

FIREWALL BEST PRACTICES

By Kevin Beaver, CISSP

Independent information security consultant, author, 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 reasonable practices to consider in order to ensure your firewall(s) is configured for optimal effectiveness. Remember, “best practices” aren’t a one-size-fits-all solution. Furthermore, reasonable firewall configuration and management doesn’t automatically minimize risks. Your mileage – and your priorities – will vary.

1. Don’t assume your firewall is the answer to your network security. Things are way more complicated.
2. Deny all traffic by default and only enable those ports, protocols, and services that are needed.
3. 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 outlines what the firewall lets in and out of the network. The latter is for internal dos and don’ts outlining ‘this is how we do things here’. You *do* have a set of security policies, right?
4. Limit the number of applications that run on the firewall in order to maximize CPU cycles and network throughput. This will 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 and, in some cases, in front of the firewall.
5. Run the firewall service as a unique user ID instead of administrator or root.
6. Set or change the default firewall administrator or root password before you ever connect it to the public Internet. It sounds too obvious, but I often see it in my work – many firewall passwords are never set or changed from their default. Make it a long complex passphrase 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.
7. Do not rely on packet filtering alone. Use stateful inspection, proxies, and application level inspection where possible.
8. Filter packets for correct source and destination addresses to keep malicious traffic from entering and leaving your network. This will help prevent denial of service attacks.
9. Ensure that physical access to the firewall is controlled. Again, another obvious statement but you’d be amazed at how many firewalls out there are accessible to anyone and everyone who wants to wreak havoc.
10. 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. This requires auditing your rulebase periodically which can be done manually, or ideally, using a tool such as Karalon’s TrafficIQ Pro (www.karalon.com).
11. Perform regular security tests against your firewall including any VPN endpoints it’s hosting. 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, if possible, perform these tests with and without the firewall rules enabled to determine how vulnerable you will be when the firewall is not functioning properly.
12. Patch the firewall’s operating system and application software with the latest code on a regular basis. This requires continually monitoring (or subscribing to) your firewall vendor’s security bulletins. However, make sure you test these updates in a controlled, non-production timeframe or environment whenever possible.
13. Use firewalls internally to segment networks and permit access control based upon business needs.
14. Enable firewall logging and alerting if possible but **ONLY** if it’s going to be managed. Otherwise, it’s a waste of processor cycles. Treat the logs as business records and include them in your information retention policy.
15. Use a secure remote syslog server that makes log modification and manipulation more difficult for a malicious attacker.
16. Consider outsourcing your firewall management to a managed service provider so you can leverage their aggregation of expertise, network trending analysis and intelligence. This will also save you time and money by allowing you and your team to focus on your core business needs.

17. 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.
18. 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.
19. Regularly backup the firewall rulebase and configuration files and keep the backups offsite. This doesn't seem important until the time comes for you to restore after a system failure, etc.
20. Remember that firewalls are rarely in a position 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.

About Kevin Beaver

I am an independent [information security consultant, author, keynote speaker, and expert witness](#) with over two decades of experience in IT -- the last 14 years of which I've dedicated to information security. Before starting Principle Logic, LLC 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 have been a [top-rated speaker](#) at shows for RSA, CSI, and IIA. I now focus on information security seminars and keynoting IT and information security shows most recently for Hewlett-Packard, IDC, ISSA, ISACA, and The Georgia Society of CPAs.

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](#) by Auerbach Publications, 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.com/blog](#). I am also a regular contributor of information security content for SearchEnterpriseDesktop.com, SearchCompliance.com, SearchWindowsServer.com, SearchWinIT.com, SearchSoftwareQuality.com, SearchDataBackup.com, SearchSQLServer.com, SecurityInfoWatch.com and Security Technology Executive magazine.

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 two Atlanta-based colleges. I earned my bachelor's degree in Computer Engineering Technology from Southern College of Technology and my master's degree in Management of Technology from Georgia Tech. I also hold the Certified Information Systems Security Professional ([CISSP](#)) certification which I obtained in 2001.

For more information security resources please visit

www.principlelogic.com/resources.html and <http://securityonwheels.com>.

