



INSTITUTE WORKING KNOWLEDGE SERIES™

CASE STUDY

15 September 2006

IDS Selection and Implementation within Financial Services: The decision to go with Sourcefire

Steve Runyon
Security Specialist

FEDERAL HOME LOAN BANK OF NEW YORK

CATEGORY: Intrusion Detection/Intrusion Prevention

↳ **STAGE:** **Selection** – Deployment – Performance

↳ **CASE #06-90230:** Federal Home Loan Bank of New York

About the Federal Home Loan Bank of New York

For over 70 years, the Federal Home Loan Bank of New York ("HLB") has been helping community lenders in New Jersey, New York, Puerto Rico and the U.S. Virgin Islands advance housing and community growth. The HLB is part of the congressionally chartered, nationwide Federal Home Loan Bank System which was created in 1932 to provide a flexible credit liquidity source for member community lenders engaged in home mortgage and neighborhood lending.

About Steve Runyon

Steve Runyon is a Security Specialist with HLB.

During his five years with HLB, he has designed and upgraded the network infrastructure, and researched and implemented security technologies. He currently manages network and security devices for the Bank, including a Sourcefire deployment.

Steve has been in the Security and Networking field since 1989. His recent background includes research of networking and security technologies for use with the EBS Spot FX trading system. Steve currently holds a SANS GIAC Certified Intrusion Analyst (GCIA) certification.

Executive Summary

After years of maintaining and tuning a home-grown intrusion detection system (IDS), The Federal Home Loan Bank of New York (HLB) researched both open source and commercial IDS alternatives and selected an arsenal of Sourcefire Intrusion Sensors managed by a central Sourcefire Defense Center appliance. The decision to purchase Sourcefire was driven by the open source roots of the product, particularly the community that has emerged to support the product, and its ease of deployment and maintenance.

Deployment took just three days and after initial tuning, the intelligence being generated has been revealing. HLB was looking for greater control over the IDS rule base than they had with their own solution and stronger reporting. The team concluded that it was actually less expensive, figuring in all soft and hard costs, to purchase a commercial product than support their own or build their own using Snort[®], the open source intrusion detection and prevention technology also created by Sourcefire. One of the most interesting side benefits of deploying Sourcefire as their IDS has been the immediate confidence of auditors and others in terms of compliance and security because of the recognized brand.

Context

HLB is a government-sponsored enterprise with \$90 billion in assets, but has only 250 employees. It engages in a small number of very large transactions and data security is a critical concern. The bank has two physical locations, but numerous LAN segments within its network.

The information security department consists of four people, with no full time employees focused exclusively on IDS. The network environment is a mix of UNIX and Windows servers and disparate applications.

HLB had developed a sophisticated, customized, homegrown IDS solution to comply with internal security policy. The IDS was both signature-based, and enabled the team to build in its own heuristics. However, maintaining this custom application was the work of one outsourced developer who had to come in to the office for any updates.

As the need for more frequent updates to their existing IDS grew, HLB decided to investigate open source or commercial IDS options to replace their existing solution.

"It was expensive and painful to have a consultant coming in and out to update signatures and make modifications to our IDS. Yes, we had control over the software, but we had to support it. We simply didn't have the headcount to dedicate to that."

“The community that has developed around Snort is really incredible whether you decide to roll your own or buy from Sourcefire”

“Playing around with all these open source toys was fun, but we realized it was taking us WAY too much time.”

Research Approach

Two paths for upgrading the IDS were considered:

1. Build a new IDS from scratch on new hardware
2. Purchase new appliances and software (open source or commercial)

After internal debate, the team elected to go with the second option and began testing open source and commercial software alternatives.

The first step for HLB was to create an internal wish list of functionality they hoped to get from a new IDS. Among the most important requirements were:

- ✧ Greater control over the IDS rule base and configuration than their home grown solution offered
- ✧ Low installation effort and administrative overhead.
- ✧ Strong front-end and reporting dashboard
- ✧ Speed for signature updates
- ✧ Ability to get hardware replaced quickly if necessary
- ✧ Raw packet captures that would trigger rules, both for analysis and as a record of what occurred
- ✧ Selectable IP fragmentation and TCP stream reassembly algorithms to combat IDS insertion and evasion attempts

To conduct product research, the internal information security team took the SANS 503 course on intrusion detection, read various books¹ and tested open source and commercial software alternatives in house. Based on initial research, the clear path was to focus attention on learning the Snort open source software.

“The community that has developed to support Snort is really incredible whether you decide to roll your own or buy from Sourcefire. That part was compelling for us.”

The team went as far as to build Snort sensors from scratch, and test those sensors on their live network. They then researched and tested other Snort components (Barnyard, ACID, BASE, MySQL, Oinkmaster, BleedingSnort, Snort.org).

“Playing around with all these open source toys was fun, but we realized it was taking us WAY too much time. At that point we realized that we should be looking at the Sourcefire commercial product and appliances.”

Sourcefire was the most appealing commercial product they tested primarily due to its front end, its dashboard, and its rule sets.

¹ (RTFM - <http://en.wikipedia.org/wiki/RTFM>)

“With our own homegrown solution, auditors and other vendors would always question the quality and viability of what we were running. With Snort and Sourcefire, that questioning has stopped – people know we’re safe. Auditors just check the box.”

“We felt that with Snort we could get to a point of controlling the IDS quickly rather than always having to be in the mode of understanding and learning. That flexibility and simplicity gave us a lot of comfort.”

Results

HLB purchased three Sourcefire Intrusion Sensor appliances, for a total of ten sensing interfaces, and one Sourcefire Defense Center for centralized reporting, management and software updates.

Procurement took six weeks and installation took just three days. The team concluded immediately that they were in better shape than with their old IDS, and better off than with the other commercial products they evaluated.

About a ½ day per week is still required for tuning mostly for filtering down the information to just what HLB wants to see on a daily basis.

Lessons Learned

- **Choosing a product with a strong brand name helps with auditors (compliance), developers, and other vendors**

The Snort and Sourcefire brands are now well known among auditors, developers, and other IDS vendors. Generally HLB found that they didn’t face the same level of questioning from auditors when asked which IDS protected their perimeter when they answered Sourcefire.

“With our own homegrown solution, auditors and other vendors would always question the quality and viability of what we were running. With Snort and Sourcefire, that questioning has stopped – people know we’re safe. Auditors just check the box.”

- **IDS must be open and flexible, integrate well.**

As a leading financial institution, HLB is a common attack target, and needs tools that are open and flexible to respond to the changing threat landscape in a timely fashion. The institution has no time to wait around for a programmer to make changes to the product; things must move in an automated way.

“We felt that with Snort we could get to a point of controlling the IDS quickly rather than always having to be in the mode of understanding and learning. That flexibility and simplicity gave us a lot of comfort.”

HLB also found that given Sourcefire’s roots in open source, that they could customize the product in ways that were useful to them. Specifically, designing rule sets and writing signatures brought a level of customization that has been very useful.

“It’s a lot like Firefox vs. IE. Being able to write extensions in Firefox doesn’t box you in the way IE does. The same has been true with the Sourcefire product. Since we got to know Snort up front, that same flexibility exists for us today. That’s been really nice.”

In addition, HLB is considering a Security Information and Event Management (SIEM) deployment in the future, and Snort/Sourcefire was viewed as easy to integrate with any SIEM on the market today.

“We spend our time doing analysis now, not setup. If the hardware fails, Sourcefire is there to swap in another box.”

“We’re now using the product to watch for rogue DHCP requests and to detect information disclosure. We didn’t expect to be able to do that. It even told us we had a faulty IOS out there on some of our Cisco boxes – that was interesting.”

- **There is never enough time – keep it simple.**

“Whatever you go with has to be fast, easy and effective to implement and maintain. We, like most, have such a small staff and are always having to switch contexts – different projects and interruptions. We needed a solution that was simple enough that we could always go back to it and quickly make sense of the messages it was sending us.”

- **Follow the crowd using Snort.**

HLB started their research among open source solutions and were particularly impressed by the popularity, resources, and expertise of the Snort community built up around the product. In particular, the huge library of signatures that has been built by the Snort community has been particularly help for the team.

This fact that Snort is considered the de facto standard for intrusion detection and prevention technology added to the confidence the internal group had in purchasing the commercial product from Sourcefire.

- **Benefit from the unexpected.**

Sourcefire’s product has provided an unexpected set of capabilities and benefits to HLB. The breadth of rule sets that have been developed within the Snort community have yielded some interesting facts about HLB’s infrastructure that they didn’t know prior.

“We’re now using the product to watch for rogue DHCP requests and to detect information disclosure. We didn’t expect to be able to do that. It even told us we had a faulty IOS out there on some of our Cisco boxes – that was interesting.”

- **Editing scheduled tasks a minor annoyance.**

HLB’s one complaint about Sourcefire has been the inability to edit or change pre-scheduled tasks after they had been scheduled.

“It’s really more of an annoyance than anything, but I wish you could edit tasks like reports after they had been scheduled. You have to create a whole new task if you want to change it after it’s been scheduled.”

- **Buying is cheaper than building.**

HLB learned through this process that the ongoing hidden cost of building their own IDS far outweighed the costs of a solid commercial solution. Research and Development time once used to build features, and rule sets in their own product has now gone away.

“We’re not spending all our time building boxes any more. We didn’t do an extensive cost comparison of our hard and soft costs between COTS and open source, but on the back of an envelope, the costs were at least equal. Why not get reliable support for that money?”

Sourcefire was up and running in days and has been extremely easy for them to maintain.

“We spend our time doing analysis now, not setup. If the hardware fails, Sourcefire is there to swap in another box.”

Building and maintaining a homegrown system – if all hard and soft costs are considered – is more expensive.

About Sourcefire

Sourcefire, Inc., a world leader in intrusion prevention, is transforming the way organizations manage and minimize network security risks with its 3D Approach - Discover, Determine, Defend - to securing real networks in real-time. The company's ground-breaking network defense system unifies intrusion and vulnerability management technologies to provide customers with superior network security. Founded in 2001 by the creator of Snort[®], Sourcefire is headquartered in Columbia, MD and has been consistently recognized for its innovation and industry leadership by customers, media, and industry analysts alike – with more than 18 awards and accolades since January 2005 alone. Recently, the company was positioned in the Leaders Quadrant of Gartner's "Magic Quadrant for Network Intrusion Prevention System Appliances" report and the Sourcefire 3D System was named "Best Security Solution," at the 2006 SC Magazine Awards. At work in leading Fortune 1000 and government agencies, the names Sourcefire and founder Martin Roesch have grown synonymous with innovation and intelligence in network security.

For more information about Sourcefire, please visit <http://www.sourcefire.com>.

About the Institute for Applied Network Security

THE INSTITUTE FOR APPLIED NETWORK SECURITY is the premier membership organization for practicing information security professionals. The Institute's mission is to provide key technical and business insights to help members solve their most pressing technical and professional challenges.

The Institute achieves this mission through a broad offering of services provided to its members – insightful events, thought-provoking publications, best-practice research and unique networking opportunities.

The Institute is committed to providing its members with unbiased, relevant insights to increase their productivity and effectiveness as emerging technical leaders inside their organizations.