

Feature
Brief

Optimizing IP-based Services with Allot's NetEnforcer AC-1000 Series

© 2006 Allot Communications Ltd. Allot Communications, NetEnforcer and the Allot logo are registered trademarks of Allot Communications. NetXplorer is trademark of Allot Communications. All other brand or product names are trademarks of their respective holders. All information in this document is subject to change without notice. Allot Communications Ltd., and/or its affiliates (collectively "Allot Communications") assume no responsibility for any errors that appear in this document.

Introduction

This document describes the competitive features of the Allot NetEnforcer AC-1000 series. These features concentrate on the various solutions offered to service providers and carriers, and focus on the following subjects:

- Monitoring
- Quality of Service (QoS)
- Quality of Experience (QoE)
- Home User Policies
- Unidirectional Classification
- Centralized Management
- Security

Monitoring

NetEnforcer is the only device that provides both real time and long-term monitoring. It offers extensive “drill down” capabilities that enable customers to troubleshoot and understand the traffic on their networks in real time, and thereby take any necessary actions immediately. The NetEnforcer’s monitoring tools enable real time monitoring of the type of traffic flowing through the network, as well as determination of the patterns of current network applications. Additionally, since network peaks, bursts and bottlenecks are hard to predict, this real time monitoring enables viewing of them as they occur, which is a crucial feature in the management of such unwanted phenomena.

Quality of Service (QoS)

Allot's Per-Flow Queuing (PFQ) algorithm for QoS enables the NetEnforcer to guarantee delay-sensitive traffic such as VoIP and video on demand (VOD). This is particularly important as many service providers begin to offer multiple services to their subscribers, compelling them to guarantee delay-sensitive traffic over bandwidth-consuming traffic such as P2P. NetEnforcer enables service providers to guarantee specific bandwidth to specific applications and subscribers.

Quality of Experience (QoE)

To provide subscribers with optimal QoE, the NetEnforcer enables the creation of a range of policies suitable for different levels, from all network traffic to each separate subscriber. Using the NetEnforcer, service providers can open up to 80,000 virtual channels (dynamic or static), meaning that they can simultaneously create a different policy for 80,000 subscribers. Furthermore, in each policy it is possible to control the traffic of each subscriber by limit, and to guarantee and control the number of connections for each subscriber.

Home User Policies

Today, many service providers are offering more and more added-value services to their subscribers, such as Internet, VoIP and VOD. However, without appropriate management, such services will congest home user traffic.

Since the NetEnforcer's policy provisioning technology is based on pipes and virtual channels, service providers can open a pipe for each home user that will control and guarantee the different services provided. In particular, using the NetEnforcer AC-10x0, service providers can assign up to 10,000 pipes and up to 80,000 virtual channels. For example, a service provider seeking to provide multiple services such as Internet, VoIP and VOD for each home user with 100 Mbps will create a pipe home user policy with the following configuration:

- VoIP virtual channel: guarantee 1 M
- VOD virtual channel: guarantee 2 M
- P2P virtual channel: limit outbound to 1 M
- Fallback virtual channel: all other traffic

The implementation of such a policy will ensure that each user receives the best quality when using VoIP or VOD, while P2P will only limit foreign users from using the customer's bandwidth. Naturally, this can also be combined with inbound control.

Unidirectional Classification

Many service providers are using Mesh topologies in which sessions can be separated into different paths that usually cannot converge into the shaping device. The NetEnforcer's unidirectional classification capability allows service providers to identify and classify traffic when only one side of the traffic is routed through the NetEnforcer. This is extremely effective for P2P and VoIP traffic, which does not necessarily follow the same incoming and outgoing route.

Consequently, while the NetEnforcer sees bidirectional traffic and uses the data to classify protocol signatures, its improved unidirectional support enables the full classification of many unidirectional protocols, such as FTP, Skype, QQ, eDonkey, RTP UDP, Kontiki, Skype Out.

Centralized Management

Allot's NetXplorer server provides all 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, it is a highly scalable system that uses a single, easy-to-use GUI to deliver unsurpassed network analysis suitable for both short-term network troubleshooting and understanding long-term trends and usage patterns. Control capabilities include simultaneous provisioning of policies and configurations, updating, and distribution of data to all managed NetEnforcer devices. Additionally, the NetXplorer server can fully integrate with Allot's SMS (Subscriber Management System).

For service providers, NetXplorer provides the visibility and tools that deliver traffic and subscriber information and control in broadband networks. This is particularly important in controlling operation costs, reducing subscriber churn, increasing revenues (ARPU) and providing new, differentiated services.

Enhanced Security Features

Allot's NetEnforcer is an ideal tool for detecting and mitigating a range of security threats which affect service providers, such as outgoing spam and DoS / DDoS (Denial of Service / Distributed Denial of Service) attacks. Such threats can severely hinder service provider capabilities to their subscribers, and consequently affect their ability to generate revenues.

The NetEnforcer's enhanced security is based on the use of policies based on pipes and virtual channels. This enables service providers to control the live connections for each subscriber and for specific services/applications. For example, to protect their networks from outgoing spam mail, service providers can create a dynamic virtual channel for each subscriber for the "mail" services only. In this way, the policy will only control the connections of mailing applications, leaving other traffic of the subscriber's connections free. For example:

Name	Source	Destination	Service	QoS
VC subscribers	Any	Any	Email*	Max. 70 connections

* Contains SMTP, Exchange, IMAP, POP3

Alert Mechanism

Allot's NetEnforcer is equipped with an alert mechanism that can automatically be triggered whenever suspected malicious activity is detected on a virtual channel, on a pipe, or on the entire NetEnforcer, such as:

- Any user-defined application / traffic type / protocol breaches a user-defined threshold for active connections
- Any user-defined application / traffic type / protocol breaches a user-defined threshold for new connections
- Any user-defined application / traffic type / protocol breaches a user-defined threshold for bandwidth consumption
- Automatic triggering according to user-defined time intervals
- Any combination of the above

Whenever an alert is triggered, the NetEnforcer can take automatic action, according to the service provider preferences, such as:

- Send an immediate alert mail to the network administrator.
- Activate the outgoing spam detection module for detailed identification of suspected outgoing spammers and/or automatic enforcement of spam prevention policy.
- Any combination of the above.

Automatic Detection Module (ADM)

Allot's NetEnforcer AC-1000 series provides an automatic detection module for identification of various types of malicious/infected users, including suspected outgoing spammers and suspected DoS / DDoS attackers. Using this module, service providers can perform a range of activities, such as:

- Identify top users generating malicious activities.
- Define exclusion lists of users which should not be treated as malicious, irrespective of the malicious activity detected e.g., the service provider test network.
- Define lists of users who must be included in the ADM report, irrespective of the malicious activity, thereby enabling the monitoring of the behavior of known infected users.
- Define automatic actions:
 - Send email to the network administrator, including:
 - Lists of all users identified as malicious, and connection information for connections suspected as malicious.
 - List of active connections that are not defined as malicious for every user identified as generating malicious traffic. This list can help in identifying the source of the infection and offer value added services for infection removal.
 - Associate suspected users to pipes / virtual channels designated to control malicious traffic. Such suspected user pipes / virtual channels can have strict QoS restrictions that disable the user's ability to generate malicious traffic e.g., limit the number of connections for mail (outgoing spam control), limit bandwidth (DoS / DDoS flood attacks control), and limit the number of connections (DoS / DDoS SYN attack control).

Summary

In today's highly competitive market, Allot's NetEnforcer AC-1000 series of traffic management devices offers service providers and carriers a range of features and advantages. These focus on the provision real time and long-term network monitoring; Quality of Service which guarantees business-sensitive traffic such as VoIP and VOD; Quality of Experience through the creation of different policies for different levels; home user policies to enable the management of added-value services and prevent congestion of traffic; unidirectional identification and classification of traffic when only one side of the traffic is routed through the NetEnforcer; centralized management through NetXplorer, offering all the necessary in-depth insight and analysis to understand network traffic and streamline efficiency; and enhanced security solutions to detect, mitigate and alert administrators about security threats.