Reducing Costs With Next Generation Firewalls

Investing in Innovation Pays Cost Savings Dividends

December 2008

Palo Alto Networks
232 E. Java Dr.
Sunnyvale, CA 94089
408.738.7700
www.paloaltonetworks.com

Table of Contents

Executive Summary

For enterprise IT security organizations, the evolution of applications and threats, coupled with the stagnation of traditional network security technology has resulted in a loss of visibility and control. Despite efforts to regain visibility and control by adding more security appliances, most organizations remain stymied – unacceptably. In today's economic climate, however, any further increase in cost and complexity is similarly unacceptable. Some leading enterprises, however, have found that investing in innovation, and bucking the trend of seemingly never-ending appliance sprawl in network security can result in the restoration of visibility and control, and substantial reduction in cost of ownership of security infrastructure. This paper examines three different organizations, the legacy infrastructure they replaced, the Palo Alto Networks next generation firewalls they deployed, and the substantial savings they realized – cutting both capital and operations costs by an average of 50%.

IT Security: Regain Visibility and Control While Reducing Costs

Contemporary IT security organizations face a host of challenges - some of them understood (rapidly evolving threats, organizational issues, compliance), and others brand new (rapidly evolving applications, employee cultural changes, and the current economic climate). More than ever, it is incumbent on IT security to address two seemingly conflicting mandates:

- Regain visibility and control of enterprise networks in the face of evasive applications and threats
- Given the economic climate – reduce costs

While on first blush, these requirements seem to pull organizations in different directions; this paper will demonstrate how organizations can, by investing in innovation, meet these requirements with a common initiative.

Legacy Firewalls are Ineffective in Today's Application and Threat Landscape

To comply with most regulations, business covenants, and auditor findings, most organizations have to understand and control the applications, user behavior, and content on the enterprise network. Unfortunately, modern applications, users, and content have evolved beyond the legacy set of network-based security infrastructure – and can easily circumvent most firewalls and other port- and IP address-based network security devices. Using encryption, proxies, port-hopping, or other evasive techniques, or tunneling over ports 80 or 443, most applications and threats easily knife through enterprise network security defenses. With over 2/3 of enterprise Internet traffic moving over port 80, it has become clear to most enterprise information security professionals that the old mapping of applications to ports is no longer relevant. Thus making the firewall largely useless, despite the firewall's position in the network and its long history of ubiquitous adoption.

Firewall "Helpers" Lead to Complex and Costly Appliance Sprawl

To the chagrin of many IT professionals, the industry's traditional response to new applications and threats has been to add more appliances – each "helping" the firewall with a piece of the network security function. This unsustainable approach has long proven complex and costly, and now appears to be broken – since these firewall helpers either can't see all of the traffic, rely on the same port- and protocol-based traffic classification that has failed the legacy firewall, or proxy a very limited number of applications (a dozen instead of hundreds or thousands). Given that enterprises had little choice, most have adopted an array of firewall helpers – resulting in a network security infrastructure that is expensive, difficult to manage, and increasingly ineffective at controlling application or the threats that applications might carry – characteristics proving unacceptable to enterprises today.

Bleak Financial Climate Means That IT Must Reduce Costs

In today's economical environment, many IT groups are struggling to fund operations. Budgetary pressures are extreme, cost-saving mandates are commonplace, and green IT initiatives continue. Given this climate, IT security staffs must innovate or risk obsolescence – incremental changes to ineffective infrastructure can't solve these issues.

Incrementalism Isn't The Answer – Its Time to Fix the Firewall

The firewall is the network security foundation for nearly every enterprise – with good reason: the firewall is in-line, sees all traffic, and thus is in a unique position to enforce control. It also demarcates the trust boundary. The problem, as stated above, is that legacy

firewall implementations are not effective in today's application and threat environment, and "helpers" don't help. Next generation firewalls from Palo Alto Networks fix the firewall, enabling enterprises to regain visibility and control over the applications, users, and content on their networks – and greatly reduce the number of security appliances that they have to maintain.

Investing in Innovation and Reducing Costs With Palo Alto Networks

By "fixing the firewall," with Palo Alto Networks next generation firewalls, organizations can regain the visibility and control that they have been lacking, and cut down on the expensive and complex security appliance sprawl they've been forced into over the last decade. Cost savings come in two major areas: capital expenditures, and operational expenses.

Capital Expenditures: Next Generation Firewalls Enable Consolidation

Capital expenditures are relatively well understood – one device is typically cheaper than three. The issue when modeling security device consolidation is the timing of those purchases. Very few enterprises decommission multiple types of devices across the enterprise at the same time. The scope and size of these costs, however, even being mindful of phased purchases and depreciation schedules, merit serious consideration – since by consolidating security devices utilizing the budget for one type of device might obviate the need for an additional purchase in the future. The traditional issue with consolidation – performance – isn't an issue with Palo Alto Networks next generation firewalls, because of their purpose-built design (see the Appendix for more detail on consolidation and performance).

Operational Expenses: Reduce Support and Subscriptions with Palo Alto Networks

Looking at "hard" operational expenses, there are 3 or 4 major categories: support/maintenance contracts, URL filtering subscriptions, threat prevention/IPS subscriptions (in not captured in IPS device maintenance/support), and power/HVAC. There are other "soft" operations costs that can be significant in a case for consolidation – IT staff productivity, end user productivity, help desk calls, training, vendor management – but for maximum credibility, these costs are often better characterized rather than counted. Rack space is a potential exception, as some organizations have done enough analysis and can characterize all of their data center costs per unit of rack space (real estate, power, cooling, management, etc.).

Operational Expenses: Device Consolidation Helps Green IT and Power Consumption

Regarding power and data center HVAC, many organizations have "green" efforts, attempting to reduce energy use and the amount of waste they generate. Given the amount of energy used by a typical data center, IT is often called upon to reduce the amount of power consumed by IT infrastructure and data center cooling. Effectively consolidating security devices can offer substantial energy savings – both directly (i.e., the power consumed by the security device) and indirectly (i.e., the power consumed by the data center cooling system to cool the device). A good rule of thumb is a watt of power consumed is a watt of power needed for cooling. Furthermore, fewer devices means less waste – combined with reduced energy use, makes a compelling "green" argument for effective security device consolidation.

Customer Examples Show Savings

Perhaps the best way to understand potential savings is by looking at a few examples. Here are three real-world examples – a very large organization, a medium-sized organization, and a smaller organization – their issues, expenses, and how – using Palo Alto Networks next generation firewalls – they were able to regain visibility and control of their networks, while significantly reducing complexity and costs.

Customer Example #1: Large Financial Services Organization

Saving $331K/year with Palo Alto Networks: Using Palo Alto Networks, a large ($100 billion+ annual revenue), multinational financial services organization is undergoing an enterprise network security device consolidation project – and will save $331K/year in network security operations costs – at one location.

Legacy Deployment – Lots of Sprawl: Examining the legacy deployment at that location (mid-Atlantic, US, serving 5000 users), the IT organization maintained Cisco firewalls, Sourcefire IPS appliances, Secure Computing Webwasher appliances, and Blue Coat proxy appliances. The sheer number of security appliances dictates significant additional infrastructure just to accommodate their connectivity – including a dedicated switch and a pair of F5 Local Traffic Managers.

Palo Alto Networks – Greener and Faster: Given the state of the financial industry, operational cost reductions are welcome. Furthermore, "going green" has a significant value for many organizations (including this one), both internally and externally. In just one data center, this customer is showing a reduction in power and HVAC costs of nearly $40K annually – a savings of 90%. Palo Alto Networks could show substantial functional consolidation (firewall, URL filtering, threat prevention), and could also reduce the overall number of firewalls due to the PA-4000 Series' superior performance and increased port density. Furthermore, the PA-4000 Series' application visibility and control gave the IT organization the tools they needed to better manage application use on their network – safely enabling desirable applications, while preventing the use of undesirable applications.

Large Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$2,424,940.00	$480,000.00	**$1,944,940.00**
Annual Operations Costs			
Support Contracts	$424,785.60	$76,800.00	
URL Filtering	$40,000.00	$48,000.00	
Threat Prevention	n/a	$48,000.00	
Power/HVAC	$44,106.30	$4,403.20	
	---	---	
Total Annual Ops Costs	$508,891.90	$177,203.20	**$331,688.70**
Legacy Equipment:		Palo Alto Networks equipment:	
Firewall: 12x Cisco ASA 5580 (previously planned refresh), IPS: 2x Sourcefire 3D9800, URL filtering/proxy: 6x Secure Computing Webwasher 1900E + 5x Blue Coat ProxySG 8100, Traffic management: 2x F5 6800 Local Traffic Manager		10x PA-4050	

Customer Example #2: Global Manufacturer

Saving $147K Per Location in Capital Costs With Palo Alto Networks: With Palo Alto Networks next generation firewalls, this 30-site, $1B global manufacturer has reduced its annual remote site network security operations costs by 40%.

Legacy Standard Security Infrastructure Was Expensive: This customer's standard security rack at each location included Cisco PIX firewalls, Tipping Point IPS, and a Microsoft ISA Server running on Dell hardware. The expenses surrounding the customization and upkeep of the ISA Server coupled with the Cisco PIX end-of life announcement prompted the IT group to look to Palo Alto Networks to simplify the security infrastructure – and in doing so, give control of the network back to the IT group.

Palo Alto Networks is the New Standard: The visibility, control, and cost savings were significant enough that the organization quickly deployed across 3 sites, and declared Palo Alto Networks next generation firewalls as the standard deployment for all sites going forward. Looking at just the 3 deployed sites, the IT group was able to show a reduction in capital costs of over $147,000. Similarly, across the 3 deployed locations, the IT group was able to show annual savings of nearly $24,000. Once deployed across the remaining 27 sites, this will represent an enormous annual cost reduction.

Medium-sized Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$243,555.00	$96,000.00	**$147,555.00**
Annual Operations Costs			
Support Contracts	$38,968.80	$15,360.00	
URL Filtering	$15,000.00	$9,600.00	
Threat Prevention	n/a	$9,600.00	
Power/HVAC	$6,489.22	$1981.44	
	---	---	
Total Annual Ops Costs	$60,458.02	$36,541.44	**$23,916.58**
Legacy Equipment – for each of 3 locations:		Palo Alto Networks Equipment – for each of 3 locations:	
Firewall: 2x Cisco PIX 525, IPS: 1x TippingPoint 600E, URL filtering/proxy: 1x Dell 2950 and Microsoft ISA Server – Enterprise		2x PA-2050	

Customer Example #3: City Government and Schools

Cut Operational Expenses by 64%: The last example is a smaller organization, a city government and school system on the East Coast of the United States, who was able to show operations cost reduction of 64%.

Legacy Infrastructure Couldn't Perform: This organization was using Watchguard firewall/UTM devices and St. Bernard iPrism filtering appliances. Unfortunately, the city employees and school staff and students were able to use less than 10% of their Internet bandwidth due to the poor performance of their security infrastructure. Additionally, the fees associated with URL filtering and maintenance subscriptions were very high. Finally, and most importantly, students and staff easily bypassed these network security controls using proxies, encrypted applications (like Skype), and tunneling applications like UltraSurf and TOR.

Palo Alto Networks Restores Visibility, Control, and Performance: Replacing the end-of-life and poorly performing Watchguard and St. Bernard infrastructure saved the city thousands of dollars per year. The IT staff was able to present a compelling case for the PA-2050 next generation firewall – showing a capital cost savings of nearly $7000 over replacing the $20,000 legacy infrastructure. Perhaps more importantly, by consolidating existing functions, and adding the application visibility and control that the city needed, IT staff was able to reduce network security operations costs from over $25,000 to just $9,200 per year – a savings of over $16,000/year. Functionally, the city was able to see and control

evasive applications, comply with federal and state regulations regarding school technology use, and safely enable a wide variety of Internet applications for staff.

Small Organization	Legacy	Palo Alto Networks	Savings
Capital Costs	$22,957.00	$16,000.00	**$6,957.00**
Annual Operations Costs			
Support Contracts	$3,673.12	$2,560.00	
URL Filtering	$20,000	$3,200.00	
Threat Prevention	n/a	$3,200.00	
Power/HVAC	$2,008.96	$330.24	
	---	---	
Total Annual Ops Costs	$25,682.28	$9,290.24	**$16,391.84**
Legacy Equipment:		Palo Alto Networks Equipment:	
Firewall/UTM: Watchguard Firebox x8500e-F, URL filtering – St. Bernard iPrism 50h (M11000)		1x PA-2050	

Investing in Innovation With Palo Alto Networks Saves Money

In all three cases, the savings in both capital costs and operations costs were substantial. On average, the three organizations examined in this paper reduced their capital budgets by more than 50%, and cut their annual operations costs by a similar number. Granted, there are differences across these examples, but many Palo Alto Networks customers can easily demonstrate a rapid return on their investment – covering the upfront cost of the solution with the reduction in operations costs in the first year. Regaining control of the applications, users, and content on the network was of equal importance to the IT staffs in the enterprise customers examined in this paper, but demonstrating the cost advantages enabled these projects to move forward quickly – even in a tough economic climate. In brief summary:

- **Save 30%-80% in Capital Expenditures.** In all three examples, reducing the number of security appliances resulted in substantial reduction of capital expenditures – from 30% in our "small" example (we only replaced 2 boxes), to 80% in our "large" example.
- **Save 40%-65% in Operational Expenses.** In all three examples, hard operations costs went down significantly – what organizations spent on support/maintenance contracts, URL filtering subscriptions, and power was reduced: from 40% in our "medium" example to 65% in our "large" example.
- **Save on "Soft" Costs Too.** We didn't attempt to quantify "soft" costs, which, while significant, are difficult to quantify and often undermine the impact of a cost analysis. In our examples, the medium and small organizations reported substantial soft costs savings. For the manufacturer, deployment and integration efforts were greatly reduced, resulting in demonstrable savings. In our small example, the customer cited a reduction in the time it took to find and resolve security problems – often before they resulted in a help desk call, for which they could easily demonstrate savings.

The bottom line for many organizations is that while they have security and compliance needs that must be met, very few projects that don't demonstrate significant cost savings will move forward in today's economic climate. For Palo Alto Networks customers, investing in innovation with next generation firewalls has helped them regain visibility and control, and has enabled substantial cost savings – a rare combination of benefits that has resulted in increased stature within their organizations.

Appendix: Reduce Cost, but Maintain Enterprise Performance

As previously mentioned, most enterprises today have a network security infrastructure that is less and less effective. This ineffectiveness, coupled with the spiraling costs of maintaining this array of security devices, has pushed many organizations to attempt security device consolidation. Unfortunately, most enterprise network security device consolidation efforts backfire – poor performance of consolidated devices quickly forces IT security teams to turn off security functions to enable business traffic to flow. This is often because typical unified threat management devices are built by grafting various acquired and open source security functions onto a legacy port-based firewall running on PC-based hardware. As an aside, UTM devices still don't offer additional visibility and control beyond the usual port/protocol/IP address-based control of legacy infrastructure – just consolidated hardware.

Palo Alto Networks' next generation firewalls can consolidate many of the existing security functions, and enables IT organizations to regain visibility and control as mentioned previously. The PA-4000 and PA-2000 Series platforms can deliver all of these functions with enterprise performance – because they've been designed from the ground up to do so. In building a next generation firewall that focuses on applications, users, and content, Palo Alto Networks had to start with a clean sheet of paper. This enabled the designers of the PA-4000 and PA-2000 Series firewalls to solve many of the problems associated with previous device consolidation attempts.

First, Palo Alto Networks addressed hardware – using principles commonly employed when designing networking devices. Separation of data and control planes means that heavy utilization of one doesn't negatively impact the other. The control plane has it's own CPU, RAM, and disk. Additionally, dedicated, specialized processing and memory for networking, security, and content analysis – all connected via a high-speed data plane (10Gb on the PA-4000 Series, 1Gb on the PA-2000 Series) means that traffic won't bog down. Figure 1 depicts the PA-4000 Series hardware architecture.

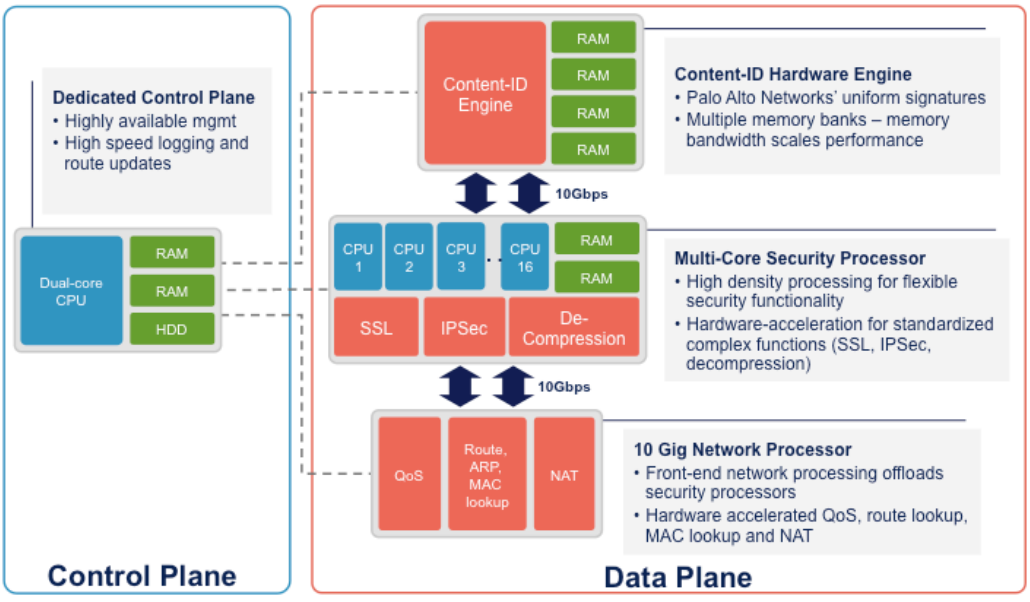

Figure 1 - PA-4000 Series Hardware Architecture

Second, Palo Alto Networks engineers addressed the path that traffic takes through the security infrastructure. In legacy network security infrastructure, traffic flows through several security devices, each with it's own networking engine, classification engine, pattern matching engine, and policy engine (see Figure 2). This duplication of effort is not only inefficient, but slow. Even with UTM devices, there is often a great deal of redundancy.

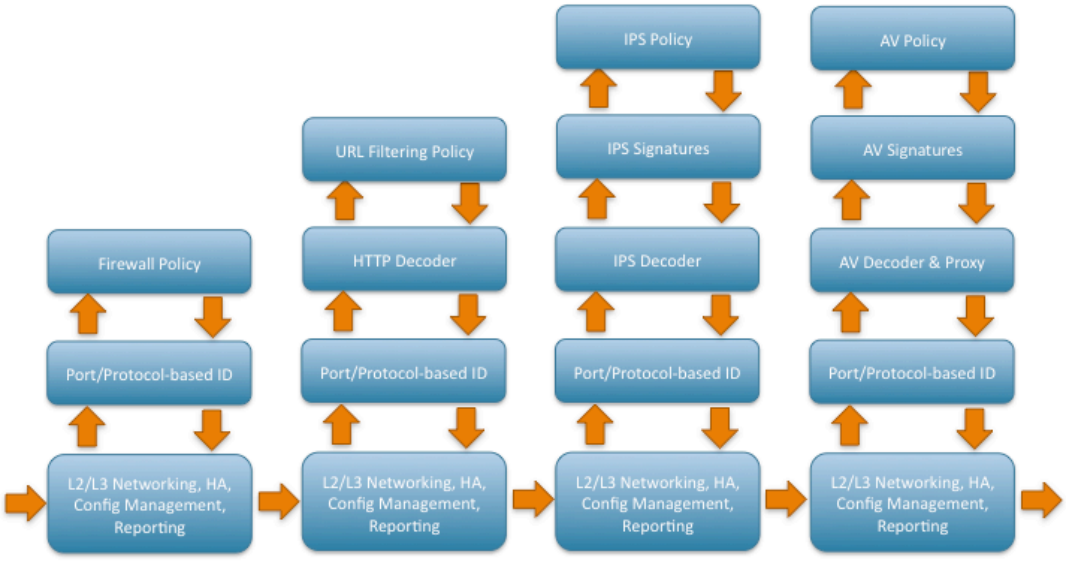

Figure 2 - Legacy Multi-Pass Architectures

Palo Alto Networks next-generation firewalls utilize a single pass architecture, with traffic flowing through a single networking component, a single application classification engine, a user classification capability, and a single content/pattern matching engine – resulting in the ability to see and enforce policy control across applications, users, and content (including threats) – without slowing traffic. Figure 3 is a graphical representation of Palo Alto Networks' single pass architecture.

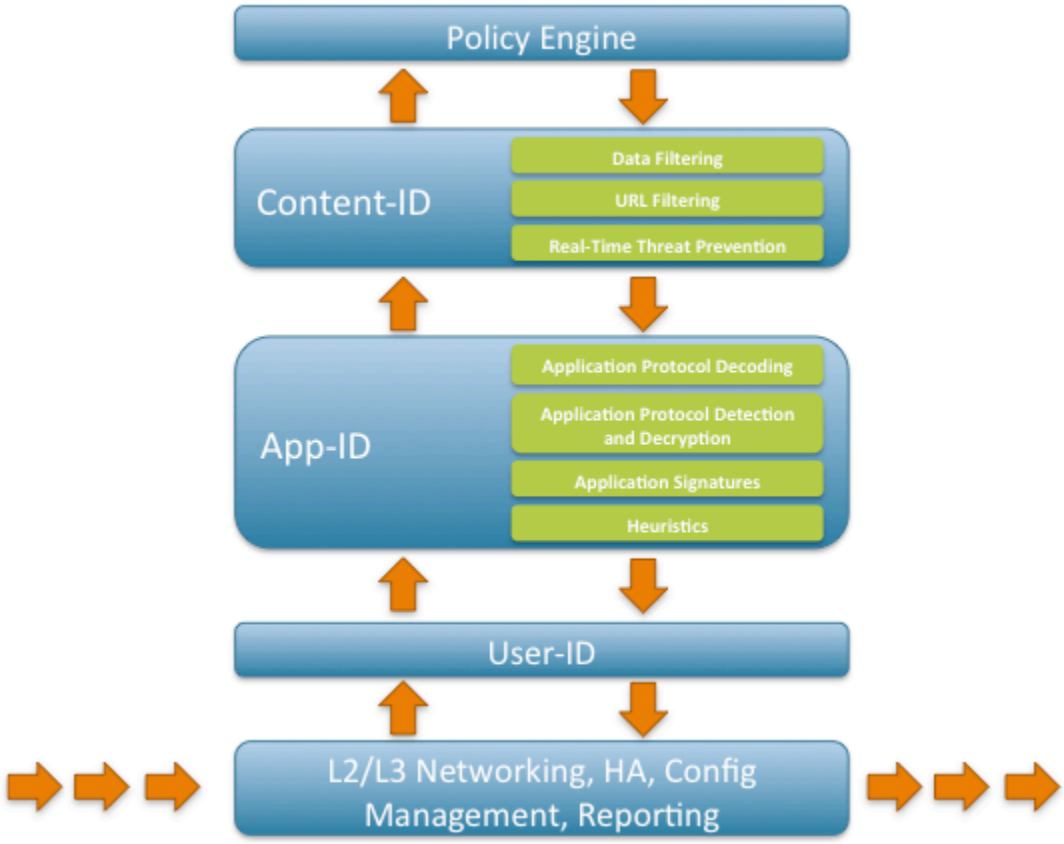

Figure 3 - Palo Alto Networks Single Pass Architecture