It’s Time to Fix the Firewall

Seriously, it is.

Find out why, and what you can do about it.

paloalto NETWORKS

A Summary for Skeptical Readers

OK, if you don't read anything else, read this!

In a nutshell, here's the essence of this little document: Traditional port-blocking firewalls have not changed much in 15 years and are no longer effective in protecting the perimeter of your corporate network. That's because they were never designed to control all of the evasive, port-hopping, or encrypted Internet applications, content, and threats that are so common in today's networks. You've tried to compensate for their deficiencies by adding a bunch of other stuff, like intrusion prevention systems, proxies, AV systems, URL filtering, and much more. But you know that "adding more stuff" is not a security solution.

It's time to fix the firewall!

So if you manage firewalls, or care about the value they should deliver to your organization, take 10 minutes to review this. Most of the content helps you understand how we got to where we are today – it's a much bigger issue than just firewalls! You'll see some interesting research data along the way. And yes, there is some information toward the end on Palo Alto Networks next generation firewalls, but it's mostly links you can choose to ignore if you prefer.

Bottom line: The firewall should be the most important security device in your network. But if it's not delivering the value and performance you want and need, that's a problem and it will only get worse. So as you consider your security strategy moving forward, you owe it to yourself and your organization to be well informed as you consider the options before you.

Palo Alto Networks has helped hundreds of organizations worldwide restore visibility and control of their corporate networks. We can help you fix your firewall too.

Introduction

About a year ago, a sales representative from Palo Alto Networks was giving a product demo to a group of IT people from a large, very well-known company based in the northeast US. The IT team leader was skeptical and somewhat reluctant to consider a serious evaluation of a next generation firewall from Palo Alto Networks.

But one of the guys on his team (we'll call him Joe) listened carefully to the presentation, watched the demo, and saw the possibilities. Joe convinced his boss to support a 30-day evaluation. During that time, the team performed exhaustive testing and the firewall worked flawlessly. Still, the IT leader was not convinced and suggested they play it safe and select a product from one of the traditional firewall vendors.

But Joe would not be denied. He was the guy responsible for managing the firewalls, and he knew Palo Alto Networks next generation firewalls were unlike anything he had ever seen. So Joe lobbied hard and finally convinced his boss to invest in Palo Alto Networks. The installation went smoothly, the products delivered value beyond expectations, and Joe got promoted within 30 days.

True story! Just one of many great stories we've heard from our customers.

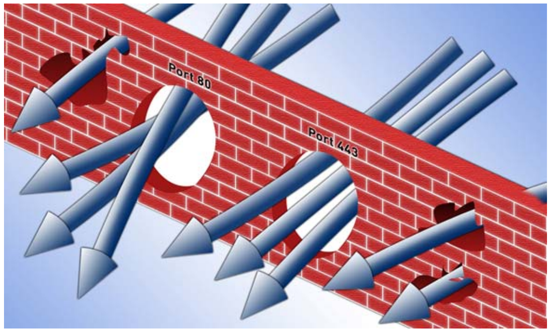
So now we want to explain why you should be like “Joe the Firewall Guy”!

Let's get started.

Whatever Happened to The Firewall?

Have you noticed that nobody gets excited about a firewall anymore? It's kind of sad in a way. There was a time when it was the most strategically important security device in your network. Now it's more like one of your old uncles, stuck in the 70's and ignored at family reunions. OK, maybe that's a bad analogy, but the point is that the traditional firewall is slightly out of step with the times. But why is that?

The answer is a bit of a cliché, but… the Internet has changed everything. You see, 10-15 years ago most firewalls did a pretty good job controlling traffic in and out of corporate networks. That's because application traffic was generally well behaved. Email would typically flow through port 25, FTP was assigned to port 20, and the whole "web surfing" thing funneled through port 80. Everybody played by the rules that "ports + protocols = applications" and the firewall had everything under control. Blocking a port meant blocking an application. Nice and simple.



Unfortunately the Internet didn't stay nice and simple. Today the Internet often accounts for 70% or more of the traffic on your corporate network. And it's not just port 80 web surfing. Typically 20-30% of it is encrypted SSL traffic on port 443. Even worse, there is a plethora of new Internet applications that insist of making their own rules. They wrap themselves in other protocols, sneak through ports that don't belong to them, and bury themselves inside SSL tunnels. In short, they just don't play fair.

All these applications carry some inherent risk to your business. And they play host to clever new threats that can slip through your firewall undetected. Meanwhile, your firewall just sits there like nothing is wrong because it's still playing by rules that don't exist anymore!

When Worlds Collide

Just to be clear, we're not suggesting all Internet applications are bad. On the contrary, the Internet is a vitally important extension of today's corporate networks. The outsourced cloud computing model is increasingly being used to support business processes and growth. But there is also an endless stream of consumer and recreational applications that employees are bringing into your network – even while you're reading this! You know some of them – P2P, IM, Social Networking, Video, and Gaming. But there are many more you've never heard of – including apps that allow them to get around your Internet security controls – like UltraSurf, Zelune, and Anonymizer – and your port-blocking firewall (or IPS!) can't stop them!

There's a simple reason why this is happening. Your network users are becoming more Internet-savvy every day. Not surprising, since the Internet is an integral part of their personal and professional life. But now their two worlds are colliding! So when they come to work, they're not asking for help or permission to access whatever they want on the Internet for business or personal use. It's no wonder that Internet traffic dominates your corporate network.

Not convinced? Check out this recently published report on the actual network traffic in more than 60 large enterprises representing 960,000 users. We discovered that these organizations were running a total of 424 different Internet applications on their networks! Some were legitimate business applications, many were non-essential consumer applications, and all of them carried some level of risk to their businesses. Unfortunately, none of these applications were identified by the existing port-blocking firewalls in those organizations! Again, that's because the rules have changed: ports + protocols no longer = applications.

The Risk of Not Doing Anything

Let's talk about application risks for a moment. As noted earlier, Internet applications are becoming a threat vector for a new generation of spyware, viruses, and other malware (see report for more details). Many of these applications use evasive tactics to escape detection, including hiding in your encrypted SSL tunnels. Sorry to pick on the port-blocking firewall again, but it is totally blind to encrypted content. The best it can do is tell you that traffic is coming through port 443 – assumed to be SSL, but it can't tell you for sure. Not particularly helpful in stopping an attack!

But if that's not worrisome enough, there's also another side of application risk to consider. That is, the risk of sensitive information leaving the network as a result of uncontrolled applications. For example:

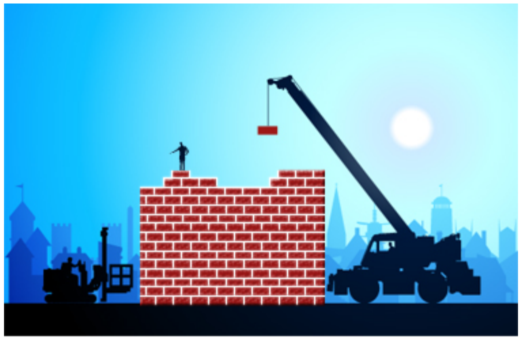
- Credit card and social security numbers contained in various files
- Confidential information sent through Webmail accounts like Gmail
- Lost information when you give up desktop control through applications like WebEx

These are just a few examples. The truth is that most applications – good and bad – carry some level of risk that can result in loss of confidential information. A recent report by the Ponemon Group surveyed users across 193 organizations and found that 33% of them have already experienced this problem from using Internet applications. Even more shocking, about 45% of these users kept using the same applications – no change in their behavior!

Admittedly, this all sounds a bit discouraging – so many apps and so many risks, yet so little visibility and so little control. But don't despair – keep reading! There is a way to regain the control you've lost!

It’s Time to Fix the Firewall

Let’s be honest. Old port-blocking firewalls really don’t provide any value anymore – not in a world where network boundaries are disintegrating and Internet applications are exploding. But you already know that. Which is why you’ve been forced to make up for their glaring deficiencies with more specialized appliances - intrusion prevention systems, proxies, anti-virus, anti-spyware, URL filtering, yada, yada, yada. Sure, these tools add some incremental value, but it’s getting harder to justify their additional cost and complexity – especially during challenging economic times.



The CISO from Cigna, recently referred to his growing stack of security products as the “leaning tower of Pisa”! Clearly, it’s a strategy that does not scale. More important, however, none of these additional products give you the visibility and control you need over the applications running on your network. So now what do you do?

It’s time to address the core problem. It‘s time to fix the firewall!

Makes sense, doesn’t it? After all, the firewall sits at the most critically important place in the network, and really should be that centralized point of visibility and control over everything entering and leaving the network. Of course, you may have long ago given up on that dream – and we don’t blame you. The complete lack of firewall innovation has left a bad taste in everyone’s mouth.

But, before you give up on the possibility of an effective firewall, you owe it to yourself to take a closer look at something completely different. A firewall for the next generation, but available now. Joe the Firewall Guy saw the possibilities, took a chance, and he got promoted! OK, we can’t guarantee a promotion, but we can – and did – fix the firewall!

The Next Generation is Here

Palo Alto Networks created a next generation firewall by starting with a clean sheet of paper. . We began by identifying 5 critically important IT requirements:

1. Visibility into all applications, regardless of port, protocol, evasive tactic – or even SSL encryption
2. Identification of application users by name – not just by IP address
3. Granular control of application access, by user or groups of users
4. Real-time threat prevention, content control, and URL filtering
5. In-line throughput up to 10 Gbps, with no performance degradation

We then we built a family of firewalls that combine innovative new identification technologies, such as App-ID, User-ID, and Content-ID, all leveraging an underlying Single-Pass Parallel Processing Architecture (SP3), which ensures maximum throughput with minimum latency.

First introduced in 2007, just a year later these firewalls won the Interop 2008 Best of Show Grand Prize, and were named one of the 10 most influential biztech products of 2008. Today, Palo Alto Networks firewalls are empowering hundreds of IT organizations worldwide to address some critical priorities of their own:

- See and control applications on the network – good, bad, and evasive – by user
- Protect gateways and data centers with high performance firewall and IPS capabilities
- Consolidate security devices to reduce complexity, and save CapEx and OpEx costs
- Simplify PCI compliance through intelligent network segmentation by application and user
- Stop leakage of confidential data (social security and credit card numbers) at the firewall
- Block bad applications; scan permissible applications in real time for all types of threats

Is Any of This Really True?

Be honest, that's what you're thinking, aren't you? It's OK, we understand. It's clear by now that the firewall is the last place you'd expect to find any innovation. And then along comes Palo Alto Networks claiming to have fixed the firewall. You have a right to be skeptical!

So, to be fair, we asked some of our customers to say a few words. No script. We asked them to say whatever they want in about 60 seconds or less. Here are three examples:

Sinclair Community College
With 24,000 students and a big focus on online curriculum, the network plays a big role at this Ohio college. Watch Chad Rumbarger talk about the visibility and control he now has with Palo Alto Networks.

Nordson Corporation
This global manufacturing company has more than 4,000 employees in 32 countries around the world, so simplifying IT cost and complexity is an important requirement. George Morse shares his perspectives.

ThedaCare
A large healthcare organization in Wisconsin, Thedare has 5,000+ employees across 14 locations. For this customer, our threat mitigation and IPS capabilities made them believers. Listen to what Rick Rohde has to say.

As you can tell, these guys shot their videos themselves. Maybe not Oscar-worthy, but we think they made their points very clearly. So now the question is, are you ready to start "livin' the dream"?

What to Do Next

OK, if you've stayed with us this far, we think you may be serious about knocking down your own personal "tower of Pisa" and putting that old port-blocking firewall to rest. If that's true, here are a three suggested next steps:

1. **I didn't read this e-book, but want to learn more** – Hey, no worries. We live in a sound bite world. Tell you what, watch this 3-minute video (click on the red brick wall) and you'll get the basic idea of everything we've discussed here. Then you can go to step 2.

2. **Sounds great, but I need more product details** – OK, no problem. Grab a cup of coffee, a fat-free muffin, and watch this great demo by Lee Klarich, VP of product management for Palo Alto Networks. Mind you, this is 28 minutes long, but it will give you a great introduction to the real power of our next generation firewalls.

3. **Details, shmetails, I'm ready for an eval unit!** – Hmm, aggressive, we like that! OK, just give us some basic info on this form and we'll follow up with you faster than you can find all the false positives from your IPS.

Or, if you just feel like a basic phone conversation, you can always call us at 1-408-738-7700.

Thanks for your interest in Palo Alto Networks. We hope you'll join the growing number of IT organizations worldwide who are now "livin' the dream" with next generation firewalls.