

A Fault-Tolerant Approach to Network Security

Jonathan Lundell

Chief Technical Officer, Resilience Corporation

The increasing use of the Internet, especially for internal and business-to-business applications has resulted in the need for increased security for all networked systems to avoid unauthorized access and use. A failure of network security can effectively close the business, its availability is vital to operations. Vital functions such as firewalls and VPNs must remain in operation without loss of time for failover, without loss of data and must be able to be placed even at remote locations where support personnel may not be readily available.

Network firewalls are the first, and often are the only, line of defense against an attack. However, the firewall can be a double-edged sword. In operation, the firewall protects the network from everything from Denial of Service attacks to the entry of known viruses and unauthorized intrusion. If the firewall fails, there are generally only two options: Leave the network open to all or shut down access by anyone. The default condition is to close everything off, but this can be as disastrous as leaving the network open.

Due to the importance of the firewall, most leading firewall software provides some method of establishing a form of fail-over redundancy for high availability. Yet in most cases this means some form of clustering using a secondary system as a backup with specialty software to detect and respond to a failure of the primary firewall. Such a clustered approach introduces additional complexity when establishing and configuring the firewall and additional complexity when upgrading. It also adds dramatically to the cost, not only in the hardware for the firewall, but in additional software copies and in the expertise for clustering support software required to establish and maintain the cluster.

The approach we will discuss examines the creation of network security based on a hardware approach to fault tolerance. This approach will dramatically reduce the system complexity, simultaneously eliminating the need for special clustering software and special expertise for configuring the system for the kind of continuous availability that is the objective of the network security application.

In addition, because the hardware approach is something that is designed in from the inception of the system, there are additional advantages. The fault tolerance is not an afterthought, but rather the purpose of the hardware, meaning that the system can be made to function very smoothly with very little administration. Failure of a part of the system is seamlessly recovered by the redundant elements, without loss of data in memory or loss of state for the system.

In sum, this paper will discuss the ability to create network security that reaches the standard of being continuously available, what is often referred to as the “Holy Grail of reliability,” 99.999% uptime.