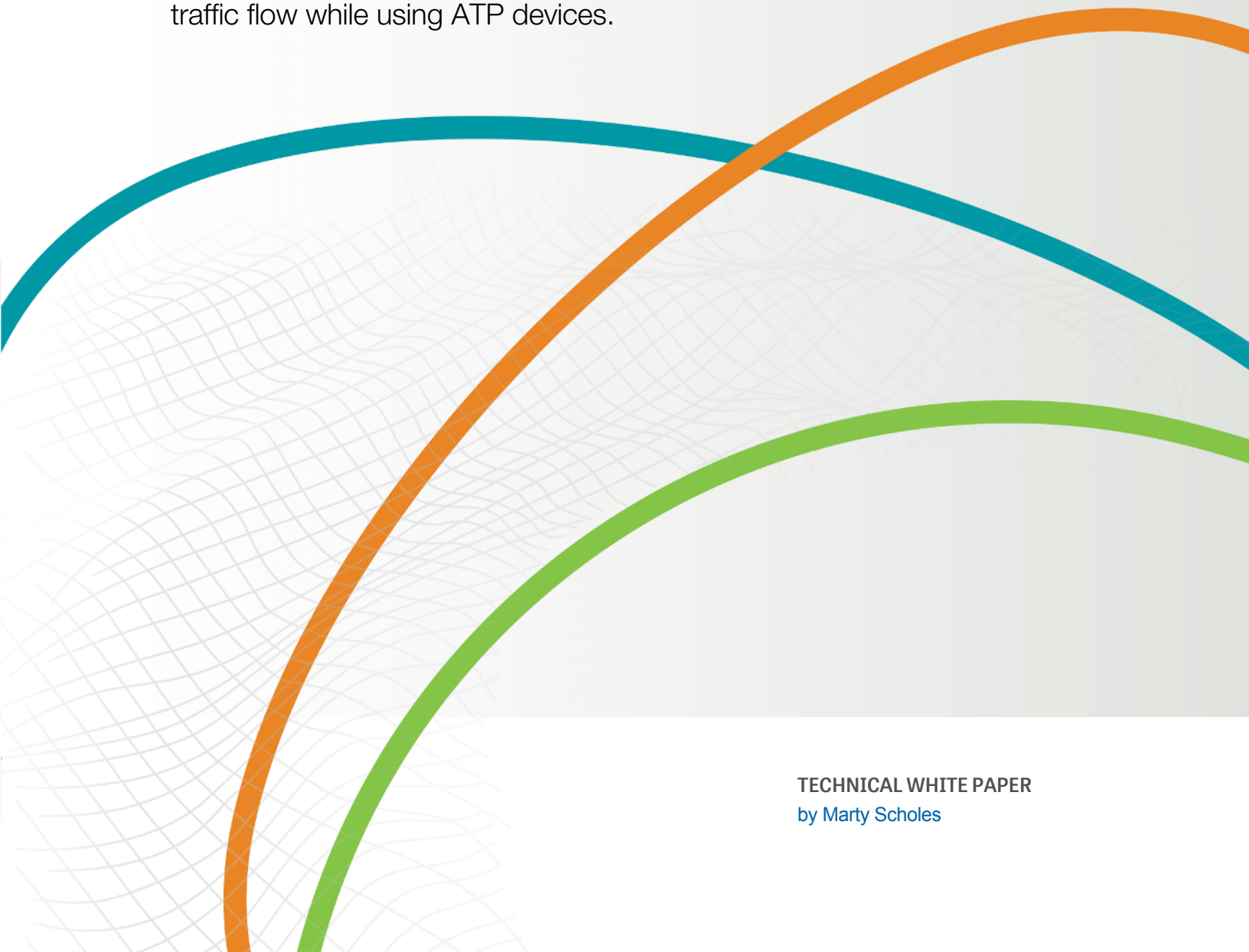
Beyond Advanced Threat Protection

Advanced threat protection systems bring a new level of malware protection to the enterprise, overcoming the weaknesses of intrusion detection and prevention solutions by detecting zero-day malware. ATP devices might also introduce bandwidth constraints and intermittent availability, leading to network outages. Proper use of Application Delivery Controllers can mitigate these limits, ensuring traffic flow while using ATP devices.



TECHNICAL WHITE PAPER

by Marty Scholes

Introduction

As advanced persistent threats dominate the malware landscape, signature-based detection no longer provides adequate protection for the evolving threat environment. Signature-based detection depends on vendors providing signature updates to their platforms. Unfortunately many of today's threats are targeted or even built specifically to infiltrate a particular organization. Often these threats are only used once and then repackaged and modified to evade detection.

In contrast to intrusion detection and prevention solutions, advanced threat protection (ATP) systems trap and execute suspicious objects before they cross the wire, ensuring that the traffic being inspected does not pose a harm to the endpoint. ATP systems can also stop a threat, such as a zero-day attack, even if it has never been seen before. Since ATP systems are so effective at stopping malware, more of these systems are being deployed for an increasing share of ingress and egress traffic. This increased deployment has uncovered three areas where ATP systems can be complemented to increase their effectiveness—SSL assistance, high availability approaches, and traffic steering.

Beyond Advanced Threat Protection

SSL usage is growing. Cryptographic protocols are more complex with longer key lengths, while malicious payload is being encrypted with SSL. These trends not only introduce the need for SSL inspection, but they also place an ever-increasing burden on ATP systems. A solution is needed to offload SSL processing, freeing the ATP systems to focus exclusively on detecting malicious objects.

Like all computing equipment, ATP systems can fail, sometimes blocking traffic. Critical sites must enable high availability in case of a sensor failure. Horizontal scaling allows for ease of growth and elasticity. Ideally a solution would intelligently balance the load across multiple ATP systems, allowing the site to remain available when a sensor failure or overload takes place. Additionally, such a configuration would allow administrators to add or remove sensors without impacting the site availability. This flexibility ensures the ability to scale without disruption.

Ideally, a network would be able to identify and steer traffic intelligently either through the ATP systems or around them. The same traffic steering should avoid decrypting SSL for sensitive sites, such online banking websites.

Comprehensive ATP Solution

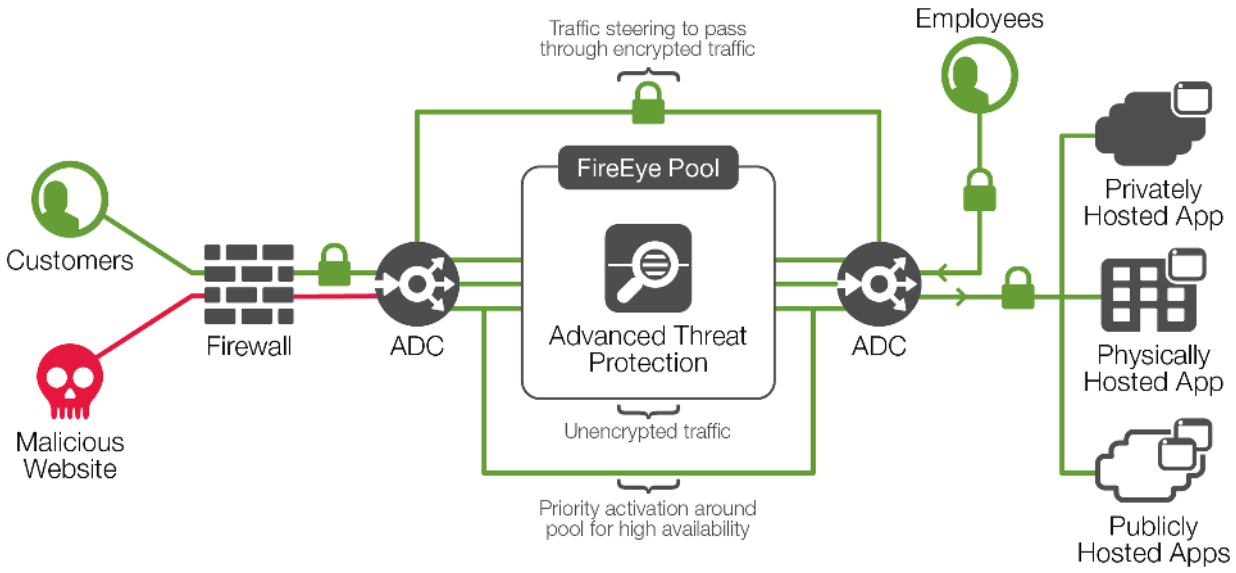


Figure 1: Comprehensive ATP solution showing both inbound and outbound traffic flows.

Figure 1 depicts a comprehensive solution exploiting the full capabilities of an ATP system while providing elastic scalability. A network operations team can architect a solution that provides SSL visibility, high availability, and traffic steering by using existing Application Delivery Controller (ADC) technology.

The diagram shows a pair of ADCs "sandwiching" a pool of ATP devices. The ADC near the perimeter (left) performs the following:

1. Decrypts inbound SSL traffic for delivery to the ATP pool
2. Encrypts outbound SSL traffic which was passed through the ATP pool
3. Performs load balancing on the ATP pool to provide high availability
4. Enables a pool bypass when all of the members are down
5. Steers appropriate traffic around the ATP pool without decrypting it, reducing load on ATP devices

The ADC inside the ATP pool (right) performs a similar set of functions:

1. Decrypts outbound SSL traffic for delivery to the ATP pool
2. Encrypts inbound SSL traffic which was passed through the ATP pool
3. Performs load balancing on the ATP pool to provide high availability
4. Enables a "hairpin" whereby the pool is bypassed when all of the members are down
5. Steers appropriate traffic around the ATP pool without decrypting it, reducing load on ATP devices

This architecture enables the ATP devices to operate at their fullest capabilities without compromising traffic throughput. Key management is centralized at the outer ADC, freeing the ATP pool from having to perform any SSL functionality yet still having full visibility into the traffic. Traffic steering allows for uninteresting (such as VDI) traffic to bypass the ATP pool, increasing the pool's effective capacity. The hairpin enables traffic to continue to flow, even in the case of slowdown or failure of all ATP sensors. The architecture protects traffic to the fullest while eliminating all bottlenecks.

Putting It All Together

At the heart of the comprehensive solution is the ATP appliance. As the number one company listed on the 2015 Cybersecurity 500, FireEye appliances provide advanced threat protection to identify and contain malware, even if the exploits have not previously been seen. FireEye ATP devices stop zero-day attacks before signature-based systems are even aware of an attack. Sites also rely on FireEye for real-time threat prevention.

To complement the FireEye appliance, F5® BIG-IP® Application Delivery Controllers (ADCs) help websites stay available by enabling high availability, SSL offload with proxy, intelligent traffic steering, and traditional load balancing.

The combination of FireEye and F5 gives organizations best-in-class threat protection and offers the critical application availability they need.

Conclusion

Today's daunting security challenges require both advanced threat protection and the capabilities to ensure application availability. FireEye and F5 have partnered to deliver solutions that offer the most effective technology, intelligence, and expertise to identify and stop malicious activity. F5 and FireEye solutions allow you to find hidden threats with SSL visibility, deliver advanced threat protection with greater scalability, and improve operation efficiency with enhanced architecture. To learn how F5 and FireEye solutions can help your business succeed, visit f5.com/fireeye.

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