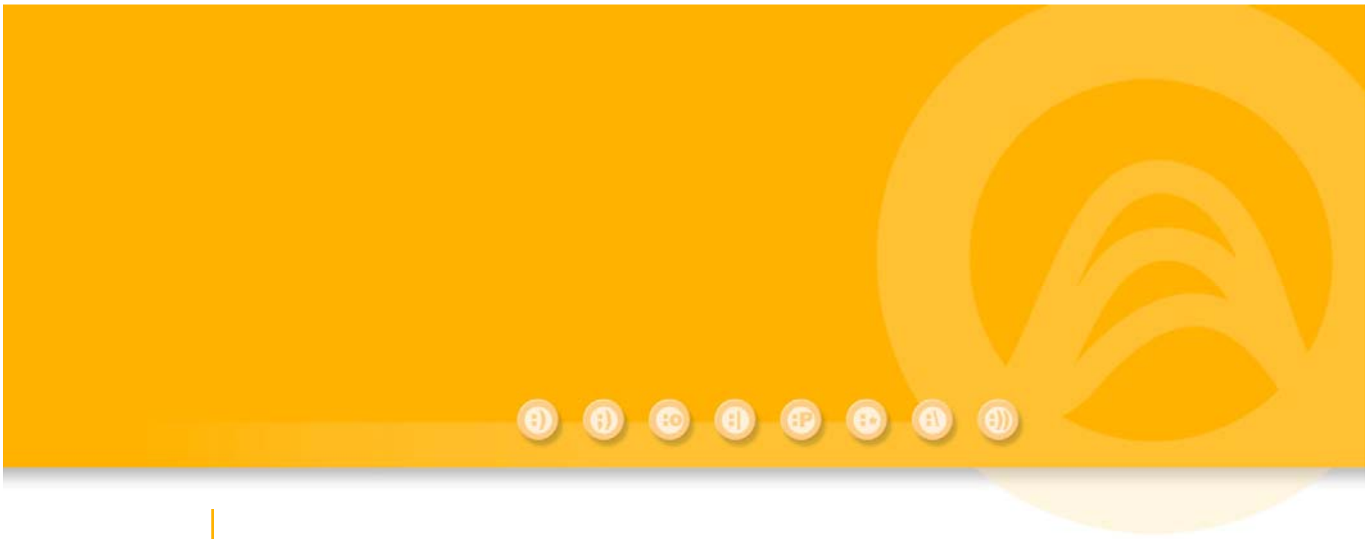


Solution Brief

Mitigating Outgoing Spam, DoS/DDoS Attacks and Other Security Threats

Introduction

Broadband service providers (SPs) have traditionally dismissed security threats as subscriber problems. However, they have not accounted for the constantly growing threat of malicious hackers who exploit subscriber vulnerabilities and the generous bandwidth capacity of broadband networks to launch distributed denial of service (DDoS) attacks, spam mails, and other electronic pests.

These network security threats are somewhat unique to SP networks, and cannot be solved by the tools commonly used by individuals or enterprises. For example, if a provider's IP scanning threat is not mitigated at the outset, malicious code will spread quickly, ultimately bringing down the network.

Consequently, to prevent problems such as degraded user performance, drained network resources, impaired infrastructure, increased help-desk costs and lost business as disgruntled users switch to other providers, broadband SPs need to deploy special tools capable of recognizing and isolating security threats.

The traffic management solutions offered by Allot Communications provide SP network administrators with a range of security solutions which guarantee secure, available and controlled broadband access. The Company’s NetEnforcer® devices offer robust capabilities that empower network administrators to reliably identify and deal with every possible source of infection. These include the configuration of early-warning mechanisms that trigger automatic actions to mitigate attacks before they become a liability to the network, and on-the-fly policy allocations to minimize the possibility of similar attacks in the future.

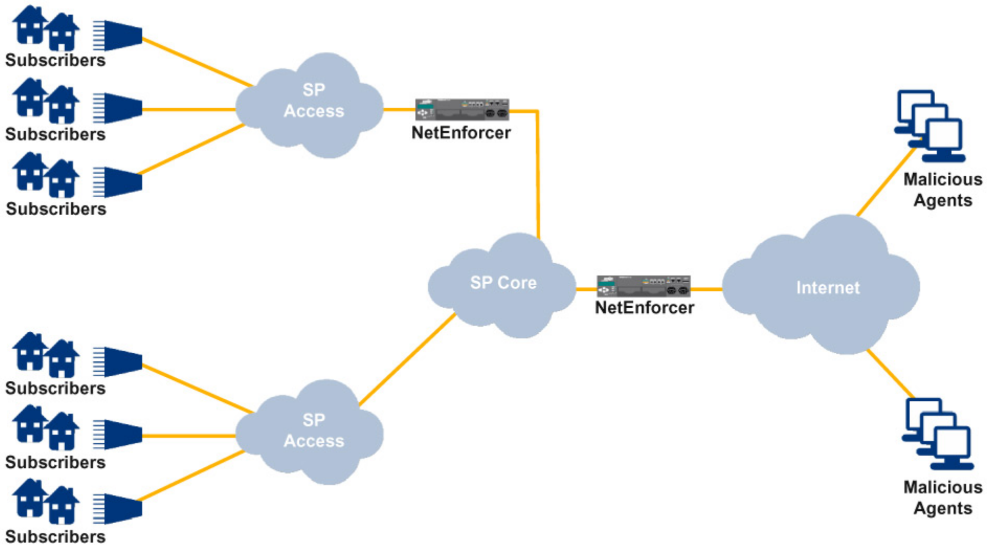


Figure 1: Typical Deployment of Allot NetEnforcer in SP Environment
The Allot NetEnforcer can be located between the SP access and SP core, where it safeguards the SP core against malicious subscribers such as outgoing spammers, and between the SP core and the Internet, where it safeguards the SP core against external attacks on the network, such as DDoS attacks. Optimal security is provided when the NetEnforcer is positioned in both points of presence.

The Challenge

The most prevalent and problematic attacks for today's broadband SPs are:

- Denial of Service (DoS) / Distributed Denial of Service (DDoS), such as SYN attacks, DNS flooding and ICMP attacks
- Outgoing spam
- Other security threats, such as IP scanning and port scanning

DoS/DDoS Attacks

A recent Symantec report (Symantec Internet Security Threat Report, Volume VIII, September 2005) shows that two out of the ten most common Internet attacks are DoS/DDoS attacks - assaults which flood networks with so many additional requests that regular traffic is either slowed or completely interrupted. DoS attacks interrupt network service for a period of time, while DDoS attacks use multiple computers throughout a previously infected network to send out bogus messages and thereby increase the amount of phony traffic.

DOS/DDoS attacks work by sending a lot of SYN packets which generate many half-open TCP connections, but fail to establish a connection. Typical SP network behavior indicates that on average, 5% of new TCP connection requests fail. However, DoS/DDoS attacks greatly increase this failure rate to more than 50%. Exploiting faulty resource management vulnerabilities on servers and network elements, today's most common DoS/DDoS threats on the Internet succeed via unintentional cooperation among many infected computers.

Such SYN attacks are successful because the target computer allocates resources to establish connections. However, since the connections are never established, resources quickly become fully consumed, resulting in a denial of service to legitimate clients. Network elements sensitive to the number of flows – such as firewalls or routers running NetFlow - may also be seriously affected by such SYN attacks, because of the sudden burst in connection requests.

Other DOS/DDoS attacks are based on DNS floods which overwhelm DNS servers with DNS requests until resources on the server are exhausted and server availability is blocked. Such DNS server malfunctions may eliminate the ability of subscribers to browse.

Finally, ICMP attacks are DoS/DDoS attacks launched using the ICMP protocol. Overwhelming a target computer/router or any other network element with ICMP requests until all resources are consumed, they result in denial of service e.g., the sending of many ICMP requests to a router can degrade its forwarding performance. ICMP attacks take advantage of ICMP protocol vulnerabilities (such as broadcasting and echoing), and vast traffic loads are generated by sending only minimal information. Despite the fact that such attacks are now less prevalent since routers and other network elements have incorporated defense mechanisms (for example, most deployed routers will not forward an ICMP echo sent to a broadcast address), this threat still requires identification and mitigation because ICMP attacks are primarily used in IP scanning to detect vulnerable computers.

Outgoing Spam

Outgoing spam consists of unsolicited, undesirable email created by malicious agents monopolizing subscriber computers to send out large volumes of email messages. We are all well acquainted with this phenomena, whether it's commercial advertisements, fraudulent messages, false information, hoaxes, technical errors, junk, false undeliverable messages, or foreign language fonts, bad encodings and unreadable messages. Distributed from the SPs domain (usually without using the SPs mail servers) to the Internet, it takes less than 100 infected subscribers to send enough spam to blacklist an entire SP domain by other SPs, thereby blocking access to mail servers. A typical example is the recent blacklisting of a major Asian-Pacific provider for outgoing spam, which was traced to 84 spam-relay sources.

In the past, SPs mitigated the distribution of spam email using anti-spam tools on their mail servers. However, spammers are constantly seeking more sophisticated methods for spreading their malicious packages, such as using SMTP-relays resident on unwitting subscriber systems.

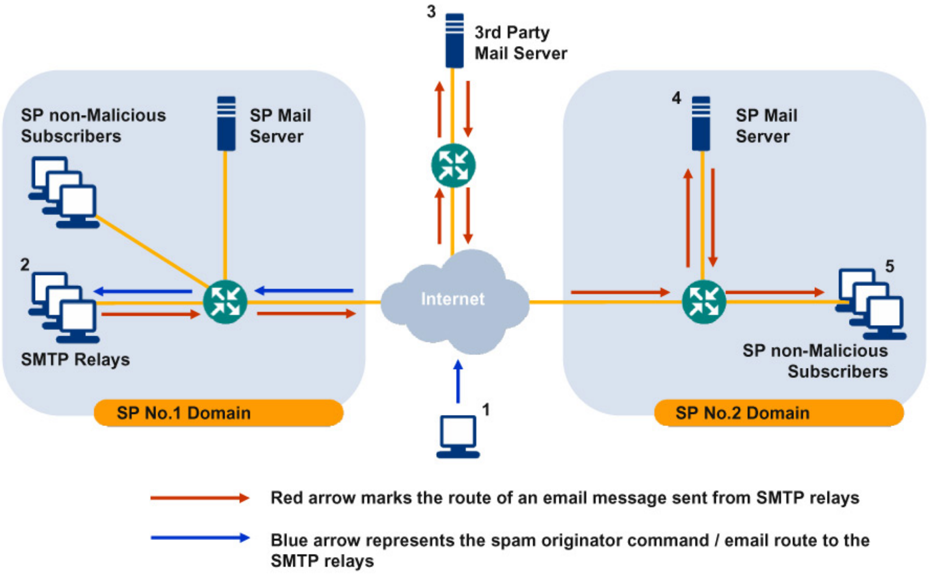

3
3rd Party Mail Server
SP non-Malicious Subscribers
SP Mail Server
2
SMTP Relays
SP No.1 Domain
Internet
1
4
SP Mail Server
5
SP non-Malicious Subscribers
SP No.2 Domain
Red arrow marks the route of an email message sent from SMTP relays
Blue arrow represents the spam originator command / email route to the SMTP relays

Figure 2: Typical Example of SP Blacklisting
The spam originator (1) sends a command/email to the SMTP relays (computers sending outgoing spam) in SP No. 1 domain (2). The SMTP relays (2) send spam mail through a third-party mail server (3), possibly through a legal account with the third-party mail server, such as a MS Hotmail account. The mail is received at SP No.2 mail server (4), which sends it to its clients (5).

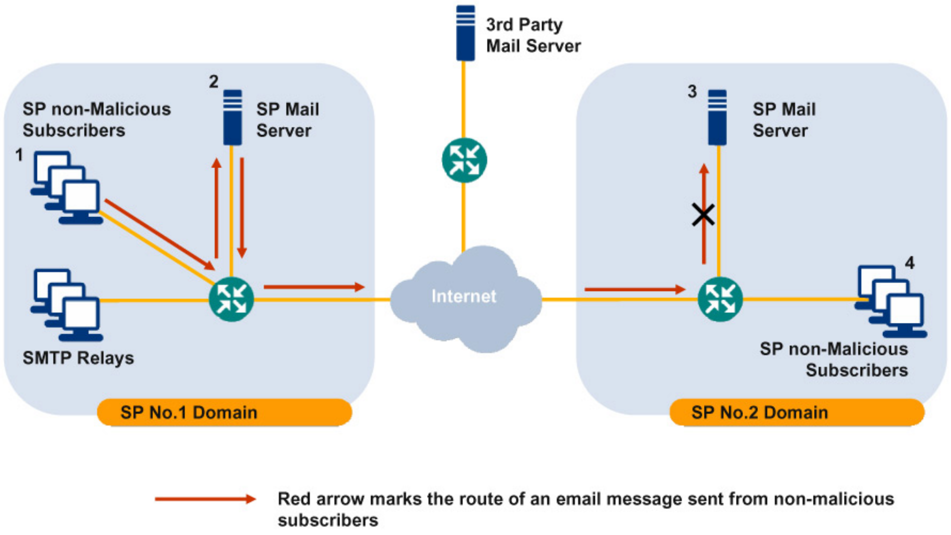


Figure 3: Typical Example of SP Blacklisting
SP No.2 mail server (3) classifies the mails sent from the SMTP relays as spam and blocks SP No. 1's entire domain. SP No.1's subscribers (1) try to send legitimate mails to SP No. 2 subscribers (4) but the mails are blocked by SP No.2 mail server (3).

Other Security Threats

SPs face a range of other security threats, such as IP scanning and port scanning.

In IP scanning attacks, one or more computers generate many SYN requests to a specific port number - or sometimes generate ICMP requests - to random or sequentially numbered IP addresses in order to identify computers present and listening on that port number. Such computers are then targeted for different types of malicious activity. For example, IP scanning is often used by worms to rapidly identify vulnerable computers, while in other cases, attackers can remotely take control of an IP address and use it to launch distributed attacks.

In this way, IP scanning can often devastate broadband networks by causing immediate threats, such as performance degradation of network elements sensitive to the number of connections, and secondary threats, since the scanning activity is often a symptom of an infection’s attempt to spread. Consequently, by mitigating scanning, administrators can diminish the spread of worms in the network. Furthermore, if IP scanning activities are not detected and minimized at the outset, they spread like an epidemic, as other infected computers start scanning the network, bringing down networks in a very short period of time.

Port scanning is used to detect active services (port numbers) on the target machine, exploiting known vulnerabilities related to those services/ports. For example, computers with port 445 (the common port for Microsoft File and Printer Sharing) open are often targeted by malware, such as the Sasser worm.

Meeting the Challenge: Allot NetEnforcer

The impact of any given threat is often very different for SPs and individual subscribers. A relatively harmless threat to subscribers, such as SMTP relays, may present a severe security threat to network infrastructures. However, it is clear that carriers, SPs, subscribers and enterprises are all threatened by the following most prevalent and problematic attacks:

- Denial of Service (DoS) / Distributed Denial of Service (DDoS), such as SYN attacks, DNS flooding and ICMP attacks
- Outgoing spam
- Other security threats, such as IP scanning and port scanning

The Allot NetEnforcer traffic management platform presents today's broadband operators with an integrated threat management solution. A robust suite providing visual evidence of potential abusers and malicious applications at Layer 7, it enables on-the-fly policy management to identify and isolate problems at their source, and integrates early-warning mechanisms to alert administrators to malicious traffic patterns and protect network availability through pre-designated network actions.

The advantages of the Allot NetEnforcer solution concentrate on three main areas of activity:

- Real-time identification of attacks
- Real-time reporting
- Mitigation of threats through enforcement

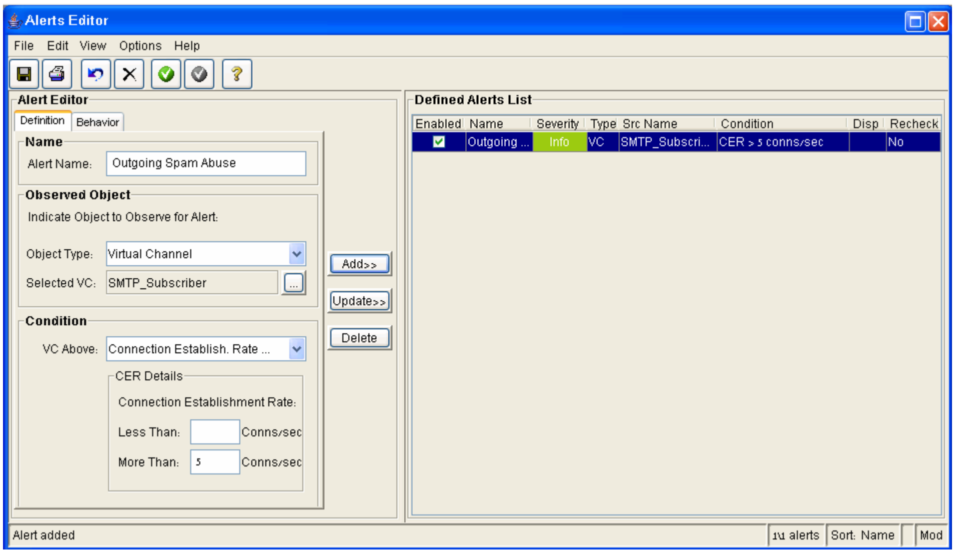
Real-Time Identification of Attacks

The Allot NetEnforcer applies deep packet inspection (DPI) to facilitate rapid, real-time identification of malicious traffic behavior over the network. It provides network administrators with a range of monitoring and detection tools according to the traffic class/application/network/subscriber, and includes hundreds of real-time distribution graphs to track subscribers, applications, flows, connections, ports, protocols, trends and other parameters.

Typical examples of these capabilities include:

- Monitoring the number of active connections (since sudden, rapid increases in active connections is indicative of many forms of security attacks).
- Monitoring the rate of new connections establishment (since sudden, rapid increases is another strong indicator of an attack).
- Monitoring ongoing connection establishment (half-open connections).
- Monitoring connections that are not application-specific (can be any TCP protocol).
- Monitoring live connections that are rarely established from SYN attempts (outgoing spam is identified per protocol, and SYN attacks are identified per subscriber or per NetEnforcer device).

- Monitoring of specific protocols, such as DNS and ICMP.



Name

Alert Name: Outgoing Spam Abuse

Observed Object

Indicate Object to Observe for Alert:

Object Type: Virtual Channel

Selected VC: SMTP_Subscriber

Condition

VC Above: Connection Establish. Rate ...

CER Details

Connection Establishment Rate:

Less Than: Conns/sec

More Than: 5 Conns/sec

Defined Alerts List

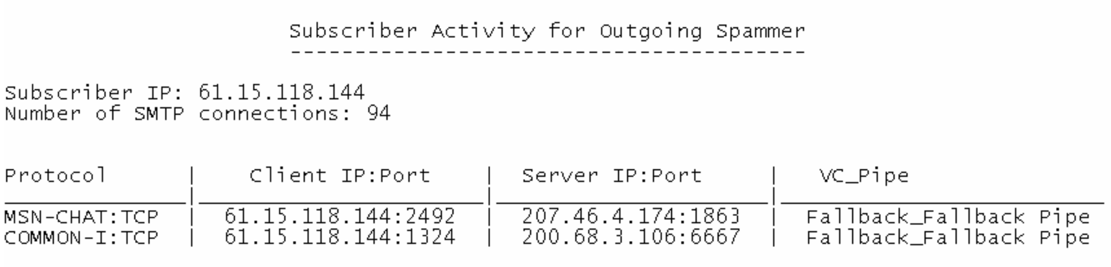
Enabled	Name	Severity	Type	Src Name	Condition	Disp	Recheck
☑	Outgoing ...	Info	VC	SMTP_Subscri...	CER > 5 conns/sec		No

Alert added | 1/1 alerts | Sort: Name | Mod

Figure 4: Alert Configuration for Outgoing Spam Detection
The alert is configured to be activated whenever a subscriber has more than 5 new SMTP connections per second.

To further identify various types of malicious/infected subscribers, the Allot NetEnforcer also features a user-configurable automatic detection module (ADM) which can:

- Identify top outgoing spammers by SMTP connections (all internal subscribers that have more than a user-defined number of active SMTP connections).
- Identify top SYN attackers (all internal/external subscribers that have more than a user-defined number of half-open connections).
- Detect any user-defined protocol activities instead of SMTP and/or SYN (the NetEnforcer is delivered preconfigured to SYN, SMTP, ICMP and DNS).
- Define exclusion lists of subscribers that should not be considered as malicious traffic, regardless of their activity (for example, SP mail servers or the provider's lab).
- Define inclusion lists of subscribers that must be added to ADM reports regardless of SMTP or SYN activity, thereby enabling SPs to monitor the behavior of subscribers known to be infected.
- Define automatic actions, such as automatic enforcement of **prevention policies against malicious attacks and emailing network administrators** with critical information concerning the network. Such information can include lists of subscribers identified as attackers and the number of active connections per attack and per subscriber; lists of the IPs and number of open/half-open connections per subscriber (depending on the type of attack) of attacking subscribers; and lists of active connections not associated with an attack for every subscriber identified as an attacker.



```
                    Subscriber Activity for Outgoing Spammer
                    ----------------------------------------

Subscriber IP: 61.15.118.144
Number of SMTP connections: 94

Protocol       |    Client IP:Port     |   Server IP:Port      |   VC_Pipe
_______________|_______________________|_______________________|__________________________
MSN-CHAT:TCP   |  61.15.118.144:2492   |  207.46.4.174:1863    |  Fallback_Fallback Pipe
COMMON-I:TCP   |  61.15.118.144:1324   |  200.68.3.106:6667    |  Fallback_Fallback Pipe
```

Figure 5: Subscriber Activity for Outgoing Spammer
This list sent to the network administrator displays detailed information concerning each subscriber suspected of spamming. With two connections open other than SMTP, the subscriber may have been infected by a worm that exploits the vulnerabilities of these connections.

Real-Time Reporting

Effective threat management needs more than just identification of security threats. It needs real-time reporting through early warning alarms. The Allot NetEnforcer includes a completely automated and flexible early-warning mechanism which informs administrators of potential threats in advance, enabling them to take appropriate actions before any damage is done.

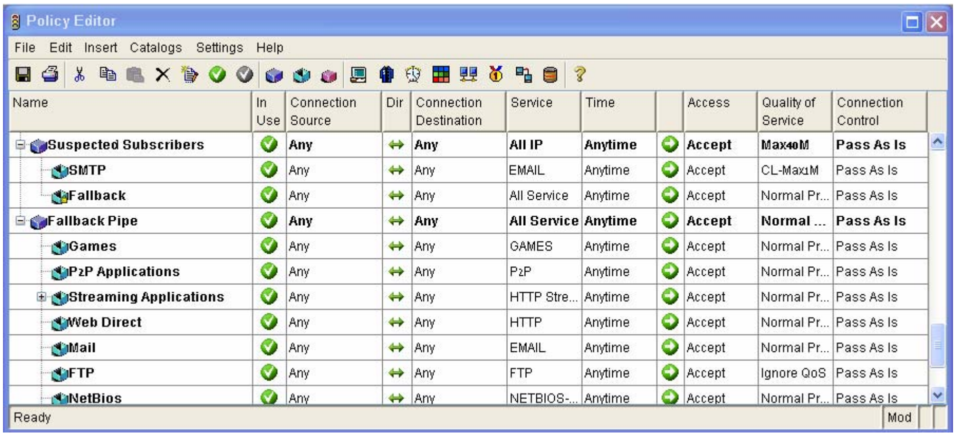
This is achieved by defining a range of parameters which determine optimal network operation. Typical examples of such parameters include predesignated thresholds for active connections, new connections and bandwidth consumption, and even provision of network activity reports at predefined time intervals. When any breach occurs in the designated parameters, an alert mechanism activates the NetEnforcer to take customized, predefined automatic actions. Examples of actions can range from sending an email to the network administrator with all the information provided by the automatic detection module to a shutdown of part or all of the network.

Mitigation of Threats through Enforcement

The Allot NetEnforcer permits broadband network operators to be proactive in mitigating malicious threats. This is achieved by the availability of various traffic enforcement measures, such as limiting the number of connections, allocating special policies for dealing with suspect attackers, and redirecting HTTP traffic to captive portals.

Limiting the number of connections is a very effective method for handling high-severity DoS/DDoS attacks and outgoing spam, since it blocks spammers from sending massive amounts of emails and prevents SYN attackers from overwhelming targets with enormous numbers of half-open connections. To mitigate DoS/DDoS attacks, administrators can limit the number of connections for the entire NetEnforcer, per application, per subnet, per host subscriber, per traffic type or any combination. For outgoing spam, they can limit the number of SMTP connections per subscriber or block access completely for suspected spammers.

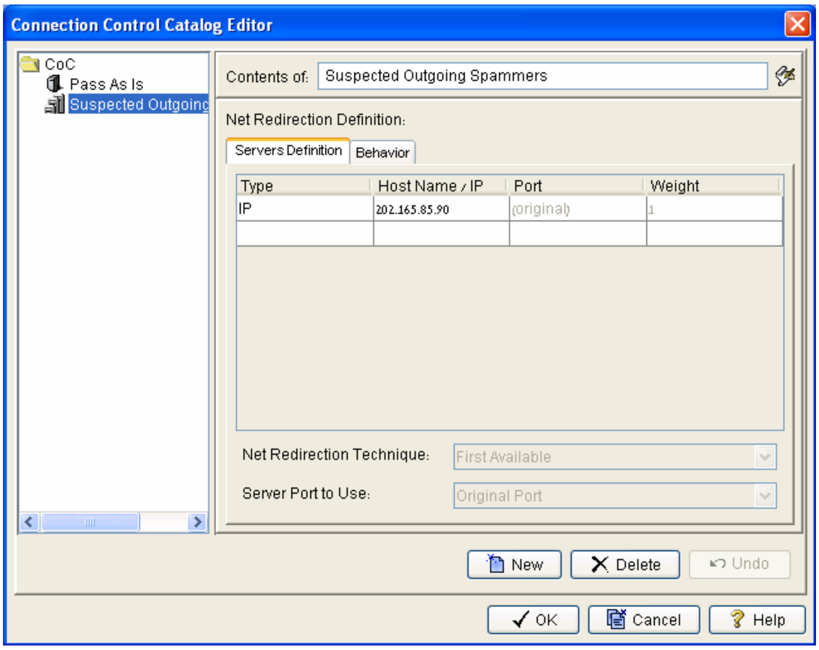
Allocating special policies that restrict usage as a means to deal with suspect attackers is also an effective way to mitigate threats and attacks. Typical examples of restrictions that can be allocated using NetEnforcer include blocking or restricting the number of SMTP connections, the bandwidth for all SMTP traffic, all TCP connections and all TCP traffic.



Name	In Use	Connection Source	Dir	Connection Destination	Service	Time		Access	Quality of Service	Connection Control
Suspected Subscribers	✓	**Any**	↔	**Any**	**All IP**	**Anytime**	→	**Accept**	**Max40M**	**Pass As Is**
SMTP	✓	Any	↔	Any	EMAIL	Anytime	→	Accept	CL-Max1M	Pass As Is
Fallback	✓	Any	↔	Any	All Service	Anytime	→	Accept	Normal Pr...	Pass As Is
Fallback Pipe	✓	**Any**	↔	**Any**	**All Service**	**Anytime**	→	**Accept**	**Normal ...**	**Pass As Is**
Games	✓	Any	↔	Any	GAMES	Anytime	→	Accept	Normal Pr...	Pass As Is
P2P Applications	✓	Any	↔	Any	P2P	Anytime	→	Accept	Normal Pr...	Pass As Is
Streaming Applications	✓	Any	↔	Any	HTTP Stre...	Anytime	→	Accept	Normal Pr...	Pass As Is
Web Direct	✓	Any	↔	Any	HTTP	Anytime	→	Accept	Normal Pr...	Pass As Is
Mail	✓	Any	↔	Any	EMAIL	Anytime	→	Accept	Normal Pr...	Pass As Is
FTP	✓	Any	↔	Any	FTP	Anytime	→	Accept	Ignore QoS	Pass As Is
NetBios	✓	Any	↔	Any	NETBIOS-...	Anytime	→	Accept	Normal Pr...	Pass As Is

Figure 6: NetEnforcer Policy Editor
Network administrators can use the Allot NetEnforcer Policy Editor to restrict email activity for suspect subscribers.

Redirection of HTTP traffic to captive portals using NetEnforcer enables SPs to alert subscribers of their own spamming activities or SYN attack violations and request actions to be taken to remedy the situation. Additionally, it permits SPs to offer value-added services for infection removal.



Contents of: Suspected Outgoing Spammers

Net Redirection Definition:

Type	Host Name / IP	Port	Weight
IP	202.165.85.90	(original)	1

Net Redirection Technique: First Available

Server Port to Use: Original Port

Figure 7: Defining a Captive Portal
The NetEnforcer permits network administrators to define a captive portal that will be used to capture HTTP traffic for suspected outgoing spammers and alert them of the problem.

Summary

The threat of outgoing spam, DoS/DDoS, DNS flooding, ICMP attacks, IP scanning and port scanning to the stability of SP networks is very real. As hackers become more audacious and challenged to find new network vulnerabilities, SPs must continually safeguard themselves against the constant threat.

Since the hacker threat cannot be eliminated, the solution is to be on constant guard: **to identify** possible attacks in real-time; **to report** on possible dangers in real-time; and **to proactively mitigate** possible threats through traffic enforcement. This is the only way that SPs can survive the threat.

Allot’s NetEnforcer provides all these capabilities and more: **Real-time identification** of malicious traffic behavior over the network, by sending warning emails to network administrators and providing a range of monitoring and detection tools to track subscribers, applications, flows, connections, ports, protocols, trends and other parameters. **Real-time reporting** through an automated and flexible early-warning mechanism which informs network administrators of potential threats in advance, enabling them to take appropriate actions before any damage is done. **And proactive mitigation of malicious threats** using various traffic enforcement measures which prevent successful hacker infiltration of their networks.