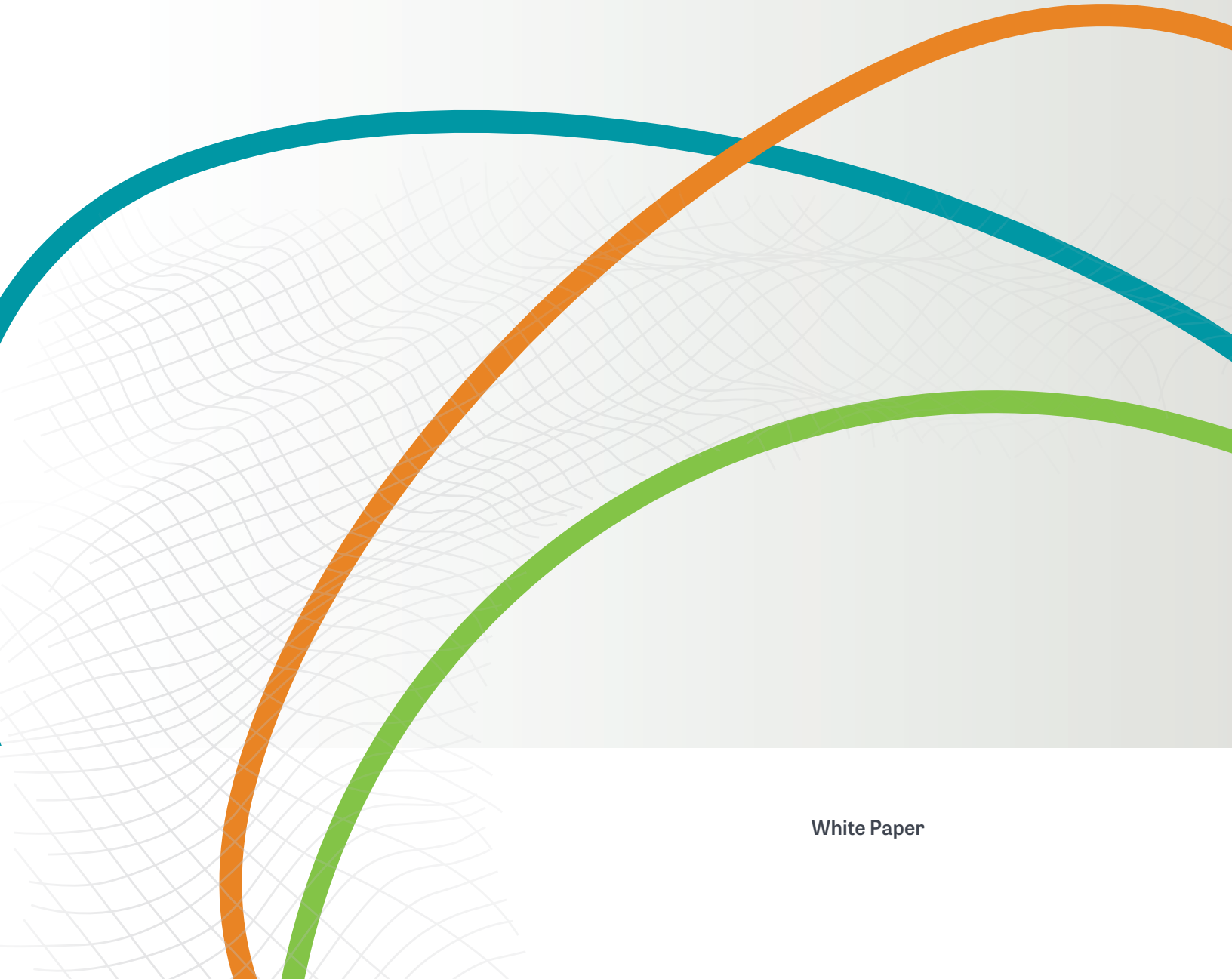
Deploying a Next-Generation IPS Infrastructure

Enterprises require intrusion prevention systems (IPSs) to protect their network against attacks. However, implementing an IPS involves challenges of scale and performance. Leveraging the power of an Application Delivery Controller allows enterprises to efficiently deploy a next-generation IPS infrastructure.



White Paper

Contents

Introduction

A rising number of malicious attacks has made implementing an intrusion prevention system (IPS) a top priority for enterprises large and small. An IPS identifies common vulnerabilities and exposures, and then mitigates them by dropping the malicious packets or blocking traffic from the offending IP address.

However, ensuring the efficiency of the IPS infrastructure has become more difficult with the increasing ubiquity of encryption. When deployed as a network device, an IPS has little visibility into encrypted packets—and the computing power necessary to decrypt and re-encrypt traffic results in decreased performance and increased vulnerability.

However, if enterprises deploy their IPS behind an Application Delivery Controller (ADC) such as the F5® BIG-IP® system, they can manage their IPS from a strategic point of control that allows them to offload SSL termination and gives them visibility into and control over the traffic being inspected by the IPS sensors. By efficiently leveraging IPS resources, you can optimize IPS performance, simplify IPS management, increase business agility, and improve your overall security posture.

Defense in Depth—Without Compromise

Malicious attacks and regulations and compliance standards such as PCI DSS have turned the implementation of an effective IPS into a must-have for any organization. Despite the necessity for a strong and flexible IPS, many enterprises struggle with the management and use of this essential tool. Questions of scalability, SSL termination difficulties, and problems managing the flow of traffic to the IPS sensors continue to trouble organizations that attempt to establish a true, in-depth defense posture.

The Challenges of Implementing an IPS

The problem is getting worse. With an increasing focus on privacy and security, the online world is moving toward ubiquitous encryption. This presents a challenge for standalone intrusion prevention systems, which are simply not designed to efficiently decrypt and

We are quickly moving into an SSL-everywhere world.

"2013 was a banner year for the SSL industry, according to Netcraft's January 2014 web server survey… . Since the January 2013 survey, SSL use among the million busiest sites has increased by 48 percent."[1] A stand-alone IPS is not equipped to deal with this explosion of encrypted traffic.

1 Burt, Chris. "SSL Use Among Million Busiest Sites Up by 48% Year-Over-Year: Netcraft Survey." TheWHIR.com. http://www.thewhir.com/web-hosting-news/ssl-use-among-million-busiest-sites-48-year-year-netcraft-survey (accessed February 19, 2014).

re-encrypt the floods of encrypted traffic that pass through them—thus preventing these systems from performing their objectives of inspecting traffic and mitigating attacks.

An IPS is designed to inspect every single packet of incoming traffic for malicious attacks. As the traffic increases—either naturally or as the result of an attack—an enterprise's IPS becomes overwhelmed with the amount of data it must process.

Because of the overabundance of information and difficulties of handling encrypted traffic, enterprises are faced with two unfortunate options. They can buy more IPSs to cope with the increased traffic, which increases CapEx obviously and OpEx with the difficulty of managing the ballooning infrastructure and associated security logs generated. Alternately, many organizations simply switch off the prevention feature of the IPS, in effect turning it into a simple intrusion detection system (IDS), which sends alerts when it's under attack, but doesn't do anything to prevent or stop the attack. Attack logs build up, and engineers have to spend more time analyzing them—which compounds the problem of having a massive amount of information, but not enough resources to leverage it.

Finally, traditional network IPS deployments occasionally open enterprises to more vulnerability as they don't support hitless upgrades. Without hitless upgrades, IT struggles to keep their IPS infrastructure updated, configured, and highly available, because they have to turn off the IPS as they add new sensors. In addition to the new vulnerability windows opened, organizations have the added pain of scheduling these service changes only during low-traffic hours or on weekends.

Implementing Next-Generation IPS Strengthens the Security Posture of the Enterprise

A comprehensive security architecture necessarily includes a strong network firewall, robust DDoS protection, a web application firewall, and an efficient IPS. One of the keys to building that security posture is freeing IPS sensors to do what they do best: detect and prevent malicious attacks. The best way to do this involves managing those IPS sensors from one high-performance platform that provides for load balancing, traffic management, and offload of decryption.

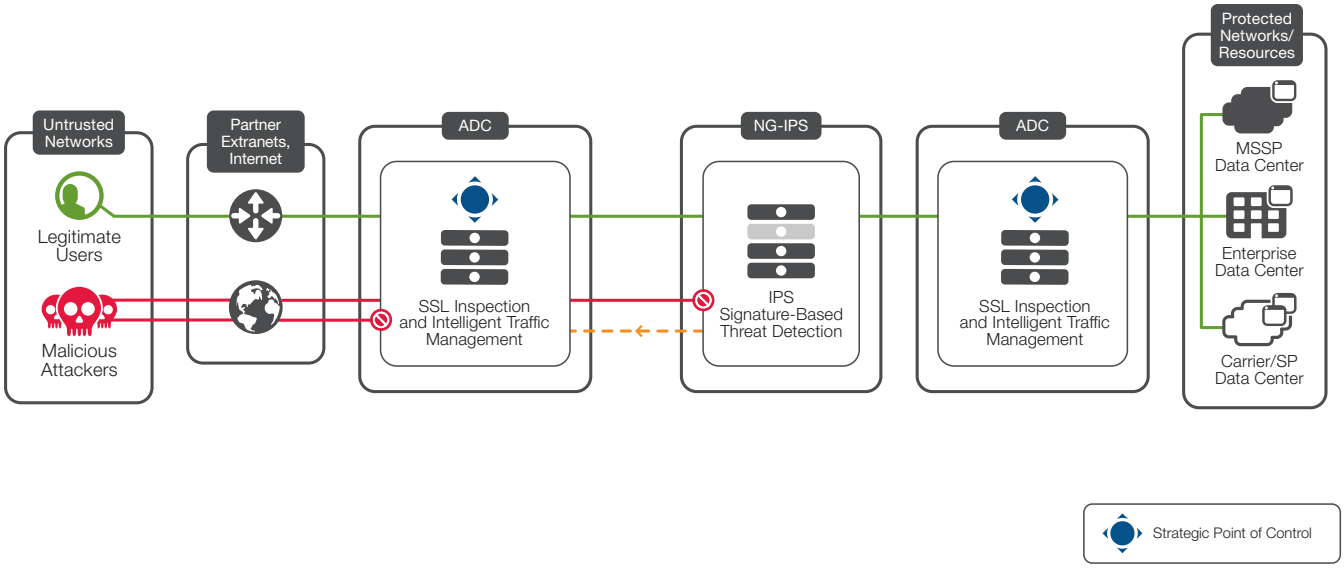
Security from a strategic point of control

Enterprises can benefit by implementing a strategic point of control from which to manage their IPS sensors. Placing a high-performance ADC, such as the BIG-IP system, in front of a pool of IPS sensors enables you to more easily manage your IPS, decrease total cost of ownership, reduce the amount of time spent on reviewing logs and running analytics, and enhance the ability of your IPS sensors to identify and mitigate attacks.

No Application Left Unprotected

Combining a next-generation IPS with the BIG-IP system empowers you to optimize your IPS, augment your security posture, and better protect your network and your mission-critical applications.

The full-proxy architecture of BIG-IP ADCs increases the usefulness of the IPS through policy-based traffic steering that involves inspecting and pre-dropping malicious traffic before it reaches the IPS sensors. BIG-IP ADCs also load balance the traffic among a pool of IPS sensors, ensuring that they are all working efficiently and that no one sensor ever becomes overwhelmed with traffic. In addition, when intensive decryption and encryption functions are offloaded to a BIG-IP ADC, you ensure that your IPS remains highly available—and enables the IPS sensors to focus on identifying and mitigating attacks on the network.



Deploying a Next-Generation IPS Architecture

When you deploy a next-generation IPS, you can realize the many benefits of managing your IPS from a strategic point of control:

- Achieve improved security posture via a comprehensive security services architecture.
- Ensure regulatory compliance with standards such as PCI DSS.
- Optimize IPS performance by offloading SSL termination.
- Gain insight into and control over encrypted traffic.
- Realize efficiencies in your IPS by steering the necessary traffic to the IPS sensors without overloading them.
- Easily scale, manage, and update IPS sensor pools.
- Ensure business continuity through hitless upgrades.
- Reduce OpEx through the ease of maintenance.
- Reduce CapEx through more efficient IPS utilization.

Conclusion

In today's security climate, implementing a strong IPS infrastructure is a requirement, not a luxury. Enterprises can mitigate the traditional difficulties of deploying and managing a robust IPS infrastructure when they deploy a BIG-IP ADC in conjunction with a pool of IPS sensors. You can realize greatly increased efficiency in your IPS infrastructures by offloading SSL termination and allowing BIG-IP ADCs to intelligently steer and load balance the incoming waves of traffic. These increased efficiencies allow the IPS to focus on identifying and mitigating threats to the network—and ensure that no application is left unprotected.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.

WP-SEC-23752-next-generation-IPS