



BORDERWARE MXTREME

BorderWare's MXtreme and F5's BIG-IP Provide High Availability, Security and Scalability for Enterprise Email Systems

Executive Summary

To protect the value and availability of email, enterprises increasingly recognize the need for products and architectures that ensure high levels of availability as well as robust security. Responding to that need, BorderWare Technologies, the industry leader in comprehensive email security, and F5 Networks, a pioneer and market leader in intelligent application traffic management, have developed a solution that delivers unprecedented levels of availability, reliability, scalability, and security for business-critical enterprise email.

By combining the stateful fail-over of BorderWare's MXtreme™ Mail Firewall with F5's BIG-IP® devices, enterprises achieve unprecedented levels of email availability, reliability, scalability, and security. With this unique solution, email systems now benefit from high availability load optimization that had been previously dedicated only to other business-critical applications.

Challenges

As the intrinsic value of email messages has increased, so has the importance of timely delivery. Traditionally, email messages have been relayed from server to server, and if a destination system cannot accept receipt of a message, the sender just resends the message repeatedly until the message is finally delivered. This is no longer acceptable; users expect delivery to occur in a matter of seconds, regardless of message size. For most enterprises, these new concerns have not been properly addressed.

To handle spam, viruses, and related security issues, enterprises are deploying perimeter email security and mail-hygiene systems. Enterprises are unwilling to leave valuable internal mail servers directly connected to the Internet, where they are exposed to a wide range of attacks. These email security systems are deployed on the perimeter of the network and receive all inbound email messages. Their architectural placement has made them integral parts of the messaging infrastructure. If these systems are unavailable, the whole enterprise is effectively unreachable by email.

In nearly all cases, however, these are single systems that offer minimal fault-tolerance. Where they are deployed in clusters, they provide little more than a parallel email traffic stream, controlled by simple round-robin DNS. This is clearly an inadequate response, which does not offer protection against the possibility of loss of email messages or an assurance of timely message delivery.

Solution

The F5 and BorderWare solution ensures business critical email systems have the highest level of availability and security possible. F5's BIG-IP systems offer the industry's most comprehensive local and global traffic management solution to ensure high availability of MXtreme Systems by intelligently distributing traffic across them. MXtreme's stateful failover technology ensures that any message received by the cluster will always be delivered, regardless of any failure by an individual member of the cluster.

Security

MXtreme is being certified to Common Criteria EAL4, a level of security usually only attained by network firewalls. This high level of security ensures that the system's reliability cannot be compromised by malicious attacks, such as denial of service (DoS) attacks, buffer-overflows, or other attacks. MXtreme's MTA (Message Transfer Agent) is specifically designed to manage surges and peaks in email traffic, preventing the system from being flooded and ensuring the smooth receipt and delivery of messages.

The BIG-IP system offers strong device level protection to ensure the highest level of availability for MXtreme devices, as well as the security services offered by MXtreme Email Firewall. The BIG-IP system's Dynamic Reaping capability offers an adaptive and layered defense to mitigate DoS attacks, supplementing the DoS mitigation capabilities of Email Firewall itself. The BIG-IP system also provides rate filtering to effectively rate-limit and block spam-traffic, working in conjunction with MXtreme Email Firewall, allowing customers to prioritize and manage their SMTP traffic more effectively.

Balancing the Load

The F5 BIG-IP Global Traffic Manager (GTM) ensures high availability by distributing the incoming SMTP connections intelligently across MXtreme systems. This is useful in cases where the mail servers and redundant MXtreme systems are not necessarily in the same geographical region. The BIG-IP GTM distributes traffic using either a static load balancing mode, which selects a virtual server based on a pre-defined pattern, or a dynamic load balancing mode, which selects a virtual server based on current performance metrics.

F5 BIG-IP Local Traffic Manager (LTM) devices can reside on both sides of the MXtreme systems, and distribute bi-directional traffic load across them. The F5 BIG-IP LTM can perform deep packet inspection to route traffic based on L4 or L7 protocols like HTTP and SMTP. The customer can distribute the SMTP traffic across an MXtreme cluster using a wide variety of static and dynamic load balancing methods.



BORDERWARE MXTREME

Solution - Continued

Health Monitors

High availability requires that any one of the clustered systems is capable of processing the mail stream. The failure of one system should not interrupt overall service. F5 devices, working in conjunction with MXtreme devices, provide high availability and intelligent load balancing by checking the health of these systems before sending the SMTP traffic to them.

The BIG-IP LTM provides high availability by monitoring the health of the MXtreme devices and directing traffic away from slow or unavailable systems. The BIG-IP LTM provides address, services, path, content and interactive checks using TCP, HTTP and HTTPS monitors.

The BIG-IP GTM performs wide area health checks before routing traffic to a site. It provides TCP, SNMP and HTTP health checks and monitoring to ensure application and system availability. The BIG-IP GTM also collects and measures path metrics to direct traffic to the best performing site.

iControl

iControl is F5's open application program interface (API), made available as a free SDK, for creating quick and easy intercommunication between applications and the network via F5 products. Working through iControl, an MXtreme cluster can ensure high availability and optimum load balancing by communicating information on email content and traffic load directly to a BIG-IP device. The result is that SMTP traffic can then be intelligently distributed across individual systems within the MXtreme cluster. iControl can also be used to filter traffic based on criteria such as the client's source IP address, port, and so on.

By working together, BorderWare's MXtreme and F5's BIG-IP ensure the continuous operation of corporate email systems by delivering unprecedented levels of availability, reliability, security, serviceability, manageability, and scalability.

Benefits

High availability - Through the use of its advanced health checking capabilities, the BIG-IP product can recognize when a resource is unavailable or under-performing and direct traffic to another resource. For example, the product's EAV health monitor can verify applications on the node by running those applications remotely, using an external service checker program. The BIG-IP contains service checking programs for POP3 and IMAP, among others.

MXtreme hardware is fault-tolerant, with redundant disks, redundant hot-swappable power supplies, redundant network links, and field replaceable parts. This promotes reliability and removes the risk of downtime resulting from single component failure.

Reduced administration - Using F5 products with iControl allows enterprises to easily create intercommunication between applications, like BorderWare MXtreme, and the network. iControl can be used to automate processes, freeing administration personnel to attend to more important tasks. MXtreme's centralized management allows administrators to easily manage MXtreme clusters and to synchronize configuration settings across all systems in the cluster.

Simple scalability - The BIG-IP device provides a highly scalable solution that allows enterprises to meet growing organizational demands on application and Web resources. If one server is nearing capacity, scaling it is as simple as adding another server to your network and then to the BIG-IP load balancing pool; the BIG-IP device automatically begins directing traffic to the new server.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability—all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.

About BorderWare

BorderWare Technologies is a global vendor of messaging security, privacy and compliance solutions. BorderWare has been protecting enterprises of all sizes and governments worldwide for over 13 years against the risks and threats associated with today's converging Internet threat landscape across Email, IM, Web, VoIP and the network perimeter. BorderWare has developed partnerships and affiliations with some of the industry's most prominent companies in Internet infrastructure, security and messaging including CommVault, Ericsson, F5 Networks, FaceTime Communications, Kaspersky Labs, LignUp, Marconi, McAfee, Mitel, Natural Convergence, PostX, PGP, RSA Security, Radware, snom technology, Sun Microsystems, SurfControl, Symantec, Ubiquity, Utimaco, Zfone. Thousands of customers worldwide have selected BorderWare for its superior security, high performance and lower total cost of ownership.