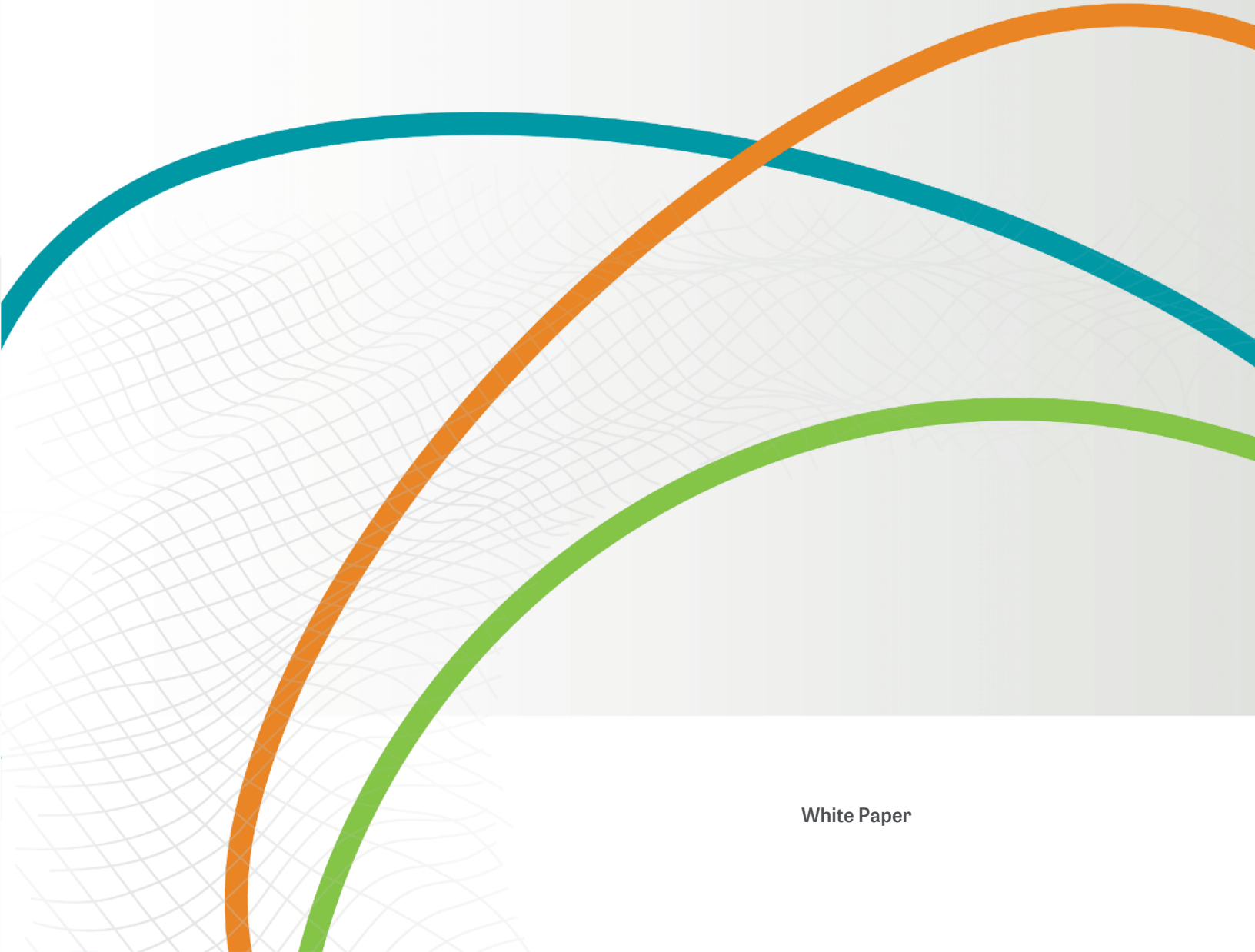
Security Solutions for Messaging Systems

Security Solutions for Messaging Systems



White Paper

Overview

With F5 solutions, organizations can provide employees with reliable and secure access to email, from wherever they are, no matter what type of device they're using. Employees can rely on email that is efficiently delivered, with minimal latency times and a dramatic improvement in performance. Organizations can also reduce their bandwidth expenditures, use fewer server resources, and lower their overall infrastructure costs.

Challenge

Organizations today depend heavily on applications like email to increase productivity and reduce the cost of doing business. These applications must be fast, available and secure in order to accommodate a geographically dispersed world of employees.

The answer to poor performance or lack of security isn't more boxes, more complexity or more point solutions. The answer is found at the critical juncture, where the application connects to the network itself - where all the application optimization, availability and security required is integrated in a cohesive architecture.

Solution

While F5 solutions can improve the performance and security of many different types of applications, this document provides a quick view of how F5 solutions can help make your email more secure.

Load Balancing Anti-Spam Servers

The BIG-IP Local Traffic Manager (LTM) is an advanced application delivery networking appliance that allows you to load balance email traffic across your anti-spam devices. This solution has been proven across numerous Fortune 500 customers that are currently load balancing their Ironmail or other anti-spam devices. Load balancing across anti-spam devices ensures that you get the maximum performance out of your existing anti-spam investment, and reduces the risk that a single downed device will significantly impact email performance.

The BIG-IP LTM includes rich static and dynamic load balancing methods, including Dynamic Ratio, Least Connections, and Observed Load Balancing, which tracks dynamic performance levels of servers in a group, ensuring that the best resources are always selected for improved performance and scale.

Anti-Phishing

To perform phishing attacks, malicious code is used to replicate the site of the company whose customers the attacker wants to scam. The attacker then typically uses email to lure unsuspecting customers to that phishing site to gather sensitive personal information. Eliminating phishing requires a multi-layered approach. The most common way to prevent phishing is to block suspected or known phishing emails coming to your employees. However, if you want to prevent your customers from being phished, without necessarily having control over their email protection systems, there is an additional option. You can use BIG-IP to prevent your web site from being replicated. By using a BIG-IP iRule, you can:

- Check for suspicious HTTP requests that originate from a referrer that hasn't been authorized to use your site's content
- Either stop them outright, or inject code into your HTTP response to help negate their ability to duplicate your site.

This is done in 3 separate steps:

1. Define a list of valid referrers. This is a list of those sites that you expect to be linking to content on your site.
2. Define a list of file types that should not be linked to by anyone but valid referrers.
3. Use the BIG-IP iRule to inspect traffic from invalid referrers (not someone in #1) that are trying to serve data from your site. If the file types match the list in #2, the iRule can either insert some custom code to help prevent phishing attempts, or block it entirely.

For more information on preventing phishing, see the F5 White Paper on using iRules to prevent phishing, at http://www.f5.com/en-us/pdf/white-papers/antiphishing-wp.pdf.

Network Attacks on Email Servers

The BIG-IP system combines a suite of security features to provide comprehensive protection against DoS Attacks, SYN Floods, and other network based attacks. Features such as SYNCheck provide comprehensive SYN Flood protection for the servers that sit behind the BIG- IP device. The BIG-IP device acts as a security proxy that is designed to protect the entire network. Combined with Dynamic Reaping capabilities, an adaptive method for reaping idle connections, the BIG-IP system provides robust security to filter out the heaviest attacks while simultaneously delivering uninterrupted service for legitimate connections.

Secure Remote Email Access

Ensuring secure access to email for remote users is another critical part of protecting the email infrastructure. F5's FirePass controller is an SSL VPN solution that sets up a secure channel of communication between the client and the corporate network/applications. It enables remote workers to have secure access to network resources using any web-enabled device (like airport kiosks, PDAs, and laptops). Email access can be provided from within the FirePass console directly to any POP or IMAP email server, securely through Microsoft Outlook Web Access, or by providing secure access to the corporate network whereby the remote user can connect to their email server directly.

The FirePass controller can also automatically perform endpoint security checks to ensure each client system is up-to-date with security patches, anti-virus levels and so on, before permitting the connection. It can also create a Secure Virtual Workspace on the client that erases all confidential information upon logout. Additionally, the Secure Virtual Workspace can prevent sensitive file attachments from being downloaded on un-trusted clients. This prevents sensitive information from being saved from corporate email, or any information about the session left-over on the client system. Finally, the FirePass can also integrate with a wide variety of two-factor authentication systems for maximum security.

Web Mail Encryption

It is always important to consider the weakest link in the stream of email communication between the client desktop or laptop and the company email servers. No matter how strong the authentication may be, without encryption, the communication itself becomes the weakest link. This is why it is useful to encrypt email communications between the end user and the email application using SSL. In the past this was difficult due to the server load required to perform such large volumes of encryption. However, the BIG-IP product's SSL Acceleration Module allows organizations to easily encrypt 100% of the communication in SSL. This can extend beyond email communication to all LAN or WAN traffic. The module removes all bottlenecks for secure, wire speed processing by offloading CPU-intensive processing from servers and migrating SSL decryption onto a high performance device designed to efficiently handle SSL transactions. In addition, all SSL certificates can be consolidated directly onto BIG-IP — saving hundreds of dollars per certificate.

Ensuring Availability Across Data Center

BIG-IP Global Traffic Manager (GTM) is designed for managing application traffic like email that runs across multiple and globally dispersed data centers. It improves the security of email applications because if there's an email outage at one site, the BIG-IP GTM can automatically redirect requests to other data centers that are still available. This happens seamlessly such that the user is unaware that anything has happened. Similarly, F5's BIG-IP Link Controller ensures continuity between multiple ISP links. Data centers which have multiple ISPs for redundancy and disaster recovery can be managed by BIG-IP Link Controller, where it can seamlessly shift traffic from one ISP to the other in the case of failure, ensuring high availability at all times to your critical business traffic.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com