



<http://www.jagatreview.com/2011/11/pr-traditional-%E2%80%9Cport-blocking%E2%80%9D-firewalls-useless-in-today%E2%80%99s-application-and-threat-landscape/>

## Traditional “Port Blocking” Firewalls Useless in Today’s Application and Threat Landscape

By [Patrick Gerard van Diest](#)

November 18th, 2011 | Categories: [Direct Release](#)

The Internet now accounts for the majority of traffic traversing enterprise networks. And it’s not just web surfing. The Internet has spawned a new generation of applications being accessed by network users for both personal and business use. Many of these applications help improve user and business productivity, while other applications consume large amounts of bandwidth, pose needless security risks, and increase business liabilities.

Traditional firewalls are unable to identify or effectively control any of these Internet applications. That’s because legacy firewalls classify traffic based only on ports and protocols. For example, most web traffic would be identified as simply HTTP coming through Port 80, with no information on the specific applications associated with that port and protocol. But this problem is not limited to Port 80. Internet applications are increasingly using encrypted SSL tunnels on Port 443, and use clever evasive tactics to disguise themselves or use port-hopping to find any entry point through the firewall. Again, legacy firewalls cannot see or control any of that traffic.

For all of these reasons, legacy firewalls are no longer an effective security solution to manage the risks and rewards of today’s Internet applications in the enterprise. This is not surprising since firewalls have seen no innovation and have changed very little over the last 15 years. IT organizations have tried to compensate for their deficiencies by surrounding them with proxies, intrusion prevention systems, URL filtering and other costly and complex devices that also are ineffective in today’s application and threat landscape. The real answer is to fix the problem.

### It’s Time to Fix the Firewall

Palo Alto Networks was founded by security visionary Nir Zuk, with a mission to re-invent the firewall so it can once again become the most strategically important security device in the network. Today, Palo Alto Networks offers real innovation in the firewall, enabling

unprecedented visibility and 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, these next generation firewalls accurately identify applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop targeted 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.

Here are some of the unique capabilities available only in next generation firewalls from Palo Alto Networks.

- The only firewall to classify traffic based on the accurate identification of the application, not just port/protocol information.
- The only firewall to identify, control and inspect SSL encrypted traffic and applications.
- The only firewall with real-time (line-rate, low latency) content scanning to protect against viruses, spyware, data leakage and application vulnerabilities based on a stream-based threat prevention engine.
- The only firewall to provide graphical visualization of applications on the network with detailed user, group and network-level data categorized by sessions, bytes, ports, threats and time.
- The only firewall with line-rate, low-latency performance for all services, even under load.
- The only firewall to identify unknown malicious files, often used in targeted attacks, by directly and automatically executing them in a virtual cloud-based environment.

Learn more about the Palo Alto Networks firewalls and the solutions they provide to enterprise customers.