Shifting to an Application-Aware Strategy and Solution

IANS WORKING KNOWLEDGE SERIES™

CASE STUDY

2010

Featured Enterprise

This case study is 100% factual and is based on the actual experience of the information security team at a *Fortune* 100 global technology company.

This case study was written by IANS based on interviews with a senior technology leader at this company. After the case study was complete, the company's communications department decided not to allow the company's name to be used, as doing so might be seen as an implied endorsement, which is against the company's policy.

Quick Read

Featured Enterprise:

- Perceived that information security has changed over the past decade but firewalls have not.
- This company's information security strategy focuses on application awareness. But traditional firewalls have major gaps related to awareness of applications.
- Incumbent vendor roadmaps didn't adequately address application awareness.
- After thorough lab testing of multiple use cases, this company was convinced that Palo Alto Networks filled the requirements and had truly unique capabilities.
- The information security group developed a compelling business case that showed short-term ROI and significant long-term benefits.
- Since deploying Palo Alto Networks, this organization has seen increased application awareness and visibility, improved context-based information protection, and improved management capabilities.

Palo Alto Networks:

- Leader in next-generation firewalls (NGFW).
- Enables unprecedented visibility and granular policy control of applications and content—by user, not just IP address.
- Company's firewalls accurately identify and control applications—regardless of port, protocol, evasive tactic, or SSL encryption—and scan content to stop threats and prevent data leakage.
- Enables enterprises to embrace Web 2.0 while maintaining complete visibility and control.
- Provides a platform for consolidating existing devices and reducing the total cost of ownership.
- Palo Alto Networks delivered on the company's application-awareness strategy.

Overview

The senior security leaders at the featured enterprise concluded that traditional firewalls had not kept pace with the changes and threats in the world of information security. This company wanted to pursue an "application-aware" strategy and wanted an application-aware firewall. But the incumbent vendors didn't have application-aware or next-generation firewalls (NGFW) and it wasn't an important part of their road map.

Enter Palo Alto Networks. Palo Alto Networks' next-generation firewall was exactly what this company envisioned. After extensive lab testing on multiple use cases, they became convinced that Palo Alto Networks' product is a superior solution. Palo Alto Networks provides outstanding visibility about applications and threats, provides context-based security for all key applications, and provides enhanced management capabilities to control access to important applications.

The robust capabilities of this solution mean that this major enterprise can use Palo Alto Networks as a platform that consolidates/replaces other solutions. Not only does this provide better visibility and security, it produces both short-term and long-term cost savings.

Longer term, this company's goal is to completely move from traditional firewalls to multi-threaded, application-aware enforcement devices.

Case Study

Traditional firewalls no longer meet the needs of major enterprises.

The senior security leaders at this company know firewalls. They are familiar with all of the leading products in the space, and claim that, "We know firewalls inside and out." Within five minutes of evaluating a product in the lab, they will know if a firewall is useable or not.

"The context for security changed which caused traditional firewalls to be less effective."

Based on this level of firewall expertise, it had become clear that while the context for information security had changed, traditional firewall technology had not kept pace. This hurt the security status of the entire network environment.

Among the pitfalls of firewall technology that this company saw: the need for a firewall to go to the bit level, and to layer 7 to identify applications, and the inability of traditional firewalls to provide protection from advanced persistent threats.

"Application-aware security has been missing for a decade. It is a big gap."

Required from a next-generation firewall—complete application awareness.

In thinking about the shortcomings of existing firewalls, a security leader at this company was able to articulate a vision for a next-generation firewall solution that provides complete application awareness.

> *"We view the future as moving [from our current firewall] to application awareness. Applications are the target for next-generation threats. We have to understand the networks, threats, and applications, especially in a Web 2.0 / cloud environment."*

In fact, even without knowing if any products fit this vision, this company decided that their optimal long-term firewall strategy was one that focused on application identification and control.

But, a big gap existed in the market as the incumbents' roadmaps failed to address application awareness.

A gap existed in the marketplace. Traditional firewalls no longer adequately met this enterprise's needs. No products fit with this company's vision of complete application awareness.

"I was disappointed to hear that they [the incumbents] had indentified it [lack of application awareness] as a gap, but they were not tremendously focused on a solution."

This company spoke with all of the incumbents and usual suspects—all of which are household names. They sought to understand each vendor's roadmap in the area of application awareness and were disappointed to learn that while the existing incumbents saw the lack of application awareness as a gap in their offerings, they weren't focused on filling this requirement. The incumbents were looking at firewalls that provided some form of application awareness as a bolt-on, and their solutions and roadmaps were not very impressive.

Palo Alto Networks was selected for its differentiated capabilities.

Because this company has relationships with the existing firewall suppliers, it was preferable and would have been easier to use one of their solutions. However,

these companies simply didn't have next-generation capabilities focused on application identification and they had no immediate plans to develop them.

In contrast, Palo Alto Networks shared the same vision of the firewall, and had the exact solution that this company envisioned.

As the company's senior security leader pointed out:

> *"We don't just jump to buy new products from new vendors. We put vendors through the wringer."*

"From a differentiated capability perspective, Palo Alto Networks blows people away. It provides great contextual threat analysis."

The company developed multiple use cases for what it wanted its next-generation firewall to do and then evaluated Palo Alto Networks' solution in the lab for almost a full year. As a result of this thorough evaluation, they concluded that Palo Alto Networks' solution was the primary solution on the market focused specifically on enabling the company to proceed with its application-aware strategy.

The next step: developing a compelling business case.

The security team at this company developed a short-term and a long-term strategy for application awareness.

- **Short-term strategy**. Because the name of the game today is short-term cost savings, pursuing application awareness had to demonstrate immediate cost savings and a 12-month return on investment.

  "We needed short-term ROI and then long term we see it [Palo Alto Networks] replacing several capabilities, making it a big win."

  The information security group identified four important capabilities that could be consolidated onto one platform (that of Palo Alto Networks) in order to save on hardware, software, and maintenance. The capabilities that could be consolidated were:
  - *IM filtering and protection*.
  - *URL filtering*.
  - *IDS/IPS*.
  - *Replacement of traditional firewalls*.

  Products to address all four of these capabilities were already deployed on this company's network. The business case that was developed was to show savings by using Palo Alto Networks to initially replace just one of these existing capabilities. That would provide the rationale to bring Palo Alto Networks in and deploy it.

- **Long-term strategy.** While Palo Alto Networks had been deployed to replace one capability, this company's longer-term plan is to consolidate and replace other capabilities. This will provide greater security awareness, improve control, and offers a very compelling business case.

Multiple benefits have been seen since implementing Palo Alto Networks.

These benefits include:

- **Increased visibility**. Palo Alto Networks' next-generation firewall provides a dashboard which gives this company a snapshot of what is happening with

"Even if Palo Alto Networks provide no protection advantages [which is does], the visibility and application awareness alone would have been worth it."

the company's top 500 applications. (This includes applications such as Web browsing and AOL instant messaging, along with HR, finance, and project management applications.)

The company can see which applications are being used and can monitor the Internet traffic associated with each application. They can look at what activity is taking place for an application globally or regionally.

One example of improved visibility involved learning that a popular application (SalesForce.com) was being used in the company even more broadly than had been previously realized. Use of Palo Alto Networks helped the company understand the enterprise-wide usage of the application and map its appropriate use from other areas where it was not authorized.

Part of the reason the visibility is so good is due to Palo Alto Networks' excellent reporting capabilities.

- **Context-based protection.** Palo Alto Networks provides enhanced security because protection doesn't start by looking at the threat; security starts by "looking at the application first."

  Unlike most IDS/IPS solutions, Palo Alto Networks knows which signatures apply to which applications. The solution identifies the application first and then matches the appropriate signatures to the appropriate applications. Users can create and enforce much more granular protection policies.

"Application identity and awareness provides context-based protection. . . . It looks at the application first."

- **Increased management capabilities**. Palo Alto Networks provides strengthened management capabilities. In particular, Palo Alto networks enables user identification per application session within the firewall, something that other vendors can't do.

In addition to these core benefits, Palo Alto Networks' user interface is simple and easy, and the company's level of support has been outstanding. The support provided during the evaluation phase was great, but that level of support has been sustained even after the solution was deployed.

> *"Whenever we call, we get a human within four rings."*

Palo Alto Networks has been responsive to comments and feedback, and is working diligently to further improve its solution. For example, this company recognizes that Palo Alto Networks has a true next generation product and the company is focused on next generation threats, but still, this user has identified a few small areas where some added functionality would be beneficial. They are confident that Palo Alto Networks will respond to these comments and get there soon.

Advice to organizations considering next-generation firewalls.

Based on this company's experience, organizations should consider the following questions:

- *Are your applications at risk?* It is hard to imagine enterprises that don't see their applications at risk.
- *What is the source of the threats faced?* The threat landscape has changed

and threats and risks are now related to applications.

- *Do you need application-aware firewalls?* For this company the answer was a definitive "yes." Many other enterprises are likely to feel similarly.
- *How effective are your current tools/solutions?* This company's experience was that traditional firewalls don't provide the level of application awareness and contextual security that is needed. Incumbent firewalls aren't able to deliver NGFW capabilities, even when application-aware bolt-on capabilities are deployed.

"The standard tools don't address threats to applications."

- *Have you explored Palo Alto Networks?* This company didn't set out to learn about Palo Alto Networks. They wanted a next-generation, application-aware firewall—and Palo Alto Networks had the best product. In their experience, the technology has more than delivered on their expectations. The visibility and customer support are important added bonuses.

About Palo Alto Networks

Palo Alto Networks™ (paloaltonetworks.com) is the leader in next-generation firewalls, enabling unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 10Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. Enterprises can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation.

About IANS

IANS is the premier membership organization for practicing information security professionals. IANS' mission is to provide key technical and business insights to help members solve their most pressing technical and professional challenges.

IANS 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.

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