Software Firewalls vs. Firewall Security Appliances Jerry Scott 2004

Firewall security appliances are slowly chipping away at the market segment held by traditional software-based firewall solutions.

Security appliances pledge to ease the burden of securing networks. They also bring many options to busy network administrators. Current appliances integrate multiple security applications, such as a Firewall and a VPN solution and possibly more into a single device. The current generation Symantec firewalls integrate deep packet inspection, virtual private networks, content filtering, anti-spam protection, and intrusion-prevention capabilities. The six Symantec models are designed to meet small branch office as well as large enterprise needs.

Software firewalls and security appliances attempt to solve the same problems; but use different approaches. Understanding these differences is the key to picking one technology over the other.

The security appliance is usually a combination of specialized hardware with either a proprietary or hardened commercial operating system. Many newer appliances use Intel CPUs with a browser-based management console. Ideally, these boxes cost less to own and operate than traditional solutions. Support costs are similar for both hardware and software solutions.

While many consider those characteristics strengths, some solution providers disagree. Some claim that a security appliance should be like other appliances, such as TV's or microwave ovens. With some security appliances, failure is silence, which is hard to differentiate from "*No security threat present*."

HARDWARE VS. SOFTWARE

	SECURITY APPLIANCE ADVANTAGES		SOFTWARE FIREWALL ADVANTAGES
1	Plug-and-play installation	1	Customizable
2	Increased vendor support	2	Can be integrated into operating systems
3	Integrated security software	3	Third-party product support
4	Lower initial costs	4	Can be integrated with applications
5	Easier administration	5	Scalability
6	Automatic updates	6	Multiple platform support
7	Subscription-based options	7	Hardware flexibility

Security appliances promise increased Return on Investment and reduced operating costs, but often cannot provide the flexibility of software firewall solutions. Integration opportunities are greater with software firewall solutions, as managers can select best-in-class solutions for individual security challenges and customize the integration opportunities to meet a specific customer's need.

Software solutions are often cheaper and generally as reliable once the host operating system is sufficiently hardened. Even under heavy loads, firewall hosts often have spare CPU. Network performance typically increases in factors of 10 every 3 to 5 years, while CPU performance tends to double every two years. This means that the ability of software based firewalls will tend to keep up with their network demands.

When an enterprise company already has IT staff in place, software firewalls provide greater control. You can more easily tailor a software solution to create best of breed solutions instead of accepting only what is available in the appliance solution. You can also tailor a security solution to fit an organization's way of doing business, instead of forcing it to change its ways to adapt to a new appliance-based solution.

Vendors such as Sonic Wall and WatchGuard strive to move security into an appliance form factor. Some will find that such appliances best-suited for smaller, single-site businesses, since some appliances provide limited scalability. To scale up, an Intel CPU based, software solution can be migrated to faster or multiple CPU's and greatly increased memory. Making the appliance faster usually means purchasing an entirely new box with greater expectations, often rendering the old appliance obsolete.

An all-in-one appliance offers speed of implementation and can demonstrate immediate benefits, such as faster up time and plug-and-play simplicity. In many cases, installation only interrupts external network access for a few minutes, while software-based solutions may require several hours of downtime.

Many security appliances offer better vigilance, such as automated subscription-based updates. This allows the devices to be automatically patched or updated to meet new threats as they are discovered. That feature helps integrators stay one step ahead of threats with minimal effort on their part.

Savvy integrators can create opportunity by combining both hardware and software-based solutions. You can use an appliance to handle secure connections and a software firewall to protect critical assets from both internal and external threats. You can even build you own security appliances, possibly using a stripped down version of Windows or a hand-tooled Linux or BSD kernel. The "roll your own" approach offers great customization opportunities, but also leaves integrators counting only on themselves to support the solution.

A bottom-line summary is as follows. *If an organization has limited resources, the appliance is the way to go. You have fewer moving parts, like a hard drive, and less to break. Conversely, the increased usability, integration opportunities, and control that a software firewall offers could easily offset the simplicity benefits of a hardware-based firewall appliance solution.*