



Perimeter Security Solutions – Comparative Analysis

	Software-Based Firewalls (on a multipurpose computer)		Hardware-Based Firewalls (on a dedicated device)				Optin Security
	Less than \$200	More than \$200	Less than \$200	Less than \$500	Less than \$3000	More than \$3000	Low monthly fee
COST CATEGORY							
TYPICAL FEATURES & CAPABILITIES							
Provide very basic security services like NAT or simple filtering	√	√	√	√	√	√	√
Secures your business with a hardened operating system and a dedicated appliance.			√	√	√	√	√
Stops security threats at the perimeter, where the dirty Internet first touches your private network.			√	√	√	√	√
Ability to provide complete Inbound and Outbound communication protection with completely customizable Inbound AND Outbound security rules.		√			√	√	√
Provide the intelligence to look into protocol behaviors to determine if they are being used in a bad way – a NECESSARY feature for the common protocols most people need to pass like HTTP.						√	√
Provide protocol level authentication/access.						√	√
Ability to integrate passwords with your Microsoft network passwords or other common sources to reduce complexity and administration challenges.						√	√
Provide granular VPN tunnel control – like participation/restriction based on users or IP, VPN routing, redundant VPN topologies (full and partial mesh).						√	√
Provide secure commonly managed VPN client software solutions and clientless options.						√	√
Provide perimeter virus and SPAM protection.						√	√
Provide mail server and mail service (SMTP) protection (prevents direct access to your mail server by allowing the firewall to answer first and then pass on valid communications).						√	√
Provide URL (website) access management.						√	√
Provide website content control Ex. The ability to allow a page to display without the ability to activate a threatening executable link.						√	√
Provide complete, continuous logging of security events and behaviors with the ability to archive and retrieve this data.						√	√
Reporting capabilities on security events and usage of IT resources to help understand risks and focus user productivity						√	√

	Software-Based Firewalls (on a multipurpose computer)		Hardware-Based Firewalls (on a dedicated device)				Optin Security
COST CATEGORY	Less than \$200	More than \$200	Less than \$200	Less than \$500	Less than \$3000	More than \$3000	Low monthly fee
TYPICAL FEATURES & CAPABILITIES							
Implementation, monitoring, and support by dedicated, credentialed, trained, experienced security professionals							✓
Ongoing network security performance review by trained professionals (security is an ongoing competitive process not a destination)							✓
Free, perpetual hardware, software, licensing updates for life. ALL MAINTENANCE IS INCLUDED.							✓
Perpetual research, development and updates to the latest best-of-breed perimeter security solutions for no additional costs							✓

Common security vulnerabilities of inexpensive firewall solutions:

- “Need to pass” communications are simply passed through the firewall without being checked. HTTP is a commonly passed and commonly exploited protocol that can be used to deliver pop-ups, facilitate background website downloads and Kazaa or Napster type network communications.
- Outbound communications are not properly protected
 - Hackers can easily use this weakness to gain access to a network
 - Provides an opening for malicious code to exploit network information, access confidential information, and to transmit security threats from your organization to others
- Software firewalls (installed on a multipurpose computer) are usually located inside the network instead of at the perimeter and must run on each computer attached to the network. This type of security solution is difficult to monitor, update and keep secure. In addition, hackers can exploit weaknesses in computer operating systems allowing them to disable the firewall. Do you keep all your multipurpose computers patched to the latest release and have you “hardened” each multipurpose computer’s operating system?
- Most inexpensive solutions will not include continuous updates, monitoring, or maintenance...Security is an ongoing race with hackers and requires ongoing attention. Without continuous security support, a firewall will provide little more than a false sense of security.
- Inexpensive, product-only solutions are no better than the security professionals that provide the installation, configuration, and updates. Who is logging, listening, and reporting on your security for you?
- No protection against viruses, SPAM, Pop-ups, or URL filtering (Additional, software and/or hardware needs to be purchased and maintained with the inexpensive firewalls).

ATTENTION! Inexpensive firewall solutions provide some protection to a network in the short-term but provide minimal protection (if any) to new security threats, common “need to pass” protocols, or, to an “aggressive” hacker who wants to damage your network.

OPTIN SECURITY PROVIDES COMPREHENSIVE PROTECTION AND PEACE OF MIND

- ✓ **Comprehensive coverage with no hidden costs**
- ✓ **Perpetually updated security from trained security professionals**
- ✓ **Ongoing security management for your protection and productivity**

Call 1 866.822.2238 for more information or visit our website at www.optinsecurity.com