Jeff Dixon

Abstract: Introduction to Cisco Firepower Threat Defense

Information Security is akin to a never ending cat and mouse game, it's rapid pace makes it one of the fastest evolving areas in technology. Every day, new vulnerabilities and new solutions are created. This paper will discuss Cisco's Next Generation Firewall technology that has evolved to help defend against new and emerging threats. While many solutions exist, the focus for this paper will be on Cisco's newest unified Firepower Threat Defense (FTD) image running on their Adaptive Security Appliance (ASA).

The paper will aim to provide a base understanding of Next Generation Firewall technology followed by a deeper dive into Cisco's newest Threat Defense solution. Presentations and documentation from Cisco as well as other industry journals will be referenced to help provide the most up-to-date information possible. Topics addressed will include a discussion of how this new image differs from previous platforms, new protection technologies (AMP, URL, IPS), and benefits and concerns when moving to the unified FTD image.

The audience for this paper includes anyone looking to gain a better understanding of Cisco's newest ASA and NGFW technology. It also assumes the reader to have a basic understanding of networking and security technology. Readers at all levels weather management, engineers, or students will all find useful information.

Table of Contents

Introduction to Cisco Firepower Threat Defense

Chapter 1: Introduction

Firewalls, Malware, and Threats, oh my! Today's internet, while amazing, poses a great deal of risks. The first line of defense for practically every user, is a firewall, and this is no different for businesses. Cisco Systems, one of the largest and most influential market leaders in networking technologies, produces some of the most widely used firewalls today. The latest in firewall systems are commonly referred to as Next-Generation Firewalls (NGFW). Cisco has made many advancements in their firewall products as of late. However, I won't dispute who makes the best firewall. My goal here is simply to layout the capabilities and new features of the Cisco ASA-X firewall, in addition to providing guidance in choosing the right solution when looking replace or add a new system.

The firewall technology discussed will focus primarily around Cisco's Adaptive Security Appliance (ASA) firewall. The newest ASA appliances, to which we will be covering, are referred to as the ASA-X series. It should be assumed any reference to ASA's will refer to this series unless otherwise stated. This paper began around answering many of the questions that arose when initially separating the marketing from the technical solutions. Additionally, it looks to provide a straight forward overview of the technology. In particular, we will focus on NGFW solutions from Cisco to include FirePOWER services, and the newest addition, the unified Firepower Threat Defense (FTD) image. Starting off, we'll look at a brief background on Cisco's firewall technology and what has lead us to this point. We will describe the next gen capabilities that have been added into their current solution, such as malware protection and IPS. Leading into a discussion around the newest unified image, guiding the future of the ASA's. We will follow up with factors to help choose the right firewall solution for your organization and end with our final remarks.

As of now, outside of Cisco, very little has been written about the new unified platform for the ASA firewalls. Although Cisco has provided information about their solutions, much of it is either wrapped in marketing or in the form of lengthy technical product guides. The

information in the paper was parsed from these resources, as well as, recent presentations (notably from Cisco Live), outside journals and personal experience. The result is a straight forward resource to better understand the Cisco ASA-X solution, what it's capable of, and where it's going. The document covers this technology from a fairly high level but does assume a basic working knowledge of networking and security. Many of the topics covered assist in management decisions, from helping to understand and select features, to capacity planning and choosing the best solution. Engineers and others interested in the technology will be presented with plenty of value as well, providing some of the most up-to-date information possible.

Chapter 2: Next-Gen Firewalls

To start off, let us briefly cover the topic of traditional firewalls. Traditional firewalls were designed to traffic based primarily on header information. That is, source and destination IP addresses and port number. The port number was also used to help determine what protocol was in use, such as port 80 for HTTP or 25 for SMTP. Firewalls have traditionally included capabilities such as NAT and VPN as well. While firewalls have gradually improved on these capabilities, this method of filtering traffic has remained the core process of traditional firewall systems for years. The internet, however, has evolved significantly. Internet based applications have created chaos in the security realm. Web 2.0, cloud based everything, IM, peer-to-peer applications, VoIP, and streaming content all creating new conduits for attack [1]. Companies now are regularly passing more traffic over the internet than to internal resources. The threat landscape has changed dramatically, with highly sophisticated malware and threats constantly evolving and showing up at every step. Malware has formed into a multi-million-dollar industry, profiting from stolen information, ransom demands, and many other malicious tactics. To compete with the numerous threats, firewalls also needed to evolve. In the past, independent systems such as intrusion detection system (IDS) and various others have been added to supplement what was missed by the firewall. However, the next evolution of firewalls referred to as next-generation or next-gen firewalls (NGFW) are designed to fill the gaps in traditional firewalls. While definitions will vary, at a minimum you could say that a NGFW provides the ability to analyze and filter traffic at the application layer along with integrated IPS services.

Application visibility is perhaps the most significant new capability in NGFW's, in that we can now tell what the traffic is, and not just it's most basic source and destination information. For example, application visibility can tell that the traffic is BitTorrent, Gmail, or a particular IM client. It could see that your accessing games on Facebook and not just browsing a feed. [2] This granular insight opens the door for many new types of filtering capabilities. Beyond application visibility, NGFW's will include IP, and often many other features, such as SSL decryption and URL filtering.

In the world of VPN, Cisco is often considered unmatched. However, when it comes strictly to firewall technology, the top vendor is a highly debated topic. Nevertheless, Cisco has managed to provide the most popular NGFW solution on the market for many years. While Cisco had a solid solution with their last generation of ASA's, they took notice of the many new capabilities brought by the competition and the ASA was in need of an upgrade. Cisco's answer came with the acquisition of Sourcefire and the ASA-X product line.

Chapter 3: Sourcefire and Cisco

As those familiar with Cisco know, they frequently acquire leading technology companies to expand their products and capabilities. These acquired solutions are then typically integrated and streamlined into their existing lineup. Cisco seeing a need to expand on their already popular firewall solutions, chose to purchase a company called Sourcefire for approximately $2.7 billon [3]. This acquisition was completed on October 7th, 2013 [4]. Sourcefire, founded in 2001, was a leader in cyber security. They provided a significant portfolio and would give Cisco the platform and technology they needed to bring their firewalls to the next level.

Sourcefire's product line added the following major components: Sourcefire Defense Center, which was renamed to the FireSIGHT Management Center, FirePOWER 7000/8000 series appliances, Advanced Malware Protection (AMP) for networks/endpoints, and an SSL Appliance [4]. In addition, Sourcefire's Vulnerability Research Team joined with groups from Cisco to form the threat intelligence organization, Talos [5]. Following the acquisition, Cisco

made the introduction of ASA with FirePOWER services, released in 2014 and updated again in 2015 [6].

In 2015, the ASA with FirePOWER services was in full swing and its evolution has continued to grow with each new update. ASA FirePOWER services provides the following licensed components running on top of the existing firewall: Advanced Malware Protection along with Threat Grid integration, Next-Gen IPS built on Snort technology, and URL filtering with updates from Talos. Management also received some enchantments with the introduction of the FireSIGHT management center that provided centralized management over the ASA's FirePower Module. An overview concerning each of these new features, AMP, URL Filtering, and IPS, is provided in the following section.

Advanced Malware Protection, or AMP, is a major addition to Cisco's security line-up and comes in essentially two forms. AMP for Endpoints, which is an elaborate malware protection system that would be deployed on each host, much like you would deploy and manage your AV solution. The second form is in AMP for networks, which is available to run on platforms such as the ASA and others like the Email (ESA) and Web (WSA) security appliances. While the firewall is busy inspecting traffic flows, AMP is busy inspecting the files that are transmitted. AMP supports scanning a variety of file types including many of the most common such as PDF and MS Office documents. For the most up-to-date listing, refer to Cisco's product guides online. AMP's goal is to detect, track, store, analyze, and optionally block the transmission of malware into the network by inspecting files [7]. Based on the rule configurations, AMP will analyze files in the following manner: For eligible files, the file structure is analyzed and a Spero signature is sent to the AMP Threat Grid cloud to against known malware [7]. Threat Grid, another acquisition in 2014, complements AMP by providing a global view of malware attacks, campaigns, and their distribution. Threat Grid combines advanced malware analysis and deep threat analytics. It provides a system, updated in near real-time, for AMP to analyze potential malware threats against. [8] Following the first stage of analysis, a local malware engine inspects the file and its composition, reviewing its properties, embedded objects, and any possible malware. Files containing confirmed malware are blocked by the engine. AMP will mark a suspicious file as possible malware if it cannot make a

confirmation. It then submits the file to AMP Threat Grid (hosted in the cloud or on premise) for dynamic analysis. At this final stage the file is run in a sandbox environment to help determine if it's actually malicious in nature. A threat score is assigned to the file which denotes the likelihood of the file containing malware and can be blocked or passed through based on the results. [7]

URL filtering is the next component and I'll admit, a lot of what I have to say, is based on my personal thoughts and opinions. The URL filtering feature allows you to perform reputation based and manual filtering for HTTP and if decrypting, HTTPS traffic. I've used both this and various other products and my personal thoughts are as follows. If you do not currently have a dedicated or capable web filtering solution you should consider this one. If you have an existing filtering solution, this could also provide a good complementary level of filtering, as it does not require a large additional investment. When initially looking at the new ASA-X series, it was mentioned to me, on more than one occasion, this could potentially replace our WSA. At first, unsure of the true capabilities, this sounded plausible. However, as an avid user of Cisco's Web Security Appliance (WSA) for many years, I was rather skeptical. After doing my research and now having used ASA's URL Filtering first-hand, it does appear to be a very capable solution. However, this is not a replacement for WSA. The capabilities of WSA are far more granular and robust than that of the ASA. That said, I still felt it was a competent and viable solution depending on your needs. Personally, I choose to double down, adding URL filtering at the ASA while still maintaining the WSA. Since the URL filter analyzes traffic somewhat differently than the WSA, I felt it could still bring value to the table. In essence I used the ASA to focus on blocking malware, while leaving WSA to continue doing the heavy lifting, providing two separate layers of web protection.

So what's my verdict with ASA's URL filter? It's a good solution, however, if you need a more robust filtering solution and you can afford it, there are better ones available. On the other hand, it would be great for smaller companies that can't afford an expensive dedicated appliance. Companies that may want to supplement or replace their current solution or companies with no current solution could easily benefit from such an addition. Ultimately, be

sure to closely evaluate its capabilities with other options and see that it meets all of your company's needs.

When it comes to intrusion prevention systems (IPS), many people may be familiar with the name Snort. Snort is an open source IPS project that was started in 1998 and has stood true as an industry leader in IPS technology. In 2001, Sourcefire created a commercial version of Snort, and with Cisco's Sourcefire acquisition, Cisco gained ownership of Snort. [9] The open source project is still alive and well today, now maintained by Cisco and the open source community. IPS solutions already existed in Cisco's prior ASA platforms, and for the time, they were pretty good. However, times have changed and their IPS solution was ready for a refresh. The commercial Snort based IPS, that had been developed prior by Sourcefire, was brought in with the FirePOWER services to fill this need. Cisco removed their old IPS technology in lieu of this, which now provides them with a Next-Gen IPS (NGIPS) solution. With new levels of application visibility and control (AVC) at work, invoking IPS policies, significantly improved planes of threat detection are now possible. By utilizing network analysis and intrusion policies, this new IPS system helps to detect, alert on, and protect against network traffic that threatens availability, integrity, and confidentiality of hosts and data. Firepower comes with preconfigured policies from Talos that help configure an overall IPS policy. Preconfigured policies may favor security over connectivity, connectivity over security, or a balanced approach which is typically the default. Additionally, customized policy settings can be used for advanced users. [7] Moving to the Snort based IPS appears to have been a great move for Cisco and to help this solution stand the test of time moving forward.

ASA with FirePOWER services provides many great advantages and improvements over prior systems, unfortunately, it still has one major caveat. Although fully capable, the ASA with FirePower Services platform is not truly a unified solution. It is actually two machines running on one device, the ASA module and the FirePOWER module. It consists of two operating systems passing traffic to each other. All traffic is received in through the ASA module and then after being processed, is forwarded on to the FirePOWER module. The FirePOWER module analyzes the traffic and then sends it back to the ASA module. The ASA module is then ultimately responsible for denying or allowing the traffic. [9] The two modules are also

managed independently. The FirePOWER module through the FireSIGHT management center and the ASA module through ASDM. The competition often in-directly points out this difference and Cisco is fully aware of the short coming. In fact, some would even say this even disqualifies the device from being a NGFW altogether [2]. Working diligently to address this situation, we arrive at our next evolution of the ASA, the Firepower Threat Defense unified image.

Chapter 4: Firepower Threat Defense

Cisco has been busy creating a fully unified NGFW solution and in doing so provide numerous needed updates. (Can anyone say, no more Java!) On March 20th, 2016 Cisco released a new unified image for the ASA-X platform, version 6.0.1, and is referred to as Firepower Threat Defense (FTD). An additional upgrade to 6.0.1.1 was released June 20th, 2016. This provided only security and bug fixes, no new features or functionality where presented in this update. A unified image means that the FirePOWER components are no longer processed separately from the ASA components, they all operate on a single OS. The need to process packets two or more times while passed between one OS to the other is no more. This increases speed and efficiency as well as reduces the workload on the hardware making the ASA much more productive. In addition, this also means the much loved/hated ASDM management interface (along with its reliance on Java) is no more. All management is now done through the Firepower management center. What about CLI? Good question! Cisco has always been ruled by command line, and when or if they had a GUI interface, it hasn't always been the best. With FTD and FireSIGHT they are venturing away from this and focusing configuration at the management center. This is a trend we've seen more and more from Cisco as of late. CLI is still present in the ASA, but from my understanding it's somewhat limited. I can't say at this time if the CLI configuration capabilities will be expanded in future releases but that's certainly something to keep an eye on.

Now for some bad news, at least for the time. Moving to the FTD image means a clean reload of the system. That's right, no upgrade, so you may be rebuilding all of your configurations from ground up. Having said that, Cisco has officially announced the release of a migration tool in 6.1. It's listed to support ASA 9.1.x and forward. However, it's limited in the

configuration that will be moved. Currently, the tool is listed to support migrating ASA Access-Rules, NAT Policies, and its referenced objects [10]. Future releases of the migration tool are planned that will expand this configuration support.

When moving to the FTD image the first step is to upgrade the Firepower Management Center to the same code version if not already at the same release. If, you are not changing versions, but just moving to the new unified platform at the same code level, then no upgrade is needed for the management center. According to Cisco's FTD quick start guide for the ASA [11], the following steps are needed to change to the new unified image:

- Verify device support with FTD (5506-X through 5555-X with SSD)
    - 5585-X and Firepower 7000/8000 devices not supported at this time
- Verify and upgrade ROMMON image
- Install FTD OS image
- Install FTD System package
- Configure for Firepower Management
- Register device with Firepower Management and assign Smart License

*Important note - FTD requires the use of Smart Licenses and does not support Classic Licenses. Smart Licenses should be acquired prior to installing the FTD image. A 90-day trial period can be used if needed until the licensees can be attained. Detailed Firepower license information can be found in the guide referenced here [12].

Now if you're anything like me, you're excited about this new solution, eager to see it at work, but probably not quite ready to commit to changing over your production system. On the other hand, if this is a brand new installation, it could be worth considering but there are some things to know about the current release and one should check the capabilities very close before deciding to proceed with a deployment of FTD at this time.

You may ask, when will FTD have full feature parity to the ASA with FirePOWER services? I don't have a specific answer, however, when version 6.1 is released it will be significantly closer to having full parity. The question becomes what features are not supported

and what features are added in 6.1? I don't have a complete answer, however, the following information is what I have found documented at this time.

For 6.0.1.1:

- Routing: no support for EIGRP, or multicast routing
- No support for: Clustering, Site-to-Site VPN, On box management, Multi-context

Version 6.1 appears to be the next release and on the verge of being published. At the Cisco Live conference in Los Vegas, taking place as I write this paper, a presentation was done on 7/11/16 that provided many updates regarding the new capabilities in 6.1 [10]. The slide presentation is currently posted but at my last check the session video had not. I would highly advise anyone interested in this topic to review this session once the video is made public. Within this presentation the following new features specific to FTD were noted to be included in the next release of 6.1:

- Inline Security Group Tags
- Shared NAT
- Rate limiting prefilter policies
- Site-to-Site VPN support
- Routing enhancements
- On box management (Firepower Device Manager)
- Traffic rate Limiting

In addition, many improvements have been made to Firepower management center 6.1 (note the rebranding from FireSIGHT). Outside of the FTD image enhancements, the 6.1 code release is also bringing many new capabilities that are applied across all platforms and looks to be very promising. Again, I highly recommend reviewing the Cisco Live presentation referenced here for more information [10].

Before wrapping up this section it's important to note some of the other important features included with the Firepower module. These are included in code releases since 6.0 with both

FirePOWER services and FTD unless otherwise noted [13]. These work primarily in conjunction with licensed features (IPS/AMP/URL) to enhance their capabilities.

- URL and DNS-Based Security Intelligence – A new feed that helps detect malicious URLs and DNS records to block malware that may have been missed by IP based filtering alone. Also used in Indications of Compromise (IoC)
- DNS Inspection and Sinkholes – intercept, inspect, and block or redirect malicious DNS traffic
- SSL Decryption (Excludes FTD image for 6.0.1)
- OpenAppID-Defined Applications – an open source addition to the existing application detection engine that allows creation and sharing of application detection signatures
- Captive Portal and Active Authentication – can require users to authentication through a browser portal. Maps users to IP's and policies. Used for non-AD, guest, and BYOD
- Integration with Cisco Identity Services Engine (ISE)
- Improved AMP capabilities

Chapter 5: Choosing a firewall

When choosing your next firewall solution there are many questions and aspects that should be addressed. Choosing a device that's too small or missing needed features might end up being a catastrophe and choosing one that's too big or too complex could waste valuable resources. Once you've gathered your prospects and ensured they fall within your budget, it's time to start narrowing things down. Below are a few questions that can help get you started in evaluating the right solution: [14]

- Does the staff have current working knowledge or expertise with this solution?
- Is the solution easy to use? Will it require specialized training?
- Does it reduce time for malware remediation?
- Does it reduce time and aid in identifying which events are meaningful and actionable?
- Does it provide security automation to aid in an ever-changing environment?
- How good is the tech support and what level of support is offered?
- Is additional training available for the platform?
- Will this perform both VPN and Firewall? If so, does it meet your VPN requirements?

- What features & advantages does it offer over other solutions?
- Will the solution meet your performance requirements? Will it do so with all the optional features enabled?

Since you're reading this paper, there is no doubt you have an interest in Cisco ASA's. This being the case, it's a fair assumption that you have, are planning to, or should be looking at Palo Alto Networks as well. Now wait, I'm not changing my tune or recommending Palo over Cisco. What I'm saying is, you should be aware of what they have to offer. Palo Alto has risen quickly over the past few years as one of the top firewall vendors and often competes head-to-head with Cisco. This is a topic we could spend a lot of time on but I only bring it up to ensure you are aware of the competition. While I admit to having a slight Cisco bias due to my background, I will admit Palo Alto has a very alluring solution. That said, Cisco's integration of the Sourcefire line with their ASA's has really put them back in the game. I don't think either solution would be a wrong choice for anyone and notably these two aren't the only ones in the game. Instead, the right choice comes down to which is the right "fit" for the organization. If you have a very strong Cisco knowledge base among your staff, that might be enough to make Cisco the better choice. To counter, if your staff has no knowledge of Cisco products, Palo Alto has a reputation for having a superior management interface and a transition there or to another competitor could make since. However, you certainly shouldn't make the choice on that alone. Remember, having one superior feature doesn't mean they all are. You must evaluate the total solution and then evaluate the fit for your organization. We all have different needs and different resources and therefore we typically need different solutions. Other companies also make very good competing products and while I won't name them out here it's important to find the one that's right for your organization.

Assuming you're still with me and haven't jumped ship, let's continue on with selecting the right device. When it comes to performance it can be tricky. Very often we're just making refined guestimates as to what we need and what a device can do but it's possible to get close enough to make the right choice. In the world of Nex-Gen Firewall's we are no longer talking about a device dedicated to a single function, those are the days of the past. New firewalls are performing many tasks, from the base firewall functionality to IPS, malware protection, and

more. The point I'm getting at is that just like every other computing device, the more you request of it, the more it taxes its resources. Cisco provides the following guidelines when evaluating performance demands using FirePOWER services [15].

- If you run IPS with Application Visibility and Controls (AVC) or Advanced Malware protection (AMP), that is (IPS + AVC) or (IPS + AMP), you can expect to reduce the throughput by 30-40%
- If you run all three services (IPS + AVC + AMP) you can expect a reduced throughput by 50-60%
- URL filtering also reduces throughput by 5-10%, however, it would be reduced further if performing AVC App Discovery

Those are pretty significant impacts and if you haven't properly sized your device to take this into consideration you may run into a lot of trouble. Cisco also notes these percentages to be consistent across FirePOWER appliances [15]. However, once migrated to the new FTD image these numbers are surely to decrease with the improved packet flow through a single unified image. While the above percentages are for Cisco Firepower, performance reductions can be expected on any solution for each additional feature you enable, as is the nature of computing. The take away from this is to decide what features you want now and possibly in the future and research the impact of those features in helping to select the appropriate device.

Once you've moved to configuring and managing your NGFW, there are some strategies that can be used to help manage them in a more optimized manner. With the additional capabilities of these devices the complexity of managing them can at times also increase. In an article written by Sam Erdheim, he proposed the following seven steps for optimizing management of your NGFW: [16]

1. Gain visibility of polices – regularly review application use across the network to help add, remove, or modify rules as needed
2. Reorder rules to improve performance – reorder rules based on throughput, heavier application use should move the rule toward the top to improve performance

3. Identify rules to remove from the rule base – review rules and ensure they are still needed. Are they unused, duplicated, disabled, etc, if so remove them
4. Run regular risk queries – use best practice standards to evaluate rules. Define exceptions for business requirements
5. Ensure continuous compliance – create baseline and ensure regular compliance with industry and internal standards.
6. Automate firewall change request processes – consider firewall-aware change workflow solution
7. Manage all of you firewall policies – standardized rule interpretation, centralized management, and reporting across all devices (across vendors, model, function, etc)

Conclusion

Next-generation Firewall and IPS technologies have entered an exciting and quickly evolving time. Vendors are adding new capabilities and changing the landscape of firewalls at an incredible rate. Cisco Systems is one such vendor, with the ASA being the world's most widely deployed firewall and having many advanced features. The acquisition of Sourcefire marked the beginning of many significant changes and enhancements for the ASA. A new IPS platform, AMP, AVC, URL Filtering, and many other new additions have dramatically changed the capabilities of this device. Although, it's still evolving with many needed and promising changes in the works, the current ASA with FirePOWER services platform offers a very compelling and competent solution worthy of any company's needs. When selecting a new solution many factors come into play. With many vendors and products on the market, each with their strengths and weaknesses, it's important to carefully evaluate the solution that best fits your organization's needs. New and advanced capabilities will help to protect us against threats of today but remember they require additional resources, both in hardware and manpower to operate. Whether you choose Cisco's firewall or not, they are a solidified market leader and their firewall solutions will be one to keep an eye on for some time.

References

*[1] Malecki, F. (2012). Next-generation firewalls: Security with performance. *Network Security, 2012*(12), 19-20. doi:10.1016/s1353-4858(12)70114-9

*[2] Thomason, S. (2012). Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology Network, Web & Security, 12*(13), 1st ser. Retrieved July 17, 2016, from https://globaljournals.org/GJCST_Volume12/6-Improving-Network-Security-Next-Generation.pdf

[3] Cisco Announces Agreement to Acquire Sourcefire. (n.d.). Retrieved July 17, 2016, from https://newsroom.cisco.com/press-release-content?articleId=1225204

[4] Cisco Completes Acquisition of Sourcefire. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/sourcefire.html#~overview

[5] About Talos. (n.d.). Retrieved July 17, 2016, from http://www.talosintelligence.com/about/

[6] Sankar, P. (2016). Deploying FirePOWER Threat Defense for ISR (2016 Berlin). Retrieved July 17, 2016, from https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=89271

[7] Firepower Management Center Configuration Guide, Version 6.0.1. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601.html

[8] Cisco AMP Threat Grid - Cloud - Products & Services. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/products/security/amp-threat-grid-cloud/index.html

[9] FP NGIPS Deployment and Operationalization (2016 Melbourne). (n.d.). Retrieved July 17, 2016, from https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=90074

[10] ASA Firepower NGFW typical deployment scenarios (2016 Las Vegas). (n.d.). Retrieved July 17, 2016, from https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=90909

[11] Cisco Firepower Threat Defense Quick Start Guide for the ASA. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html

[12] Licensing the Firepower System. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Licensing_the_Firepower_System.pdf

[13] Firepower System Release Notes, Version 6.0.1. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/en/us/td/docs/security/firepower/601/relnotes/firepower-system-release-notes-version-601.html?referring_site=RE

[14] NGFW Requirements for SMBs and Distributed Enterprises. (n.d.). Retrieved July 17, 2016, from http://www.cisco.com/c/dam/r/en/in/internet-of-everything-ioe/assets/pdfs/Security_ASA_for_SMB_Whitepaper.pdf

[15] All About the Threats: How to Deploy the Industry's First Threat-Focused Next-Generation Firewall. (n.d.). Retrieved July 17, 2016, from https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=80687

*[16] Erdheim, S. (2013, October). Deployment and management with next-generation firewalls. *Network Security, 2013*(10), 8-12. doi:10.1016/s1353-4858(13)70113-2