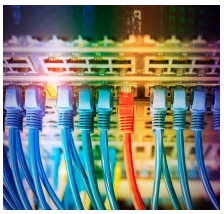
CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

FIREWALL CYBERSECURITY CHEAT SHEET

① Firewalls

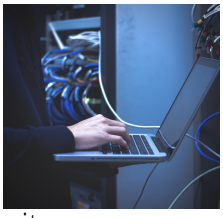


Firewalls are one of the oldest network security defenses and today remain a foundation of that continually remain a crucial foundation of network protection. However, to be secure, firewalls must be correctly installed, updated and maintained. Additionally, the firewall rules and criteria must be configured and then regularly reviewed and updated.

② Firewalls Basics

Firewalls stand as an organization's first line of defense, and as such they get a lot of attention from attackers. Firewall technology can either be software or hardware. Hardware firewalls are also known as perimeter firewalls and is installed between the businesses network and the Internet to protect internal systems. A software firewall is used to protect the single device it is installed on and many computers come preinstalled with software firewalls. Most of the time, we find that firewalls are riddled with configuration flaws, and aren't accurately protecting systems. In summary, a hardware firewall protects environments from the outside world, and a software firewall protects a specific device from internal threats.

Addressing Problems ③



1. Spend time on (and revisit) configuration - Establish Access Control Lists that dictate to the firewall exactly what information will allowed to leave your system.

Firewall rules give firewalls their security power, which is why they must constantly be maintained and updated to remain effective. With these rules you are able to whitelist, blacklist, or block certain websites or IP addresses. Some set up large rule sets which end up negatively impacting the performance of the network. If your network is running slow you should check the size of your firewall rule set. When you begin to fine-tune and optimize your firewall rules, take the time to revisit all existing rules and make sure you have all the necessary documentation for each of them.

2. Document everything - Documenting the network helps your team visually identify the state of the system including: What has been done, what still needs to be done, and where problems exist. At minimum these should include:

- The purpose of the firewall rule
- The service(s) it affects
- The users and devices it affects
- The date the rule was added
- When the rule should expire (if it is temporary)
- The name of the person who added the rule

Continue reading on next page >

FIREWALL CYBERSECURITY CHEAT SHEET

③ Addressing Problems (con't)

- Network flow diagrams - provide an accurate view of the set up of your network and shows the location of all the associated equipment an the flow of data through the system. They identify exactly what areas must be protected, and the unnecessary services, protocols, and ports to disable.
- Description of groups, roles, and responsibilities - Identifies who is involved in the firewall process, so that you can ensure those assigned are aware of their responsibilities, and assure that no devices are left unmanaged.
- Business justification for allowed services, protocols, and ports - The most common places for breaches to occur is where a vulnerability exists. These vulnerabilities are usually found in areas that are unmonitored, un-patched or unused.

Firewalls should be configured to only allow the minimum number of connections required for active business operations. If you require ports or services to be opened to support business operations, the documentation will show why they have been left open and give an explanation of tactics being taken to protect against those open areas.

3. Restrict and minimize traffic - firewalls should be configured to protect the sensitive data environment at all costs which means restricting and controlling the flow of traffic wherever possible. Having a number of firewalls can ensure that your network is segmented correctly. Firewalls should ensure blockage of all unwanted traffic through segmentation and rule sets. A segmented network allows you more finite control. A well protected system provides less opportunity for a hacker to find an unprotected Internet connection.

Continue reading on next page >

(CONTINUED)

Addressing Problems (con't) ③

4. Protect new technology - With the increase in network connected devices a business's network perimeter is harder to keep well defined. To help mitigate these problems every businesses should make sure they install personal network firewalls software on mobile and other employee-owned devices (fitbits, smart speakers, etc) that connect to the Internet and also access the network.

5. Monitor and tighten control - As much as you might like to think that of Firewalls as being plug-and-forget technology -- They are not! Your business environment changes and this requires changes to your firewall. I recommend that businesses review firewall and router rule sets at every quarter. This type of periodic review allows you to check for vulnerabilities and correct them by revamping your firewall strategy. Log management is vital to firewall security. Firewall logs keep track of both normal and potentially damaging user actions involving your firewall and help prevent and detect vulnerabilities under attack and minimize the impact of any data breach. By correctly configuring your event log software, administrators can be alerted if the firewall logs indicate an attack. Firewalls only have a limited amount of space available for logging. In order to keep accurate logs, I recommend setting up a logging server and configuring your firewall logs to write them to that server.

6. Organize firewall rules for maximum speed - Most firewalls will apply rules in the order that they are listed in your firewall configuration software or rule base. That means that it is a good idea to place the more specific rules first followed by the less granular rules to prevent a more general and less defined rule from taking precedence over a definitive or specific rule.

FIREWALL CYBERSECURITY CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

③ Addressing Problems (con't)

Additionally, frequently used rules should be placed higher than ones that are not used as often.

Here is a list of example rules in order of importance:

1. Anti-spoofing filters
2. User permit rules
3. Management permit rules
4. Noise drops
5. Deny and Alert
6. Deny and Log

7. Utilize upstream traffic blocking - You can configure your routers to handle some traffic-blocking activities. Giving you more throughput on your firewall and increasing performance

8. Upgrade Firewall Software and Firmware - It goes without saying, but as you update your firewall rules, it's also a good time to make sure that you have installed all the latest patches to your firewall. The greatest list of firewall rules in the world won't stop an attack if your firewall has a known vulnerability that hasn't been patched.

Next Generation Firewall (NGFW) ④

The main difference with a next generation firewall is that you can set application controls and policies. These types of firewalls allow you to gain far more visibility and control over the users, devices, threats, and vulnerabilities in your network. A next generation firewall is a combination of threat-centric hardware and software that seamlessly integrates your network defense capable of neutralizing cyberthreats while allowing simplified management through a single interface.

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies
- Ease administration and reduce complexity with unified policies

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH