Network Optimization and Security Architecture

Introduction

Since no one does it all, effective cybersecurity in the enterprise requires collaboration between best-of-breed technologies. Budgets are also limited which puts pressure on IT organizations to pick products that adhere to performance and total cost of ownership requirements, and to integrate them in ways that realize maximum value. At times, constraints have created environments and the notion that best in class performance does not allow for hardened security or visa versa, that hardened security postures and performance are mutually exclusive or unattainable without unrealistic investments.

Sourcefire, now part of Cisco, has partnered with F5 Networks, the global leader in Application Delivery Networking. Through the partnership, F5 and Sourcefire have validated two deployment architectures that help customers secure critical networks, applications and end-points while achieving optimal performance. In addition, customers can architect for scale and redundancy by eliminating single points of failure.

To improve security through automation, Sourcefire and F5 have created a remediation capability that allows critical security events such as malware (FireAMP) and IPS/IDS events to initiate rule configuration on F5's BIG-IP appliances.

Two Industry Leading Products

Sourcefire Next Generation IPS (NGIPS), Advanced Malware and the FirePOWER Platform

Sourcefire Next-Generation IPS (NGIPS) and Advanced Malware Protection (AM) set a new standard for advanced threat protection, integrating real-time contextual awareness, intelligent security policy automation and unprecedented performance.

These two solutions take advantage of the best hardware technology in the industry on the same device, providing IPS inspected throughput options ranging from 50Mbps to 60 Gbps, providing market leading performance with greater energy efficiency.

F5 Networks BIG-IP

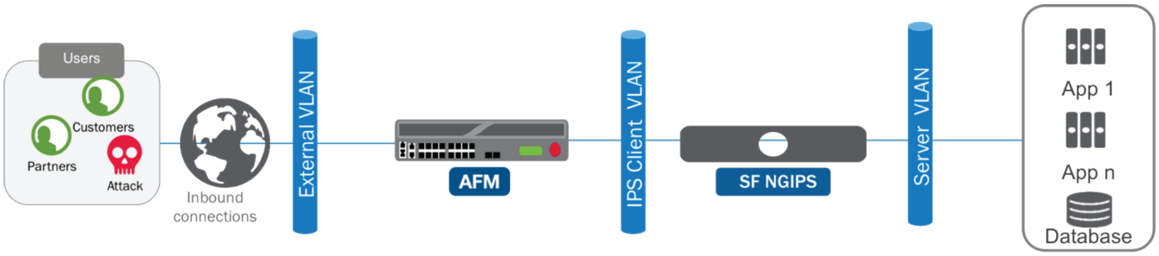
Recognized as the industry-leading series of application delivery controllers (ADCs), the BIG-IP family of products ensure applications and infrastructures are fast, available, and secure. All BIG-IP products share a common underlying architecture, F5's Traffic Management Operating System (TMOS), which provides unified intelligence, flexibility and programmability. Together, BIG-IP's powerful platforms, advanced security modules, and centralized management system make up the most comprehensive set of application and security delivery tools in the industry.

Often positioned at the edge of the network, BIG-IP Local Traffic Manager and BIG-IP Global Traffic Manager allow you to scale applications and infrastructures and turn the tables on security threats. And you can rapidly scale and adjust your security solution as your security objectives or threat spectrum changes simply by activating additional BIG-IP security modules.

Deployment Architectures

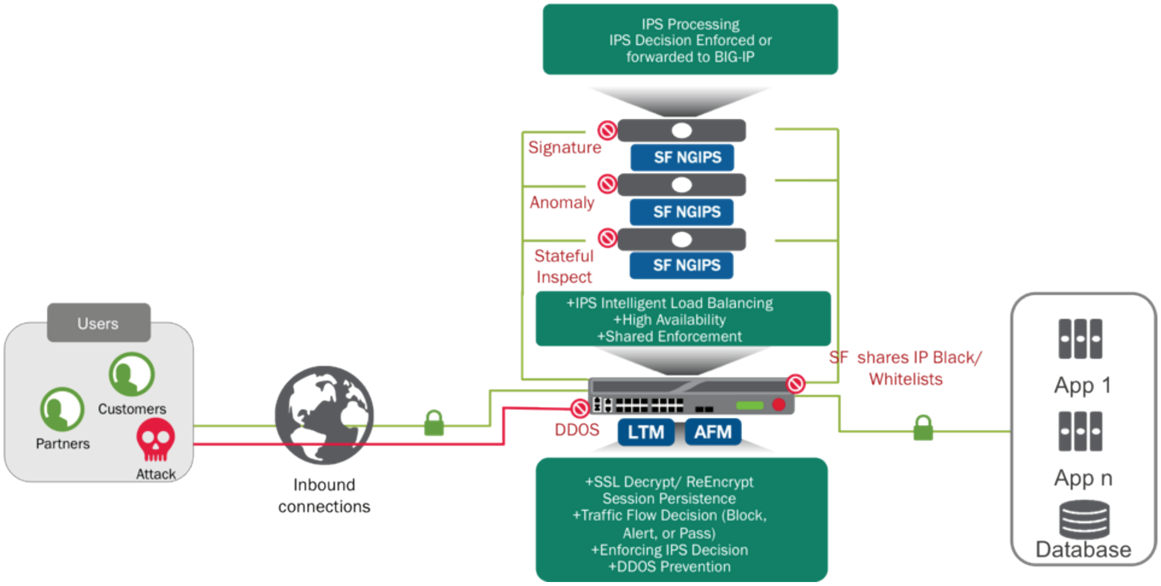
Traditional ADC for NGIPS Design (In-Line Layer 2)

The first validated architecture is a simple configuration with the IPS placed behind the F5 BIG-IP ADC. This architecture ensures that traffic is directed to the back-end servers with all of it being inspected by the IPS before connections are made to the back-end application servers. The IPS must be adequately sized to meet the application's performance requirement.



F5 Security Services for NGIPS Design – Layer 3, Remediation Integration Architecture

The second validated architecture is a load-balanced pool of Sourcefire NGIPS / Advanced Malware Protection (AMP) sensors protecting application servers. Traffic is pre screened for DDoS attacks, then depending on the policy, balanced to the pool of Sourcefire sensors and then routed back through BIG-IP to the IPS protected servers. This ensures that traffic can be inspected and, if necessary, be blocked before forwarding on to their respective application servers.



Real Time Response to Critical Security Events

Remediation capability

Sourcefire's FirePOWER appliances running NGIPS and FireAMP are managed by the FireSIGHT Management Center. FireSIGHT centralizes the management of all FirePOWER policy related configurations including IPS and Malware detection and collects all event data for analysis, correlation and reporting. A correlation rules engine allows users to configure a variety of actions in response to security events. Rules can be very simple or be more powerful by including multiple conditions and qualifiers. Actions include the ability automatically configure rules on the F5 appliance, such as blocking a device that is originating an attack, or exhibiting some other form of suspicious or unwanted behavior. Event types supported by the remediation engine include:

- IPS Events
- FireAMP (malware) Events
- Compliance Events
- Connection Events

Where to get more information

- f5.com
- f5.com/cisco
- synthesis.f5.com/
- https://community.sourcefire.com/downloads

Key Benefits

- SSL Visibility and Control: SSL termination provides clear text for IPS inspection
- Scalability: Add or remove NGIPS appliances as performance requirements change
- Flexibility: Appliances can be the same or different capacities allowing incremental increases in performance as needed
- Redundancy: Use multiple appliances in conjunction with load balancing to remove potential single points of failure
- Remediation: Automatically block suspicious flows and compromised devices
- Security Services Ease: Simple high-performance fabric to add more, IPS, Malware protection, WAF, DDOS and/or other Security Services from Cisco and F5

About F5 Networks

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, and software defined networking (SDN) deployments to successfully deliver applications to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and data center orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

You can also follow @f5networks on Twitter or visit us on Facebook for more information about F5, its partners, and technologies. For a complete listing of F5 community sites, please visit www.f5.com/news-press-events/web-media/community.html.

F5, BIG-IP, Access Policy Manager, Global Traffic Manager, and Software Defined Application Services are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

About Sourcefire

Sourcefire, now part of Cisco, is a world leader in intelligent cybersecurity solutions. Together with Cisco, Sourcefire provides a broad portfolio of integrated solutions that deliver unmatched visibility and continuous advanced threat protection across the entire attack continuum, allowing customers to act smarter and more quickly—before, during and after an attack. Sourcefire's innovation in open source security, as well as commercial next-generation network security platforms and advanced malware protection solutions has been trusted for more than 10 years. Sourcefire has earned a reputation for innovation, consistent security effectiveness and world-class research all focused on detecting, understanding and stopping threats. For more information about Sourcefire, please visit www.sourcefire.com.

4.14 | REV1