SANS

Using Palo Alto Networks Next Generation Firewalls to Increase Visibility into Threats and Reduce Threat Risks

SPONSORED BY

WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know about? Let us know.

www.sans.org/whatworks

ABOUT NORTHWEST SAVINGS BANK

Northwest Bancshares, Inc. (NASDAQ: NWBI) is the holding company of Northwest Savings Bank. Founded in 1896, Northwest Savings Bank is a full-service financial institution offering a complete line of personal and business banking products including employee benefits, investment management services, insurance and trust. Northwest operates 165 community banking offices in Pennsylvania, New York, Ohio and Maryland and 50 consumer finance offices in Pennsylvania through its subsidiary, Northwest Consumer Discount Company.

ABOUT THE USER

Lance Spencer is the Lead Data Security Engineer at Northwest Savings Bank and is responsible for maintaining the confidentiality, integrity, and availability of information within the organization. He has 20 plus years of experience as an IT professional with 10 of those concentrated in information security. He holds a degree in computer science, is certified by ISC2 as a CISSP, and by GIAC as a GCFA (GIAC Certified Forensic Analyst)

SUMMARY

Northwest Savings Bank was at the refresh point for its perimeter security and content filtering solutions. Given the threat environment and the demands of auditors in the highly regulated financial vertical, Northwest wanted to get increased visibility into threats and network traffic without increasing procurement cost or staffing requirements. The Palo Alto Networks Next Generation Firewall met all those needs and identified threats that other security solutions had not detected.

Q Tell us a little bit about yourself and the role you play in Northwest.

A I'm a Lead Data Security Engineer at Northwest. We're a smaller sized security team being a community bank. The data security group consists of myself, as lead security engineer. We have a CISO who reports to the CIO, and then we also have a couple of security analysts that work within our group – a pretty small group, but we cover anything that's data security related for the corporation.

Q Is everything pretty much under data security, whether it is network security, endpoints, data, systems – it's all under there?

A Yes. It all falls under our data security group.

Q Since you're using the Palo Alto Networks products, what sort of problems, or what reasons did you start out looking for something like what you're now using from Palo Alto Networks?

A A big part of it was, being a smaller group, we need to have as much visibility into our network and security controls as possible. We're also heavily audited and heavily regulated in the financial industry. So, we really needed to gain visibility not just into network traffic, but what was contained within that traffic. We also had a number of challenges with content filtering. So, Palo Alto Networks was really appealing to us from day one. It unifies so many of the security controls that we were looking at as niche players here and there to solve a certain task. Palo Alto Networks really gave us that extra visibility and kind of tied everything into one package.

Palo Alto Networks really gave us that extra visibility and kind of tied everything into one package.

Q So, was this a scenario where you had a number of products – maybe firewalls and some other products – and you wanted the additional visibility and you said sort of "roll them all together" and reduce the number of products you had, so that you were replacing some things with Palo Alto Networks?

A In some sense, yes, we did rip and replace some controls when we put Palo Alto Networks in. In other areas, it's complementary to existing controls. A big part was tying a lot of those controls together so we more or less had "one pane of glass" to manage those functions. While inspecting traffic content, we're only seeing that through a management tool that's network based while our content filtering is a whole separate component. This really brought it all together so we could aggregate a lot of the security data and focus in one place to see what's going on with our traffic. In some areas Palo Alto Networks is complementing our existing controls. We still follow the mindset of defense in depth and layered security. So, while we didn't go out and just rip and replace everything, while some services we did replace; others, Palo Alto Networks is working in conjunction with.

Q Since it was a little bit of both, did you need get additional budget then? Did you have to go to management and justify additional budget, or was it just part of a yearly refresh kind of thing?

A The cost offsets weren't necessarily in areas where we did replace equipment, such as pulling out our existing technology and putting Palo Alto Networks in. From a cost standpoint, that was almost a wash. Typically, we were getting to the point where we had to renew some equipment anyway, and it just made sense to put Palo Alto Networks in as a replacement. But, then we saw the other feature sets that we could enable and where we could collapse other services. A good example is our content filter licensing agreement. We were using a third party for providing web content filtering. The contract was coming up about the same time we were looking to say, "Hey, is it time to move off our existing platform for an application layer firewall?" So, we looked at that contract and said, "Well, the Palo Alto Networks could basically act as the firewall, and it can do content filtering." We were able to eliminate the content filter service altogether. So, in the grand scheme of things, there were significant cost savings. I hate to throw out cliché terms, but it was almost a no-brainer to move to Palo Alto Networks.

I hate to throw out cliché terms, but it was almost a no-brainer to move to Palo Alto Networks.

Q Did you start out by looking at a bunch of competitive products, or did you just start out looking at Palo Alto Networks?

A We were looking at upgrading our existing technology solutions with our same vendor, with the same platform. Our management team had some prior experience with Palo Alto Networks and more or less said, "Before we jump right back in and sign an agreement and keep going down this road, let's take a look at what Palo Alto Networks has to offer." And after a very short time of looking at Palo Alto Networks in comparison, it was night and day. It was time for a platform change, and we'd get a lot of value for our buck. So, that's how the migration path went. We didn't go through the traditional stack up three vendors and have a bake off. It was comparing Palo Alto Networks to our existing platform and seeing if we still wanted to go forward with our existing platform.

Q You mention additional visibility and some of the other features, like the web content filtering and the like. Were there any other criteria you were looking at to compare the two that were important to you in this area?

A Yes. We are experiencing a growing demand to be able to perform SSL inspection. Again, we're regulated and we have to keep a close eye on what data is transmitted. We started looking at a separate niche solution for doing SSL decryption. That's rolled in as one of the feature sets of Palo Alto Networks, and was very appealing to us. It's one of the features that we turned on almost day one out of the box.

Q How about intrusion prevention? Are you using them as firewall and intrusion detection/prevention, or do you have a separate layer for that?

A It's used in combination. So, it's complimentary to our existing IDS/IPS solutions. But, I'm finding my team leveraging the data that we're seeing out of our Palo Alto Networks more than out of our existing IDS/IPS solutions. I think a lot of that's attributed to the usability of the data that's presented out of the Palo Alto Networks. I think it's a little bit friendlier for our analysts to understand the data that they're seeing.

... for a small shop where we need to get services up and running quickly, it really is a lifesaver.

Q Give me an idea of the scope. How many firewalls, or how many appliances are you talking about?

A We're currently using two Palo Alto Networks firewalls for our primary data center. That's our main ingress/egress. Everything that's Internet based within our corporation traverses those Palo Alto Networks firewalls. And then, we have a second set that's in an HA pair that we have in our backup data center. So, we have a total of four units. Again, they're acting as Internet ingress/egress points. We're now looking at bringing the Palo Alto Networks technology inside to do manage zoning of different network segments.

Q One of the fears rational people usually have from changing firewall platforms is converting the old firewall policies into what's going to run on the new platform. How did you find that? Did you use any tools? How did you go about doing that?

A Good question – that was one of our greatest concerns when we were looking to go to a whole new platform. I think in most of our initial meetings, we knew what technology we wanted. It was pretty obvious to us. The big challenge was just that – coming up with a strategy of how we were going to migrate off this technology that we've been operating for years and our network and security team are comfortable with. We had accumulated years of network rules and NAT tables that we implemented and rely on. We formed an internal team between data security and networking to come up with a strategy.

The very first thing we did, which is a benefit of Palo Alto Networks technologies, is we put the Palo Alto Networks in line on a V-wire (virtual wire) configuration. So, we placed Palo Alto Networks "in front" of our existing firewall, and we just let the traffic patch through so, we could see the behavior, see how it reacted, how it responded, see what it was seeing above and beyond what our typical port and protocol firewall could do. We ran in that configuration for maybe three to four months. I think it was a full business quarter that we ran in that mode of just observing and seeing its capabilities/learning the tool.

We sent our security and network engineers out to get training on the Palo Alto Networks platform. And then, when our "go-live", it was relatively easy to migrate the rules – to export the rules out and migrate them into our Palo Alto Networks and move out of a V-wire mode. We were paranoid so we actually found a third party – a partner of Palo Alto Networks – that specializes in migrations. We flew a guy in and he sat right next to us in the datacenter and we waited for anything and everything to go wrong. After two hours into our change control window when we "flipped the switch" and rewired our cabinets, the Palo Alto Network firewalls came online. I think we had to adjust maybe two or three firewall rules. By Monday morning, it was seamless – no notable business interruption. We prepared for the possibility of a large disaster, and it was a non-event.

Q You had three months or so of running them in parallel - essentially, it then took you less than a week to make the actual switchover once you decided to go.

A Yes that's an accurate statement. The biggest migration change that we had to adapt to was when we went from just your standard protocol rule set over to Palo Alto Networks, which, obviously, is application based. The rules migrated as they were. So, if we say "To this destination, port 80 is open…" we went back and did clean up afterward, and instead of specifying port 80 to that destination we changed that to an application level rule which moved the focus from an IP port to application web-browsing. That was something that took about two hours of going through those rules and identifying the applications to adjust accordingly.

Q Have you added any application level rules since you got the baseline going? SAP, Oracle, or any other?

A Absolutely – we've added numerous rules with new business services. The ease of doing it is night and day from where we were at. I don't know how familiar you are with the Microsoft Lync environment. It's very firewall rule intensive. There are pre-defined applications built inherently into the Palo Alto Networks. So, one could say "Allow outbound Lync access," or, "Allow inbound Lync." It dynamically knows which ports it's going to use and needs to open to make that application work. So, in a sense, it kind of dumbs down some of the deep tech work that you need to do to manage a firewall, but for a small shop where we need to get services up and running quickly, it really is a lifesaver.

Q Were you using your older firewalls and now the Palo Alto Networks for remote access VPN from external laptop employees?

A We haven't migrated VPN services off of our existing VPN solution to the Palo Alto Networks. We're not using the global connect type features on the Palo Alto Networks. We have tested them. We're evaluating whether or not we want to put all those eggs in one basket at this time. So, that's pretty much where we're at at this point. We're also using the Palo Alto Networks units as a web content filter – day one we didn't migrate off our web content filter. It was 90 days after we migrated over to our Palo Alto Networks firewall. We migrated the current rule set and performed rule clean up from our existing web content filter and started having the Palo Alto Networks, play the role of being our primary filter.

Q Are you using any of the Palo Alto Network data feeds, such as the URL, IDS or malware feeds?

A We are using Wildfire for malware. We're also using their BrightCloud service for the web content filtering. The good thing with that is our existing third party content filtering service was using BrightCloud as their back-end category database.

That was almost a one-to-one migration and it was a very simple migration for us. Wildfire services are relatively new to us. Just last month, we purchased the license to use the full WildFire service to inspect and detonate any attachments that we receive or that are downloaded through services such as Dropbox. We automatically forward those to WildFire for inspection and detonation. We've seen immediate results from that service. I think within the first week of turning it on, we found a few items that probably would have slipped through the door undetected and possibly propagated. Our existing anti-virus controls didn't detect anything malicious. Through WildFire, they were identified as malicious. After performing a deeper inspection, we determined they actually were. So, we've had some success with WildFire right out of the gate.

Q Since you've been using the four Palo Alto Networks boxes, is managing the firewalls a fulltime/part time job? Do you have an idea of how much effort it takes you in the steady state?

A I would say no more time than what we used on our prior solution. I spend maybe two hours a day performing health checks and looking to see what type of activity is detected via Palo Alto Networks. We have another analyst that handles more of the web filter management when we have to create exceptions, or make any filter adjustments. So, again, if someone's doing a rip and replace from a port and protocol firewall over to Palo Alto Networks application firewall, I could honestly say there's not an increase in administration that needs to be done.

Q How long has it been since you switched over, or turned on the Palo Alto Networks firewalls?

A We've been running a little over a full year.

Q Are there any lessons learned that you'd like to pass on, or things knowing what you know now that you would have done differently?

A Some of the lessons learned are more around the web content filtering. It is kind of a double-edged sword. Palo Alto Networks is very granular in its capabilities – and, again, that's where it becomes a double-edged sword. Let's say on our past web filter solution, if an end user put in a request to go to a website and that website just happened to have a video clip on it, and it had an audio stream, as long as we allowed that individual to go to that URL, they would have access to every component within that site. So, if it was streaming media, it would just work for them. When we switched over to Palo Alto Networks, it breaks apart the individual applications and web components that make up a webpage – so, even if we say, "Okay, they're allowed to go to sony.com," for example – if there are embedded YouTube videos and such within that page, they won't have access to the video content. So, we find ourselves having to break down pages a little bit more to understand what access we're granting. From a security standpoint, it's great, and from a system performance it's great. (We're a widely distributed network and we have some slow bandwidth going out to some of our branches. We don't want branch users watching YouTube videos and such.) But, on the flip side, from a management standpoint, our Analyst maintaining our web filter or web content rules, is finding himself having to inspect and trouble-shoot web pages a little bit more, or grant access to sub components and sub applications to individuals, or to groups.

Q Have you used their tech support? How would you rate Palo Alto Networks' tech support?

A Yes. I've used it. During our implementation, we ran into what we thought was a snag from a technical standpoint, but it turned out to be human error on our part. The technician we called pinpointed it within seconds. He knew the architecture inside and out. Since then, I think I've opened four support cases. And those typically had some odd scenario or odd rule unique to us. We wanted to validate how we would accomplish what we needed to do and make sure we did it right, bringing Palo Alto Networks in to vet the work and say, "did we do this right?" or "do you recommend we do this a different way?" They've been very helpful with that.

I could honestly say I haven't really had anything break, or go haywire to where we had to call them and say, "Come bail us out," or "Help, we don't know what to do." Even the upgrades we implemented from one of the lower code versions to the latest and greatest version of code. (There were like two or three significant jumps in between versions). From a paranoia standpoint - just from working with our prior environment, we knew that we would be on a call with support for probably hours, and there would be significant down time trying to jump that many levels in an upgrade; and then when we're done, cross our fingers and see what broke and hope for the best. For the upgrade on Palo Alto Networks, we had support on standby in case we did have an issue, and it was basically two clicks of a mouse button and the system was upgraded. So, even that was a non-event.

During our implementation, we ran into what we thought was a snag from a technical standpoint, but it turned out to be human error on our part. The technician we called pinpointed it within seconds. He knew the architecture inside and out.

Q The performance, throughput: have they met their claims and are you happy with the performance ratings?

A Yes. We're not the largest shop. As for our firewall rules and net rules – we're talking about hundreds of rules, not thousands, or tens of thousands, like some larger organizations. When I look at our CPU performance and our throughput, we're not even breaking a sweat. We're running at five percent CPU utilization on the data plane, and the management plane has almost no notable performance.

Q Since you've been using them for a year--any requirements, or new features you've told them you'd like to see them in?

A Yes, I've expressed some interest in the area of reporting. There are a lot of canned reports that one can generate. I'm hoping to get some of the report formats customized so that they can be presented to a higher-level audience. There are decent reports for letting us know from a network and from a security standpoint of what's going on, but, I often have to take that same data and massage it to make it "CIO friendly". The data is there, it's just that the report templates don't really have the data organized in a format that our CIO or anybody can understand. That's a feature request that I've put in, but typically every time I upgrade there's a new feature that comes out. At this point I haven't really had to put in too many requests. DNS sinkholing is a new feature that recently came out, and I implemented within a week of it coming out in the new code version. It's a wonderful feature to help us try to detect botnet traffic and spyware, malware in our environment.

Q Anything else that you'd like to bring up that I didn't ask about?

A No. I can't say this about every vendor that we deal with, but it's been a very pleasant experience and I'm hoping Palo Alto Networks keeps developing their products and staying ahead of the curve. If they do that, I'm sure we'll have a long relationship with them.

SANS Bottom Line on Palo Alto Next Generation Firewall at Northwest:

- Next Generation Firewalls provide both visibility into application layer traffic and the ability to enforce application level polcies vs. port/protocol-centric policies.
- Switching firewall platforms does require translation of existing policy bases. Northwest took multiple steps to ease that transition, initially installing the Next Generation Firewall in front of the legacy firewall to passively observe how new policies would impact business traffic.
- The Palo Alto Networks Next Generation Firewall enabled inspection of SSL traffic as well as more granular enforcement of web site access policies. This increased granularity does increase complexity – administrators should attend training courses.
- Product performance and vendor support met all promises and expectations. Northwest is looking at expanding its use of the product's capabilities.