

The Perfect Firewall - Cris DeWitt, CISSP

Firewalls come in so many flavors, pricing models and feature sets - what should I be looking for?

Many advantages can be obtained by combining several separate point based security systems into a unified security platform. Look for a statefull firewall, antivirus, intrusion detection & prevention, IPSec virtual private network (VPN) - (not PPTP or something proprietary), web content filtering, anti-spam (including spyware/grayware), and quality of service provisioning (bandwidth shaping). Make sure that key functionality is certified by a third-party like ICSA Labs.

A unified security platform eliminates multiple security devices and collapses them into one security ingress/egress-point. A single platform decreases the Capital Expenditure (CAPEX) and Operating Expenditure (OPEX) costs. Implementing single purpose security products is not only more expensive, but it also lacks the advantages gained from combined technologies - which greatly increases the detection rate of modern stealth and blended threats.

In our work a consistent technology across the entire family of products helps us address scaling issues for our clients. In other words, if our client is growing quickly, we don't have to significantly change their security platform as they grow from SoHo to SMB to large enterprise. Smaller customers benefit by taking advantage of enterprise and carrier class security features while larger customers benefit from experience in designing strong security products that are intuitive, easy to deploy and use. For enterprise class solutions, look for high-availability clustering to provide redundancy and scalability to eliminate single points of failure.

"Per box" licensing. Need I say more? Have you ever had to purchase ongoing maintenance, support, and product updates, blah, blah, blah, from a supplier that (almost deliberately) confuses the purchase costs? Simple pricing is the way to go.

Hardware based security and performance provides strong security without performance penalties. A high-performance security ASIC specifically designed to speed up the computationally intensive routines commonly associated with complete content protection says the supplier has their act together. I'm not speaking of just Deep Packet Inspection capabilities that many competing firewalls are just starting to implement. Your firewall should perform real-time content reassembly and analysis for antivirus, grayware, IDS, encryption, content analysis, and related functions. It's much faster (6x or more) when compared to software-based security applications.

By leveraging the ability to perform stateful firewalling, antivirus inspection, and intrusion detection, a firewall provider can take advantage of the shared information between its security components - giving the firewall the ability to stop malicious threats that are non-signature based. This technology increases detection capabilities against modern attacks that are designed to bypass traditional security defenses such as stateful firewalls and intrusion detection systems.

The ability to detect, remove and block both known and unknown threats in real time is key. Couple real-time detection/removal/blocking with virus and attack signature updates and your networks can stop new born threats faster than traditional "identify only" and "manual update" security solutions. Firewall solutions architected in this way not only provide faster response times and better protection against attacks, but also lower IT workloads and downtime often associated with the aftermath of a virus outbreak or destructive worm - significantly minimizing the loss of information, lowering TCO, and increasing user productivity.

Modern security is not just one function such as a firewall or intrusion detection system, but an infrastructure of coordinated, defense-in-depth security components placed at various layers of the network with the ability to take the appropriate actions when threats are identified. The keyword here is "coordinated". Insure your firewall solution includes support for coordinated control, logging/monitoring, and integration with other security components either from the supplier or from a third party.

In summary, look for:

- o A unified security platform
- o Consistent technology across the entire family of products
- o "per box" licensing
- o Real-time content reassembly and analysis (emphasis on real-time)
- o Shared information between its security components
- o Coupled real-time detection/removal/blocking with virus and attack signature updates
- o Coordinated, defense-in-depth security components (emphasis on coordinated)