APPLICATION NOTE

Fault Tolerance of the NetEnforcer

Data networks today are depended upon to carry a wide array of mission-critical and time-sensitive applications. These networks need to be highly reliable to provide essential business services that can handle failures and still continue to function. Failure of a network device can be catastrophic causing network downtime and lost business. Although such a failure is unlikely, it is important to design a fault-tolerant network.

This paper outlines some of the fault-tolerant benefits and features in the Allot NetEnforcer that ensure reliable operation and guarantee continuous bandwidth management services.

Preventing Downtime

Despite adequate safeguards, network downtime can be caused by failure of a hardware component, errors in software, loss of electrical power, disconnection of a network cable or scheduled equipment maintenance.

The first step to fault tolerance is preventing failures. The NetEnforcer has gone through rigorous testing procedures to assure that all hardware components can survive the most extreme environments. The NetEnforcer software has over thirty software and hardware checks that detect most common hardware and software failures and will perform corrective actions to reset those functions that are not properly working.

Redundant Systems

The best hardware and software can still experience a failure. In order to prevent an equipment failure from causing a network outage, the NetEnforcer™ is designed to allow alternate paths for traffic.

All NetEnforcers support dual hardware-failure modes:

- Hardware Bypass - will ensure connectivity for your single unit system.
- Redundant NetEnforcer Units - will ensure functionallity is maintained in your dual unit system.

Hardware Bypass

Each NetEnforcer periodically goes through a series of both hardware and software reliability checks. Hardware checks include network cards, power supply, hard disk, RAM and processors. If, for any reason, there is a failure in one of these components, the NetEnforcer will automatically, in hardware, switch over to a “wired connection”. In this mode, all traffic will pass transparently through the NetEnforcer as if it were a solid wire connecting the two sides of the unit.

Redundant NetEnforcer Units

The NetEnforcer supports redundant configurations using two systems. This failover system works in conjunction with the hardware bypass solution. If two NetEnforcers are attached in parallel, one will become the master system. If there is any failure, the backup system will automatically start passing traffic.

Traditional Fault Tolerance Solutions

Many solutions in the industry today claim to be fault-tolerant because they support a simple “fail-over” mode. Unfortunately, this is not a complete solution. It only is effective if, for any reason, the power supply fails or is disconnected. However, there are many other vulnerable components that typically make up network devices including:

- Hard Disks
- Network Interface Cards
- Processors
- Memory
- Power Failure

If any single one of these components does fail, the system will stop working and a power supply fail-over will simply not work. Fail-over architectures must address all of the above possibilities, not just the issue of loss of power to the system.

Allot Communications

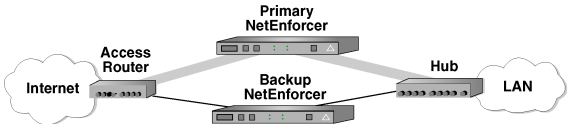

Figure 1.
Two NetEnforcers can be placed between the access router and the operational LAN network. One NetEnforcer will automatically become the primary system and the second will run in backup mode. NetEnforcers can also be instructed, in case of failure, to automatically go into a hardware bypass mode that will transparently pass all traffic.

Redundancy Architecture

Configuring two NetEnforcers in a network is simple and straightforward. A NetEnforcer comes with two Ethernet ports. These two ports bridge between the operational network and the LAN-side of the Internet or WAN access router. A second NetEnforcer can be placed in the same configuration whereby one side will plug into a hub that connects the access router and the primary NetEnforcer. The other port will again plug into a hub or switch on the operational network.

One NetEnforcer will automatically become the primary system and will pass all traffic through. The second system will be the backup system and will remain idle. It will, however, periodically check the status of the primary system. If the secondary system should determine that the primary system has gone down, it will take over responsibility for passing all connections and administering the proper policies.

One Policy for Multiple Systems

The NetEnforcers graphical user interface allows for defining a single group of policies that can then be simultaneously downloaded to multiple systems. In this manner, all primary and secondary systems will contain the same policy information. Should the primary system fail, the secondary system will take over using the same policies as the primary system.

Summary

Preventing network failure is a primary concern when running a network. The key to assuring one hundred percent up time is to design a system with solid equipment and redundancy of key components. The NetEnforcer provides network administrators peace of mind by delivering products that are designed to run in a fault-tolerant, policy-based system – a system with both hardware bypass and redundant failover capabilities.

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 908004 REV 3B 03/00