Protect your data center and application services, improve user access, optimize performance, and reduce management complexity.
WHAT'S INSIDE

Data Center Firewall Services  3
Application Security  5
DNS Security  7
Unified Access  9
Accelerated Remote Access  11
Protocol Enforcement Services  13
Protection for Enterprise Email  15
F5 Security Solutions: Flexible, Efficient, Cost-Effective

Keeping your data center services secure, fast, and available is crucial for business success. Security breaches and multi-layer cyber attacks can result in lost productivity, missed opportunities, and higher costs for your organization. These harmful situations can also damage your organization’s reputation and deteriorate customer trust.

With F5® security solutions, you can provide data center firewall services, simplify and unify access control, secure and accelerate remote access, and protect email—all while enhancing network and application performance. Your organization will have the tailored security it needs, and your users will enjoy the reliable, flexible access they demand.
Protect the data center services that power your business

THE CHALLENGES

Internet threats are widely varied and multi-layered. As these threats evolve, organizations find that traditional firewalls lack the intelligence and the scalability needed to stay effective and responsive under distributed denial-of-service (DDoS) and a whole range of other sophisticated attacks. The result is a failure to protect the business from the loss of information or interruption of service delivery.

KEY BENEFITS

- Reduced costs and complexity
- Improved business integrity
- Faster response to business risks
- High performance and scalability
F5 BIG-IP® Local Traffic Manager™ (LTM) offers native, high-performance data center firewall services to protect the entire infrastructure. From network and application DDoS protection to SSL visibility, BIG-IP LTM offers a suite of security services to protect your business applications.

BIG-IP LTM can help halt attacks that take advantage of application layer protocols and behaviors. Because BIG-IP LTM is fluent in application protocols, it can monitor and act on behavior, not just specifications and standards. BIG-IP LTM decodes IPv4, IPv6, TCP, HTTP, SIP, DNS, SMTP, FTP, Diameter, and RADIUS communications.

The programmatic ability of the F5 iRules® scripting language provides a flexible means of dynamic threat defense. Using iRules, BIG-IP LTM can be directed to enforce protocol compliance and perform rate limiting, response injection, and traffic steering and related actions. Security teams are finding that the flexibility of iRules enables them to mitigate a broad range of security threats.
Defend against web attacks and achieve regulatory compliance

**KEY BENEFITS**

- Protection from attacks from any location
- Reduced costs of security compliance
- Combined network security and data center firewall
- Out-of-the-box application security policies with minimal configuration
- Virtual and private cloud environment deployment

**THE CHALLENGES**

With the continued growth of web application traffic, an increasing amount of sensitive data is exposed to potential theft, security vulnerabilities, and multi-layer attacks. The resulting financial hit—from recovery processes, legal fees, and loss to intellectual data—can be significant.

Many administrators think their networks are safe because they have network firewalls in place, but attackers are more likely to target the application layer, where greater vulnerability exists.

Recent studies show:

- Most websites were exposed to at least one serious vulnerability every day of 2010.
- During 2010, the average website had 230 serious vulnerabilities.
- Once a breach occurs, the total average cost of a data breach is $214 per record compromised.

---

THE SOLUTION

F5 BIG-IP® Application Security Manager™ (ASM) is a flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments. BIG-IP ASM provides unmatched web application and website protection. It protects from the latest web threats like layer 7 DDoS, helps secure deployed applications against unknown vulnerabilities, and enables compliance for key regulatory mandates—all on a platform that consolidates application delivery with data center firewall capabilities and network and application access control.

With BIG-IP ASM, your organization benefits from a complete solution that reduces the need for multiple appliances, lowers maintenance and management costs, and increases the confidentiality, availability, and integrity of your critical business applications and processes. BIG-IP ASM is available as a product module on the flexible, multi-solution BIG-IP LTM platform, as a standalone device, or as a virtual edition.
Control and secure DNS and ensure high availability for globally distributed applications

The Challenges

Many of the attacks in the news are from automated bots causing DNS DDoS attacks that overload servers and cause website queries to go unanswered. The Domain Name System (DNS) provides one of the most basic but critical functions on the Internet. If DNS isn’t working, then it’s likely your business isn’t working either.

Furthermore, DNS cache poisoning and other DNS attacks can compromise local DNS servers and make it possible for attackers to hijack DNS responses, redirect clients to malicious sites, and access private information. Secure your business and web presence with DNS DDoS attack protection and Domain Name System Security (DNSSEC) as a part of DNS firewall services.

Key Benefits

- Strong DNS infrastructure security
- Compliance with government DNSSEC regulations
- Website protection
- Simplified implementation and reduced management costs
- High global application availability and performance
THE SOLUTION

BIG-IP® Global Traffic Manager™ (GTM) enables DNS firewall services that secure the DNS infrastructure, protecting applications and enabling global high performance. By providing protection against DNS-based attacks, BIG-IP GTM adds an extra layer of security and availability for your applications. BIG-IP GTM enables multiple devices to receive queries using the same IP address; scales DNS query response up to 10x, absorbing DNS DDoS attacks; secures DNS query response with DNSSEC; and delivers complete DNS control with DNS iRules. These solutions ensure application availability during volume spikes and enable a DNS firewall.

BIG-IP GTM with real-time DNSSEC from F5 ensures that the DNS query response your customers receive can be trusted. Implementing the BIG-IP GTM real-time DNSSEC feature can greatly enhance your DNS security. BIG-IP GTM helps you comply with federal DNSSEC mandates and protects your valuable domain name and web properties from rogue servers sending invalid responses.

F5 takes the only approach to DNS security that enables organizations to deploy DNS firewall services quickly and easily into an existing local or global server load balancing environment. BIG-IP GTM with the real-time DNSSEC feature provides a scalable, manageable, and secure DNS infrastructure that is equipped to withstand DNS attacks.
Provide access to networks and applications while ensuring security

THE CHALLENGES

Today, business resources, such as applications and data, are accessed inside and outside the traditional business perimeter. Local and remote employees, partners, and customers often access applications without context or security. Network administrators need more visibility and control over the increasing number of users coming from all over the world, on different networks, and accessing applications located in the data centers or in the cloud.

This requirement, however, can add complexity to your IT infrastructure and prove difficult and expensive to scale. A central policy control point that delivers access based on context is critical to managing a scalable, secure, and dynamic environment.

KEY BENEFITS

- Unified global access
- Identity and dynamic access control
- Strong endpoint security
- Simplified authentication, consolidated infrastructure, and reduced costs
- High performance, scalability, and flexibility
**THE SOLUTION**

BIG-IP® Access Policy Manager™ (APM) is a flexible, high-performance access and security solution that provides unified global access to your applications and network. By converging and consolidating remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, BIG-IP APM can help you free up valuable IT resources and scale cost-effectively.

BIG-IP APM is available as an add-on module on BIG-IP Local Traffic Manager physical and virtual editions and the VIPRION® chassis platforms. It is also available as part of the BIG-IP® Edge Gateway™ remote access product.

BIG-IP APM is a component of the data center firewall solution enabling web access management and security. Many web applications need to limit certain users’ access, and BIG-IP APM supports this requirement with multi-factor authentication, authorization, and single sign-on (SSO) services.
Deliver secure and accelerated remote access to applications

**KEY BENEFITS**

- Superior scalability for mobile workforce
- Streamlined access management and reduced costs
- Accelerated application performance through network optimization
- Increased productivity with always-connected user experience
- Strong endpoint protection and granular access control

**THE CHALLENGES**

IT departments must support ever-increasing numbers of mobile workers. Ensuring that these users have secure and seamless access to applications and data from different devices and locations becomes increasingly challenging. IT departments might deploy point solutions from different vendors to promote access, acceleration, and optimization.

But as the number of users grows, this siloed approach proves complex, inflexible, and difficult to manage. It also becomes increasingly difficult to prevent unauthorized access and attacks, as new threats are continually evolving. This costly, error-prone environment inhibits successful remote access and hinders business growth.
BIG-IP Edge Gateway is an enterprise access solution that brings together SSL virtual private network (VPN) remote access, security, application acceleration, and availability services for remote users. BIG-IP Edge Gateway drives identity into the network to provide context-aware, policy-controlled, secure remote access to applications at LAN speed.

As the industry’s most secure and accelerated access solution, BIG-IP Edge Gateway can help your organization deliver peak performance levels to users accessing the applications and networks that are critical to your business. With BIG-IP Edge Gateway, you can easily deliver accelerated remote access to enterprise applications and data for users over any network or mobile device (including Apple iPhone, Apple iPad, Android, Windows Mobile, and Windows Phone devices).
Powerful security services for HTTP/S, SMTP, and FTP

KEY BENEFITS
- Broad protection from HTTP attacks
- Spam-blocking SMTP security
- Centralized FTP security management
- One-solution decoding and enforcing protocol functions

THE CHALLENGES
If your environment requires more than network layer inspection services, the expertise and management you need to deploy a full-featured web application firewall might not be available.

As an alternative, protocol security services provide powerful protection for HTTP/S, SMTP, and FTP protocols but might only be available in multiple vendor solutions. Likewise, trying to decode IPv4, IPv6, TCP, SIP, DNS, Diameter, and RADIUS protocols would require multiple point solutions from multiple vendors for a decentralized and cost prohibitive implementation.
BIG-IP® Protocol Security Module™ (PSM) is aptly suited for environments that require inspection services, where the overhead needed to deploy a full-featured web application firewall isn’t available, or there is a need to secure other protocols. Protocol enforcement services can be implemented on a per-virtual-server basis and configured within a matter of minutes. By enforcing protocol checks for HTTP/S, FTP, and SMTP, this service prevents attacks that use protocol manipulation techniques.

In combination with BIG-IP Local Traffic Manager, this solution offers data center firewall services. The BIG-IP system natively decodes IPv4, IPv6, TCP, HTTP, SIP, DNS, SMTP, FTP, Diameter, and RADIUS communications, enabling more sophisticated analysis based on protocol as well as payload. This allows BIG-IP LTM to detect anomalies indicating an attack in progress and to take appropriate action. Organizations can control almost every element of the protocols they’re deploying. With Dynamic Threat Defense, the BIG-IP system enforces protocol functions on both standard and emerging or custom protocols using iRules and works with BIG-IP LTM for enabling data center firewall services.
Extend protection for enterprise email to the edge of the corporate network.

**THE CHALLENGES**

Each unwanted email message that crosses your organization’s corporate gateway consumes costly bandwidth and server resources, and can be a potential threat to security. When system capacity is strained and security threats increase, it becomes harder for IT departments to ensure business continuity. Organizations often react by adding additional mail security gateways, firewalls, and mail servers to the infrastructure, and paying for more bandwidth to keep pace with email volume. For these reasons, keeping messaging costs within budget is challenging.

**KEY BENEFITS**

- Reduce unwanted email and spam by up to 70 percent
- Base policies on real-time lookup of sender reputation
- Decrease overall infrastructure costs
THE SOLUTION

The BIG-IP® Message Security Module™ (MSM) is a network-edge solution that adds security intelligence to manage and filter inbound email traffic by considering the sender’s reputation when making traffic management decisions. BIG-IP MSM is the industry’s first reputation-based, network edge security module.

BIG-IP MSM takes advantage of data from Secure Computing’s TrustedSource multi-identity reputation engine to extend protection for enterprise email to the edge of the corporate network. The solution gives organizations an extremely powerful and efficient tool for dealing with a growing volume of unwanted email.
LEARN MORE

To learn more about F5 security solutions, please visit f5.com/security.
“All in all, we can now offer customers a highly reliable and secure web platform, which is an important factor for future success.”

– Steven Opstaele, Chief Infrastructure Architect at NorthgateArinso