

FIREWALL BEST PRACTICES

By Kevin Beaver, CISSP

Independent information security consultant, author, keynote speaker,
and expert witness with Principle Logic, LLC (www.principlelogic.com)

Firewalls are not the end all, be all solution to information security. They are, however, a necessary component of an effective network security infrastructure. The following list is a set of best practices, in no particular order, that you should consider to help ensure your firewall is configured for optimal effectiveness.

1. Deny all traffic by default and only enable those ports, protocols, and services that are needed.
2. Disable or uninstall any unnecessary services and software on the firewall that are not specifically required.
3. Limit the number of applications that run on the firewall in order to let the firewall do what it's best at doing. Consider running anti-virus, content filtering, VPN, DHCP, and authentication software on other dedicated systems behind the firewall.
4. If possible, run the firewall service as a unique user ID instead of administrator or root.
5. Set or change the default firewall administrator or root password before you ever connect it to the public Internet. It sounds too obvious, but it's true – many firewall passwords are never set or changed from their default. Make it a long complex phrase that'd be very difficult to guess and ideally easy to remember. Change the password every 6-12 months or if it's ever suspected to have been compromised.
6. Do not rely on packet filtering alone. Use stateful inspection and application proxies if possible.
7. If your firewall allows it, ensure that you're filtering packets for correct source and destination addresses to keep malicious traffic from entering and leaving your network.
8. If a malicious user can obtain physical access to the firewall, anything can happen. Ensure that physical access to the firewall is controlled.
9. A lot of times, firewalls are doing less (or more) than what they should be doing based on your business needs and information flow requirements. Keep your firewall configuration as simple as possible and eliminate unneeded or redundant rules to ensure that the firewall is configured to support your specific needs.
10. Make sure the security rule set on the firewall remains consistent with the organization's written information security policy. Also, be sure not to confuse your firewall rulebase with your internal 'security policy'. They're not the same. The former is for the firewall and the latter is for internal dos and don'ts outlining 'this is how we do things here'. You *do* have a security policy, don't you?
11. Run the firewall on a hardened and routinely patched operating system. An insecure and non-hardened operating system can and will render the firewall useless.
12. Perform regular security tests against your firewall including any VPNs it's hosting. Plug the holes when they're discovered. If they can't be relatively easily then find another firewall. New exploits are continuously discovered and must be tested for on a consistent basis. In addition, the slightest firewall system or rule set modifications can completely change the firewall's security capabilities. Perform these tests on every interface of the firewall in all directions. Also, perform these tests with and without the firewall rules enabled to determine how vulnerable you will be when the firewall is not functioning properly.
13. Patch the firewall's operating system and application software with the latest code on a regular basis. However, make sure you test these updates in a controlled, non-production timeframe or environment whenever possible.
14. Use firewalls internally to segment networks and permit access control based upon business needs.
15. Enable firewall logging and alerting if possible.
16. Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious attacker.
17. Regularly monitor the firewall logs. Treat the logs as business records and include them in your information retention policy.
18. Note any firewall log entries that don't look right and investigate them immediately.
19. Periodically backup the firewall logs (preferably onto write-once media such as CD-R) and store for future reference and/or legal protection in the case of a breach that must be investigated.

20. Consider outsourcing your firewall management to Managed Security Service Provider (MSSP) so you can leverage the managed security service providers' aggregation of expertise, network trending analysis and intelligence, and also to save time and money focusing on your core business needs.
21. Use change-management practices such as those outlined by [ITIL](#) for the firewall to approve changes needed, assess the reason(s) for the changes, document the changes made, and describe the necessary back-out procedures in case the changes fail. This is *extremely* important.
22. Perform ongoing audits, at least yearly, on the firewall to compare what you say you're doing in your security policy with what's actually being done and to ensure adherence to any government regulations that pertain to your organization. This can be done manually, or ideally, using a tool such as Karalon's TrafficIQ Pro (www.karalon.com).
23. Require that all remote computers run personal firewall/intrusion prevention software. Firewalls can be easily circumvented if using wireless network systems internally, so it pays to have another layer of defense on your hosts. Make this something that cannot be easily disabled by users. No exceptions.
24. Constantly monitor (or subscribe to) your firewall vendor's security bulletins.
25. Regularly backup the firewall configuration files and keep the backups offsite.
26. Remember that firewalls mostly likely won't be able to prevent attacks that originate from inside your network. An acceptable usage policy, personal firewalls and host-based intrusion prevention software, network monitoring, content filtering, and access controls on all hosts can help lower these risks.

NOTICE: The information contained herein is considered best practices for securing firewalls but may not constitute a secure firewall if implemented. Each firewall and its associated information systems are unique; therefore, these recommendations may not be completely suitable for your situation. Like any changes should be handled, please test these in a non-production environment first to ensure interoperability within your network.

About Kevin Beaver

I am a CISSP-certified independent information security consultant, [keynote speaker](#), and expert witness with nearly two decades of experience in IT -- the last 13 years of which I've dedicated to information security. Before starting Principle Logic in 2001, I served in various information technology and security roles for several healthcare, e-commerce, financial firms, educational institutions, and consulting organizations.

I have presented at seminars and conferences over 100 times and I'm consistently a [top-rated speaker](#) on information security at shows for RSA, CSI, and IIA. I am author/co-author of seven books on information security including the highly-successful ethical hacking book [Hacking For Dummies](#), [Hacking Wireless Networks For Dummies](#), [Securing the Mobile Enterprise For Dummies](#), and [Laptop Encryption For Dummies](#) (all by Wiley) as well as [The Definitive Guide to Email Management and Security](#) (Realtimepublishers.com) and [The Practical Guide to HIPAA Privacy and Security Compliance](#) (Auerbach). In addition, I am a contributing author and editor of the book [Healthcare Information Systems, 2nd edition](#), technical editor of the book [Network Security For Dummies](#) by Wiley Publishing, and technical editor for over a dozen books and whitepapers for Realtimepublishers.com.

In addition to my books, I am the creator and author of [Security On Wheels](#) audio programs providing *security learning for IT professionals on the go*. I have an associated blog at securityonwheels.blogspot.com. I am also a regular contributor of information security content for [SearchWindowsSecurity.com](#), [SearchSoftwareQuality.com](#), [SearchSQLServer.com](#), Security Technology and Design (ST&D) magazine and its sister site SecurityInfoWatch.com.

I am the founder and past president of the Technology Association of Georgia's Information Security Society and serve as an IT advisory board member for several universities. I earned my bachelor's degree in Computer Engineering Technology from Southern Polytechnic State University and my master's degree in Management of Technology from Georgia Tech.

For more helpful information security tips and best practices please visit www.principlelogic.com/resources.html and securityonwheels.com.

