Moving Network Security from Black and White to Color

Refocusing on Safely Enabling Applications

July 2009

Palo Alto Networks
232 E. Java Drive
Sunnyvale, CA 94089
408-738-7700
www.paloaltonetworks.com

Table of Contents

Less About Threats, More About Safely Enabling Applications

The old model of security was simple – there was good traffic (business application traffic) and bad traffic (threats). Network security was a simple affair – stop the threats, allow application traffic. Black and white.

But the landscape is now different – the number, types, and nature of applications have changed tremendously. Many applications are hosted outside the enterprise –enterprise users employ a mix of business-focused and consumer-focused applications for a variety of business and personal reasons. All of these applications carry risk (some carry threats), but also, in most cases, these applications have substantial benefits. Accordingly, simply blocking, or allowing these applications does harm to the business – either by slowing business down, or by taking on too much risk. Network and information security professionals need to shift their focus from treating applications as threats, to working towards the safe enablement of applications. It's time to add some sophistication to our thinking about network security. But what kind of sophistication? And how to incorporate without adding expensive complexity? Here's what organizations need to do:

1. See what applications are running on the enterprise network
2. Decide which applications are desirable from a risk/benefit perspective
3. Exert fine-grained control over application traffic – allow the beneficial applications for the right users, disallow risky applications or functions, and mitigate the risk associated with beneficial, high-risk applications

Doing this requires some changes – a shift in policy, and some additional requirements for the network security infrastructure. Palo Alto Networks next-generation firewalls enable both – first by offering enterprises unprecedented visibility into which applications are running on their networks, and second by enabling fine-grained control over those applications – well beyond simple allow or block enforcement.

Many Types of Applications…

But let's step back – from a business perspective, there are three classes of applications:

- Corporate productivity applications automate a business process
- Personal productivity applications make individual users more productive
- "Lifestyle" or consumer-oriented applications enable users to maintain their online life

Many examples of all of the above types are hosted outside the enterprise, and as stated above, all of which carry risk. Some of these applications have business value, some do not, and some are outright harmful to the enterprise. So many of these applications might be desirable for different reasons. Corporate and personal productivity applications have a well-established place in the workplace (although often, IT is not aware of the number and variety of applications in use for personal productivity). Even reasonable use of some lifestyle applications is often allowed, for cultural reasons. All of these types of applications, however, carry risk. They transfer files, consume bandwidth, carry malware, tunnel other applications, have vulnerabilities associated with them, are prone to misuse, and/or are evasive. These application behaviors impact serious business issues, including compliance, operations costs, data loss, business continuity, and productivity.

Accordingly, organizations need to weigh risk/benefit for applications. Given that most organizations want the benefit of all of these applications, but don't want to carry undue risk, IT security organizations must safely enable use by allowing the application, but somehow mitigating the risk associated with the application.

…Dictate a Variety of Responses

Because applications aren't threats, the new set of responses to application traffic should include:

- Deny
- Allow
- Limit (by user, group, time of day, or application function)
- Scan
- Shape

Deny and allow are well understood as policy actions. They are the basis for the old model of security (the black and white, to use the picture analog above). Organizations will deny known undesirable applications (e.g., peer-to-peer file sharing applications). Or allow known approved applications (with some conditions, as noted below. Obviously, deny and allow have a place in our new "color" model. But safe enablement requires more, as stated above.

Limiting applications to certain users or groups of users is one way organizations might consider reducing their exposure to risk. Other types of limitations include by schedule or time of day or by application function (e.g., allow Webex, but not the desktop sharing function).

Scanning applications for threats is another way to mitigate risk for an allowed application – and should include scanning for exploits, malware and potentially confidential data.

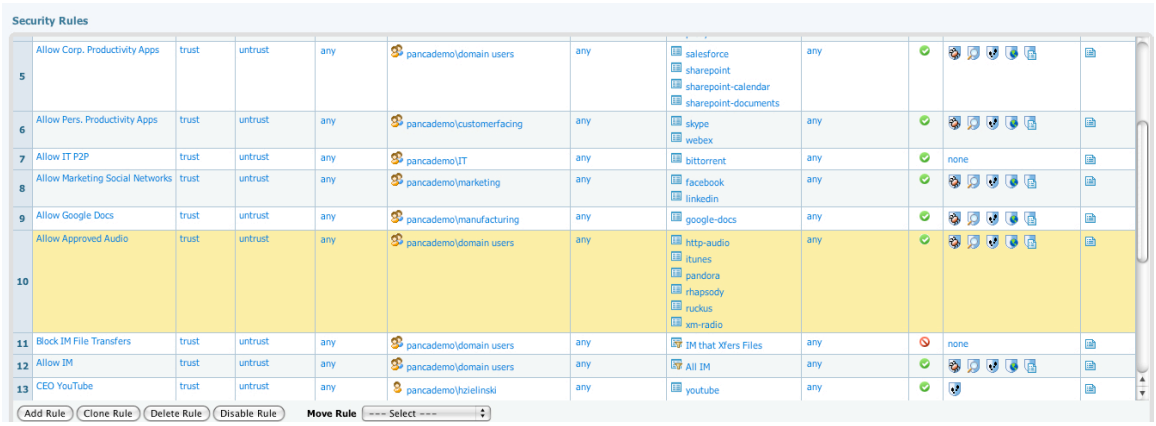
Incorporating *traffic shaping and quality of service (QoS)* as a policy response is a way to ensure that critical business applications aren't negatively impacted by less critical applications

Many enterprises are trying to expand beyond the simplistic deny/allow paradigm for network security, but the mix of enforcement points and the limitations of existing security infrastructure prohibit doing this in any effective fashion. Firewalls, proxies, IPS, and QoS technologies all have some ability to "help" with this task, but none can do it comprehensively. To use QoS/traffic shaping as an example, many components of network infrastructure have the capacity to perform QoS, but lack the intelligence to do so meaningfully. There are dedicated traffic shaping products that have good application knowledge, but they lack the performance to keep up with the requirements for high speed queue management – and perhaps more importantly, are completely disconnected from the other types of policy enforcement (e.g., scan, limit, allow, deny) – that might be performed in a variety of other devices, as mentioned above.

Palo Alto Networks next-generation firewalls recognize your network applications, regardless of port, protocol, SSL encryption, or other evasive tactics, and can apply all of the relevant

controls required by enterprises – allow, deny, limit, scan, or shape. These firewalls enable organizations to better, and more completely manage risk, but also reduce costs due to the simplification of security infrastructure, and the integration of all of the appropriate policy responses to applications into the firewall. Here's an example:

> Let's say an organization wants to enable all users to employ an externally hosted salesforce automation application (Salesforce.com), along with an externally hosted collaboration application (Sharepoint). These are corporate productivity applications. The organization also wants to enable Webex and Skype for sales and customer support people, and Google Docs for the manufacturing team collaborating with partners. Obviously, these fall more into the personal productivity applications – but clearly provide business value. As experiments, the organization wants to enable IT folks to use Bittorrent (but no other filesharing applications) to swap Linux binaries and 2 social networking applications for marketing people (Facebook and LinkedIn). Finally, for cultural reasons, the organization wants to open up IM (but eliminate file transfer capabilities) for all users, as well as enable limited, approved audio streaming (lifestyle applications).
>
> So, we will set policy to enable those corporate productivity applications, and give them high priority and bandwidth. But we're going scan the Sharepoint traffic for threats. Then, we'll enable the personal productivity applications for the sales, customer support, and the manufacturing team – but scan the Google Apps traffic for confidential data. For these personal productivity applications, we'll give them medium priority and bandwidth. For our "experiment" applications, we will allow for the right people (IT and marketing), and we'll assign low priority, but medium bandwidth. For our lifestyle applications, we'll allow for all, eliminate file transfers on IM, and assign low priority and bandwidth. All of this can be done with Palo Alto Networks next-generation firewall.



The above example illustrates the power, and risk management capabilities of fine-grained policy responses for a wide variety of applications.

Applications Aren't Threats – It's Time to Fix the Firewall

Application controls used to be in the firewall, but that was back in the days of applications respecting their assigned port numbers. That was also back in the days of a simpler black and white security model. Given today's application and threat landscape, enterprises need to adopt a new model for security. Each application has benefits; whether they are the automation of a business process, a productivity enhancement, or simply help make the workplace more pleasant for employees. But each application also carries risk – tunneling other applications, consuming bandwidth, carrying threats, transferring files, or impacting productivity. So applications aren't threats. Enterprises will have different perspectives on which applications are beneficial and appropriate to have on the network, and need a variety of responses (allow, deny, limit, scan, and shape) to mitigate the risk each allowed application carries. With its next-generation firewalls, Palo Alto Networks delivers the required application visibility, the application intelligence to make policy decisions, and the fine-grained controls to enforce those policies – empowering IT organizations to safely enable applications for their users.