# Network Firewalls

Network Firewall Usage and Configuration Basics

Gabe Gibler & Colton Hotchkiss

July 22, 2017
Version 1.3

University of Idaho

CS 439/CS 539: Applied Security Concepts

**Summary**

A firewall is a technological barrier which can be used in most computing devices to control the incoming and outgoing network traffic. Configuration is accomplished primarily through use of rules, either pre-configured or user-specified. Effectiveness of firewalls depends upon how well they are managed and not on how perfectly they are initially deployed. Therefore, in this tutorial, we will demonstrate management (usage and configuration) of network firewalls.

# Contents

## 1 Objectives of this Tutorial >

1. Learn the basics of network firewalls using pfSense.
    - Learn how to configure pfSense:
        - Create firewall rules to manage a LAN, WAN, and DMZ;
        - Create NAT rules to route between the various interfaces;
        - Use pfSense to establish VPN connections.

This tutorial is not a complete user's guide to network firewall management. It is a brief overview of pfSense in particular. We will briefly explain, through walkthroughs, activities, and challenges, the above objectives.

## 2 Required Background <>

We assume some knowledge in the following areas:

1. Experience using computers and software applications, like web browsers, and virtualization apps;
2. Fundamentals of internet and networking mechanisms like TCP/IP stack, TCP/UDP protocols and ports, etc.;
3. An introductory knowledge of data privacy, computer/network security, etc.;

It is not the goal of this tutorial to be completely self-contained and self-explanatory. As such, the tutorial assumes certain background skills and knowledge. The following are some areas where we expect the users of this tutorial to have some previous skills/knowledge:

1. Practical experience using computers, and installing and using common software applications (particularly web browsers, and virtualization platforms). The tutorial does not always explain how to navigate within the operating system's graphical user interface (GUI) or how to execute commands from the command line. Some exposure to logic notations and elementary programming skills would be very helpful with writing firewall rules. Similarly, the tutorial does not explain how to browse the Internet, or how to install software applications. If setting up the tutorial, additional knowledge is required to set up a domain, set up DNS, etc.
2. Fundamental knowledge of networking mechanisms and computer networks. This tutorial expects a user to understand technical concepts like the ISO OSI model of networks, and common networking terms such as "packets", "ports", "protocols", "accept/drop" in relation to packets, "TCP" and "UDP", etc.
3. A broad understanding of general computer-related issues will help, such as "data privacy", "network access privileges", "application permissions", and different sorts of internet-based attacks.

## 3 Hardware and Software Requirements <>

The tutorial was executed using the following environment:

1. A computer capable of hosting at least 4 virtual machines (VMs);
2. A virtualization software platform, e.g. VMWare or VirtualBox;
3. A) One standard Microsoft Windows Server 2012 R2 VM, B) one Microsoft Windows 10 VM, C) two Ubuntu VMs, D) one VyOS VM, and E) one pfSense VM.

The activities and challenges of this tutorial occur in multiple VMs. As such, it is imperative that the user of this tutorial has a machine powerful enough to boot at least 4 virtual machines smoothly at a time, since the pfSense and VyOS machines are not resource intensive. For the sake of consistency, specifics for each VM are given below:

**A**) We are using a standard Microsoft Windows Server 2012 R2 VM. Either Windows Server 2008 or Windows Server 2016 can be substituted and will be functionally equivalent.

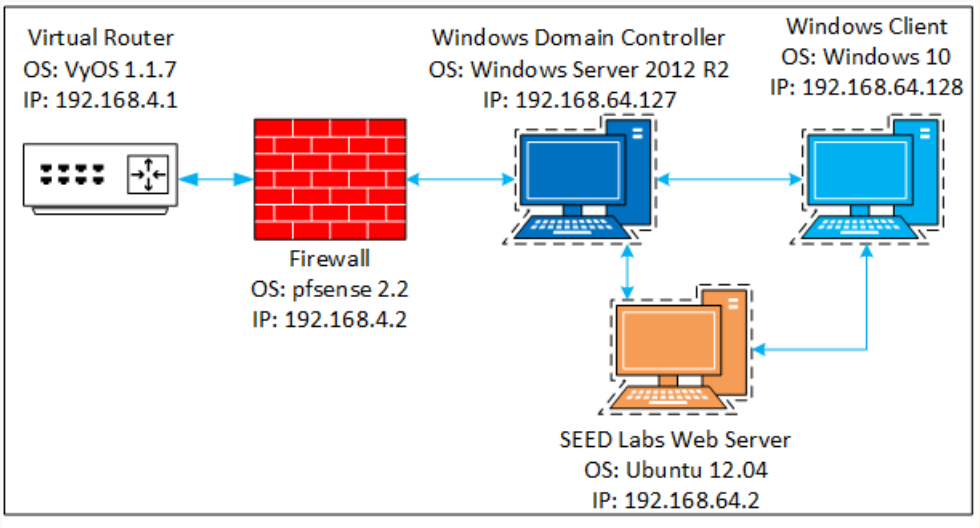
**B**) We are using a Microsoft Windows 10 VM. Either Windows 7 or Windows 8/8.1 can be substituted and will be functionally equivalent.

**C**) We are using a mixture of Ubuntu 12.04 and Ubuntu 16.04 64-bit. The Ubuntu 12.04 VM came from the SEED Lab tutorials, simply because it was ready for use as a web server. Any Linux machine hosting the LAMP stack to act as a web server will be functionally equivalent.

**D**) We are using VyOS 1.1.7 64-bit. You can download it here in the form of an ISO or an OVA template that can be directly imported into VMware. For VMware installations using OVA see the VyOS wiki, and for Virtualbox see this.

**E**) We are using pfSense 2.2 64-bit. You can download the latest version here. The GUI of newer versions may differ significantly from the version used in this tutorial.

# 4 Network Layout <>



## 5 Network Firewalls Overview <>

1. What are they?
   (a) Hardware and/or software based entities used to protect networks from unauthorized access;
2. What are their features?
   (a) Stateful Packet Inspection;
   (b) Network Address Translation (NAT);
   (c) Virtual Private Networking (VPN).

1. **What are they?**
   (a) Network firewalls are usually located at the boundary between the internal network and external networks (Perimeter Firewall) or between internal segments of networks (Interior Firewall).
2. **What are their features?**
   (a) Operating in the network layer the firewall examines a packet's header and footer and determines if the packet belongs to a valid session. Using this information the firewall decides if a packet should be forwarded to the internal network or rejected. [5]
   (b) Network Firewalls are able to change the network address of devices on either side of the firewall to hide the true addresses of devices. This can prevent devices on the outside of a network from being able to probe the true addresses of devices on a network. [4]
   (c) Network firewalls are able to create encrypted connections using VPNs between themselves. If a host on a network needs to communicate with a host on another network the firewall can establish a secure communication channel with the other host through its firewall.

## 6 Types of Network Firewalls <>

There are many types of Network Firewalls including:

1. Fortinet FortiGate;
2. Cisco ASA;
3. SonicWALL TZ;
4. Cyberoam UTM;
5. pfSense.

We are going to focus on pfSense for this tutorial.

## 7 In the News <>

1. Cisco's ASA firewalls compromised using malformed UDP packets. (11th Feb. 2016) [3] [PCWorld].
2. Cisco zero day leaked by Shadow Brokers.
3. Firestorm vulnerability permits extraction of data via TCP handshakes regardless of rules or IP address filters.

1. **Cisco's ASA Bypass:** Cisco Systems' Adaptive Security Alliance (ASA) firewalls were confronted (and subsequently patched) with a critical bypass vulnerability which had the potential to allow remote attackers to over the firewalls, which are configured as virtual private network servers by simply sending malformed UDP (User Datagram Protocol) network packets to the firewalls [3].

2. The Shadow Brokers group released Cisco zero-day vulnerability. Referred to as EXTRABACON (CVE-2016-6366) deals with the way the firewall handles SNMP protocol. This vulnerability allows attackers to remotely case the system to reload or execute arbitrary code. [2] Mitigation's for this attack are allowing only trusted users to have SNMP access.

3. Researchers at BugSec Group and Cynet discovered a vulnerability in newer firewalls that allows internal data to be extracted using the handshake of the TCP protocol. The firewalls permit any handshake from an outside entity in order to gather enough data to identify the application being used. An internal actor can then utilize specially crafted TCP handshakes to send data to an awaiting external server, effectively bypassing the firewall. Vendors responded that the vulnerability is by design, and must be allowed in order to gather enough information. [1]

## 8 Activity: Design a Network <>

For the computers and their roles given below, create a mapping of the network segments and locations of connected computers.

- Home network:
  - Ubuntu 16.04: user at home connecting across the internet;
  - Netgear: home router and firewall.
- Business domain:
  - pfSense: domain router and firewall;
  - Windows Server: domain controller and DNS Server;
  - Windows 10: employee workstation on the domain;
  - SEED: web server, for internal and external websites.
- VyOS router: acting as "the internet".

1. The design should express the appropriate segmentation necessary to separate and protect the concerns of each network of users.
2. For VyOS, consider it to have 2 interfaces: the connection to the home network, and the connection to the business network. Think of it as the ISP for the home network and simultaneously the ISP for the business network.
3. For pfSense, consider it to have at least 3 interfaces: WAN, LAN, and DMZ. Does it need more?
4. Where should firewalls be placed on a given network segment?
5. For the business domain, how do you separate computers that interact with both internal and external users?

## 9 Activity: Set up pfSense <>

1. Deploy pfSense for the "business" domain.
   - Configure the three interfaces of pfSense:
     (a) WAN;
     (b) LAN;
     (c) DMZ (OPT1).

1. Open a console to the pfSense VM.
2. At the menu, notice that initially `WAN` and `LAN` are the only network interfaces listed.
3. Enter **1** for "`Assign interfaces`".
4. Enter **n** to skip creating VLANs.
5. For the `WAN` interface, enter **vmx0**.
6. For the `LAN` interface, enter **vmx1**.
7. For the `Optional 1` interface, enter **vmx2**.
8. Press **enter**, and **y** to finish and confirm.
9. At the menu, enter **2** for "`Set interface(s) IP address`".
10. Enter **1** for "WAN".
11. Enter the IP address **192.168.4.2** . (Most of the time this would be DHCP, assigned by your ISP.)
12. Enter **30**, for a subnet mask of 255.255.255.252 to indicate 192.168.4.1-2 as the range of addresses that compose your WAN.

13. Next, enter the address of the upstream gateway for your network, **192.168.4.1** This will allow pfSense to route traffic out of your network. (Normally, this would be the IP address given to you by your ISP.)

14. Press **Enter** to skip the IPv6 addresses.

15. Enter **n** to not configure the DHCP server and **n** again.

16. At the menu again, enter **2** for "`Set interface(s) IP address`"

17. Enter **2** for "`LAN`"

18. Enter the IP address **192.168.64.1**

19. Enter **24**, for a subnet mask of 255.255.255.0 to indicate 192.168.64.1-255 as the range of addresses that compose your LAN.

20. Press **enter** to skip assigning an upstream gateway and to skip the IPv6 option again, and enter **n** to deny the DHCP server.

21. You will now be provided with a URL to access the GUI for pfSense that will be used later.

22. Repeat the process for the third interface, `OPT1`. Assign **192.168.65.1** for the IP address and **24** for the subnet mask. Otherwise, configure it the same as the LAN.

## 10 Activity: Basic Firewall Rules <>

What basic rules should be implemented for our business network? Consider:

1. WAN;
2. LAN;
3. DMZ.

Consider both incoming and outgoing rules.

**Hint**: What services will need to be allowed for each of these interfaces to be able to do their intended function? What are the common functions of a business? Do you want to allow everything from the inside to go out? Would there be downsides to that?

## 11 Activity: Log In to pfSense GUI <>

From the Windows 10 VM:

1. Open up a web browser;
2. Navigate to the pfSense interface, **192.168.4.2**;
3. Log in:
   User: **admin**;
   Password: **pfsense**;
4. What's the first thing you should do when setting up a new firewall!?
5. Browse around the variety of menus and options.

1. Is it a good idea to change the default password of the built-in admin!?
2. Look through all the menus, but particularly note System >User Manager, Interfaces, Firewall >NAT and Firewall >Rules, VPN, and Status >System Logs.
3. Note the initial state of the rules for each interface under Firewall >Rules.
4. For an initial task, rename interface `OPT1` to `DMZ`.
5. Now go to Interfaces >WAN, and disable "`Block private networks.`" Normally, you wouldn't want to do this. Why? (Because you don't want to allow requests from the outside world that use IP addresses reserved for local networks. Somebody's confused or up to no good.) In our case, however, we're configuring everything utilizing the 192.168.0.0/16 subnet. Was this necessary? or is it simply an interesting experiment in the power of subnetting?

## 12 Activity: Basic Lockdown of the LAN <>

For the LAN:

- Allow ICMP out;
- Allow DNS access;
- Allow users to browse web pages;
- Allow FTP from the LAN subnet to anywhere;
- Allow SMTP, POP3, and IMAP from LAN subnet to anywhere.

## 13 Challenge 1: Configure the DMZ <>

For the DMZ:

1. Allow ICMP and FTP originating from outside DMZ only;
2. Allow access to your web server, i.e. for requests from the Ubuntu home user, and from LAN users (think intranet site).

**Deliverables:**

1. ICMP and FTP requests originating from inside the DMZ should not work. ICMP requests and FTP requests directed at DMZ nodes from outside should succeed;
2. All requests from outside the DMZ for web pages located on the DMZ web server should succeed.

**Duration: 20-30 min.**

**HINTS:**

1. Let the DMZ respond to ICMP and FTP requests from the LAN and the WAN, but don't let ICMP or FTP requests originate from the DMZ.
2. Start with NAT Port Forwarding.

## 14 Challenge 2: Set up VPN <>

Allow the Ubuntu home user to VPN into the LAN

1. Enable the VPN service using OpenVPN;
2. Configure users for VPN.

**Deliverables:**

1. VPN services should be available for accessing nodes located on the LAN for the user accounts created.

**Duration: 60 min.**

**HINTS:**
You will be using PPTP VPN, take advantage of pfSense logs.

## 15 Conclusion <>

1. There are many types of Network firewalls to choose from. Despite the variety, their core functionality is similar;
2. Firewalls are easy to install and access, but can be relatively difficult to configure for optimal functionality;
3. Through these walkthroughs and hands-on activities, we've learned some basic pfSense configuration.

## 16 Appendix: Solutions and Change Log <

1. Solutions to the challenges:
   (a) Challenge 1;
   (b) Challenge 2.
2. Change Log.

**Solutions to the Challenges:**
**Challenge 1:**

1. Allow ICMP and FTP originating from outside DMZ only:
   (a) Go to **Firewall >Rules**, "DMZ" tab.
   (b) Click on a + button to start a new rule.
   (c) For the rule's settings:
   - Action: **Pass**
   - Interface: **DMZ**
   - Protocol: **ICMP**
   - ICMP type: **any**
   - Source: **DMZ net, "not" checked**
   - Destination: **DMZ net***
   - Log packets: **true**
   - Description: **(A descriptive name)**

   * "DMZ net" specifies any address on the DMZ subnet; whereas "DMZ Address" would specify the DMZ interface of pfSense itself.
   (d) Save and then apply changes.
   (e) Click again on a + button to start another rule.

(f) For the rule's settings:

- Action: **Pass**
- Interface: **DMZ**
- Protocol: **TCP**
- ICMP type: **any**
- Source: **DMZ net, "not" checked**
- Destination: **DMZ net**
- Destination port range: **FTP (21)**
- Log packets: **true**
- Description: **(A descriptive name)**

(g) Save and then apply changes.

(h) At the very least, test that the rule for ICMP works for a computer on the LAN and for a home computer connecting through pfSense's WAN; and that SEED is conversely unable to ping anything.

2. Allow access to your web server, i.e. for requests from the Ubuntu home user, and from LAN users (think intranet site).

(a) Go to **Firewall >NAT**, "Port Forward" tab.

(b) Click on a + button to start a new rule.

(c) For the rule's settings:

- Disable: **unchecked**
- No RDR: **unchecked**
- Interface: **WAN**
- Protocol: **TCP**
- Destination: **WAN net**
- Destination port range: **HTTP**
- Redirect target IP: **192.168.65.2**
- Redirect target port: **HTTP**
- Description: **(A descriptive name)**
- NAT reflection: **Enable (Pure NAT)***
- Filter rule association: **Rule NAT <Description >****

***** For Nat reflection, if you want to enable computers on the LAN to access the DMZ, set it to **Enable (Pure NAT)**. This enables their requests to traverse across interfaces, which is normally not permitted. If you were to wish to block requests from the LAN to the DMZ, set it to **Disable**.

****** This lets pfSense automatically create the corresponding rules that the firewall needs for this to work. Let's make this easy on ourselves!

(d) Save and then apply changes.

(e) Repeat for HTTPS, creating a new rule with all the above settings except selecting **HTTPS** for Destination port range instead.

(f) Test that a home computer connecting through pfSense's WAN and a computer on the LAN, if enabled, can connect to the default site on the SEED server. To do so, simply use the target's IP address (rather than any website name, to avoid setting up DNS or modifying Hosts files).

But what is the actual target whose IP address you need to send the request to? It's 192.168.4.2, the WAN interface of pfSense itself. Why?

**Challenge 2:**

1. Go to **VPN >PPTP**.
2. Click "Enable PPTP server".
3. Enter a **Server address**, 192.168.64.127
4. Enter a **Remote address range**, 192.168.64.128
5. Enter the Windows Server address in **PPTP DNS SERVERS** 1st slot, 192.164.64.2
6. Click "Require 128-bit encryption"
7. "Save" your entries.
8. Navigate to "Users" tab to create a VPN user.
9. Select the icon to create a new user.
10. Enter the desired "username" and "password".
11. Save and then apply changes.
12. Next navigate to **Firewall >Rules**.
13. Select the "PPTP VPN" tab.
14. Select the "Create a new rule icon".
15. For the rule's settings:
    - Interface: **PPTP VPN**
    - Protocol: **TCP**
    - Source: **any**
    - Destination: **LAN net**
    - Destination port range: **any**
    - Log packets: **true**

- Description: **(A descriptive name)**

16. Save and then apply changes.
17. On the Ubuntu Client:
    (a) Open the Network Settings
    (b) Select the + icon in the lower left pane to create a new connection.
    (c) Interface should be VPN. >"Create".
    (d) Select the no longer secure PPTP as the connection type >"Create".
    (e) Enter the IP address of the pfSense WAN for the gateway, 192.168.4.2
    (f) Enter the user name you created in pfSense.
    (g) Change IPv4 settings method to "Automatic(VPN) addresses only".
    (h) Select **Advanced**.
    (i) in addition to the current settings select "Use Point-to-Point encryption (MPPE)".
    (j) Select 128-bit security and "Allow stateful encryption".
    (k) Save and attempt to connect.

**Change Log:**

| Ver. | Date | Authors | Changes |
|---|---|---|---|
| v1.0 | Mar 03rd 2017 | Gabe Gibler & Colton Hotchkiss | First draft of tutorial. |
| v1.1 | May 10th 2017 | Gabe Gibler & Colton Hotchkiss | Changed to CC-ByNCSA license. Made introductory sections consistent among tutorials. Added the network diagram. Added in the news section. |
| v1.2 | May 12th 2017 | Gabe Gibler & Colton Hotchkiss | Making body styles consistent among tutorials. |
| v1.3 | July 22nd 2017 | Ananth Jillepalli | Standardization (network layout diagram, edits, consistency, TeX markup cleaning, and more). |

# References


[1] Cynet, "Firestorm: Severe security flaw discovered in next generation firewalls," 2015. [Online]. Available: https://www.cynet.com/blog-firestorm/

[2] Edward Kovacs, "Firewall vendors analyze exploits leaked by shadow brokers," 2016. [Online]. Available: http://www.securityweek.com/firewall-vendors-analyze-exploits-leaked-shadow-brokers

[3] Lucian Constantin, "Critical vpn key exchange flaw exposes cisco security appliances to remote hacking," Feburary 2016. [Online]. Available: http://www.pcworld.com/article/3032497/critical-vpn-key-exchange-flaw-exposes-cisco-security-appliances-to-remote-hacking.html

[4] University of Houston, "Firewalls, intrusion prevention and vpn," 2016. [Online]. Available: http://prtl.uhcl.edu/info-security/indepth/firewalls

[5] Zen Internet, "Stateful vs deep packet inspection," 2017. [Online]. Available: https://www.zen.co.uk/business/broadband/business-broadband/stateful-vs-deep-packet-inspection.aspx