Solution Brief

MPLS and NetEnforcer Synergy

Enhancing the control of MPLS-based, enterprise managed services with Allot's NetEnforcer

Abstract

Multiprotocol Label Switching (MPLS) enables service providers to offer QoS-controlled network services to enterprises and to create high-quality virtual private networks (VPNs) that can transfer voice, video and data over IP.

Allot's NetEnforcer traffic management devices are a natural addition to any MPLS network. They enable enterprises to manage their VPNs more accurately, as well as adding important, improved functionality such as:

- Implementing QoS to the network
- Accurate classification of mission-critical, delay-sensitive applications/users
- Monitoring usage and providing real-time, long-term and accounting information

Traffic Classification Options in MPLS Networks

Traffic classification is a key element in achieving QoS in MPLS networks, since it enables the differentiation of traffic according to relative importance. Typically, traffic is classified by identifying and marking it (as a type of service – ToS) at application endpoints or at intermediate devices such as switches/routers or dedicated QoS devices. Such marking consists of setting priority bits in either the Ethernet header or the IP header of each packet which determine the priority to be given to the packet in the network traffic. The marking of endpoints such as bridges is also a possibility for traffic classification, but since this also enables end users to classify their applications, network managers tend not to adopt such methods.

While switches and routers can be used for traffic classification purposes, many of them are limited to Layers 1-4 i.e., identification according to known servers and/or known TCP or UDP ports. Furthermore, many of the newer routers on the market have more advanced classification capabilities, but are harder to manage and can consume valuable processor capacity at the expense of packet forwarding.

On the other hand, dedicated QoS devices such as the NetEnforcer are based on DPI, which enables them to look much deeper into packets and accurately identify both protocols and applications using the protocols. This enables the efficient classification of and marking of WAN-bound traffic. Seamlessly integrating in MPLS networks, such devices can classify and prioritize all traffic before it reaches the access router or carrier edge router, which simply forward traffic.

Layer 7 DPI for MPLS Networks

DPI is the foremost technology for identifying and authenticating protocols and applications (IP flows or sessions in general) conveyed by IP. It provides the ability to analyze network usage, optimize network performance to achieve business goals (i.e., maximize revenues), and get ready for advanced business roles. Consequently, it plays a crucial role in the equation between supply and demand faced by every carrier, telco, service provider and enterprise.

DPI examines Layers 4-7. This is particularly important when positioning DPI and DPI devices such as Allot's NetEnforcer among other categories of devices in the industry. Switches and routers are essentially located at Layer 2 and 3, typically looking at the source and destination address of packets, plus other easily-accessible information such as the VLAN or Type of Service fields. Such equipment provides a response on where packets should be sent. Conversely, DPI devices located at Layer 4 and even higher at Layer 7 first address the question of what the packet really is, and authenticate the nature of applications by constantly monitoring traffic.

In this way, DPI helps operations improve the performance of interactive applications, preventing certain application traffic from unduly hogging resources and contributing to congestion. More and more, DPI technology in general, and Allot's DPI-based NetEnforcer in particular, is being deployed to support management of application traffic, protect against a broad range of network attacks, and more recently to introduce QoS or prioritized services.

Traffic Monitoring and Reporting for MPLS Networks

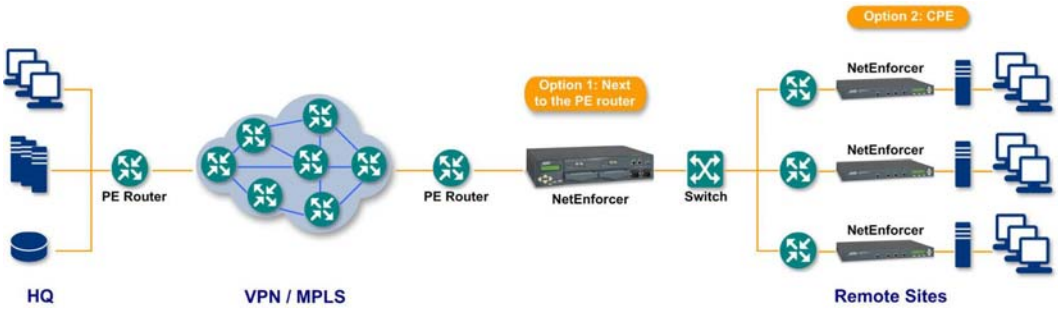
Allot's NetEnforcer provides the crucial visibility of network traffic, and utilizes DPI technology for an in-depth analysis down to single user sessions and single applications to locate and diagnose network problems and bottlenecks. It offers real-time monitoring of traffic using high-resolution, 30-second monitoring of the previous few minutes, as well as short-term monitoring for the collection of highly granular information, with 30-second data representing the last few hours and 5-minute data displaying the last few days.

This constant traffic monitoring data is then used by Allot's NetXplorer, a centralized management software which provides the necessary in-depth insight and analysis to understand networks and directly link between business goals and network traffic and behavior. Facilitating the decision-making process and streamlining network efficiency, NetXplorer uses a single, easy-to-use GUI to deliver unsurpassed network analysis suitable for short-term network troubleshooting or for understanding long-term trend and

usage patterns. Control capabilities include simultaneous provisioning of policies and configuration, updating and distribution of policies to all managed Allot NetEnforcer devices. Reporting capabilities include long-term reporting for evaluation of trends and accurate capacity planning using hourly and daily statistics stored for months or years, and for tracking usage for accounting or charge-back purposes using volume-based reports.

Deploying the NetEnforcer in MPLS Networks

There are two possible areas for deployment of the NetEnforcer: either on the user side of the PE (provider edge) router, or as a CPE (customer premises equipment) next to the customer's switch or router. The closer the NetEnforcer is to the PE, the higher the likelihood to see more accumulated traffic. If the NetEnforcer is deployed between the PE and a number of enterprise links, a more powerful NetEnforcer platform may be required. This is the preferred and cost-effective option, because it eliminates the necessity for deployment of CPEs at each remote site, and also provides each remote site with the capability of controlling network traffic using Allot's NX Policy Provisioner (NPP) self-provisioning interface.



Possible locations of the NetEnforcer in an MPLS network

Allot's NetEnforcer uses the defined policies to classify traffic based on addresses, protocols, application data and time of day, as well as to assign a ToS (Type of Service) marking on the packets. This ToS marking is read by the service provider's equipment and used to assign the corresponding priorities to traffic.

The ability of the NetEnforcer to identify and classify different services takes the load off the PE/CPE routers. This is a major advantage, since the routers do not have to perform classification which consumes a lot of PE resources.

The NetEnforcer can assign each packet a ToS marking which is readable by the PE router. This ToS marking assignment is performed according to user-defined policies, taking full advantage of the NetEnforcer's superior DPI capabilities. When the packet arrives at the PE router, the ToS marking is read. If the E-LSP method is used, the PE router copies the marking to the EXP part of the packet. If the L-LSP method is used, the

PE router decides to which path (LSP) the packet will be forwarded, according to the destination and the value of the ToS bits.

Benefits from Integration of Allot's NetEnforcer

Using Allot's NetEnforcer solution, network administrators can assign policies which define QoS levels per application, user or flow, as well as assign minimum and maximum bandwidth. Furthermore, these policies can be monitored for usage and modified on-the-fly to meet dynamic network conditions.

This offers carriers a number of clear benefits:

- **Enhanced Classification:** The integration of a DPI device on MPLS networks enables carriers to achieve the enhanced classification that will lead to better control of network traffic.
- **Integration of Application Control in Guaranteed Paths:** The NetEnforcer integration in the guaranteed MPLS path enables optimal bandwidth management through control of all running applications, such as prioritization, guaranteeing mission-critical applications, limiting bandwidth-consuming applications, and VLAN/ToS marking.
- **Better SLA Compliance and Guaranteed QoS:** The enhanced classification capabilities, such as DPI Layer 7 classification and prioritization to ensure that only important traffic gets the highest priority in the MPLS network, enables carriers to better comply with their customer SLAs and guarantee of QoS.
- **Better Troubleshooting:** The real time monitoring with 30-second updates enables immediate identification of problems (such as DoS/DDoS attacks, other security threats or connection problems), as they occur.
- **Extra Revenue:** By implementing a “traffic shaping” device on customer networks, carriers can provide enhanced classification capabilities and easier control of applications to customers requiring such services.
- **Extra Services:** Using the optimal visibility of network traffic provided by NetEnforcer's DPI technology and the range of reporting tools available with the NetEnforcer, carriers can offer customers a range of new reporting services, many of which are essential for network administrators to understand exactly what is happening on their networks.

Summary: The NetEnforcer Advantages

Allot's NetEnforcer offers a range of features for the enhanced control of enterprise MPLS networks. These include:

- **Enhanced Classification:** Using the NetEnforcer's advanced DPI capabilities which do not exist in routers and switches and which guarantee successful identification of all traffic types, carriers can optimize MPLS and ensure that class of service assignments are more accurate.
- **User-Defined Policies:** Creation of policies which enable the marking of all packets with the required ToS bit and facilitate PE routers to send traffic on an appropriate path. In addition to the management of traffic bottlenecks performed by the NetEnforcer, this also ensures that packets will travel through the WAN according to priority, while still utilizing MPLS traffic engineering.
- **High Performance:** A single NetEnforcer device can handle 5G of traffic throughput and 4,000,000 simultaneous flows (2,000,000 connections).
- **Centralized Management:** Capable of opening many policies (up to 40,000 pipe policies to manage each customer's link and up to 80,000 virtual channels to manage a variety of applications based on each class of service, the NetEnforcer aids in the management of large numbers of MPLS customers using a single unit, rather than many low-end units. Furthermore, if a multiple unit deployment is required, Allot offers the NetXplorer centralized management server, thereby ensuring that carriers can manage many links in a single, central location which can be positioned in the data center.
- **Real-Time and Long-Term Reporting:** The NetEnforcer's DPI technology coupled with the NetXplorer centralized management system offers extensive monitoring and reporting tools, including drill-down capabilities at 30-second intervals for instantaneous, at-a-glance views of overall network usage and precise identification of who is using what on the network. This is a major troubleshooting and analysis tool that includes access to over 100 real-time graphs and database storage of all reporting data.
- **Alarms:** The NetEnforcer and NetXplorer server include an alarm mechanism which can alert administrators concerning outages, congestion and security-related network events.

Americas	7664 Golden Triangle Drive, Eden Prairie, MN 55344 USA Tel: (952) 944-3100; Toll Free: (877) 255-6826 Fax: (952) 944-3555
Europe	NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France Tel: 33 (0) 4-93-001167, Fax: 33 (0) 4-93-001165
Asia Pacific	6 Ubi Road 1, Wintech Centre 6-12, Singapore 408726 Tel: 65 6841-3020 Fax: 65 6747-9137
Japan	Puri-zaido Ochanomizu 301, Kanda Surugadai 4-2-3, Chiyoda-ku, Tokyo 101-0062 Tel: 81 (3) 5297 7668 Fax: 81 (3) 5297 7669; www.allot.jp
Israel	22 Hanagar Street, Industrial Zone B, Hod Hasharon, 45240 Israel Tel: 972 (9) 761-9200 Fax: 972 (9) 744-3626

w w w . a l l o t . c o m **i n f o @ a l l o t . c o m**