Global Knowledge®

Expert Reference Series of White Papers

Cisco Completes the Security Picture with Sourcefire

Cisco Completes the Security Picture with Sourcefire

Rich Hummel, CCNA, CCNAW, CCSI

Introduction

Mobility. Cloud computing. The Internet of Everything. These are the big buzzwords in the IT world over the last few years. It's where the growth and money are. And they all have one thing in common. They pose serious security risks to your organization and its data.

On September 16, 2014, Cisco completed the most important step to date with the introduction of the Cisco Adaptive Security Appliance (ASA) with FirePOWER Services next-generation firewall combined with technical, professional, and managed security services. This integration includes the flagship products from each vendor: Cisco's ASA firewall and Sourcefire's Next-Generation Intrusion Prevention System (NGIPS) and Advanced Malware Protection (AMP) technologies.

The purpose of this paper is to examine Cisco's security solutions and how Cisco's acquisition of Sourcefire has changed the security landscape. Cisco's ASA already provided next-generation firewall protection. The addition of Sourcefire's IPS and AMP provides protection in what is being called the attack continuum: before, during, and after an attack. Sourcefire's FirePOWER Services brings contextual awareness by assessing threats proactively, interpreting that data, and then applying the optimal network defense scheme.

The combination of Cisco's ASA and Soucefire's code gives customers a fully integrated security solution providing advanced and zero-day attack prevention, policy and application control, contextual awareness with visibility into users, devices, and applications. Security personnel can now detect, track, and remediate attacks from a single architectural platform.

Security Challenges

The most basic problem with security, whether it is enterprise networks or physical security at a military base, is that everyone wants security . . . as long as it's convenient and inexpensive. Until a breach occurs, then everyone wants to know why there wasn't better security measures in place. Here are some of the challenges faced by security leadership:

- How do you make security part of a holistic network design and get security out of the silos and apply it from the ground up? One of the primary challenges for security leadership is when IT initiatives do not include the proper oversight from security personnel.
    - Think about your last IT project kickoff meeting. Whether it was a tech refresh, growth-driven expansion or relocation, how much time was spent talking about network security, with the proper oversight and controls in place? And if it was discussed, where did it fall on the priority list? This is the beginning of the problem. Everyone wants their network to be secure, but with the bean counters focused on cost, and the users focused on performance, all too often security drops to the bottom of the priority list.

- How can you be proactive when your security team is spending all of their time taking care of alerts and/or events? This is a staffing problem. As much attention as security receives, there is a critical lack of qualified staff available. As attacks become more sophisticated, staff needs to be trained to deal with those attacks. That is not possible when staff is at critical levels and is needed to react to day-to-day challenges.

- Network security is addressed by device, not workflow. Policies and controls are implemented in an inconsistent manner across different network and security technologies. There is no one way to address all devices the same way. The new paradigm is to look at security threats as a continuous process before, during, and after an attack.

- Security policies are too complex to be properly enforced, and silos are common place. The need for contextual awareness requires centralized control, data exchange, common data, and integration across technologies. This is where Sourcefire comes in.

Sourcefire Next-Generation Security

Next-generation security means three things: Next-Generation Firewall (NGFW), NGIPS, and AMP. In the case of Sourcefire, its NGFW comes with integrated IPS. Sourcefire's approach uses these tools to take a "before, during, and after" approach to an attack. What makes this different from the previous approach to security is that it moves from an instantaneous process to a continuous process. If a successful attack occurs, information on the attack is collected and the data is analyzed and used in the defense of future attacks.

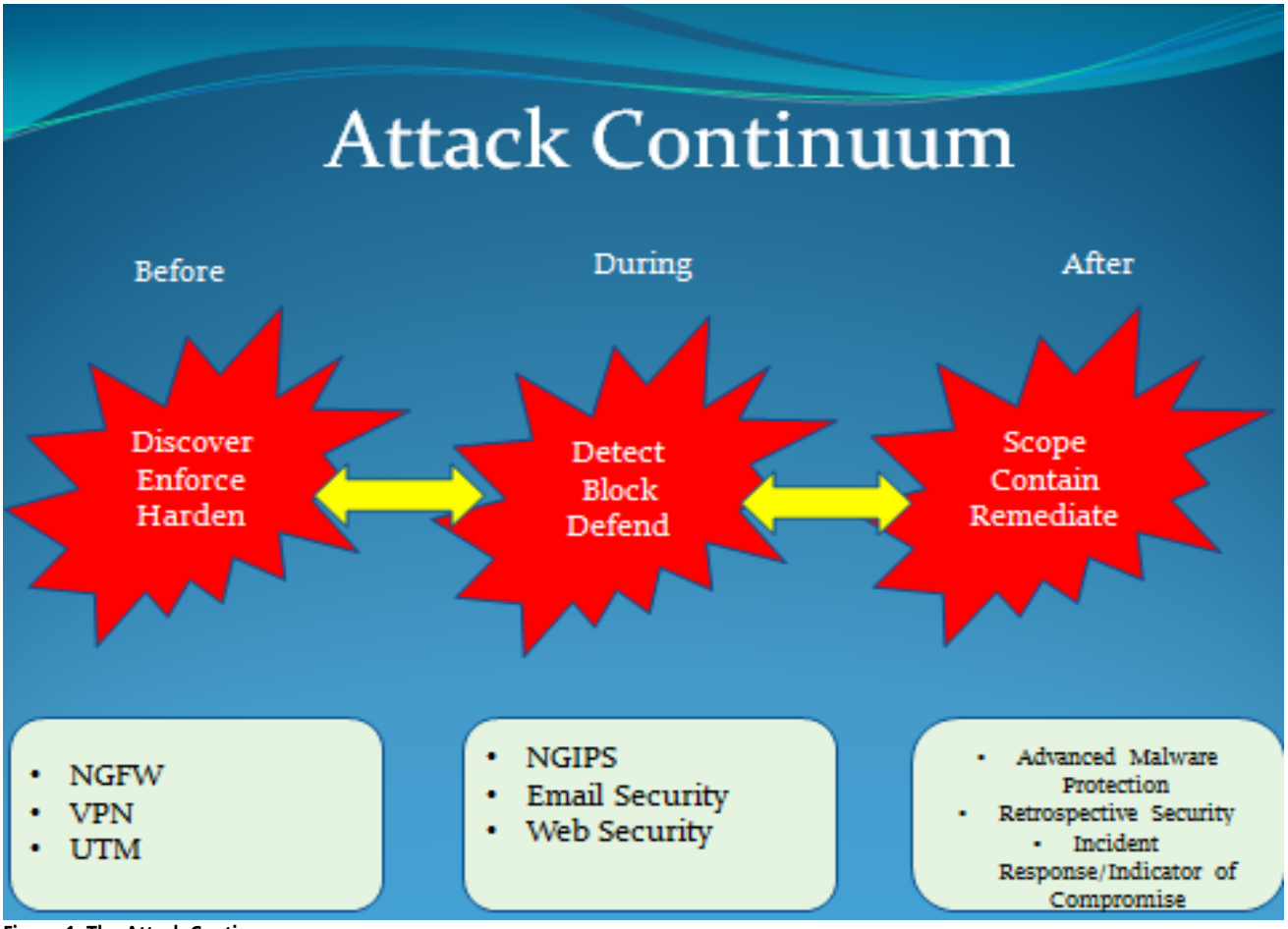

Figure 1. The Attack Continuum

Before

In today's threat environment, attackers often have more information about the network they are targeting than those individuals tasked with the defending the network. Prior to an attack, tools such as NGFW, VPN, and unified threat management (UTM) are used. But you can't secure what you don't know about, so visibility into all aspects of your network is critical. This includes users, devices, applications, OSs, and applications. To secure these resources access controls are required, policy needs to be enforced, applications need to be managed, and access to network assets needs to be controlled. Risks must be assessed based on the value of the target, any history of attacks, and whether the threat of attack is real. The surface area of the network vulnerable to attack needs to be reduced. This is accomplished through access controls. But no matter how diligent security is, attackers will find holes to exploit. Alerts need to be readily visible and responses clearly defined when security is breached.

During

This is where NGIPS comes in, along with web and email security. But first, we must have effective intrusion detection systems in place to identify threats. The IDS needs to be able to detect threats from anywhere a threat can turn up. Whether it's on the network, its endpoints, BYODs or virtual machines, the IDS needs to be passively on the lookout for new attacks. Once detected, Sourcefire's NGIPS responds to block the attack, defending the network as soon as malicious behavior is exhibited. Responses should be automated in real time and coordinated with security policies.

It bears repeating that defenses before and during an attack need to be continuous, as the attacks will be continuous. Gone are the days when you could quarantine a file and feel safe. If we do not change our thought processes from impulsive to the continuous, our defenses, no matter how robust or resilient, will be no match against modern-day attackers.

After

Once an attack has occurred, it's time to assess the damage to see how much of the network has been affected. To further the effort, Sourcefire introduces the concept of retrospective security. In the past, security worked at a particular moment in time. If a firewall or IPS allowed a malicious entity to penetrate the system, there was no way to re-trace the steps that entity took through your network. Now, with AMP, the process becomes continuous rather than instantaneous. Any time a malicious file infects the network, that file is sent up to the cloud backend where analytics are performed on it. Any time a file executes, copies itself, or installs something else, its activities are tracked and evaluated. The file's behaviors are also analyzed. That history can be used to eradicate the malicious file and prevent future attacks.

As mentioned above, vigilance must continue even after an attack. There could be files that have gone undetected, and are lying dormant, waiting to become active. This is why a threat-focused, continuous process needs to be implemented. Security professionals know that their guard can never be let down because the minute you start to feel comfortable, you're open for an attack. Like the title of Andy Grove's book, "*Only the Paranoid Survive*", the assumption must be made that your network is constantly under attack, and constant vigilance must be maintained.

Cisco/Sourcefire Security Solutions

Cisco ASA with FirePOWER Services

Hacking is no longer the purview of lone wolves, sitting in basements playing games trying to breach an organization's security. Nation-states and criminal organizations have made hacking into a profitable venture that wreaks havoc from the White House to mom-and-pop stores. Hackers no longer just try to exploit security gaps, but they seek to steal information and destroy organizations. Cybercrime has flourished, with billions of dollars to be made in this information black market, and the criminals have become more organized and process driven. These criminals understand the impulsive and stagnant nature of traditional security procedures, and take advantage of every opportunity to exploit them. They have become as sophisticated as commercial software development organizations with quality assurances procedures and facilities where they test their wares against the latest security advances.

Until now, security solutions have focused on policy and application control and have been unable to address advanced and zero-day attacks. ASA's FirePOWER Services enhancement overcomes that limitation through context-aware visibility into users; devices and apps; and analytics for detection, tracking, and remediation of attacks.

Prior to the Sourcefire acquisition, Cisco's ASA CX was the firewall of choice. In September 2014, Cisco announced it was integrating Sourcefire's FirePOWER Services with its ASA hardware. Suddenly, ASA CX was legacy software. Cisco will continue to support it as their customers migrate to FirePOWER. Cisco will continue to invest in CX, but the long-term solution is FirePOWER.

On the hardware side, Sourcefire has its own lineup of appliances, but there are few areas where the two companies' solutions overlap. Sourcefire's hardware resides in the data center. Cisco's hardware is most appropriately placed at the network edge.

Figure 2. Cisco ASA with FirePOWER Advanced Services

FirePOWER Services can be added to existing ASA 5500-X and ASA 5585-X deployments or included with new deployments of those firewalls. Cisco SMARTnet Technical Services provides access to support tools and expertise. Managed Services provides full-time threat monitoring and management. Finally, the Sourcefire Incident Response team assists customers in diagnosing, identifying, and remediating risks using FirePOWER technology. The contextual awareness that AMP provides also feeds into Cisco's big data analysis tools.

These services can be managed with the Cisco FireSIGHT Management Center. Visibility is gained into users, mobile devices, client-side apps, virtual machine (VM)-to-VM communications, vulnerabilities, threats, and URLs. Also, activity within the network and across NGFW deployments is controlled from this point.

Cisco FireSIGHT Management Center provides comprehensive, actionable indicators of compromise (IoCs) that relate detailed network and endpoint event information. It gives further visibility into malware attacks.

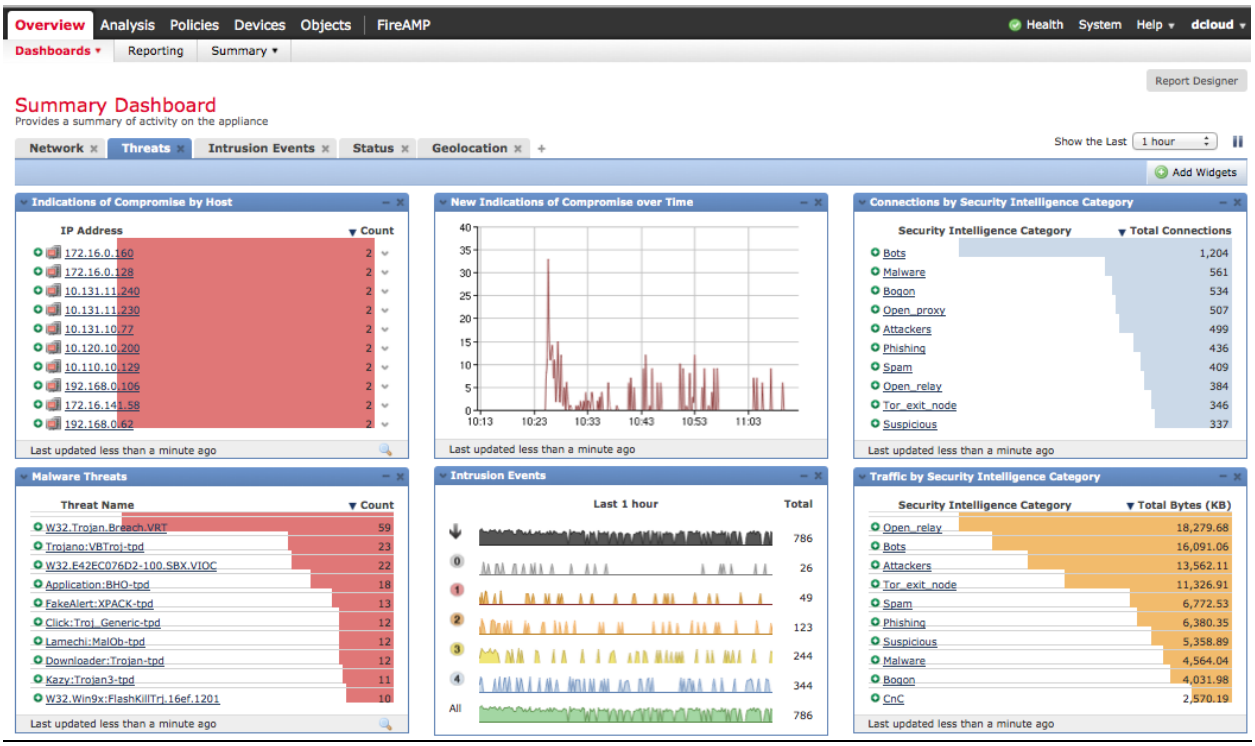

Figure 3. FireSIGHT Management Center

Conclusion

Security attacks have become more advanced; therefore, security solutions have needed to evolve to deal with those threats. Cisco's acquisition of Sourcefire brings a new paradigm to the security landscape. No longer is security a one-time, instantaneous event. Security now is threat based, network cognizant, and continuous. Threats are more sophisticated and can come from all directions with varying magnitude. The integration of NGRW and IPS was the first step in addressing this new and ever-changing attack environment. The "before, during, and after" attack continuum includes analytics after the attack that help in future network defense. All organizations, public and private, need to be aware not only of the constantly changing threat environment, but must be prepared to respond in kind.

The Sourcefire acquisition is a complimentary one for Cisco with little product overlap that provides customers with the most up-to-date technology and security framework.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Cisco Security Training

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Rich Hummel has a bachelor's degree in electrical engineering from New Jersey Institute of Technology, and a master's degree in technology management. He has worked extensively with wireless, video, and cloud technologies.