



FIREWALLS

Description of the Application

Firewalls play a critical role in the security infrastructure of an enterprise. Firewalls were designed to protect valuable information resources. These applications act as a network gateway, filtering resource requests to allow or deny access based on an organization's security policy.

Enterprises rely on firewalls to secure their networks from unwanted and unauthorized threats from the Internet, and to control internal access to external resources. Firewalls also provide a secure method for authorized remote clients to gain access to sensitive information using virtual private networks (VPNs).

Challenges to the Application Type

The increasing use of the Internet and the prevailing need for access to information has multiplied the amount of traffic traditional network firewalls have to filter. This increased use and the critical role the firewall performs generates a number of challenges for these application types. These challenges include:

Providing scalability - If a firewall is overwhelmed or underpowered, the protection it provides an organization is greatly reduced. Firewall applications offer limited scalability through the use of clustering technology. For large environments, this results in additional CPU overhead, increased network traffic, lower return on investment, and scalability limitations.

Providing high availability - Much like scalability, high availability for firewall applications is traditionally addressed through implementing clustering. However, clustering availability checks typically focus on network availability of the server through basic health checking or updates. These simple health checks fail to detect upper-layer malfunctions and return a false positive, misdirecting a portion of network traffic to unhealthy resources.

Seamless integration - Firewalls are deployed at key access points in network architectures that demand high availability and constant traffic flow. Adding firewall resources to a network can cause considerable down time and network disruption because of their deployment location and installation requirements.

Increase security - When expanding firewall resources, organizations are faced with finding solutions that broaden their scope and increase their protection. Network devices need flexible, comprehensive, and security-minded feature sets to increase control over network traffic and protect the network from existing and future attacks.

F5 Solution Overview

Implementing F5 Networks' BIG-IP® product with firewall applications and appliances allow organizations to effectively scale and maximize their existing investments. When deployed together, this powerful solution increases network security and resource availability, and provides administrators a flexible traffic management tool.

The comprehensive feature set of the BIG-IP product enables application traffic analysis for advanced load balancing and persistence capabilities. This enhances the performance of IP requests and provides preventative methods against future attack types.

To scale the performance of a firewall farm, and to provide high availability to both internal users and those coming into a site from the outside world, customers often employ a firewall sandwich. This configuration is named a firewall sandwich because of the location of the BIG-IP product, placed on either side of the firewalls. In this scenario, the BIG-IP product can intelligently load balance both inbound and outbound traffic between the firewalls - then test the availability of the firewalls based on their ability to move traffic in the most efficient manner.