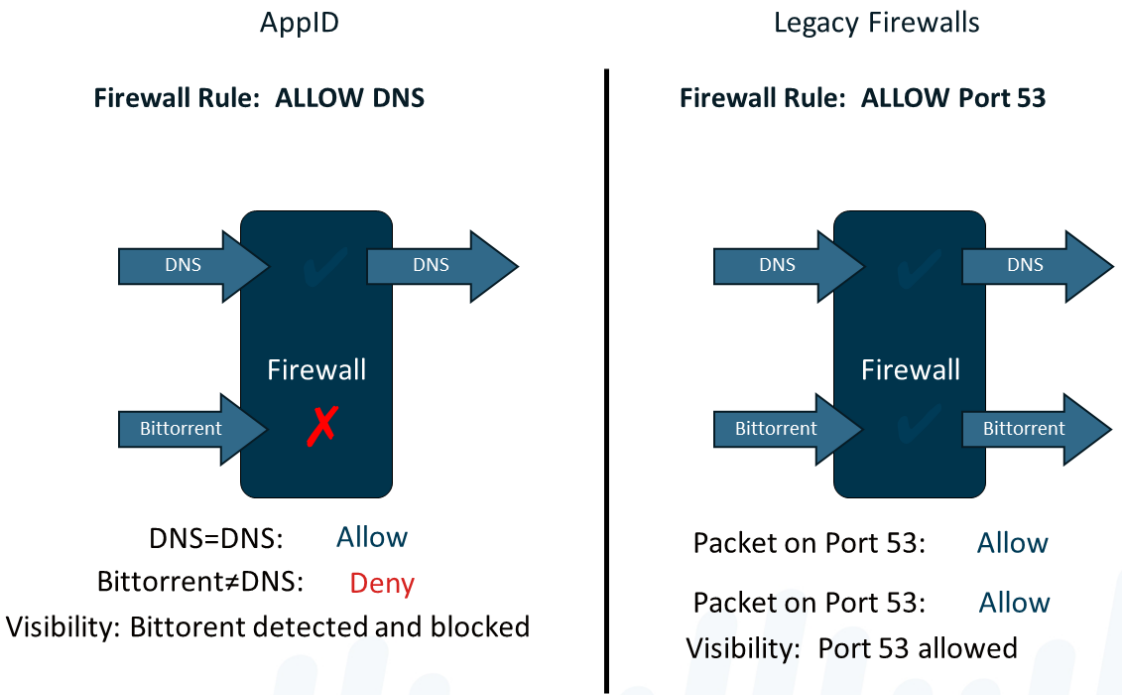
Dec. 30, 2013
Jeremy Li

Next Generation Firewall (NGFW)

Palo Alto Networks (www.paloaltonetworks.com) was founded in 2005 and shipped its first next-generation firewall product built from the ground up in 2007 and is a pure-play network security company in California. It became a public company in July 20, 2012 after its initial public offering (IPO) debuted at $52.20 a share on the New York Stock Exchange under the ticker symbol PANW.

Palo Alto Networks (PAN) has more than 14,000 customers in 120 countries with growth rate at 50% year over year in 2013 (In 2012, PAN had 9,000 customers in over 100 countries). Its revenue will go from $13 billion in 2013 to $17 billion in 2017, according to Forrester [Research]. Today, it has Market Cap at 4.2 billion.

In 2012 and 2013, Gartner assessed Palo Alto Networks (PAN) as a Leader from Gartner Magic Quadrant for Enterprise Network Firewalls, due to its unique NGFW design that includes a patent-pending application identification (App-ID) that blocks a bad application traffic right away (e.g., Bittorrent), while other firewall vendors must pass the bad traffic first via DNS port 53, then, utilize additional resources such as Intrusion prevention systems (IPS) to block it, as illustrated in two screenshots below:



Cisco's legacy stateful inspection and port-based firewall, also known as Adaptive Security Appliance (ASA) could not block any bad traffic at a port level and must accept and pass a bad traffic to other resources such as McAfee IPS appliance in order to stop

the bad application (e.g., Bittorent). This approach requires any organization to purchase additional IPS appliance in order to stop any bad traffic detailed above. As a result, Cisco purchased a very good IPS product called Sourcefire in order to match NGFW.

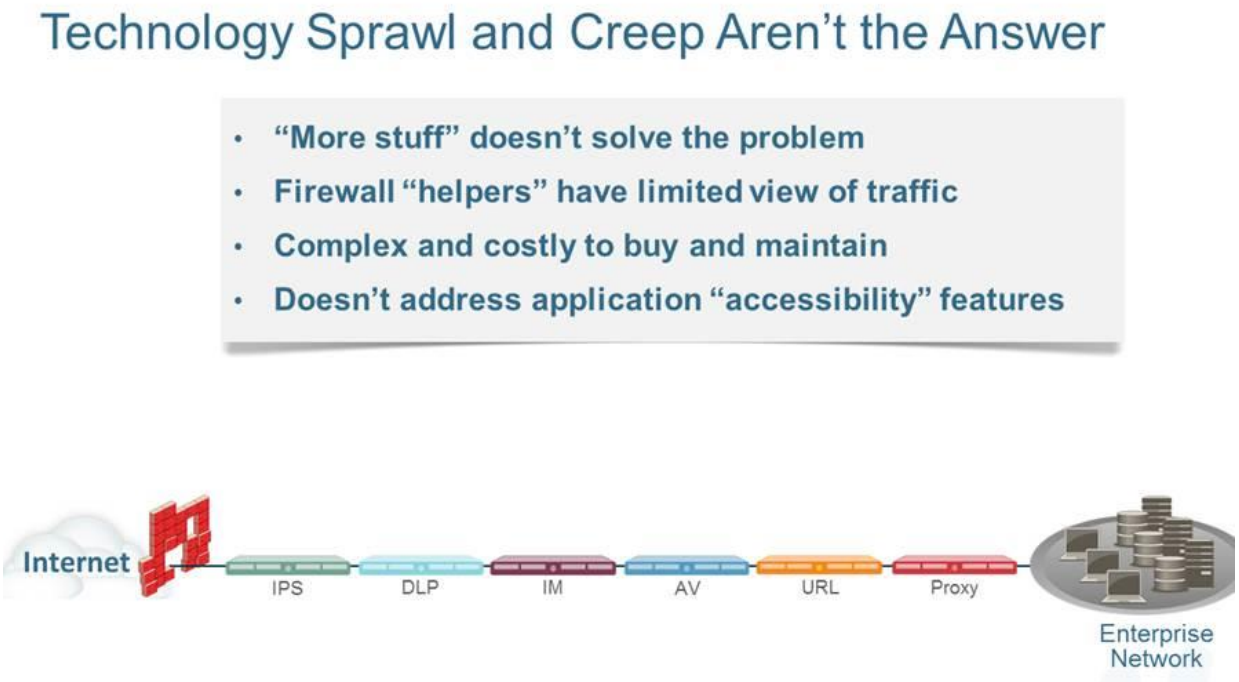
However, Cisco and other vendor's new approach does not give a customer next-generation firewall. Below is a quote from the PAN CEO's presentation

"Taking an IPS and putting it on top of a stateful inspection firewall gives you a stateful inspection firewall on a very good IPS engine. It doesn't give you a next-generation firewall."

Another advantage of NGFW is to get rid of labor-intensive management tasks, especially in a scenario of Cisco ASA as an enterprise network firewall, McAfee appliance as IPS, Bluecoat appliances as URL filter and etc.

On the other hand, PAN's NGFW and IPS can be tightly integrated with App-ID, a disruptive technology within the firewall. Its "single pass" is a crown jewel from its unique design that gives advantage over unnecessary inspection stream, which occurs in many leading vendors' firewalls that must process traffic in serial order [from firewall to IPS, and then to application control (layer 7)]. This approach also increases a troubleshooting time significantly by viewing multiple logs stored at different places.

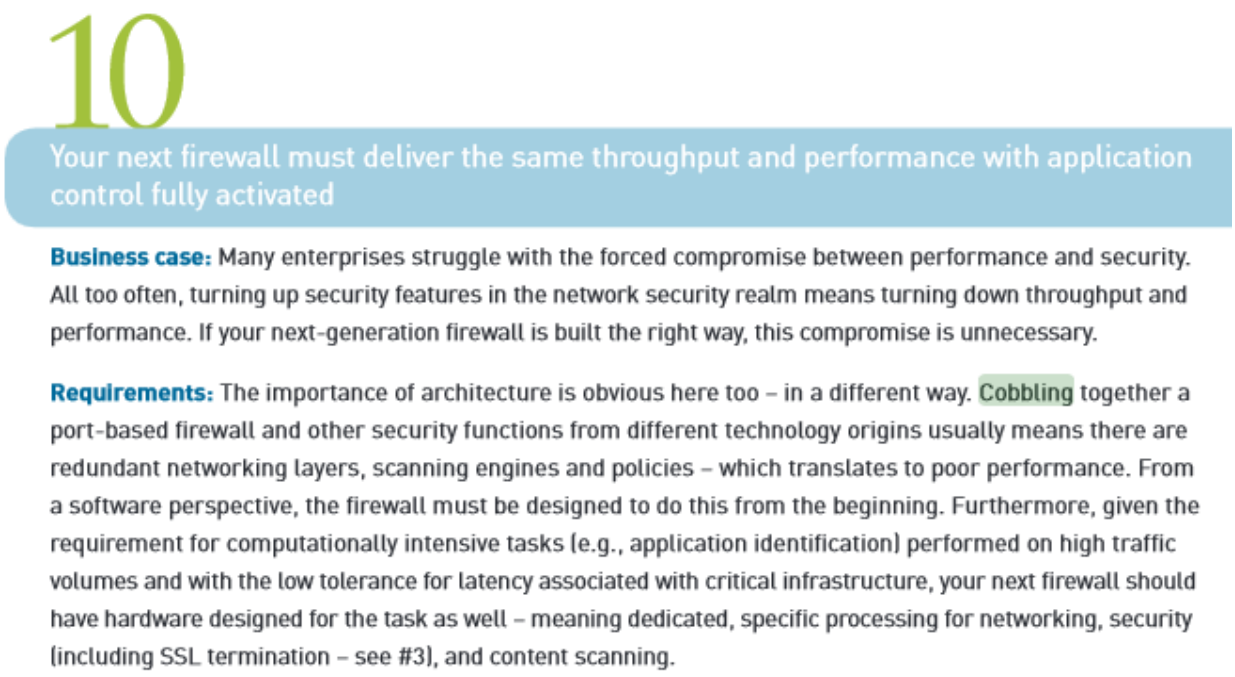
A large enterprise often uses a different team to manage each appliance, respectively, as illustrated in the screenshot below:



This multi-layer and multi-vendor approach creates a more complicated security infrastructure that leads to increase OPEX with many different security teams to manage each portion of the infrastructure.

According to the Wall Street Journal article dated May, 2012 regarding the NGFW as a next wave – path for the enterprise network firewall, PAN has been constantly replacing many legacy firewall vendors in an amazing speed at the expense of Cisco Systems, Inc. mostly, and other leading firewall vendors. This is because many leading enterprise firewall vendors must still rely on a legacy approach - port-based firewall, as illustrated in the screenshot above:

PAN has published a whitepaper titled "10 Things Your Next Firewall Must Do". Author was impressed with a live demo that is able to witness that Check Point firewall is able to meet the requirements detailed in the whitepaper - "10 Things Your Next Firewall Must Do" from which the item 10, as illustrated in a screenshot below, talks about cobbling a traditional port-based (layer 3) firewall by adding a layer 7 application controlling and security function from different technology origins, implying there are redundant networking layers or overlapping to reduce the performance, instead of "single pass" detailed in Gartner report.



10

Your next firewall must deliver the same throughput and performance with application control fully activated

Business case: Many enterprises struggle with the forced compromise between performance and security. All too often, turning up security features in the network security realm means turning down throughput and performance. If your next-generation firewall is built the right way, this compromise is unnecessary.

Requirements: The importance of architecture is obvious here too – in a different way. Cobbling together a port-based firewall and other security functions from different technology origins usually means there are redundant networking layers, scanning engines and policies – which translates to poor performance. From a software perspective, the firewall must be designed to do this from the beginning. Furthermore, given the requirement for computationally intensive tasks (e.g., application identification) performed on high traffic volumes and with the low tolerance for latency associated with critical infrastructure, your next firewall should have hardware designed for the task as well – meaning dedicated, specific processing for networking, security (including SSL termination – see #3), and content scanning.

With PAN NGFW's simplicity but powerful, PAN has been rapidly increasing revenue and market share. Per Gartner, PAN created a market disruption that forces competitors in all quadrants to react.

That's one of the reasons why PAN has been adding over 1,000 new customers every quarter in the past eight (8) consecutive quarters once its enterprise customers realize the benefit of the NGFW design, including less IT workforce to manage the enterprise firewall with a tight integration of IPS within the firewall. Less IT workforce and reducing an infrastructure from complex to less complex mean the NGFW will achieve the real

savings that may avoid many organizations filing for bankruptcy protection (see Desert Hot Springs, a city of 26,000 about 110 miles east of Los Angeles for an example).

Below is an excerpt from Palo Alto Networks CEO: 12 Reasons We're Set To Soar In 2014

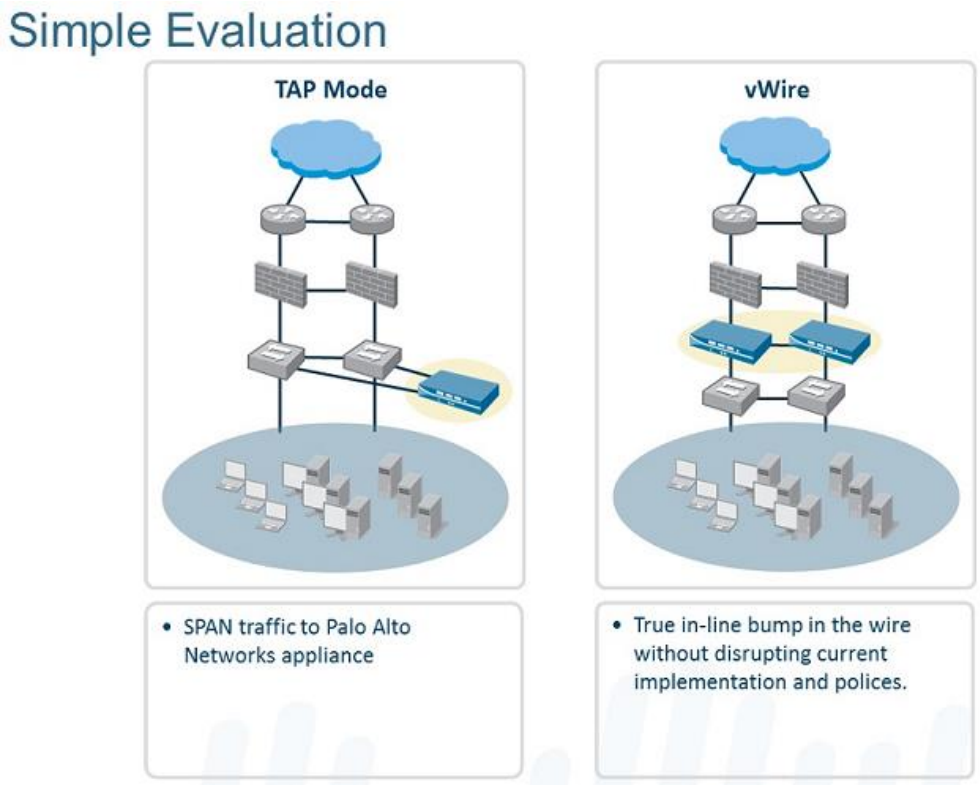
"**Security Trumps Performance And Value**
Enterprise customers buy for three reasons: security, performance and value. If you can't provide security, performance and value don't matter. What is the point? If something is free and it doesn't accomplish the goal of keeping you secure, what is the point of that?"

A next-generation firewall is able to resolve the following issues:

- Complexity
- Inflexible Configuration
- Multiple Management Interfaces
- Support Headaches (Often, many enterprises take months to resolve an issue)
- High TCO

What's the Trick with 50% Growth Rate in 2013 for PAN

It is to let customers try **the Palo Alto Networks' 'Truth Test' –** Click here for details.



As a matter of fact, over 85 percent of the time when a simple evaluation (TAP mode) happens, customers just purchase PAN NGFW.

IPS Vendors

Cisco Sourcefire beats McAfee IPS technology badly. Below is a quote from PAN CEO's presentation on page 11 in November, 2013:

"McAfee had this IPS technology, which was getting beaten badly by Sourcefire. They are smart people over there [at McAfee]."

The CEO's remark mentioned above is in line with Gartner's analysis regarding McAfee IPS capability. Below is an excerpt from the Gartner Magic Quadrant for Enterprise Network Firewalls 2013 report:

"The current Firewall Enterprise IPS capabilities are not competitive with leading NGFW vendors' capabilities, and users generally comment negatively to Gartner on the IPS configuration and performance."

Most Firewall vendors must bolt-on its IPS on top of its legacy firewall to compete with a brand new idea of NGFW.

On the other hand, the architectural paradigm shift is toward NGFW with its simplicity. An example of Bittorent detected and blocked immediately via NGFW is a typical scenario that does not need to rely on additional resources such as IPS that is required via a legacy firewall.

Additional Thoughts about TCO:

Operational efficiency

Scale is often required: more infrastructures, and more IT staff to manage the infrastructure with many different teams. This approach is expensive and limiting. The other fashion approach is to architect for scale: Simplying or build the underlying Firewall platform based on a newer technology to meet the requirements listed above efficiently and without the need for large additional investments in infrastructure and staff.

- A single appliance can scale to 100,000 devices
- Automation: Security and compliance workflow is event-driven and automated.
- Low total cost of ownership: For example, a staff of one can manage over 10,000 devices in MobileIron solution.

Below are responses from PAN regarding some weaknesses of the Next-generation firewall:

1. **The real-world performance testing: PA5020 VS. Check Point 12610 appliance – Two things about this Video:**

A: First, they are only inspecting at layer 3 not at Layer 7 so they can't identify applications in this test, they are just doing Stateful Inspection. Remember, we are ALWAYS identifying the application First, you can't not identify them.

Second we can't see what the traffic mix really is. Robert has tested the smaller PA-3050 up to 2.5Gbps real world traffic at his last job and that is 500 Mbps above the stated limit of 2 Gbps by Palo Alto Networks. We wouldn't be adding 1k new customers per quarter if they did not get the stated performance.

2. **"SIP traffic goes past PA Networks FW as HTTP traffic" ---**

A: **Please see the Attachment we understand SIP as an Application along with H.323 and other VOIP protocols this is a false statement.**

3. Check Point Advantages are: 20 years experiences on Security and etc.

A: The founder of Palo Alto Networks was on the Team that created the original Stateful Inspection Firewall at Checkpoint and most if not all of our product team has been at it just as long. The challenge for a legacy firewall company, whether Cisco or Check Point etc. is that once they have developed a platform as they have based on stateful inspection, changing to an application first model is extremely difficult. They essentially have to cancel their old product and start over. If length of experience were all that mattered you'd be doing just fine with your ASA's and Blue Coat etc. They have all been at it longer than us too.

4. Palo Alto Networks vs. Check Point - VPN Management

A: This only applies for a mesh or Star VPN topology for most VPN's it is the same process for all vendors as IPSec is a standard that all manufactures have to use. it is only when you have remote gateways for checkpoint and want to build VPN's between them is this statement true.

5. Palo Alto Networks vs. Check Point - The APP Gap

A: The numbers counting up the total number of applications is a misleading. Example: We count Facebook as one application. Others count it as Facebook, Facebook Chat, Facebook Games etc. etc. So for every micro behavior of an application they count it as a new application. Cisco does the same thing. We identify and can control all the micro behaviors, but we don't count each micro behavior as a new application.

6. Palo Alto Networks Answer to Cache Poisoning

A: This was really never an issue to begin with but it sure looks scary if you watch the video. To configure it in this fashion would have been against our best practices in the first place. You can always mis-configure a firewall and let in threats. Regardless, we have changed the App flow so all sessions will go through the App-ID signature for all traffic and not the App-ID cache session flow path. The ability to change the Application in the middle of the session flow has been removed by enforcing the App-ID signature match. The App-ID

signature match checks the entire session against the App-ID signature so if the Application is changed in the middle of the flow it will be dropped.

On the other hand a stateful inspection firewall, such as Check Point is subject to application layer exploits as it only looks at session setup and session state. When traffic flows to the IPS it doesn't look at session state, it just looks at traffic signatures with no correlation/integration between the two blades. This is why Check Point's method of using separate blades and handing off the traffic to an IPS blade is less effective. Palo Alto Networks is more than just a firewall we offer a cohesive security platform to enable safe enablement of application this doesn't mean you can't create firewall rules like you are used to in your ASA it means you can add additional security by inspecting traffic at layer 7 or the application layer.

Implementation via "Agile" Approach to "Metrics"

Due to a very complicated security ecosystem, it is highly recommended to follow the SCRUM that is a framework for managing the development and deployment of complex products, in order to implement the entire ecosystem correctly. Agile that follows the principle of "Inspect and Adapt" and advocates team empowerment uses Scrum.

A few tips to use SCRUM for achieving your goal by Michael Vincent:

- Don't be tempted to change Scrum
- Scrum exposes inefficiency
- Fix the problem
- Don't shoot the messenger
- Don't reward a wrong person
- Scrum exposes need for change

Source: 1) Scrum Fundamentals Do It Right by Michael Vincent

2) Case Study of a Difficult Federal Government Scrum Project: FBI Sentinel

Note: The FBI abandoned the VCF project in 2005 after spending $170 million. The project went live on July 1, 2012 after spending 600 million in 12 years by switching to the Scrum.

3) http://agile2013.agilealliance.org

Note: The topic of SCRUM or Agile is beyond the scope of this writing.

Challenges

1. Cisco is still the largest Enterprise Network Firewalls vendor and largest market share in the Enterprise Network Firewalls market, although its current firewall (ASA) is based on a legacy

stateful inspection and port-based firewall. With the newly acquired SourceFire as IPS, Cisco might be able to match the next-generation firewall features except for App-ID and convince its large base customers to stay with Cisco.

2. Cisco might also use One Policy, One Management and One Network slogan to convince its existing customers to stay with Cisco, even though the three ones are designed for the Wired and Wireless LAN Access infrastructure.

3. Check Point with $1.34 Billion in 2012 Revenue and approximately 2000 engineers among nearly 2800 Employees, is a pure-play network security company. Its strength is a huge security intelligence repository with more than 250 million addresses analyzed for bots discovery and over 8.5 million malware signatures. Its repository is also able to identify more than 900,000 malware-infested sites.

   Note: With App-ID, PAN NGFW will be able to block all known and unknown bad traffic right away detailed on page 1.

4. According to Check Point, its advantages over FAN NGFW can be obtained by reading "Look to the security leader to protect your business."

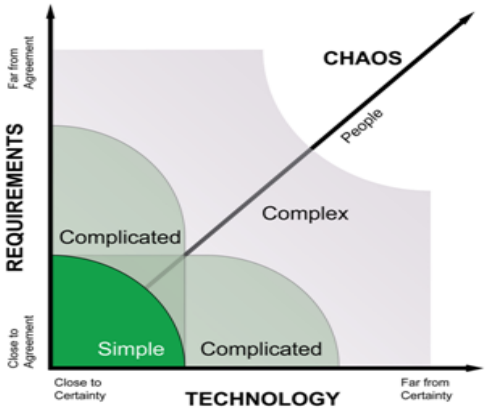
Conclusion

Generally speaking, APN ..., but Cisco has its reputation to provide an excellent presales and postsales support.

In summary, whether your organization requires…(to be continued…, it all depends on an environment by considering total cost ownership (TCO) and return on investment (ROI) carefully!

The Stacey Graph - Complexity

Simple
Everything is known
Complicated
More is known than unknown
Complex
More is unknown than known
Chaotic
Very little is known



Source: Ralph Stacey, University of Hertfordshire

Often, today's solutions will not address tomorrow's problems. The added costs associated with labor always challenge any organizations.

Recommended Reading

1. Magic Quadrant for Enterprise Network Firewalls
   7 February 2013 ID:G00229302
2. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure
   5 September 2013 ID:G00248361

Acknowledgement

Thanks Theron Parry, Account Executive at Alto Palo Networks for inviting me to attend a NGFW webcast, and Robert McIntosh, Sr. Engineer at Alto Palo Networks for presenting NGFW.

Thanks Theron Parry for allowing me to use a few graphics in my notes for clarification purpose.