Feature Brief

NetEnforcer®/NetXplorer Market Potential in Enterprise Environments:

Better Network Monitoring
Better Bandwidth Management
Enhanced Security

Introduction

Networks are not just about speed, feeds and bandwidth capacity. Networks are about providing crucial visibility of network usage and business behavior. Allot solutions offer good business sense, in terms of both network operation savings and the ability to create revenue-generating services. Throttling non-business uses of the network and solving contention and competitive situations between IP flows, Allot provides a range of monitoring and detection tools which offer visibility of network performance; enable fast, real-time identification of malicious traffic behavior; and supply extensive tracking/reporting capabilities of applications, flows, connections, ports, protocols and trends.

Purpose of this Document

This document demonstrates how Allot's NetEnforcer traffic management devices and NetXplorer centralized reporting, analysis and proactive traffic management software offer solutions for the major trends and requirements inherent in today's progressive networks, namely:

- Network monitoring
- Bandwidth management
- Enhanced security

Network Monitoring

Network monitoring is one of the largest segments in today's networking market. Enterprises, carriers and SPs are investing large amounts of money in network monitoring tools such as CA's Unicenter, HP's OpenView and Concord's eHealth.

These tools give users the ability to monitor their network devices and their availability, often providing alerts if any device or interface is down. Additionally, they can show bandwidth capacity, such as bottlenecks, and provide indicators concerning the status of the network.

However, without deep packet inspection (DPI) capabilities, all these powerful tools fail to see the full picture, since they are unable to provide network administrators with the essential visibility and understanding of the type of traffic running on their networks, as well as who is actually generating the traffic. Consequently, they are unable to make intelligent decisions concerning the network, because the actual available information concerning the network traffic is limited. To make intelligent decisions, it is mandatory to see both the traffic and the applications. This is performed by Allot's NetEnforcer.

For example: If a network monitoring tool provides an alert that a router interface is down, the network administrator is unable to know and understand in real time what has caused the crash. Could it be because of an attack from a single user or from multiple users? Could it be a DoS or SYN attack? Could it be the result of users working with P2P applications that consume all the bandwidth, causing the router buffers to overflow? Without this information, network administrators face a long and laborious task in order to reach a decision on what to do to immediately in order to solve the problem, and what to do in order to prevent the reoccurrence of such a problem in the future.

Using Allot's NetEnforcer can improve this situation, because it is a network device that integrates DPI technology in all activities, enabling it to analyze and classify all traffic from Layer 2 up to Layer 7. With its real-time monitoring GUI, it shows the exact applications that are running on the network at any given time, as well as who is working with them i.e., both the source and the destination of the traffic.

This unique feature is the missing capability of all other network monitoring tools. Furthermore, it can be used to generate reports in real time (updated every 30 seconds), as well as to generate long-term, trend-indicating reports over different periods, from days and weeks to months and even years.

Allot attaches great importance to the fact that network administrators must be able to understand, utilize and protect their networks at all times. Consequently, the company invests extensive resources and efforts to constantly improve these capabilities, including new DPI features and support for new protocols running over networks. Additionally, the recently-launched NetXplorer centralized, proactive management is designed to give network administrators the easiest tool on the market to generate graphs and reports of all network traffic network from a single, centralized station.

To conclude: Any network monitoring customers considering products such as Unicenter, HPoV and E-health should also integrate Allot's NetEnforcer to obtain the traffic visibility which combines with the networking visibility provided by these monitoring tools. In this way, they will complete their network visibility and understanding capabilities.

Bandwidth Management

Today, networks are critical for any business, with any network failures having a grave impact on business activities. Some of the most common network problems faced by any enterprise are delays in business applications, time outs and re-transmissions. Such problems can be reduced by providing protection against other bandwidth-hungry applications that are not business oriented. Furthermore, the implementation of new technologies such as VoIP and videoconferencing will be unsuccessful unless their performance and quality can be guaranteed. Network problems are further compounded by the actual network users, who often use the network for other activities that have no connection to the workplace.

For example: In any network environment, many users download applications from the web. Others bring programs from home, or receive applications and games by email. This results in a dynamic, unpredictable and constantly changing mixture of applications and protocols. Tracking of links, other network resources and the usage of the network by the different branches is becoming almost impossible.

Using Allot's NetEnforcer can improve this situation, because the NetEnforcer is designed to manage all traffic on the network. This traffic management is achieved in a number of ways:

- Optimization of the WAN Infrastructure: NetEnforcer enables the precise allocation of bandwidth for each application on the network, ensuring that heavy file transfers do not slow interactive business systems such as ERP or CRM, or that email does not degrade the performance of delay-sensitive Citrix and VoIP.
- Maximization of Business-Critical Application Performance: NetEnforcer enables the grouping and definition of policies to allocate bandwidth. For example, this can be achieved by allocating a "pipe" of bandwidth to WAN resources for each remote office, and defining virtual channels within the pipe to allocate bandwidth for applications.

- The drilldown network analysis capabilities offered by NetXplorer enable network administrators to achieve network intelligence – a real-time view of everything occurring on the network, as well as the ability to centralize policy configuration, collection and analysis, determine network bottlenecks and improve the performance of mission-critical applications.
- Classification of Layer-7 Traffic: NetEnforcer supports hundreds of protocols and applications that affect businesses, such as VoIP, P2P, Citrix, Oracle, HTTP, email and video, differentiating between multiple applications, prioritizing between traffic and limiting traffic to a defined percentage of bandwidth.
- Centralization of Management: By providing a single point for policy configuration, data collection and analysis, NetXplorer offers the visibility essential to understand mission-critical application performance by analyzing network usage and application behavior.
- Monitoring Network Activity: Offering more than 100 real-time and long-term views of traffic and performance, NetXplorer's single, easy to-read GUI enables the tracking and investigation of problematic network behavior and active management of traffic, while still guaranteeing quality of service.
- Building of self protecting and self healing networks with Intelligent Alarms: NetEnforcer enables the definition of thresholds on abnormal events and the triggering of alarms such as SNMP traps and email/SMS messages, as well as automatic invoking of corrective actions before problems become costly.

To conclude: Allot NetEnforcer and NetXplorer provide all the tools essential for streamlined bandwidth management. Offering optimal visibility into the root causes of network traffic problems challenging networks today, they enable the fair distribution of bandwidth to ensure satisfaction of all users and smooth network operation. Furthermore, they provide the ability to logically group different sources of data and easily build reports to get a complete breakdown of traffic concerning specific network behavior.

Enhanced Security

As all networks face the threat of DoS/DDoS attacks, worms and hackers, the security market is constantly growing. Everyone seeks to protect their networks by placing a Firewall on their uplink, and many further enhance the protection of their network with IPS and IDS devices. However, in today's progressive networking market, many network applications masquerade as other applications in order to overcome the Firewalls.

For example: File sharing applications such as P2P are frequently updated and change their behavior. In the past, they were just “port jumping”; however, more and more, they run on HTTP (instant messaging applications), SSL (SoftEther) and encrypted packets (Winny, Skype, Bittorrent). The problem here is that they cannot be blocked by Firewalls, and require the analysis capabilities of DPI devices to determine the nature of their behavior.

Furthermore, many networks are becoming more and more vulnerable to different types of connection attacks such as DoS, DDoS and spam mail. Most Firewalls can only control the total number of connections; however, they cannot isolate threats coming from a specific user using a specific application e.g., isolation of the spam mail of an infected user without harming the rest of the user's traffic and the traffic of all other users on the network).

Using Allot's NetEnforcer can improve this situation, because NetEnforcer can help the Firewall to protect the network by closing backdoors. The NetEnforcer's DPI capabilities enable it to block all types of P2P, even if they succeed in passing through the open port left by the Firewall. Together with its one-of-a-kind real time monitoring, the NetEnforcer can show network administrators what kind of applications were able to pass through the Firewall and who is using them. And similar to the Firewall, the NetEnforcer can drop/reject unwanted traffic, thereby completing the "line of defense" together with the Firewall.

The source of threats to network health can also be internal, as well as external. The NetEnforcer helps to protect against threats from both directions by controlling the connections generated by users from the network, and controlling the connections generated to users in the network, thereby providing another line of defense in several ways:

- Control the number of connections generated by each user (internal or external) e.g., to protect from DoS attack, port scanning attempts, etc., it is possible to define a threshold of 100 connections for each user, after which all new connections generated by the user will be immediately blocked.
- Control the number of connections generated by each application (internal or external) e.g., to protect the web server, NetEnforcer can control the number of HTTP connections running to the specific web server.
- Control the number of specific applications generated by each user (combination of two bullets above) e.g., to protect the network from outgoing spam mail, network administrators can define a threshold of 100 mail connections (such as SMTP, IMAP and MS Exchange), thereby only blocking the mail connections that exceed 100 for each user, but still permitting the user to continue generating other traffic with other applications.

To conclude: Any Firewall customer should also implement a NetEnforcer to work together with the Firewall to further enhance security. This forms an application layer security suit that protects against specific malicious and unwanted applications and creates a stronger line of defense for the network. Furthermore, the addition of traffic insight allows network administrators to foresee emerging threats as they develop, by constantly monitoring traffic changes or abnormalities.

To Summarize

Allot Communications is all about broadband traffic management solutions for intelligent, secure networks. Designed for carriers, service providers and enterprises, Allot solutions apply deep packet inspection (DPI) technology to transform broadband pipes into smart networks. This creates the visibility and control vital to manage applications and services, guarantee quality of service (QoS), contain operating costs and maximize revenue.