APPLICATION NOTE

Integrating the NetEnforcer with Your Firewall

This document details how to deploy the NetEnforcer in a network configuration that has a firewall, including the advantages and tradeoffs concerned with the placement of the NetENforcer in relationship to the firewall and its interfaces.

Configuration of Standard Firewalls

A standard firewall can be used for many purposes including:

- Controlling and protecting external access to local resources
- Providing centralized Virus Detection and Protection
- Regulating internal and external access to server resources

In addition to these functions, many firewalls also perform network address translation (NAT) functions whereby the network addresses used by any internal users will be masked to those on the Internet.

The NetEnforcer complements standard firewalls by allowing the definition of policies to improve network performance. Through the NetEnforcer, it is possible to:

- Prioritize internal and external access to resources
- Balance traffic load to a server farm
- Transparently redirect traffic from internal users to a server cache farm
- Account for traffic flowing to the Internet or WAN link

In all firewall configurations, the NetEnforcer can be installed to complement your current system. The exact placement, however, depends on various issues including:

- which NetEnforcer feature is required (prioritization, load-balancing, cache redirection, etc.)
- what kind of policies are to be defined (internal or external user address, services, etc.)

Two-legged Firewall

A standard firewall is placed between the Internet and local LANs.

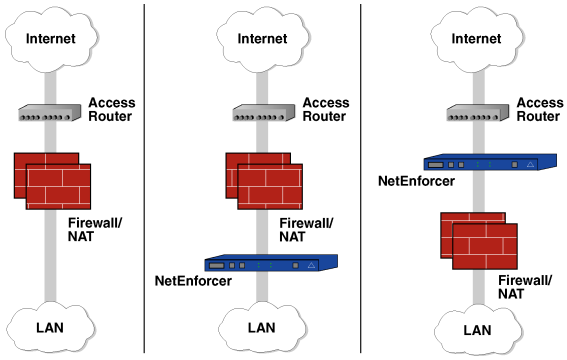

Figure 1. In a standard firewall configuration, where the firewall is placed between the LAN and Internet connection, the NetEnforcer can be inserted either on the LAN-side or Internet-side of the firewall.

In this configuration, the NetEnforcer can be placed either on the LAN-side or WAN-side of the firewall system.

- Placed on the WAN-side of the firewall, the NetEnforcer will “see” all local traffic from the internal networks. However, if the firewall performs NAT functions, it may hide the IP address of internal clients from the NetEnforcer. In addition, if the firewall encrypts any of the internal data, that encrypted data will be invisible to the NetEnforcer for purposes of policy enforcement (prioritization, load-balancing or cache redirection).
- Placed on the LAN-side of the firewall, the NetEnforcer will be able to see all the pre-firewall data. In general, this is the ideal spot to put the NetEnforcer. However, if there are any LAN configurations, the NetEnforcer must be in a “collapsed” location where all the LANs converge. In general, this will be a single gateway dividing up local LAN segments.

Allot Communications

Firewall with Third Leg (DMZ)

Many firewalls today contain a third Ethernet segment often referred to as a Demilitarized Zone (DMZ). In general, this DMZ segment allows both internal and external (Internet) users to access common servers without allowing external Internet users access to any internal (non-DMZ) resources.

With a DMZ, there are several options and tradeoffs as to where to place the NetEnforcer.

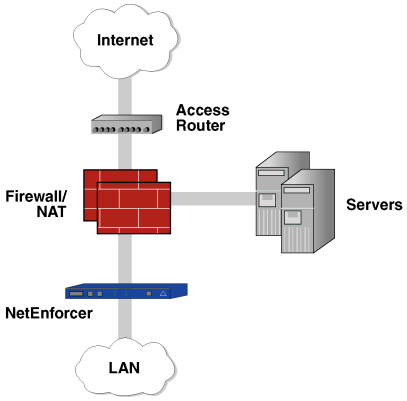

Figure 2. One option on a three-legged firewall is to place the NetEnforcer on the LAN-side of the firewall. This is an ideal solution for prioritizing internal LAN traffic destined for the Internet, WEB server or cache server. If there are many internal LANs, the NetEnforcer should be placed at a convergence point between these LANs. Usually, this is in front of an internal router.

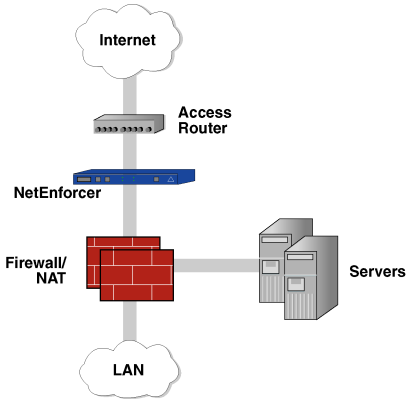

Figure 3. A second option is to place the NetEnforcer on the Internet side of the firewall. This is an ideal solution for prioritizing internal traffic destined for the Internet as well as external traffic entering both your LAN and DMZ servers. However, internal user addresses and other data (such as TCP ports) may be masked by NAT performed by the firewall. In addition, the NetEnforcer will not be able to "see" and prioritize traffic between external users and your DMZ servers.

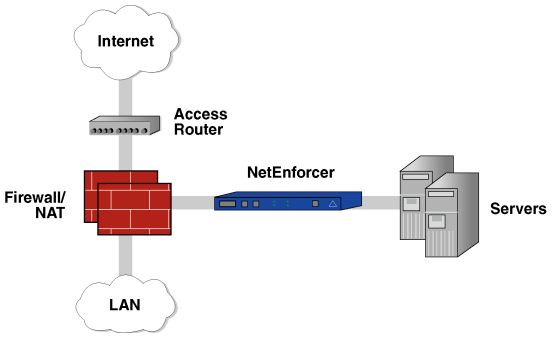

Figure 4. A third option is to place the NetEnforcer in front of the servers on the DMZ. This is ideal for improving the performance of load-balancing between the DMZ servers and internal and external users. This configuration can also be used to prioritize traffic between external clients and internal servers. However, the NetEnforcer will not be able to "see" traffic between internal clients and the Internet. This may affect the ability to prioritize all of the traffic destined for the Internet.

Conclusion

The NetEnforceris an ideal complement to a firewall system in enterprise or corporate networks. It provides added functionality to the network that extends standard firewall capabilities, including traffic prioritization, server load-balancing, cache redirection and accounting capabilities. No matter what your configuration or bandwidth management needs, the NetEnforcer will easily integrate into your network.

US Offices
433 Airport Blvd., #303
Burlingame, CA 94010
Tel (650)-401-2244
Fax (650)-401-2277

International Offices
5 Hanagar Street
Industrial Zone
Hod-Hasharon, 45800, Israel
Tel 972-(0)9-744-3676
Fax 972-(0)9-744-3626

Europe
World Trade Center
1300, Route Des Cretes
BP 255
Sophia Antipolis Cedex
France 06905
Tel 33-(0)4-92-38-80-27
Fax 33-(0)4-92-38-80-33

Japan
Kowa Shinjuku Building 7F
2-3-12 Shinjuku
Shinjuku-ku
Tokyo 160-0022
Tel 81-(0)3-3355-0450
Fax 81-(0)3-3355-2445

Web www.allot.com **Email** info@allot.com

Allot Communications

P/N 908003 REV 3A 03/00