Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

PacketShaper S-Series

This Privacy Transparency Notice describes how PacketShaper S-Series ("Product") collects and processes Personal Data. Its purpose is to provide You (our current or prospective "Customer") the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

Symantec PacketShaper helps enterprises to control bandwidth cost, deliver a superior user experience and align network resources with business priorities. It is a cloud-connected WAN and internet appliance that provides visibility into applications and web content on the customer's network, along with powerful application-level policy management. A core element of Symantec Network Performance Optimization solutions, PacketShaper is integrated with the Symantec Global Intelligence Network to provide real-time traffic discovery and classification of hundreds of applications and tens of millions of websites.

The PacketShaper delivers full visibility by automatically classifying network traffic by application and content category. Integration with Microsoft Active Directory provides group- and user-based traffic views to help the customer understand who consumes the most bandwidth on the network.

PacketShaper offers application-intelligent Layer 7+ visibility that integrates with the Symantec Global Intelligence Network to provide real-time content categorization. In addition to reporting on network and application utilization and performance, the PacketShaper validates common protocols and tracks what happens to each connection established by any application.

As the proportion of web-based traffic continues to increase, PacketShaper provides management for web-connected applications such as Cloud applications, social media, recreational video, and audio/video communication. All web content requested by users is automatically categorized under more than 80 logical headings, such as Collaboration, Games and Social Networking. This level of web content control and web threat visibility helps the customer assess the impact of recreational traffic, security threats such as malware and phishing, and undesirable content that can raise legal and compliance concerns.

Once traffic has been identified, PacketShaper monitors performance – over 100 stats per application class – in real time.

It tracks the bandwidth consumed by applications and web content categories, the response time of key applications by network and server delay, and key stats such as TCP health, efficiency, and retransmissions to aid in troubleshooting. PacketShaper also powers targeted packet traces for use with protocol analysis tools.

Real-time performance metrics include mean opinion score (MOS), jitter, delay, and loss for voice and video conferencing traffic over RTP. All these capabilities can integrate into the customer's performance management environment, providing intelligent thresholds and alerts before problems occur.

PacketShaper does more than just identification and classification: it provides powerful QoS tools to protect preferred applications and web content categories while containing the impact of undesirable traffic. To maintain high network efficiency and high performance for business-critical

applications traffic must be segmented and prioritized. Control should be built on visibility, so that network administrators can partition traffic and prioritize it by its relevant values to the customer's business. Network administrators may want to restrict recreational video or BYOD downloads to a small but reasonable portion of network bandwidth so it neither impacts important business applications nor interferes unduly with permissible recreational traffic. With the visibility and control provided by PacketShaper, the network is running at its optimal efficiency, while enabling regular monitor and appropriate adjustments if necessary.

The real-time dashboard monitoring tool, part of the PacketShaper offering, provides the customer with immediate intelligence about what is consuming network bandwidth and how network bandwidth is being utilized. The dashboard shows which applications or users are consuming the most bandwidth and how much of the available network bandwidth is being consumed at any given moment. The dashboard updates every few seconds, giving real-time visibility into the status of the traffic on the network.

Further information about the Product is available at:

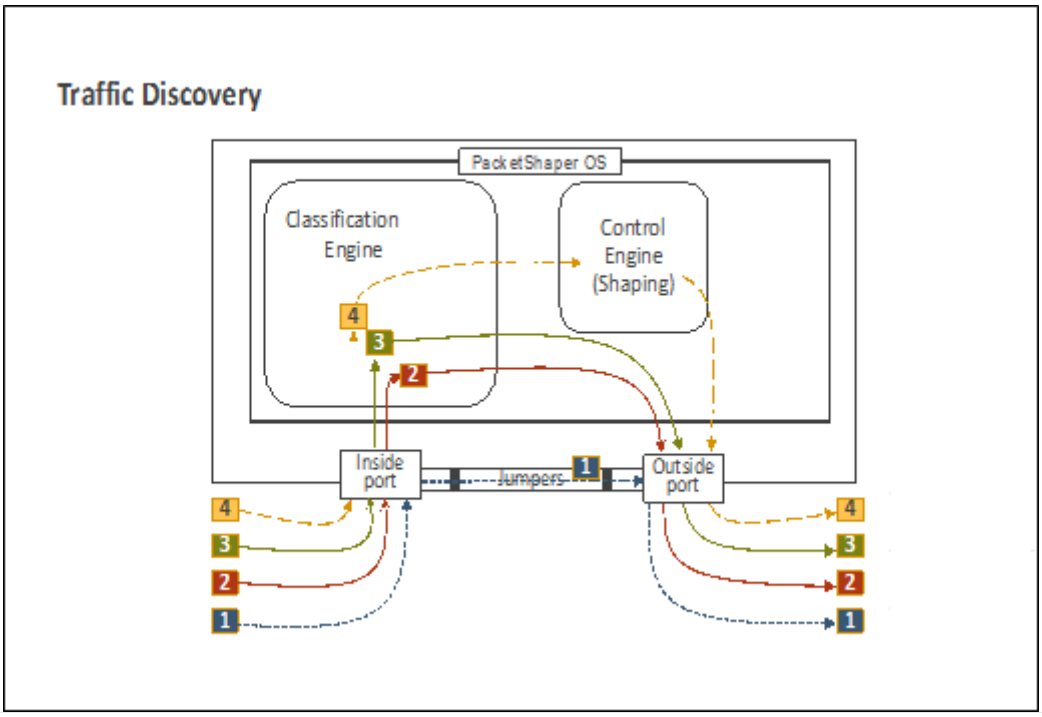
https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=1145507&locale=en_US

2. Personal Data Collection And Processing

Sources of Data

When traffic arrives at the Packet Shaper's Inside Port, the packets pass to the Classification engine for processing, and are then handed to the Control engine for shaping or output scheduling for further transmission. The Classification engine performs processing actions based on the PacketShaper's enabled features. The Traffic Inspection engine works with the Classification engine to discover and classify the traffic, if the Traffic Discovery feature is turned on. If the appliance has an active license, traffic management and shaping is added to the processing.

There are hardware bypass relay jumpers located in between the two network interface ports. This allows the traffic to bypass at wired speed if the appliance is turned off, or if the Shaping module is set to pass thru or bypass.



The 4 paths the traffic can take are:

1. If a PacketShaper that is in-line with a network is powered off, the traffic is bypassed at the hardware level via the jumpers at wire speed.
2. When the power is turned back on, and traffic discovery and shaping are off, the traffic is forcefully forwarded to the Classification engine. All the network traffic is classified in the inbound default and outbound default class according to flow direction. The traffic is forwarded to the outside port immediately.
3. If traffic discovery is on, PacketShaper takes a copy of the packet and sends it to the Classification engine for traffic inspection and discovery. The original packets are sent through the outside port immediately. PacketShaper does not hold on to the original packets for traffic discovery purpose. PacketShaper creates a class for each service type once it sees enough flows as defined in its system variables for auto-discovery.
4. If both traffic discovery and shaping are turned on, traffic that arrives at the inside port is forwarded to the Classification engine. Upon successful classification, the traffic is sent to the Control engine where shaping enforces QoS and forwards to the outside port.

Respective Roles of Symantec and Customer

With respect to Personal Data transmitted from the Customer to Symantec for the purposes of the Product, the Customer is the Controller, and Your Symantec contracting entity as specified in Your applicable Agreement ("Symantec") acts as a Processor. The rights and obligations of both parties with respect to Personal Data processing are defined in the applicable Data Processing Addendum available on the Symantec Privacy - GDPR Portal.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Online identifiers and trackers	Customer employees and contractors, clients and other individuals interacting with customer	To classify traffic information of source and destination application
Network activity data	Customer employees and contractors, clients and other individuals interacting with customer	To manage usage and consumption of Wide Area Network (WAN) Bandwidth
Admin credentials (username and password)	Customer employees and contractors	To administer the appliance

The Product does not need and is not meant to collect or process any Special Categories of Personal Data.

Personal Data Retention Schedule and Deletion

The appliance administrator can delete the admin username and password at any time. Other personal Data is retained for 30 Days for Flow Detail Information, and up to 5 years for Traffic Assessment Reports.

Removing the Flow Details Records requires a Reset to Factory Default. Traffic Assessment Report PDF files are stored in the /public/reports folder on the appliance for five years. The customer can use the PacketShaper File Browser to zip, download, or delete the files.

Further, for the duration of the contractual relationship with the Customer, Personal Data transmitted by the Customer to Symantec is retained as described in the applicable product

description. After the expiry or termination of the contractual relationship, Personal Data is decommissioned except where its retention is required by applicable law, in which case Personal Data covered by such requirement will be further retained for the legally prescribed period.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and external recipients (third party sub-processors), in the facilitation or provision of the Product.

The list of Symantec affiliated entities and their geographical locations are available on the Symantec Privacy - GDPR Portal.

Third-Party Sub-Processors

Symantec involves no third-party sub-processor in delivering the Product to the Customer.

International Transfers of Personal Data

You are advised that Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area based on European Commission Decision C (2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

Management of personal data is the responsibility of the administrator of the PacketShaper appliance. The process for deletion and removal of personal information stored and processed by the appliance is managed via the following factory reset process:

Reset Unit to Factory Default Settings

The quickest way to clear all the PacketShaper configuration settings is to use the Reset All command. This command resets all configurations to the factory default settings:

- All classes are removed, and the traffic tree reverts to its original configuration: /Inbound and /Outbound folders with a Default class for each and a Localhost class for the inbound and outbound directions
- All policies and partitions are removed
- All measurement data is cleared
- Passwords are reset to their defaults

To reset the appliance:

1. Click the Setup tab
2. From the Choose Setup Page list, choose unit resets so that the Unit Resets options appear on the Setup screen
3. Click reset all

Reset the Measurement Engine Data: When measurement data is reset, the data stored in the measurement database is cleared. It's necessary to reset measurement data after upgrading PacketShaper software, to use any new measurement variables introduced in the new software loading a license that affects the number of classes. The customer has the option of resetting all measurement data or certain types of data: link, partition, or class.

To reset the measurement data:

1. Click the Setup tab

2. From the Choose Setup Page list, choose unit resets so that the Unit Resets options appear on the Setup screen

3. Select the type of measurement data to reset: Link, Partition, Class or All

4. Click reset measurement data

After the administrator issues the command, the administrator is prompted to confirm the reset request. Accumulated measurement data is cleared and the unit resets. Measurement and reporting data will not be available for several minutes. Following the reset, loading a new software image should not be attempted, as the file transfer will conflict with measurement engine processing.

Further, pursuant to the applicable Data Processing Addendum, and to the extent possible taking into account the nature of the processing, Symantec will assist the Customer, insofar as this is feasible, with the fulfillment of the Customer's obligation to respond to requests for exercising Data Subjects' rights such as the rights of access, rectification, deletion and objection laid down in Chapter III of the EU General Data Protection Regulation (GDPR).

5. Information Security

Technical and Organizational Measures

PacketShaper offers a variety of methods to make the appliance and its user interfaces secure. The methods range in complexity, security level, and requirements for third-party products. If the customer's LAN is protected by a firewall, then the unit is protected to the same extent that the rest of the hosts are protected. In addition, the customer can choose any of the additional methods described here: https://originsymwisedownload.symantec.com/resources/webguides/packetguide/11.10/index.htm#Topics/solutions/security/add-security-to-packetwise.htm?Highlight=administration

It is Symantec's and all of its affiliated entities' commitment to implement, and contractually require all sub-processors to implement, appropriate technical and organizational measures to ensure an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of Data Subjects. Additional security documentation is available on the Symantec Customer Trust Portal.

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.