Firewall Configuration Review

Firewalls are a spot of contention for many within the information security community. Many people put too much faith in a network firewall and assume that because there is one on the network somewhere, that they're “hacker proof.” Others do not put enough faith in a network firewall because many are deployed improperly or they're deployed in the wrong spot on the network, or not enough firewalls are deployed to provide adequate protection within their environment. There are seemingly endless technical challenges when it comes to proper deployment, configuration, management, and review of firewalling technology.

Regular review of firewall configurations and how they’re deployed is considered a best practice and really helps promote good configuration from the simple act of looking at it from time to time. If best practice isn’t enough reason, regulatory requirements such as PCI require you to perform regular firewall configuration reviews (Requirement 1.1.6). The firewall isn’t a black box that you setup and walk away from. Many times, this is the heart of your critical network, and to continue smooth operations, it requires maintenance. Improper segmentation and rule set configuration are also likely one of the core reasons you failed your most recent penetration tests, but this is often lost on a lot of people. Sure the initial access vector was MS08-067 on a test server, but why was someone from the user segment able to talk directly to the test network in the first place? Take my word for it, periodic configuration reviews are very important, regardless of the technology.

Unless you’re intimately familiar with firewall technologies, performing a useful review of a firewall is quite difficult. Many businesses don’t have the luxury of a dedicated firewall configuration employee or team.

There are a lot expensive tools that will look at your configuration and give you some rule set and configuration recommendations, but those require capex and opex budget allotments as well as the expertise to get the most out of the tools to maximize your investment. Unless you’ve mastered the basics, buying a tool isn’t going to be a good use of limited information security budget dollars. If you don’t want a tool, there are a plethora of clumsily put together checklists that attempt to help you solve this problem. However, even the better checklists seem to be a response to regulation and ignore best practice and availability items.

So what is my brilliant revelation, you ask? Well, I’ve created a checklist of course! Before you run to the wood shed and grab the pitchfork, take a look at what I have. My checklist isn’t specific to a product, platform, or regulation. This should be a good general checklist that you can use in any environment and the risky items should become self-evident as you work through the checklist.

Here are the goods:

- **Firewall checklist (short)** - short and to the point – for use on a regular basis. Use one form per device per quarter (or more frequently if you're able). NetSPI recommends that you look at your firewalls as often as you can, within reason.
- **Firewall checklist (long)** - same as above, but this includes some long form descriptions about why this is on the list, as well as example values. The example can be neutral, positive, or negative.

So how do I use these documents, you ask? Print out one of the checklists above. The first couple times
it may help to use the long form with the explanations so you know what I’m asking and why. Once you’re comfortable, you can start using the short form. Every quarter, or whenever your firewall configuration cycle rolls around, print out a form for each of your firewall and access control devices. Go through the device configuration and fill out the form to the best of your ability. If you get stuck, reach out to any internal network and firewall administrators to help you understand what to write down. When you find an item that needs attention, create an internal project or ticket to correct that configuration or deployment problem. File the form away in a safe place. That’s it!

Over time, you should see the overall configuration of the firewalls improve, and you have a review trail that you can give your auditor if they ask about a firewall review requirement. When the business considers buying new firewalls or access control devices, pull out a form and run through it for each proof of concept deployment in your demo environment. If you buy a product and deploy it in demo, run through the checklist before you sign off on the deployment to your production environment.

This is version 1 of the document. If you have any feedback, or you know of other useful firewall checklists, please let me know.