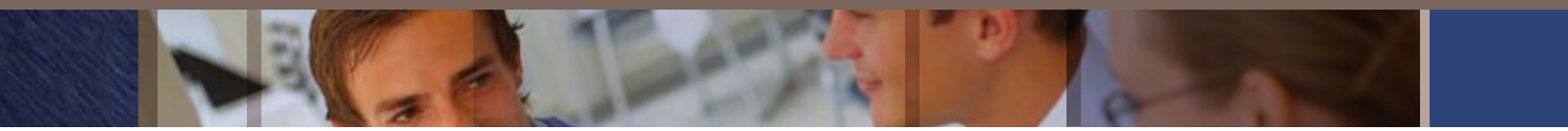


SGOS 5 Series

Integrating PacketShaper with ProxySG

What is PacketShaper?

Blue Coat® PacketShaper® is a network appliance that provides extensive monitoring and shaping capabilities to offer unprecedented visibility, control and reporting of network traffic across a distributed enterprise.

Successful distributed enterprises depend on timely collaboration of customer-critical applications and can't afford operational paralysis due to rigid networks that are unable to support these applications. The PacketShaper is an intelligent overlay that bridges the gap between the network and applications, delivering integrated visibility, control, compression and acceleration in a single device, ensuring optimal application performance and a superior user experience.

What is ProxySG?

The foundation of Blue Coat's application delivery infrastructure, ProxySG® appliances establish points of control that accelerate and secure business applications for users across the distributed organization. As the world's leading proxy appliance,the ProxySG is a powerful yet flexible tool for improving both application performance and security, removing the need for compromise.

The ProxySG features include acceleration for WAN optimization, control for proxy services, performance, reliability, and manageability; the ideal basis for establishing an Application Delivery Network across the organization.

Why Integrate PacketShaper with Blue Coat ProxySG?

PacketShaper and ProxySG together provide a best-of-breed solution for WAN optimization and application delivery. PacketShaper provides extensive application visibility and extended bandwidth management capabilities, while ProxySG offers a comprehensive WAN optimization solution for distributed locations.

Deployment Scenarios

Configuration of the ProxySG for use with the PacketShaper depends on how the devices are deployed. In this document, it is assumed that ProxySG and PacketShaper are deployed in both the core (data center) and branch offices. There are many other deployment scenarios available and you should discuss your specific needs with your Blue Coat Systems Engineer.

Logically, the ProxySG can be placed on either the WAN side or the LAN side of the PacketShaper device (in either the core or branch). The recommended deployment is for the ProxySG to exist on the LAN side of the PacketShaper device.

If the ProxySG is deployed on the WAN side on both sides of the WAN network (see figure 1 below), then all traffic passes through the PacketShaper without any modifications. Any traffic that you want to optimize should not be restricted (shaping needs to be disabled). This is not the recommended configuration. PacketShaper will be unable to give you an accurate view of the traffic volumes going across the WAN if the statistics are taken prior to ProxySG WAN optimization, which includes technologies such as caching and compression. With shaping turned off on the PacketShaper, you also cannot protect the performance of any applications. The value of this deployment scenario is that the PacketShaper is able to accurately classify all traffic across the WAN; the cost is an inability to shape traffic or collect accurate WAN traffic data.

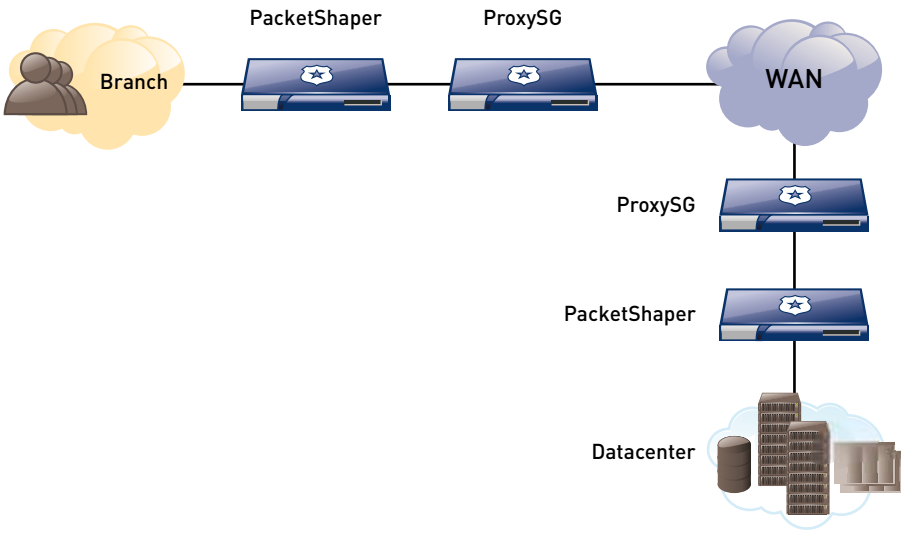


*Figure 1. In this deployment scenario, the ProxySG can be physically or logically on the WAN side of the PacketShaper (*NOT* recommended for deployment)*

If the Blue Coat ProxySG is deployed on the LAN side of the PacketShaper (see figure 2 below), the PacketShaper can detect and classify traffic from the ProxySG automatically with the appropriate plug-in installed. The reporting functionality of the PacketShaper can then provide the actual (optimized) volumes of traffic going across the WAN. If you need to both monitor and control accurate traffic data on the WAN, this is the recommended configuration and deployment. In addition, with the ProxySG Plug-In available from Blue Coat, the PacketShaper can identify Application Delivery Network (ADN) tunnels and show traffic data by tunnel classification.

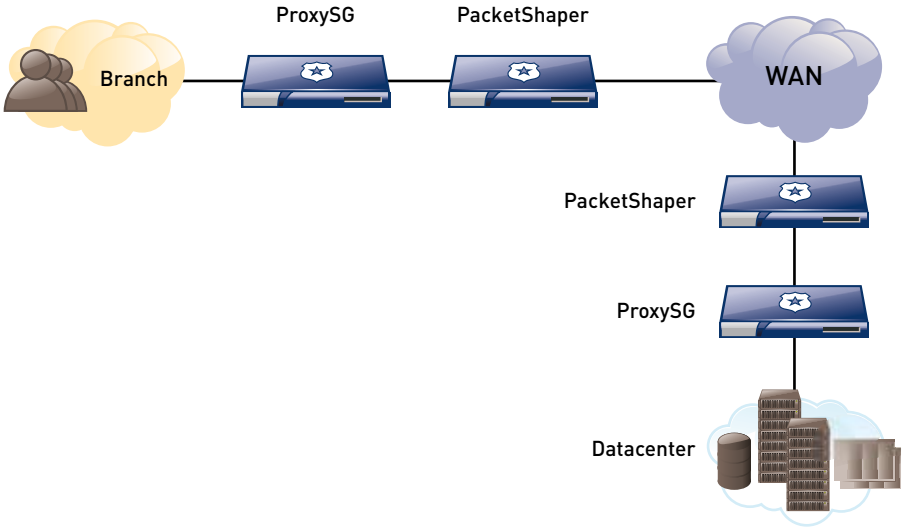


Figure 2. In this deployment scenario, the ProxySG can be physically or logically on the LAN side of the PacketShaper (recommended for deployment)

Configuring the Blue Coat ProxySG and PacketShaper appliances

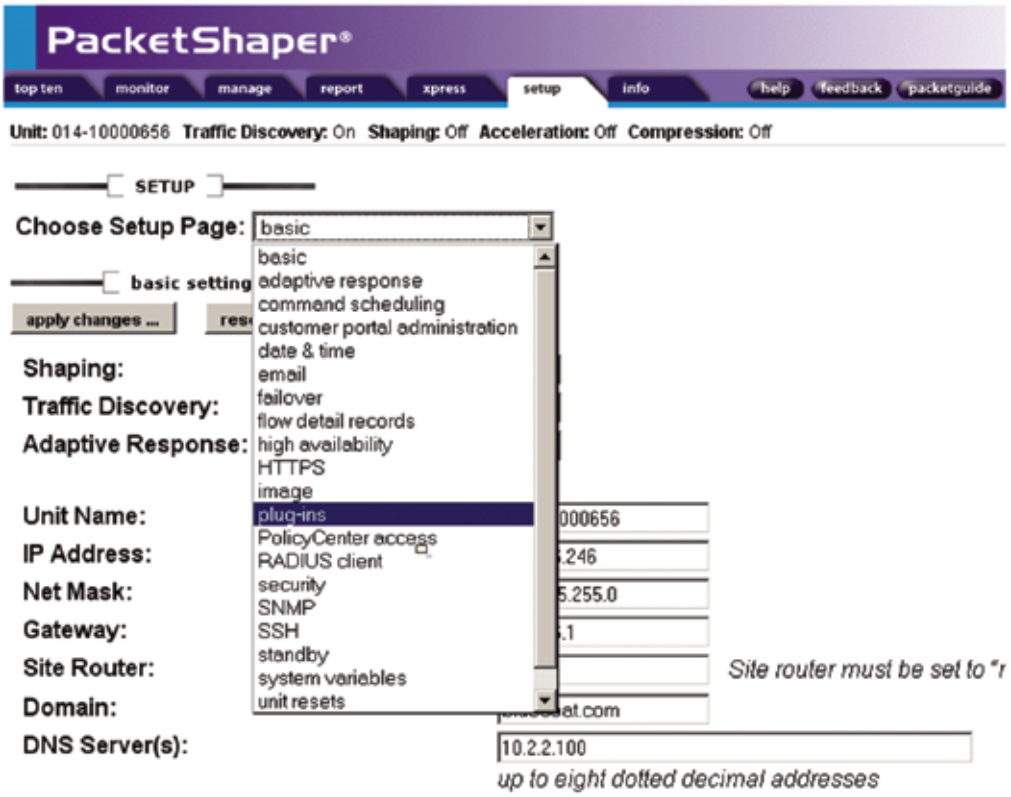
In the deployment scenario where the ProxySG is on the LAN side of the PacketShaper, you should install the ProxySG Plug-In on the PacketShaper. You can also configure partitions, priority policies, and rate policies to provide QoS. Partitions provide aggregate min/max bandwidth for all flows in a class. Priority policies prioritize individual flows and rate policies allocate bandwidth to individual flows.

Installing the ProxySG Plug-In

Plug-Ins are downloadable files that extend the functionality of an existing PacketShaper software release. The ProxySG Plug-In is a Classification Plug-In, which adds the ability to classify and sub-classify ADN tunnels used by the ProxySG to optimize traffic across the WAN.

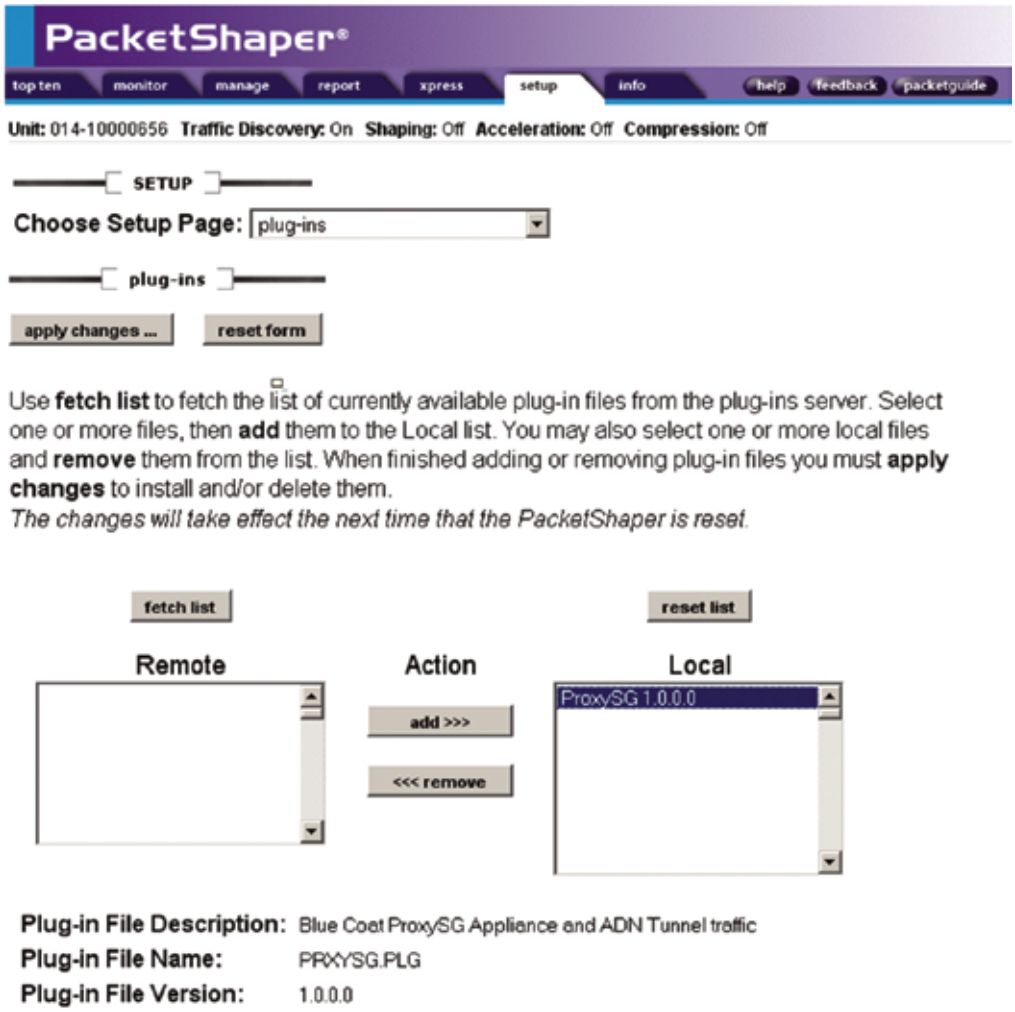
Additional information on Plug-Ins, as well as instructions are available at
http://www.packetshaper.com/documentation/packetguide/current/nav/overviews/plugin-overview.htm

There are a number of ways to install a Plug-In, and instructions on these methods are found on the website above. If your PacketShaper has access to the Internet and is under a Support contract, you can simply add the Plug-In through the GUI administration of the PacketShaper. To install the Plug-In using the Web GUI, access the PacketShaper using a touch login. After you have logged in, select the "setup" tab. Select "plug-ins" using the drop down menu next to "Choose Setup Page" as shown below:



After you have selected "plug-ins", click the "fetch list" button. As long as your PacketShaper has access to the Internet, you should see a list of available Plug-Ins. If you do not have access, or do not see a list, you should visit the URL on Plug-Ins listed earlier, and follow the instructions on manually uploading a Plug-In to the PacketShaper.

After you have fetched the list, select the "ProxySG 1.0.0.0" Plug-In[1] in the "Remote" box and click the "add >>>" button. If there are additional Plug-Ins you'd like to install you can do so at this time. Your screen should appear similar to the one below:



After you have completed your selections, click "apply changes..." You also need to reset the PacketShaper to make the Plug-In take effect. You can reset the box through the GUI or the CLI. After resetting the PacketShaper, your PacketShaper should start using the new classifications immediately, as long as you have Traffic Discovery turned on.

[1] Note: The version number of the plug-in changes as newer versions of this plug-in become available.

A sample view of the monitor page with ProxySG-ADN classifications is shown below:

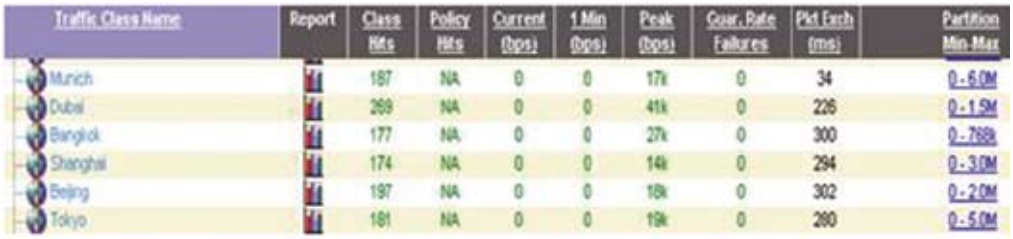
Traffic Class Name	Report	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Diffserv Code Point	Pkt Exch (ms)
Inbound				946k	80k	36.7M		NA
Localhost		20243	20243	946k	80k	1.4M	any	2
FTP		0	NA	0	0	0		NA
HTTP		317	NA	0	0	1.6M		12
Lotus-IM		4043	NA	0	0	15.6M		2
mDNS		219	NA	0	0	2622		NA
MS-Exchange		11	NA	0	0	6.7M		8
ProxySG-ADN				0	0	137k		NA
ProxySG-ADN-1026		55	NA	0	0	35k		33
ProxySG-ADN-1119		1	NA	0	0	2		NA
ProxySG-ADN-135		2	NA	0	0	163		62
ProxySG-ADN-31110		0	NA	0	0	0		NA
ProxySG-ADN-37		0	NA	0	0	0		NA
ProxySG-ADN-60679		0	NA	0	0	0		NA
ProxySG-ADN-88		1	NA	0	0	7		1
ProxySG-ADN-CIFS		10	NA	0	0	1876		31
ProxySG-ADN-FTP		0	NA	0	0	0		NA
ProxySG-ADN-HTTP		26	NA	0	0	46k		24
ProxySG-ADN-MAPI		0	NA	0	0	0		NA
Default		55	NA	0	0	34k		38
SSDP		68	NA	0	0	554		NA
SSL		675	NA	0	0	36.7M		0

Configuring Rate Policies

Rate Policies on the PacketShaper are typically used in conjunction with a partition or traffic flow, and is used to allocate a min and max amount of bandwidth per traffic class. Rate Policies are optional for ProxySG and PacketShaper integration.

Rate Polices are not configured by default. The traffic tree (assuming auto discovery is on) will be populated with all of the inbound and outbound traffic and then partitions. Rate policies and priority policies can be applied to traffic classes and partitions

The extract below shows traffic types, which have been grouped to remote offices (this example uses partitions—you can see the partition size on the right hand side). If you were to select a partition on the left by clicking on it, the following screen allows you to set the rate policies controlling the maximum bandwidth per flow.



Traffic Class Name	Report	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Pkt Exch (ms)	Partition Min-Max
Munich		187	NA	0	0	17k	0	34	0 - 6.0M
Dubai		269	NA	0	0	41k	0	226	0 - 1.5M
Bangkok		177	NA	0	0	27k	0	300	0 - 768k
Shanghai		174	NA	0	0	14k	0	294	0 - 3.0M
Beijing		197	NA	0	0	18k	0	302	0 - 2.0M
Tokyo		181	NA	0	0	19k	0	280	0 - 5.0M

You can create a partition for the tunneled traffic and allocate a maximum % of overall bandwidth for optimized traffic and then continue to shape traffic which cannot be effectively optimized (VoIP, etc) using the PacketShapers.

The Policy Flow Limit feature is enabled by default on any classes in the tree.

It means that the PacketShaper will drop any new connections exceeding this 10,000 flows limit for a specific source IP, such as the ProxySG with ADN traffic, when reflect client IP is not enabled.

The same feature is enabled by default for server but the limit is increased to 100,000 flows.

The only way to disable it is to use CLI with the following command:

```
# policy flowlimit <class_name> none
```

In most deployments where reflect client IP is not being used on the ProxySG, this should be disabled.

You can also decide to not disable it when using reflect client IP on your ProxySG, as it can be a good DoS prevention tool and can monitor if the PacketShaper is dropping packets

Use the CLI to do so. Type the following command :

```
# sys set showdebug 1
# mib tcp
```

It will display the following info :

tcp MIB:		
[0] packets	2844683 [1] pktsScheduled	2802212
[2] pktsClocked	41960 [3] pktsDiscarded	511
[4] dataPkts	1376959 [5] ackPkts	1063592
[6] retransPkts	14992 [7] lruHits	2711077
[8] lruMisses	15432 [9] lruCompares	15458
[10] tcbsReused	0 [11] tcbAllocFails	0
[12] randomEarlyDrops	0 [13] overflowDrops	0
[14] rcFlowsBursting	5 [15] rcFlowsBurstPeak	19
[16] connsAttempted	88300 [17] connsEstblshed	87326
[18] connsAsymmetric	3699 [19] connsClosed	81909
[20] connsReset	1535 [21] connsTimedOut	1660
[22] synRetries	15881 [23] connRefuses	438
[24] modWinScales	0 [25] mssMinimized	8
[26] abortPktsTossed	258 [27] abortBytesTossed	36360
[28] abortPktsNotTossed	58 [29] abortBytesNotTossed	4499
[30] dsChanged	10186 [31] clientFloodBlocks	0
[32] serverFloodBlock1	0 [33] serverFloodBlock2	0

Be sure to examine **[31] clientFloodBlocks** and verify the counter is set to 0 meaning that flowlimit has not dropped any packets.

Additional Technical Tip

Prior to deployment, during your evaluation/test, you should verify if the PacketShaper is enforcing QoS policies. For TCP flows (depending on the policy), the PacketShaper can significantly decrease the TCP window size.

This is typical behavior of TCP rate control (when enforced). Any new TCP sessions start with a 1480 byte window. The window size field of a TCP packet is 16 bits long, so 65535 was the maximum until RFC1323 window scaling allowed for window sizes up to 1 gigabyte, or 16 bits left-shifted up to 14 times.

To clarify, 1GB is a theoretical maximum for window size. 4 MB is the actual recommended maximum supported by the ProxySG.

Summary

PacketShaper and ProxySG offer a value rich solution for application delivery deployments. PacketShaper provides unparalleled visibility and monitoring while ProxySG offers industry leading WAN optimization technology. The optimal deployment is to place the ProxySG on the LAN side of the PacketShaper, to provide visibility into the ProxySG's ADN traffic and provide accurate WAN usage data. Using the ProxySG plug-in, these two platforms provide an easy-to-use, automaticed application discovery that is unmatched in the industry. Together they solve the needs of application delivery to branch offices of every organization.

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000