



WhatWorks in Intrusion Detection and Prevention with Palo Alto Networks

Tapping Unexpected Benefits of IPS + Next-Gen Firewall at Farm Credit Financial Partners

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 more about? Let us know.

www.sans.org/whatworks

About Carl Boyer

Carl Boyer, CISSP, CISM, is the Director of Information Security for Farm Credit Financial Partners. Carl has worked in IT roles for over 20 years and has 19 years of experience as an information security manager. He is a former US Air Force pilot, has a Bachelor of Science degree in Compute Science and a Master of Science degree in Information Systems. He is currently also a technical adviser for IANS (formerly known as the Institute for Applied Network Security).

About Farm Credit Financial Partners

Farm Credit Financial Partners, Inc. (also known as Financial Partners or FPI) is a dedicated information services corporation that provides high-quality, cost-effective business solutions for Farm Credit associations. They are based in Agawam, MA just outside of Springfield, MA. FPI customers serve many regions of the United States — the Northeast, Midwest, Southwest, Northwest and West Coast. FPI began operations on January 1, 1995 to serve 4 agricultural credit associations in the Northeast states of New England, New York and New Jersey establishing a model as the Farm Credit System's first association-owned 4.25 service corporation. It is currently owned by seven partner Farm Credit associations across the country and by CoBank, of Denver. FPI currently has over 150 employees assisted by 25 plus contractors to support approximately 2,200 users working out of over 120 association main office and branch locations. The seven associations currently hold approximately \$25 billion in loans.

SANS Summary

Frustrated with a lack of integration with his end of life intrusion prevention system, the Information Security Director at Farm Credit Financial Partners began a search for a new solution. The product he chose offered the added benefit of a next generation firewall, as well as significant cost savings in people, software, maintenance and hardware.

~~~~~

## **Interview**

### **Q. Tell us a little bit about Farm Credit Financial Partners.**

A. We are effectively an IT service company to farm credit associations. One needs to understand the farm credit system to understand what that means. And you have to look at the Farm Credit Act of 1916. So, the government decided that farmers financial needs are somewhat different than the general commercial industry, for them to go to a commercial bank and say "I need money to build my farm and my collateral is the potential crop growth that I'm going to have in coming years," just didn't work." So, a Farm Credit System was born and you're set up with these loan offices spread out all over the country.

When it was first in its heyday, there were about 3,000 country-wide, and now that number has consolidated over time to about 90 offices. Of course, each of those major offices has branch offices, but it's 90 major organizations. In the Northeast, there are Farm Credit East (formerly First Pioneer and Western New York), Yankee, and Maine. This Northeast group, 15 years ago, worked together to develop a software package that better enabled them to manage their loans from an agricultural perspective as opposed to using a commercial loan solution. And once they had developed that software package, those groups got together and said, "You know, maybe we'd be better off if we put together an IT company that managed and continued to develop the software for us and potentially sold it further down the road to other associations."

"...we found all this great functionality."

**Q. And that became you?**

A. And that became us.

**Q. But you have customers all over the place that you provide service?**

A. Correct. So our staff is about 150 people which is about 100 in Massachusetts and about 50 in Spokane, Washington. In addition to those four associations in the northeast, we picked up four more out in the west, one in the Midwest and three on the west coast. We currently manage about 2,300 users and somewhere close to 450 production servers.

**Q. And are they mostly non-virtual, or is there a lot of virtual stuff in it now?**

A. Primarily non-virtual. The lab environment is becoming more and more virtualized, and this year we're expecting to start virtualizing some of our production systems.

**Q. Tell us about you.**

A. I am the Information Security Director and I've been here 1 1/2 years.

**Q. And you were looking at your environment, what led you to think it would be a really good idea to do something in network security with a next generation firewall rather than just continue to do what you were doing?**

A. We were on ISS Proventia through a monitoring service company and we were ending that contract with that group. We were also not particular happy with how well the Proventia systems were integrated with our environment so we wanted to look for a different IPS solution. Initially, though, we were still looking at traditional IPS options.

**Q. So, it started as an IPS initiative?**

A. Right. I happened to attend one of the IAN's conferences last year and came across the Palo Alto Networks product but didn't initially look at it as an IPS solution. I had some further discussions with them about what my real need was and found that they did IPS. And we did a little bit deeper dive and I found it very interesting. Not only is it built around next generation firewall, but it also does IPS and I thought about its potential further down the road. But in the meantime, I needed a new IPS. Now, in parallel, I was looking still at the traditional solutions, so my focus was on the industry leaders, which were Tipping Point and Snort and Juniper. We were pretty well focused on either Sourcefire or Tipping Point with my favor being towards Tipping Point, but they were somewhat of a costly application. I was becoming more and more intrigued by the Palo Alto Networks option.

**Q. Now, what was it about Palo Alto Networks that made you think it might be a more innovative solution to your problems than the standard stuff?**

A. If you pull out just your IPS solution, it's really similar to a traditional model, but it's bundled with this next generation firewall so now I have the ability to look at more data through one system and deal with it more holistically. And I can look at it through one interface. I can now see in one solution how is my firewall addressing a particular

"When we saw the net savings, I just was like -- holy mackerel!"

threat, and at the same time, how the IPS is reacting to it--both sets of information side-by-side. And the way you can craft rules, in effect, it becomes a singular solution as opposed to two different solutions where I'm building an IPS rule set and a firewall rule set.

And this was built from the ground up and they've effectively built-in parallel processing in the unit so that you don't see the negative performance impact that you see with other solutions where you're cobbling existing solutions together.

**Q. What won you over, the financial benefit or that they were woven together?**

A. It was both. And for me, specifically, I had my immediate need to solve and that was the IPS solution.

**Q. And you had a deadline for that, which makes this all a lot easier.**

A. Right, and that's what I was just focusing on. But, because this is really a network security appliance, I had to have our senior network engineer take a look at this solution. And when he did, he liked it and wanted to talk to them about using it for a firewall.

So we had our discussion with them and he came away and he said, "I really want to do

an evaluation with them.” And I said, “I don’t have the time or resources to do that.” He said, “That’s fine. I’ll take care of it. I’ll set up the evaluation.” It happened that a number of our Check Point firewalls were getting a little bit long in the tooth, so he was looking at replacing those and we had some network environment changes that we wanted to make -- he thought that maybe we had an opportunity to address his firewall need.

**Q. How do you evaluate?**

A. We did do some features comparisons, what we were looking for especially since from a line item perspective, this was being charged against my IPS requirement.

**Q. Why is the firewall not yours? It’s just tradition?**

A. Yes. It is not unusual for this to be laid out that way in that firewalls are seen as a network control as opposed to a security control. It’s not that way in every organization, but in the last three or so organizations I’ve worked for, that has been the case.

Timeliness is vital.  
"And we were seeing the updates coming through consistent with the competition."

**Q. No, I see that a lot, I just was wondering why. And it sort of makes sense because it’s really an inline device that needs to be managed everyday and it sort of fits, but then somebody might say so of IPS, and that’s what you found.**

A. Right. Now granted in IPS you’re doing inline resets and that has an impact to the network traffic, but you’re not necessarily rerouting traffic based on where it’s coming from which a firewall may do. I’m going to bring it through the firewall and then I’ll send it somewhere else or I might use a switch somewhere else, or a router to do the same thing. And in fact, there are firewall routers and switches out there now, or routers and switches with firewall capability built into them.

**Q. So, you decided to try it, to run a test.**

A. Yes.

**Q. How long did the test take? What were the positive and negative things you learned? What went right and wrong?**

A. It was planned for a minimum of two weeks. It ended up going about six weeks. The firewall management and certain functionality seemed to be simpler than what we were used to with Check Point. And the reporting on the firewall side and on the IPS side was better than what we had seen with our existing products.

**Q. Do you remember what about the reporting was better and what kind of question it would allow you to answer that the other ones didn't?**

A. Well, one of the things was the timeliness. Check Point, from a firewall perspective, reported the data comes in to you oldest first, so you had to wait for the page to fill up before you got to the current data. This system is built to bring you the most current data first, and then it will back in the older data. You can get into an existing problem right away and start scrolling down to your older data, which for us worked a lot better.

**Q. So you put it in and it took six weeks. Why did it take that long?**

A. Well, it didn't have to take that long. The first thing was to see if it would do the sorts of things we needed from a firewall aspect and also take a look at the IPS functionality. And the firewalling, from our engineer's perspective, was just a much better platform to work with than he had experienced with Check Point--and he's been working with Check Point for a long time.

"The Palo Alto Networks guys were very, very responsive to any of our concerns."

On the IPS side, I was looking for a basic level of functionality because I would probably be comfortable with it if it was going to solve more than one problem at the same time. I can't say if it's really on the same par as Tipping Point, that's questionable, but it's certainly a worthy competitor. So, we looked at things, we were very happy with what we were seeing.

Now, there's a third piece of the pie there and that was the web content filtering. And it turned out that we had a renewal coming up on that contract as well. Staying on Surf Control was a non-starter for us because we were very unhappy with the reporting capabilities there; it was very inconsistent. So, at a minimum we were thinking we were going to have to move to Websense and possibly upgrade, which was going to be a lot more expensive.

The Palo Alto Networks boxes included that with their basic web filtering and at a much lower price than what we would be been paying, even if we stuck with Surf Control. So, we took a look at that and it was much more accurate than Surf Control. Palo Alto Networks' reporting capability isn't in the same class as Websense, but it is definitely better than what we had with Surf Control.

**Q. How was the learning curve?**

A. We've only more recently had an opportunity to look at that now that we've actually acquired the boxes. From an implementation standpoint, our expectation was whether we went with Sourcefire or we went with Tipping Point or Palo Alto, we would work with that organization to tune it. We'd also look at where we were with our existing

platforms to understand what we'd already adjusted. Now, understand that we probably were white listing certain things with the ISS boxes that maybe we wouldn't have to once we changed platforms. And I say we were white listing things, for odd reasons we were having traffic blocked that signatures really shouldn't have been blocking on ISS.

**Q. And you weren't sure why?**

A. No. And our provider couldn't explain it either.

**Q. Can you tell how well it works?**

A. It's looking very effective. We haven't turned on any of the active blocking, but we can see how the basic configuration reacts to things because in preparation for cutting out the existing systems, we put these systems on either side of the existing platforms. So, they're on both sides of the firewalls and IPSes.

We can see how the system would react to the data if it were hitting it on the front side, and then we can see what happens. In other words, if I'm expecting data to get filtered as it comes in, we're going to see the rule react when it first hits on the front side. So, we know Palo Alto Networks would have done "X," well now let's see how the other systems

will react to the hit. And when the data comes out the other side, we again see what data comes back into Palo Alto Networks and say, this data didn't come through or, the ISS platform didn't block this, but the Palo Alto Networks device would have said, "Yes, block it."

"...the firewalling, from our engineer's perspective, was a much better platform to work with than Check Point."

**Q. That's very cool because you very rarely get to test two of them inline that way. So what have you learned?**

A. Generally speaking, the filtering aspects marry up very closely. After about two weeks of watching, we did encounter some high items that were coming through that ISS was not blocking.

**Q. Any idea what type of thing they might have been?**

A. Some Java, Internet Explorer and Adobe vulnerability activity.

**Q. Now, you haven't really gone into tuning the IPS yet, so you don't know how much you're going to have to deal with false positives yet, is that fair?**

A. True.

**Q. How about on the firewall side?**

A. Well, I've learned that--on the IPS side--we only have to focus on those few things that ISS is letting through that the Palo Alto Networks device is saying, I would have blocked that.

"Palo Alto Network boxes give us a huge amount of flexibility compared to anything else."

Q. Okay, that makes sense. So, because you had one in place before, you really are just doing a delta.

A. Yes.

Q. And it really is a much smaller job than starting from scratch.

A. And our existing provider has

provided us with the rules that are currently in place on that, after that, there isn't much to do.

**Q. Well, there's an extra thing to do which is, after a bad thing happens, going back and using it as an IDS, you have to figure out how to do that, right?**

A. Yeah, I think it's more challenging to have to adjust rules, or potentially build new rules than it is to pull the data out of it. And really, the management of the box is going to fall to our network team.

**Q. Oh, because they were partners in buying it. That's really a cool idea, isn't it?**

A. Yes, and previously I was a one-man shop, now I've got one other body, but we have a lot of other responsibilities to take care of. So, from a tool management perspective, the network guys will do this. They manage the box, but the authority to make any changes to policies and rules goes through me. So, if there's something going wrong, we as a group talk about it, they're going to say, "Here's how we're going to make the rule changes to correct the situation," and then I provide approval before they implement it.

**Q. Nice. So, you're a partner in the process, not the full operational director of it.**

A. Exactly.

**Q. What did it do for you in terms of a cost-benefit perspective--not just improving security, but what was the overall effect?**

A. Mind you, we haven't actually turned these on yet from a production standpoint, but right now they're in a parallel mode with our existing gear. From the standpoint of costs, we're going to be saving about \$150,000 a year this way as opposed to doing the traditional IPS firewall in the firewalls.

**Q. Why is it? Where is the savings in the people costs, or in the software and maintenance and hardware?**

A. All of the above. When I put in the request for the purchase, I had to show what it was going to cost the organization. It could have been a strict replacement cost of, we're paying "X" now for these products and now we're going to be paying "X" for the replacement products. In this case, we're paying "X" for three different products and now the new product was going to cost us \$150, 000 per year less just in hardware, software and maintenance. It does not even factor in the soft cost of reduced personnel resources to manage the systems.

**Q. And would you just point to anything that you don't get because you didn't have all three of them. I mean, was there--even if it wasn't important to you--something that you don't get for the lower price?**

A. The only thing really, is the product maturity, specifically in the IPS and web content filtering aspect.

**Q. That's kind of new to Palo Alto Networks and it's old hat to the other guys.**

A. Right. IPS we're doing fairly well. Web content filtering, you know the basis is there, they don't have the same depth of reporting options a product like Websense will have right now.

**Q. Good. Okay. So, there's no completely free lunch, but it's a pretty good deal.**

A. Exactly.

**Q. How about tech support?**

A. The Palo Alto Networks guys were very, very responsive to any of our concerns during our evaluation.

**Q. During the eval, everybody is responsive. How about after that?**

A. When we went to apply a software upgrade to one of the boxes, one of the memory modules went bad. We called their service team; they dialed in to take a quick look at it, and said, "Yep, it's sick. We'll send you a new box right away." Done. Since going into production, we've had a few questions come along for their support team and they've been very responsive.

"...you don't see the negative performance impact that you see with other solutions where you're cobbling existing solutions together."

**Q. How long was that total process for troubleshooting the memory issue?**

A. I wasn't involved in it, but I think about an hour. So, we're satisfied with that and we're confident that they're going to be there. And we talked to some of the other

users and they said whenever they've had issues, they call them up and their response is immediate.

**Q. How about the updates? With an IPS in particular, and actually web filtering, which is even more so, timeliness is vital.**

A. Yes. And we were seeing the updates coming through consistent with the competition.

**Q. So, it wasn't worse than ISS, and was it as good as Tipping Point?**

A. I thought so.

**Q. And that's a wonderful metric because they're the industry leaders. I think of Palo Alto Networks as kind of a super firewall. How does that play out for you?**

A. Well, they're marketing it as a next generation firewall. And if you look at the papers coming out of Gartner, the model Gartner suggests for a next generation firewall is exactly what Palo Alto Networks built.

**Q. How does it actually help you?**

A. What Gartner is recommending is spot on because no longer are applications limited to working with a specific port. The application industry has recognized that port 80 and port 443 are open through standard firewalls because you need it for web services. And they've figured out, gee, we can send our stuff through those same ports. And so now just about everything is going through those ports.

Palo Alto Networks has been designed in a way that it recognizes the traffic for what it is. So, I could have a telnet session going on over Port 80, and it's going to say, hey, this isn't browsing, this actually telnet going over Port 80. And I can say, no, we're not allowing that. Flip side is, I could say, "I don't care what port telnet goes out, and I

"...the model Gartner suggests for a next generation firewall is exactly what Palo Alto Networks built."

don't want to have to specify what port it's going out, I can just say telnet is allowed."

**Q. Have you done any comparisons to see whether other things are not being caught by your existing firewalls?**

A. We don't look at it from that perspective as catching, per se, as the existing firewall platform isn't designed the way is the Palo Alto Networks box is. Our Check Point firewalls are designed as port filters and

therefore, if we opened up a port to allow traffic, then anything can potentially use it. And, yes, we have seen traffic that you would expect to go on a default port going on some other non-default port.

**Q. That's what I meant. It's not just a theoretical value; it's an actual value because you've seen that kind of traffic coming through the wrong port.**

A. Yes. We'll initially just mirror our existing port base rule set that we have on Check Point into Palo Alto Networks, but then as we become more comfortable with the product, we'll start moving to a more application based rule and policy process.

**Q. And will you do it initially as a watcher and then as a stopper? Is that, I mean, can you set it up so that it sees what it would block, but it doesn't block it?**

A. Correct.

**Q. So, you get the value of combining them, the economic value.**

A. Right.

**Q. And you get slightly less than you might have gotten with Websense.**

A. If we went to Websense, the same base functionality from a control perspective would have cost us more. We gave up some of the reporting capability. And when you come right down to it, the control is more important.

**Q. Agreed. So, other than a little more reporting on the web stuff, what are the other future features you would love to see?**

A. When we went through the eval process, the types of things that really irritated us were all report related. There was nothing from a functionality aspect that we found significantly lacking.

**Q. Was the implementation process as smooth as you wanted it to be?**

A. If you look at any of the traditional IPS solutions, typically unless you buy a really big box, you're going to get eight ports which is going to allow you to cover usually four segments. These mid-level Palo Alto Network boxes come with 16 copper and eight fiber ports, which gives us a huge amount of flexibility compared with where we were. That allows us to plug more into these boxes than we could have with anything else we had and even when you match firewall per firewall, it's got more ports than Check Point had.

"...now I have the ability to look at more data through one interface and deal with it more holistically."

**Q. Any capacity issues when it's doing that much application watching? Any capacity issues you're anticipating?**

A. No. We have the 2 gig box, and for us it's quite sufficient. We've looked at the numbers that, I think were generated by Network World, and they were seeing, I think,

1.8 gig throughput. We've talked to a couple of users that have done their own testing and actually loaded up the boxes and they were seeing similar numbers to what Network World's are. For us, that's more than sufficient and based on the loads that we've then thrown at them, these boxes have not been breathing hard at all.

**Q. If you do run out, is it a really big jump in price for the next size up, or can you climb with little blades that you stick in?**

A. It's a box change. And pricing wise, I don't know off the top of my head.

**Q. It doesn't sound like it's going to be an issue for a long time anyway.**

A. Right.

**Q. So, you're in great shape. What's your bottom line on the box?**

A. Yeah. We can't wait to get these things in and running in an operational mode. We are really excited about it. When it came down to it, the big positive is like I said, here we found all this great functionality, but then we had to turn around and say, "Okay, well what is it going to cost us to do this?" And when we saw the net savings, I just was like -- holy mackerel!

#### **SANS Bottom Line on Palo Alto Networks at Farm Credit Financial Partners:**

1. Significant cost savings in people, software, maintenance and hardware;
2. Identifies network traffic by type rather than only by port;
3. Could benefit from better reporting functionality for web content filtering;
4. IPS solution bundled with a next generation firewall provides a more holistic view of data;
5. Reliable technical support.



#### **For more information on Palo Alto Networks**

Visit: <http://www.paloaltonetworks.com/cam/IPS/>

E-mail: [contact\\_sales@paloaltonetworks.com](mailto:contact_sales@paloaltonetworks.com)

Phone: 1-866-320-4788