Step 1: Secure your firewall

If an attacker is able to gain administrative access to your firewall it is “game over” for your network security. Therefore, securing your firewall is the first and most important step of this process. Never put a firewall into production that is not properly secured by at least the following configuration actions:

Update your firewall to the latest firmware.

- Delete, disable, or rename any default user accounts and change all default passwords. Make sure to use only complex and secure passwords.
- If multiple administrators manage the firewall, create additional administrator accounts with limited privileges based on responsibilities. Never use shared user accounts.
- Disable simple network management protocol (SNMP) or configure it to use a secure community string.

Step 2: Architect your firewall zones and IP addresses

To protect the valuable assets on your network, you should first identify what the assets are (for example, payment card data or patient data). Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.

For example, all of your servers that provide services over the internet (web servers, email servers, virtual private network (VPN) servers, etc.) should be placed into a dedicated zone that will allow limited inbound traffic from the internet (this zone is often called a demilitarized zone or DMZ). Servers that should not be accessed directly from the internet, such as database servers, must be placed in internal server zones instead. Likewise, workstations, point of sale devices, and voice over Internet protocol (VOIP) systems can usually be placed in internal network zones.

Generally speaking, the more zones you create, the more secure your network. But keep in mind that managing more zones requires additional time and resources, so you need to be careful when deciding how many network zones you want to use.

If you are using IP version 4, Internal IP addresses should be used for all of your internal networks. Network address translation (NAT) must be configured to allow internal devices to communicate on the Internet when necessary.

Once you have designed your network zone structure and established the corresponding IP address scheme, you are ready to create your firewall zones and assign them to your firewall interfaces or sub interfaces. As you build out your network infrastructure, switches that support virtual LANs (VLANs) should be used to maintain level-2 separation between the networks.

Step 3: Configure access control lists

Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic needs to be able to flow into and out of each zone.

This traffic will be permitted using firewall rules called access control lists (ACLs), which are applied to each interface or sub interface on the firewall. Make your ACLs specific to the exact source and/or destination IP addresses and port numbers whenever possible. At the end of every access control list, make sure there is a “deny all” rule to filter out all unapproved traffic. Apply both inbound and outbound ACLs to each interface and sub interface on your firewall so that only approved traffic is allowed into and out of each zone.

Whenever possible, it is generally advised to disable your firewall administration interfaces (including both secure shell (SSH) and web interfaces) from public access. This will help to protect your firewall configuration from outside threats. Make sure to disable all unencrypted protocols for firewall management, including Telnet and HTTP connections.

Step 4: Configure your other firewall services and logging

If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don’t intend to use.

To fulfill PCI DSS requirements, configure your firewall to report to your logging server, and make sure that enough detail is included to satisfy requirement 10.2 through 10.3 of the PCI DSS.

SEE ALSO: Understanding the HIPAA Application of Firewalls

Step 5: Test your firewall configuration

In a test environment, verify that your firewall works as intended. Don’t forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing.

Once you have finished testing your firewall, your firewall should be ready for production. Always remember to keep a backup of your firewall configuration saved in a secure place so that all of your hard work is not lost in the event of a hardware failure.

Remember, this is just an overview to help you understand the major steps of firewall configuration. When using tutorials, or even if you decide to configure your own firewall, be sure to have a security expert review your configuration to make sure it is set up to keep your data as safe as possible.

Firewall management

With your firewall in production, you have finished your firewall configuration, but firewall management has just begun. Logs must be monitored, firmware must be updated, vulnerability scans must be performed, and firewall rules must be reviewed at least every six months. Last of all, be sure to document your process and be diligent about performing these ongoing tasks to ensure that your firewall continues to protect your network.