need to contact internal systems, e.g. an SQL database server. However, you know that the rate at which such communication needs to take place only needs to be modest. Marking such traffic as slow means that a compromised system in the DMZ could not be used to saturate the internal network with traffic.

The other thing to understand about internal interfaces is that, unlike external ones, traffic is only ever shaped on the outgoing interface. This means that each network only has statistics for outgoing traffic. To shape both incoming and outgoing traffic for internal networks would have slowed down routing through SmoothTraffic too much as through traffic would be queued twice instead of just once.

The last thing to remember with internal interfaces is that the traffic classes are all percentages of specified interface speed, rather than absolute values, for example, normal traffic is guaranteed 40Mbit of 100Mbit ethernet, and slow is limited to 2% – or 2 MBit. So traffic from a DMZ marked as slow will be shaped as if it was coming from a 2 MBit Internet connection.

SmoothTraffic Reports

SmoothTraffic adds the following reports to the reporting system.

- SmoothTraffic Rule Statistics – A report listing the hourly, weekly, daily and monthly traffic statistics for each user-defined rule.
- SmoothTraffic Class Statistics – A report listing the hourly, weekly, daily and monthly traffic statistics for each traffic priority tag that is available in the currently active traffic scheme.

Note: The information reported will not mean very much if you chop and change traffic rules. We recommend that you create traffic rules you need and stick with them in order to have reliable information on traffic.

For information on working with reports, see your *Smoothwall System Administrator's Guide*.

Chapter 5

Creating and Managing Traffic Rules

In this chapter:

- How to create the rules that apply SmoothTraffic bandwidth management settings to your network traffic.

About Traffic Rules

Traffic rules are used to prioritize Internet traffic according to its protocol, service and direction. Rules can be applied by SmoothTraffic in two ways:

- Globally – If the rule is enabled, it can be applied to all Internet traffic.
- As part of an address Rule – If the rule is not applied globally, it can be selectively applied as part of an address Rule.

SmoothTraffic comes with some sample rules that you are free to use, modify or delete.

Creating Traffic Rules

You can create the following traffic rules:

- **Port rules**, for more information, see *Creating a Port Traffic Rule* on page 15
- **Diffserv rules**, for more information, see *Creating Diffserv Traffic Rules* on page 18
- **Peer-to-peer rules**, for more information, see *Creating a Peer-to-Peer Traffic Rule* on page 19
- **Address rules**, for more information, see *Creating an Address Rule* on page 21.

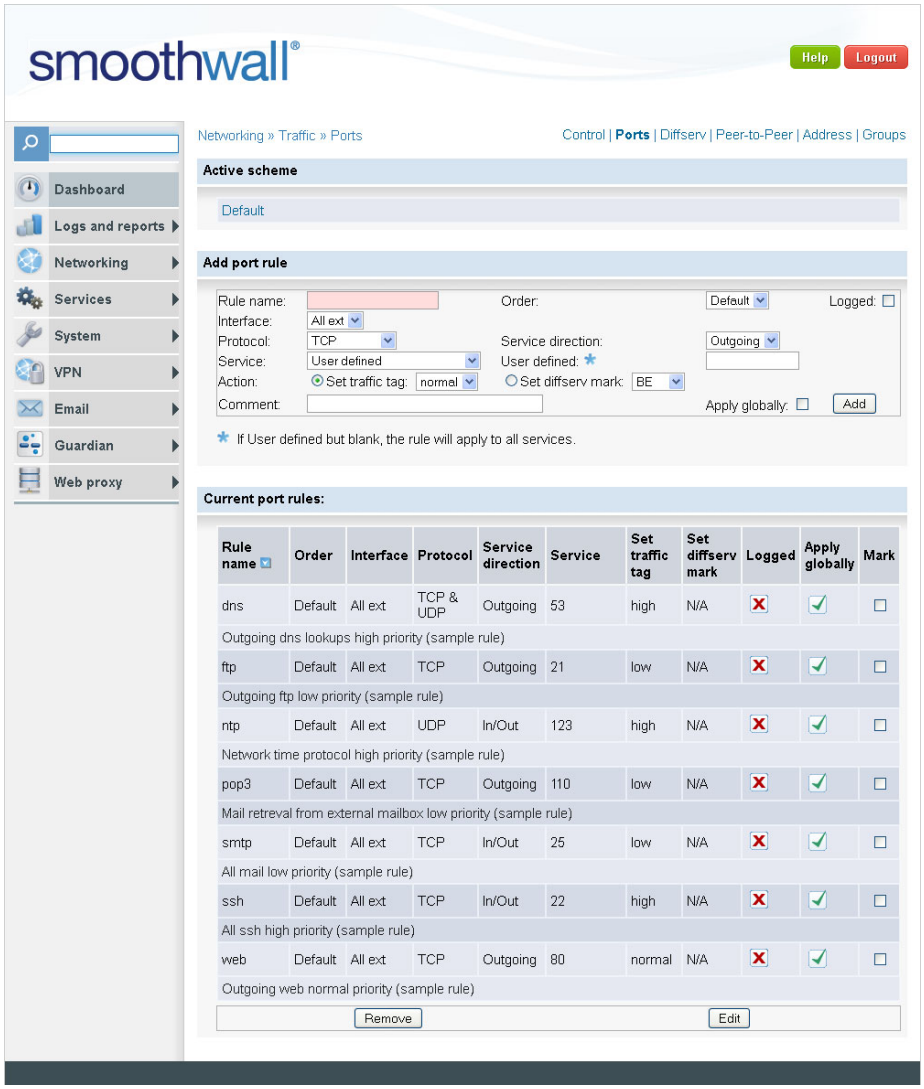
Creating a Port Traffic Rule

Port traffic rules identify and categorize network traffic based on the traffic's destination port.

Port traffic rules can be applied globally to all Internet traffic or as part of an address rule which can be selectively applied to particular network hosts.

To create a port traffic rule

1 Browse to the **Networking > Traffic > Ports** page.



2 Configure the following settings:

Control	Description
Rule name	Enter the name for this rule. Rule names may contain only alpha-numeric characters and the underscore (_) character.
Order	Determine the order for explicitly controlling the order of rules if it is important which rule gets ambiguous traffic. Without explicit order, SmoothTraffic will generally do as follows: • traffic classification associated with a logged in user takes precedence over everything then • rules with both source and destination addresses are tested before • rules with only one address which are in turn more important than • rules with a port component then • any other sort of rule. With order, any rules with a specified order will get tried after the logged in user test but before everything else. Order 1 rules then order 2 and so on.

Control	Description
Logged	Select to generate log entries for this rule. **Note:** This option can generate large amounts of data, and rapidly consume resources, processing power, disk space, etc. It should be used with care.
Interface	Specify which external or internal interfaces the rule will apply to.
Protocol	Select which protocol the rule will apply to. Note that for some protocols, the Service and Direction fields may not apply. **UDP** – applies this rule to UDP traffic. **TCP** – applies this rule to TCP traffic. **TCP & UDP** – applies this rule to TCP & UDP traffic. **ICMP (1)** – applies this rule to ICMP traffic (Ping etc.) **GRE (47)** – applies this rule to L2TP VPN traffic. **ESP (50)** – applies this rule to ESP/IPSec VPN traffic. **AH (51)** – applies this rule to AH/IPSec VPN traffic. **All** – applies this rule across all protocols. The default option is TCP, which should work in the vast majority of cases, as most services use the TCP protocol. The behavior of protocols other than TCP to having packets delayed and dropped will differ. SmoothTraffic will try its best to delay rather than drop packets to achieve rate slowing.
Service direction	From the drop-down list select the direction. The default is **Outgoing** which is used when a computer from the local network is accessing an external data source on the Internet. If the rule is to be applied to computers on the local network that provide a service to external users on the Internet, select **Incoming**.
Service	Select from the list of the common IP services, including POP3 and SMTP for email and HTTP and HTTPS for web browsing. The list also contains services that many organizations will want to control, such as Real Audio and MSN Messenger. **Note:** The list is not exhaustive, since many different Internet enabled applications specify their own default port usage. Choose the User defined option to cater for unlisted services and specify the particular port or range of ports it uses in the adjacent User defined field.
User defined	This must be left blank if a pre-defined service has been chosen from the Service drop-down list. If User defined was chosen as the service, a single port number or port range can be specified. A port range is specified as two port numbers separated by a colon (:) character. For example, `71:74` would make the rule apply to all ports from 71 through to and including 74. Except for the colon separator character, port numbers must be numeric and have a value of between 1 and 65535. Ports only apply to TCP and UDP protocols. If a protocol other than these is chosen, including All, then the service must be set to User defined with the User defined field blank.

Control	Description
Action	Used to select the traffic tag or differentiated services (diffserv) mark that will be applied to the traffic managed by this rule. **Set traffic tag** – Sets an internal traffic tag which categorizes the traffic according to the active scheme **Set diffserv mark** – Assigns a TCP/IP diffserv mark. Diffserv marks are a way of assigning a special marker to a particular packet which can then be honored by any computers, routers or traffic management systems lying upstream of your Smoothwall System. **Note:** SmoothTraffic will also allow these options to be preserved in IPSEC (encrypted) traffic.
Comment	Enter a description of the rule.
Apply globally	Select to apply the rule globally to all applicable traffic. If this option is not selected, apply the rule to IP addresses and networks as part of an address rule. See *Creating an Address Rule* on page 21 for more information.

3 Click **Add**, the rule is added to the list of current port rules.

4 To enable the rule, in the Current port rules area, select **Enabled**.

Creating Diffserv Traffic Rules

The Diffserv (differentiated services) page is used to create rules which SmoothTraffic can interpret and use to either assign a new diffserv mark, or assign traffic containing a specific diffserv mark to a specific tag as defined by the active traffic scheme.

To configure diffserv settings:

1 Browse to the **Networking > Traffic > Diffserv** page.

2 Configure the following settings:

Control	Description
Rule name	Enter a name for this rule. Rule names may contain only alpha-numeric characters and the underscore (_) character.

Control	Description
Order	Specify the order in which rules are processed. This option can be useful in certain cases where one rule is similar to another rule.
Logged	Select to generate log entries for this rule. **Note:** This option can generate large amounts of data, and rapidly consume resources, processing power, disk space, etc. so it should be used with care.
Interface	Select which interface the rule will apply to.
Mark	Specify the diffserv mark to identify traffic by. Choose from: **BE** – Best Effort (BE) – no special treatment **AF** – Assured Forwarding (AF) provides assurance of delivery as long as the traffic does not exceed the subscribed rate. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs. **EF** – Expedited Forwarding (EF), commonly used for VOIP, minimizes delay and jitter and provides the highest level of aggregate quality of service.
Action	Select the traffic tag or differentiated services (diffserv) mark that will be applied to the traffic managed by this rule. **Set traffic tag** – Sets an internal traffic tag which categorizes the traffic according to the active scheme **Set diffserv mark** – Assigns a TCP/IP diffserv mark. Diffserv marks are a way of assigning a special marker to a particular packet which can then be honored by any computers, routers or traffic management systems lying upstream of your Smoothwall System. **Note:** SmoothTraffic will also allow these options to be preserved in IPSEC (encrypted) traffic.
Comment	Enter a description of the rule.
Apply globally	Select to apply the rule globally to all applicable traffic. If this option is not selected, apply the rule to IP addresses and networks as part of an address rule. See *Creating an Address Rule* on page 21 for more information.

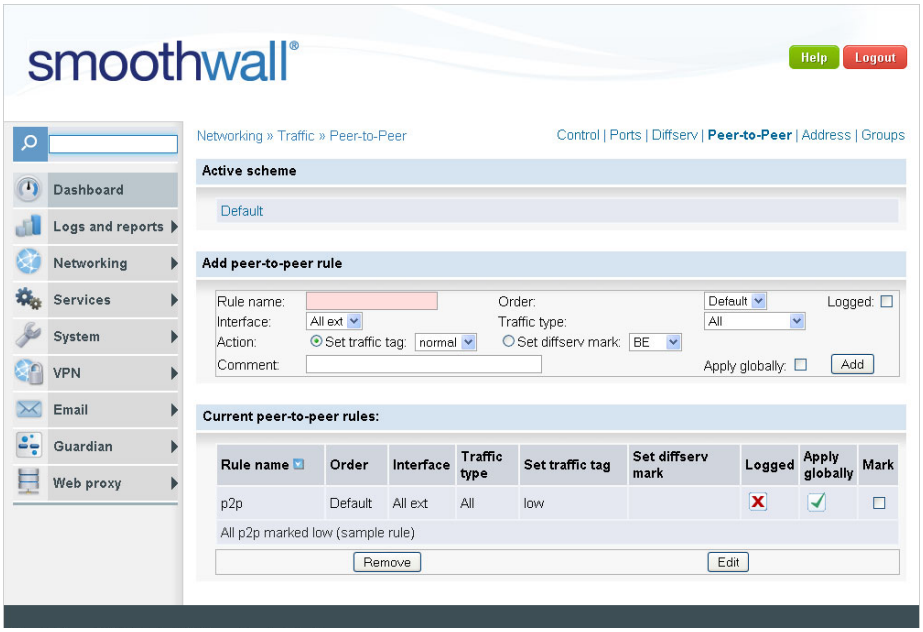
3 Click **Add**, the rule is added to the list of current diffserv rules.

Creating a Peer-to-Peer Traffic Rule

The Peer-to-peer page is used to create rules which SmoothTraffic can interpret and use to manage peer to peer traffic, such as BitTorrent or Kazaa.

To create a peer-to-peer rule:

1 Browse to the **Networking > Traffic > Peer-to-peer** page.



2 Configure the following settings:

Setting	Description
Rule name	Enter the name for this rule. Rule names may contain only alpha-numeric characters and the underscore (_) character.
Order	Determine the order in which rules are processed. This option can be useful in certain cases where one rule is similar to another rule.
Logged	Select to generate log entries for this rule. **Note:** This option can generate large amounts of data, and rapidly consume resources, processing power, disk space, etc. so it should be used with care.
Interface	Specify which interface the rule will apply to.
Traffic type	Specify the diffserv mark to identify traffic by. See *Creating Diffserv Traffic Rules* on page 18.
Action	Set the traffic tag or differentiated services (diffserv) mark that will be applied to the traffic managed by this rule. **Set traffic tag** – Sets an internal traffic tag which categorizes the traffic according to the active scheme **Set diffserv mark** – Assigns a TCP/IP diffserv mark. Diffserv marks are a way of assigning a special marker to a particular packet which can then be honored by any computers, routers or traffic management systems lying upstream of your Smoothwall System. **Note:** SmoothTraffic will also allow these options to be preserved in IPSEC (encrypted) traffic.
Comment	Enter a description of the rule.
Apply globally	Select to apply the rule globally to all applicable traffic. If this option is not selected, apply the rule to IP addresses and networks as part of an address rule. See *Creating an Address Rule* on page 21 for more information.

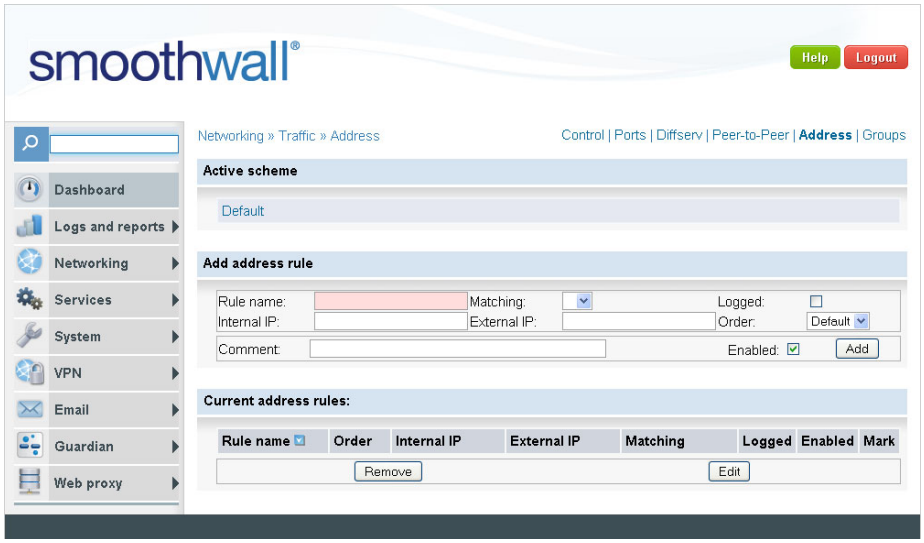
3 Click **Add**, the rule is added to the list of current peer-to-peer rules.

Creating an Address Rule

Address rules are used to selectively apply port, diffserv and peer-to-peer traffic rules to particular network hosts and subnets.

To create an address rule:

1 Browse to the **Networking > Traffic > Address** page.



2 Configure the following settings:

Setting	Description
Rule name	Enter a name for an address rule.
Matching	Specify the rule that will match a particular type of network traffic for this address rule. Only port, diffserf and peer-to-peer rules that are not global will be available here. If there are no such rules, you cannot create an address rule.
Logged	Select to generate log entries for this rule. **Note:** This option can generate large amounts of data, and rapidly consume resources, processing power, disk space, etc. so it should be used with care.
Internal IP	Specify the internal IP address or subnet range to which this address rule will apply. This will be an IP or subnet on a local network. IP addresses, subnets and IP ranges can be specified using the normal SmoothTraffic IP address conventions.
External IP	Specify the external IP address or subnet range to which this address rule will apply. This facility is rarely required but could be used to prioritize traffic to another company site for example. IP addresses, subnets and IP ranges can be specified using the normal Smoothwall System IP address conventions.

Setting	Description
Order	The traffic sub-system will intelligently apply address rules to ensure that they are applied in an appropriate order. However, in some circumstances it may be necessary to use this setting to specifically enforce a particular rule precedence. Address rules can be ordered so that subnet rules can be layered. For example, a generic address rule can be created for an entire subnet such as `192.168.10.0/255.255.255.0`. An additional address rule for administrator systems in the `192.168.10.0` to `192.168.10.10` range could be added. To determine which rule will be applied, assign a higher order value to the administrator's address rule. If you choose not to create layered address rules, the value should be left at Default. It is important that this control is used in a considered manner, as the precedence it specifies will always be enforced, regardless of whether it is optimal to do so or not.
Comment	Enter a description of the address rule to be entered.
Enabled	Select to ensure that the address rule is activated following the next restart SmoothTraffic.

3 Click **Add**, the rule is added to the list of current address rules.

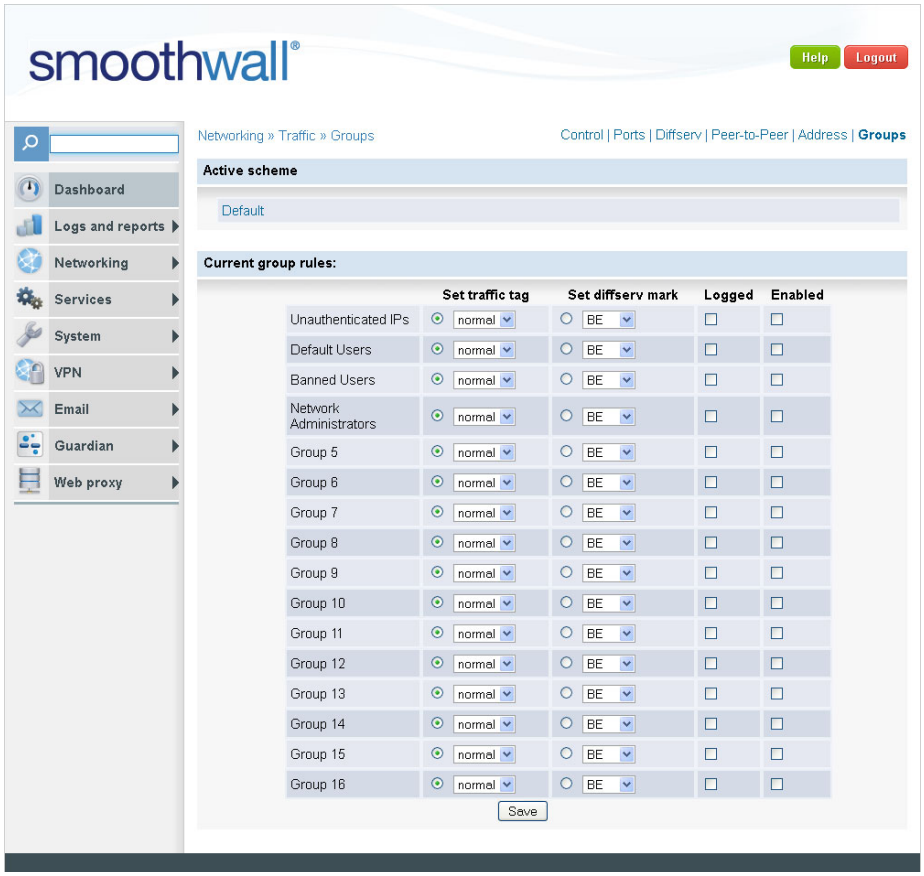
Applying Traffic Rules to Groups

SmoothTraffic enables you to apply traffic tags and diffserv marks to traffic from groups of users.

Note: These settings over-ride any other traffic rules you have configured and applied.

To create and assign a group rule:

1 Browse to the **Networking > Traffic > Groups** page.



2 In the Current group rules area, locate the group you want to assign the rule to and configure the following settings:

Setting	Description
Set traffic tag	From the drop-down list, select to set an internal traffic tag which categorizes the traffic according to the active scheme. For more information, see *Chapter 4, Selecting a Traffic Scheme* on page 10.
Set diffserv mark	From the drop-down list, select the diffserv mark to identify traffic by. The following marks are available: **BE** – Best Effort – no special treatment **AF** – Assured Forwarding – provides assurance of delivery as long as the traffic does not exceed the subscribed rate. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs. **EF** – Expedited Forwarding – commonly used for VOIP, minimizes delay and jitter and provides the highest level of aggregate quality of service.
Logged	Optionally, select to log rule information.
Enabled	Select to apply the rule to the group.

3 Click **Save** to apply the rule.

Removing Rules

To remove a rule:

1 Connect to your Smoothwall System and navigate to the page containing the rule.

2 Select one or more rules to remove in the Current rules area.

3 Click **Remove**.

Note: Before you remove a rule, any address rule that refers to it must also be removed.

Editing a Rule

To edit a rule:

1 Connect to your Smoothwall System and navigate to the page containing the rule.

2 Select a rule to edit in the Current rules area.

3 Click **Edit**. The configuration values for the selected rule will be loaded into the Add rule region.

4 Alter any of the configuration values using the controls in the Add rule region.

5 Click **Add**.

Note: If the name of the rule is changed, a new rule will be created. If you no longer require the original rule, remove it.

Note: Any changes made to a rule will not be applied until SmoothTraffic is restarted.

Chapter 6
Scenarios and Examples

In this chapter:

- A number of typical network scenarios and SmoothTraffic configuration examples for improving Quality of Service.

Guaranteeing Web Browsing

ABC Company's main requirement of their Internet connection is web browsing. However, large amounts of data are regularly transferred over the VPN network to branch offices using FTP. Sometimes branches need to send files back to Head Office. Occasionally Head Office staff need interactive communication with systems at branch offices using SSH.

The problem that the company faces is that web browsing is disrupted and becomes sluggish for lengthy periods of time while the file transfers are in progress.

Solution

To solve the problem:

- Select the Default scheme.
- Choose normal priority for unassigned traffic
- Create a rule configuring Outgoing FTP as low priority.
- Create a rule configuring Incoming FTP as low priority.
- Create a rule configuring Outgoing SSH as high priority.
- Create a rule configuring Incoming SSH as high priority.
- If necessary, create and enable address rules to selectively apply these rules.
- Restart SmoothTraffic.

Note: There is no rule configured for web browsing traffic (i.e. for HTTP protocol). By default, any traffic that does not match any of the configured rules will be given normal_priority so there is no need to configure a rule for the web traffic.

Maximizing Fair Use and Discouraging Inappropriate Use

An educational institution wants to maximize the use of their Internet connection and ensure fair distribution of bandwidth. They also want to discourage students from using P2P software – such activity currently consumes large amounts of system resources, wastes bandwidth and is often used for illegal distribution of copyrighted materials.

Attaining this level of control requires some additional work in configuring extra rules, as all legitimate traffic needs to be identified so it can be allocated to traffic priority categories. This means that any unusual or unauthorized traffic will be allocated to the slow traffic category and be logged.

Solution

- Select the Default scheme.
- Select the slow traffic category for unassigned traffic.
- Enable logging of unassigned traffic.
- Identify all legitimate (i.e. expected) traffic. Web browsing traffic does not require rules to be configured as the Guardian web content filter proxy server is in use. A rule will be required for any use of FTP that does not go via the Guardian proxy – for example, transfers to other systems on the campus VPN.
- Create a p2p rule that identifies all known p2p traffic and puts it into the slow category. Optionally, this can be logged. It will mean that you can differentiate between well known p2p protocols like Kazaa and BitTorrent and some, possibly new, p2p system that will be classified as default.
- Create rules then address rules for all expected type of traffic. If some traffic is only supposed to be coming from specific systems (e.g. PCs belonging to staff and not students) then restrict those rules to specific Internal IP addresses.
- Restart SmoothTraffic.
- Keep a check on the Kernel log file for packets captured by the slow traffic category. If there is any traffic that was overlooked and is to be allowed, create appropriate Core and Address rules for it.

  The end result of this process will be that legitimate traffic is classified and if the students start using some as yet unknown P2P software it will only be able to operate very slowly.

  The advantage of slowing down P2P traffic is that the resources of the computers involved get tied up but not resources in your network connection. Users of the software will most probably give up trying.

Partitioning Internet Connectivity

The Split scheme allows a connection to be split into a number of equal 'Partitions' at the top level. Each of these partitions has its own set of traffic priority categories as per the Default scheme, so the scenarios for the Default scheme are equally applicable to the Split scheme.

As partitions created using the Split scheme do not share bandwidth in any way, it is possible to run completely different sharing scenarios in each scheme without them affecting each other. The downside of this is that the maximum speed of any traffic on an otherwise idle line is the line speed divided by the number of ways it has been split.

Solution

For example, a 1 Megabit (1024 Kbit) line divided four ways gives a maximum speed of 256 Kbit.

- Select the Split scheme.
- Set the required number of partitions using the Optional scheme parameter control.
- Select which traffic priority category from which of the Split partitions should be used for Unassigned traffic. As all unassigned traffic has to go into one partition it is fairest to use the slow traffic category for unassigned traffic and log it, creating explicit rules for all expected traffic as in Example 2.
- Decide which traffic goes in which partition by qualifying address rules with an Internal IP address or a network mask.
- Create port, diffserv and peer-to-peer rules and then address rules for each type of anticipated traffic. It would be a good idea to have known IP addresses using one partition and all 'other' addresses using a different partition. To do this the address rules for the first partition need to be qualified by internal address and the rules for the second partition can be left unqualified. This means that the second partition will be used for any traffic not matching the Internal addresses specified in the rules for the first partition.

- Restart SmoothTraffic.
- Keep a check on the Kernel log file for packets captured by the slow traffic category. If there is any traffic that was overlooked then decide which partition is should belong to and create the appropriate rules for it.

Managing Bandwidth Intensive Applications

XYZ Company has a number of users who want to run a bandwidth hungry application. Ideally, these users should get enough bandwidth to run their jobs properly, while ensuring that there is enough free bandwidth left for other Internet activities like web browsing.

The Multiway scheme extends the high_priority traffic priority category of the Default scheme into a number of equal high priority categories. The sum of all guaranteed categories must not add up to more than 100% the guaranteed bandwidth. However, having several tags of equal priority means that any spare bandwidth will get shared fairly between the multiway tags – before any spare bandwidth is given to the normal or low priority traffic categories.

Solution

- Select the Multiway scheme.
- Set the required number of high priority multiway tags using the Optional scheme parameter control.
- Decide what to do with unassigned traffic. Using normal_priority for unassigned traffic means that rules will only have to be configured for the bandwidth hungry applications/users.
- Decide if all traffic from specific users is to go into their multiway traffic category or just certain protocols. If all traffic needs to be matched then a rule that matches 'All' protocol types to the chosen Multiway traffic category can be used. Otherwise, one or more rules that match specific protocols (e.g. H323) need to be created.
- If necessary, create address rules to bind the rules to particular IP addresses or networks.
- Restart SmoothTraffic.

Note: It must be remembered that SmoothTraffic does not make the Internet connection run faster, it ensures that is used more efficiently.

If too many high priority multiway users are active at once then each may get less bandwidth than they desire but it will be fair share and more than normal or low priority users receive.

If this is not enough to satisfy the bandwidth requirements of an application such as h323 video conferencing then there are two possible solutions to the problem: reduce the number of users that have the high priority multiway privilege or upgrade the Internet connection.


smoothwall®
Web Filtering + Security