Cisco Next-Generation Firewall Evolution

by Samo Jerman, CCIE Security #20241

10. 11. 2014

Cisco introduced the first ASA firewall in 2005. The device inherited most of the features from its predecessor, Cisco PIX.

It was a long and successful story, integrating over the years several additional features on the same platform. Beside the firewall and address translation, ASA also integrates the great Remote Access solution with Anyconnect (or portal access with WebVPN).

However, Cisco always had a competition. One major argument was lack of real application inspection. The ASA hardware, unlike the old PIX, ha the possibility to inspect most of the common known protocols and applications, like DNS, HTTP or FTP. But the user has to define the traffic and port, a specific application is using. There is no general application recognition nor anti malware protection on a bas ASA platform.

The first attempt to solve the lack of application inspection was to introduce the **Content Security and Control Security (CSC) Service Module/Card**. It utilized Trend Micro's Antivirus and AntiMalware

technology for protection and was also capable of filtering URLs. The same hardware was also used for Intrusion Protection (IPS) solution.

While the IPS module was generally well adopted, the CSC had some performance issues. Customers looking for real content security had to find other technology solutions, like WEB Proxy Mail Antispam Solution. A step in this technology was a Cisco acquisition of IronPort in 2007 which gave them an advanced antispam solution. Along with Ironport, Cisco also got the largest email reputation service, *SenderBase.*

However, the Next-Generation market was growing so Cisco had to offer a simple and application-aware solution as a firewall. Integrating **Ironport's** content inspection into a software service module for the ASA created a first real Next-Generation firewall in 2012 – **ASA CX**. But if the customer was going for the CX, the ASA was unable to offer an IPS protection. Even with only the IPS, the service itself was getting old and was not able to keep up with the competition which offers more and more next-generation services into a single device.

With the acquisition of **Sourcefire** in 2013, Cisco adopted one of the best IPS solutions on the market. Integrating the technology from the acquisition and the ASA platform, Cisco combines proven ASA firewall with Sourcefire's threat and advanced malware protection in a single device.

With the **FirePower** services, as Cisco named the SourceFire services for the ASA, Cisco provides great application awareness to proactively assess threats and optimize defenses to protect networks. And the user doesn't have to migrate the firewall.

The **FirePower** is offered as a software service on a small ASA 5500x platform or as a service blade for the bigger 5585x. For now, the configuration and administration for both services is done with two different tools, but for the migration itself, the user gets even more relaxed while migrating only the next-generation services from the old solution and leaves the old legacy features intact (access-list, nat rules, VPN solutions...).

NIL – More Than Just a Training Company

NIL Learning delivers the leading-edge Cisco training to IT professionals and companies around the globe. Through field-proven experts — each both active engineer and instructor — NIL Learning enhances the standard learning curriculum with real-life experience and helps clients to maximize their training investment.

NIL Learning is part of NIL, a leading global IT solutions provider. Since 1992, NIL has been at the forefront of advanced contributors to strategic partner Cisco's technologies, learning curriculum and value-added solutions deployed to clients around the globe. Today, NIL has earned the highest certifications offered by Cisco, VMware, EMC, HP, IBM, Microsoft, F5, Jive, MobileIron, RSA, VCE and others. Their portfolio of solutions consists of managed services, professional services and learning services.

NIL is headquartered in Slovenia, with regional offices in Croatia, Serbia, Saudi Arabia, the U.S., Turkey, South Africa, Morocco, Nigeria, Kenya and Botswana.

Why Learn at NIL LEARNING?

- All NIL LEARNING instructors are **field-proven experts** - each both active engineer, content developer and instructor.
- **75% of NIL LEARNING engineers hold CCSI certifications**, and **20 have already achieved the respected CCIE rank**.
- NIL LEARNING **enhances the standard learning curriculum with real-life experience** and helps clients to maximize their training investment.
- NIL has been a Cisco training partner since 1993; today NIL holds **Cisco Learning Partner Specialized** status and **Cisco Business Learning Partner** status.
- NIL was awarded the **Cisco Most Business Relevant Learning Partner in MEA** in 2010 and the **Most Innovative Learning Partner** in MEA.

- NIL received the **Innovation Award** for its Technology Led Training and its extensive contribution to Cisco learning solutions at the Cisco EMEAR Learning Partner Summit in 2012.
- NIL received the **Innovation Award** for its Technology Led Training and Advanced Engineer Program at the Cisco Global Learning Partner Summit in 2013.
- NIL won the **Cisco Global Learning Partner of the Year** award at the Cisco Partner Summit in 2014.
- NIL Learning runs a centralized training schedule across the whole EMEA region.

More Info

Slovenia

T: +386 1 4746 500

E: sales-support@nil.com

Botswana

T: +267 318 1684

E: training@it-iq.bw

Croatia

T: +385 (0)51 583 255

E: info-nilcroatia@nil.com

Kenya

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Morocco

T: +212(0) 660 808 394

E: info-nilmorocco@nil.com

Nigeria

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Saudi Arabia

T: +966 1 465 4641

E: info.nilme@nil.com

Serbia

T: +381 11 2282 818

E: info-nilserbia@nil.co.rs

South Africa

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Turkey

T: +902 123 81 8639

E: info-nilturkey@nil.com

USA

T: +1 612 886 3900

E: info-nilusa@nil.com

learning.nil.com