pfSense Training Course

https://agix.com.au

AGIX

Introduction

The trainer

Andrew Galdes, owner of AGIX, a cybersecurity and open source support business based in Australia. Andrew's history includes achieving RHCE (Redhat Engineer), Cisco certified, Security certified (Security+, CySA+ and CASP+). AGIX is a Netgate (pfSense) partner.

Resources:

1. Find out about AGIX at "https://agix.com.au".
2. Find the videos on youtube at: https://www.youtube.com/user/andrewgaldes
3. Find this course material at: https://shop.agix.com.au/pages/tutorial-and-explanatory-videos

Course scope

Getting started with pfSense, firewall management, Remote Access VPNs, Site to Site VPNs, GEO filtering, DNS filtering, VLANs, network services, high availability, multi-wan configuration and troubleshooting.

Course Material and Help

Learn how to contact the trainer and other students for help getting started, understanding the content and furthering your education.

Resources:

1. Email: pfsense-course@agix.com.au
2. Discord: https://discord.gg/yWbjTVrN
3. Videos: https://shop.agix.com.au/pages/tutorial-and-explanatory-videos

Tips

Consider the following tips to help you get the most out of this course:

1. Be patient. When starting out with firewalling or using a new product, you might get frustrated, angry or upset that things aren't working as you'd expect. The trainer is here to help. You can ask questions. Just try first. Have a go and expect to fail the

first few times. You will get there if you keep at it. We all start from nothing and learn from there.
2. Watch the context videos before the lab videos. Most topics start with a short video to give you context. The lab videos are carefully made to be short, to the point and skip explanations. This allows you to follow them without getting bogged down in details. But if you need details, refer to the context videos. The context videos are where the trainer spends time to explain concepts.
3. Spend some time to get your lab ready. The trainer doesn't provide a download for this. It's simply too difficult to do given how much the environment changes to fit the various scenarios. Additionally, the environment is half the challenge. A firewall administrator is also an architect - they must understand the environment that they're working in. Neglecting to learn the environment will likely result in a failed attempt to control access to (and the services within) the network.

Lab Environment

The lab environment used throughout this course was hosted within VirtualBox. However, some labs such as the VLAN Switch-Port lab were based on a real pfSense appliance in a production environment.

The lab can be described as:

1. One VirtualBox host running Windows 10 Pro.
2. Two pfSense appliance guests (within VirtualBox).
3. One ubuntu guest (within VirtualBox) acting as a router.
4. The host is connected to an upstream router allowing the guests to access the Internet.

The lab environment is fluid (changed regularly to fit the lab) and therefore cannot be provided to students. However, support is available to students looking for help setting up a lab.

Tips

When setting up your own environment, consider these tips:

1. Use VirtualBox or any other environment you're familiar with. AWS (Amazon) is another place that would be suitable. However, AWS and other cloud environments may present issues with NAT. VirtualBox is freely available (costs you nothing), easy to install and there is plenty of support available.
2. Design your environment on paper first. Make sure you have it well designed with subnets, routing, the Internet, etc all considered. That will save you plenty of time later if your design is inadequate.

3. Install one pfSense appliance and then duplicate/clone it so you have two identical. Then configure their network settings independently of each other (eg, they need their own IP addresses, etc).
4. Consider creating a “router” virtual machine that connects to both your primary and secondary pfSense appliances. Make sure the router isn’t blocking traffic between your pfSense appliances.
5. Remember that you will experience problems with your lab. That’s part of learning. Even the instructor had problems and had to try and retry different setups to get the labs to work properly. It’s all part of learning.

First time with pfSense

What is pfSense?

pfSense is a firewall based on FreeBSD. pfSense is open source and was started in 2004. It’s available as a physical appliance from Netgate or Virtualized in the cloud or locally run on your own hardware or virtual infrastructure. pfSense is supported and distributed by Netgate in the US with partners (like AGIX) around the world. The prefered management method is via the web console but can be managed using the command line too. pfSense is expandable with plugins that extend the functionality of the firewall. The pfSense community is active and discussed across multiple platforms such as Reddit and Netgate’s community forums.

The Dashboard

When you log into pfSense, you’re presented with the Dashboard. The Dashboard can be customised with tiles to present various details such as interface status, network bandwidth usage, error logs, and more. This topic demonstrates how to manage the Dashboard.

Resources:

1. Video: Learn to Configure the Dashboard on pfSense 21.x
    a. https://youtu.be/FuhhHtimt68

Themes

pfSense supports themes. This is not a functional topic but it helps you customise the pfSense experience for yourself. Additionally, you can set the theme of different pfSense appliances that you manage to help you quickly identify which appliance you're managing at the time.

Resources:

1. Video: Learn how to use Themes with pfSense 21.x
    a. https://youtu.be/LgooCwLC4rQ

System Maintenance

Backup and restore

pfSense allows you to download a backup file in XML format. The backup can be uploaded later to restore back to the point when the backup was taken. You can also revert back to a point in time using the (automatically generated) backups that pfSense takes for you. Learn how to take a backup and restore from it.

Resources:

1. Video: Learn Backup and Restore pfSense 21.x
    a. https://youtu.be/CtBu_j6Nyz4

Reboot pfSense

This is a quick video that shows the console of a pfSense appliance as it reboots. You'll see the text-based information stream up the screen and end with a menu allowing you to manage the device.

Resources:

1. Video: Learn Backup and Restore pfSense 21.x
    a. https://youtu.be/CtBu_j6Nyz4

Troubleshooting

pfSense is a complete operating system. It has the tools that you'd expect from an operating system such as ping, trace-route, ifconfig, netstat and more. There may come a time when you need to recover from a bad firewall design (locking you out) or a corrupt hard disk (it's a computer and it has a hard disk) that can only be fixed by using the command line tools. Learn how to access the console using a USB-to-Mini-USB console cable or a virtual machine console.

Resources:

1. Video: Learn to use the Console on pfSense 21.x
    a. https://youtu.be/hdBAcWwI1BY

Certificates

Managing certificates

Learn how to create a certificate authority (CA) and then create server certificates signed by the CA. This is necessary for VPNs and SSL/TLS termination that you may want to create while managing a pfSense appliance.

Resources:

1. Video: Learn Configure the Certificate Authority on pfSense 21.x
    a. https://youtu.be/LM53RRuH9ZA

Reliability and Logging

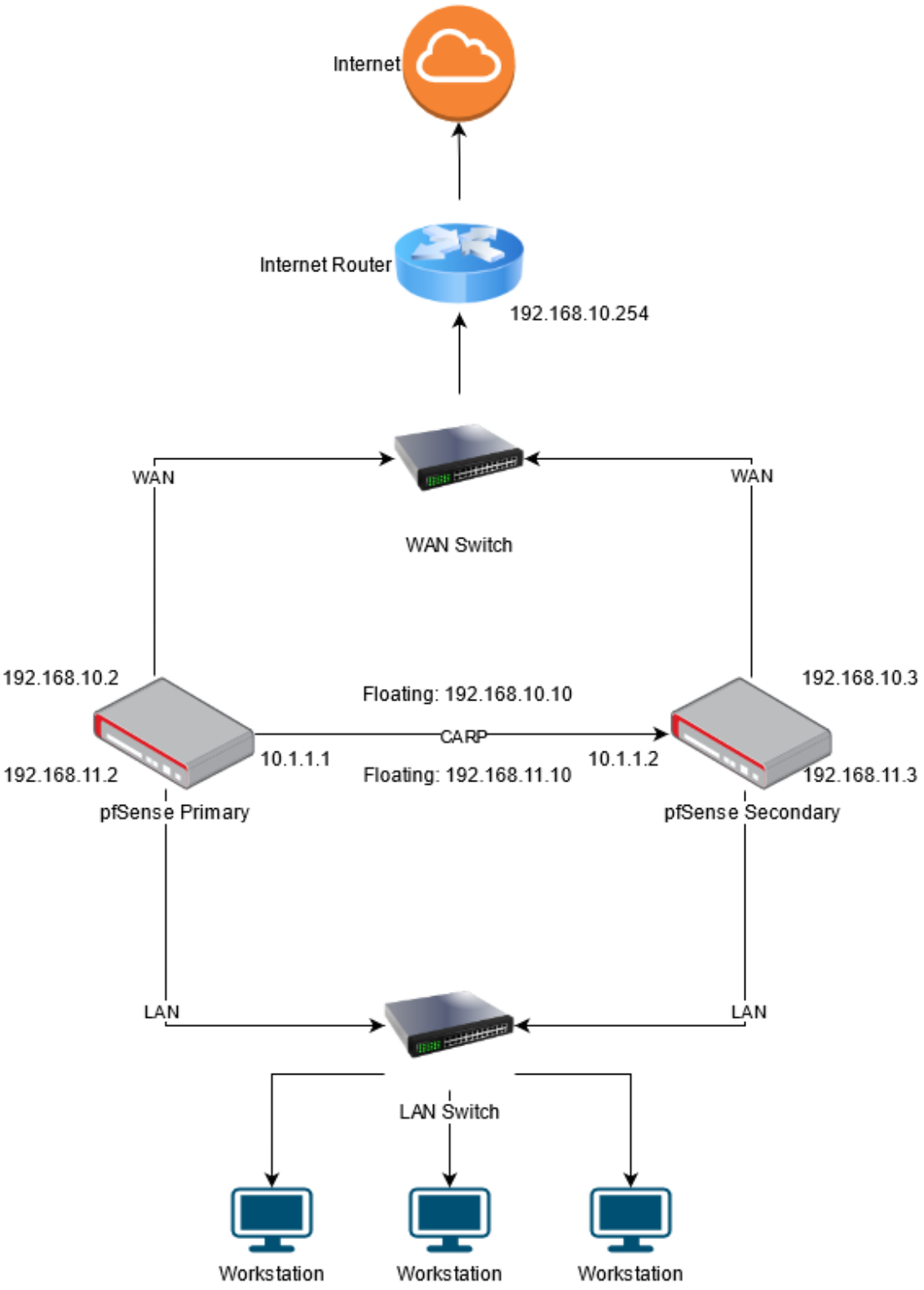
High Availability

pfSense supports a primary/secondary High Availability (HA) configuration. In the event that the primary pfSense appliance fails, the secondary takes over the primary role. The secondary reverts back from primary when the original primary pfSense appliance comes back online.

This (HA) lab environment is complex to create and you might need help from the official Netgate documentation (listed below in the Resources section). However, you're encouraged to try this in your lab. The very experience of designing and implementing this in your lab will be a significant asset in your educational process.

Resources:

1. Video: Learn to High Availability on pfSense 21.x
    a. https://youtu.be/N5DKdLJfTQo
2. Documentation: https://docs.netgate.com/pfsense/en/latest/recipes/high-availability.html
3. Diagram:


Internet
Internet Router
192.168.10.254
WAN
WAN
WAN Switch
192.168.10.2
Floating: 192.168.10.10
192.168.10.3
CARP
10.1.1.1
10.1.1.2
192.168.11.2
Floating: 192.168.11.10
192.168.11.3
pfSense Primary
pfSense Secondary
LAN
LAN
LAN Switch
Workstation
Workstation
Workstation

Remote logging

pfSense supports remote logging using the Syslog protocol. You can configure pfSense to send some or all logs to a centralised logging server such as Syslog, Graylog or any SIEM that supports the Syslog protocol.

Some firewall administrators purchase additional disk space for their pfSense appliance to accommodate large log files. However, they could save that money and simply send the logs to a centralized logging server.

Resources:

1. Video: Learn to Configure Remote Logging with pfSense 21.x
    a. https://youtu.be/s1TF8EmFRQ8

Network Service

DHCP Server

pfSense can be a DHCP server or a DHCP Relay server. But not both at the same time. A DHCP server is required on each VLAN that you create - pfSense can be the DHCP server. However, if you have an Active Directory server on the VLAN, that server should be the DHCP server. If you have a remote office with no Active Directory server on the LAN but one does exist on the head office LAN, and the two LANs are connected by a VPN (Site to Site), you can configure the pfSense (in the remote office) as a DHCP Relay server - therefore the Active Directory server can be a DHCP server for the remote office LAN using the pfSense as the relay.

Resources:

1. Video: Learn to Configure DHCP services on pfSense 21.x
    a. https://youtu.be/kJoGLZ4fF2Q
2. VIdeo: Learn to Configure DHCP Relay services on pfSense 21.x
    a. https://youtu.be/nNKy83xgQlU

DNS

pfSense is often configured as a DNS caching server. In this configuration, workstations on your LAN make DNS requests to the pfSense, which in turn makes a request to an upstream DNS server (such as your ISP or an Active Directory server across a VPN) and then caches the answer for future reference.

Resources:

1. Video: Learn to Configure DNS services on pfSense 21.x
    a. https://youtu.be/SPxeVKWMhFA

Traffic Management

Basic firewalling

pfSense is a stateful firewall. That's a fancy way of saying - pfSense tracks network sessions and can make decisions based on what it knows of the conversation. There aren't really any stateless firewalls these days. pfSense has features that make firewall access control lists (ACLs) simpler, such as Aliases.

Resources:

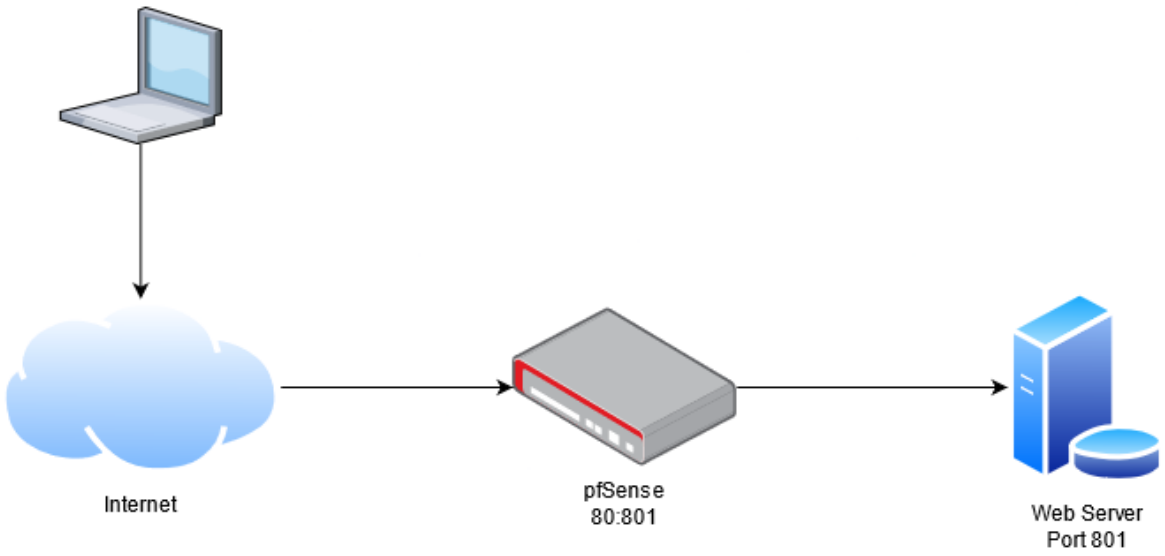
1. Video: Learn to Create Firewalls with Aliases on pfSense 21.x
    a. https://youtu.be/1v_dQjip1LM

Port forwarding

Port forwarding allows you to permit traffic from the Internet to communicate with servers on the inside of your network via the firewall's NAT features. pfSense supports port forwarding and simplifies the management.

Resources:

1. Video: Learn to Configure Port Forwarding on pfSense 21.x
    a. https://youtu.be/Taiz0YEbTAI
2. Diagram:

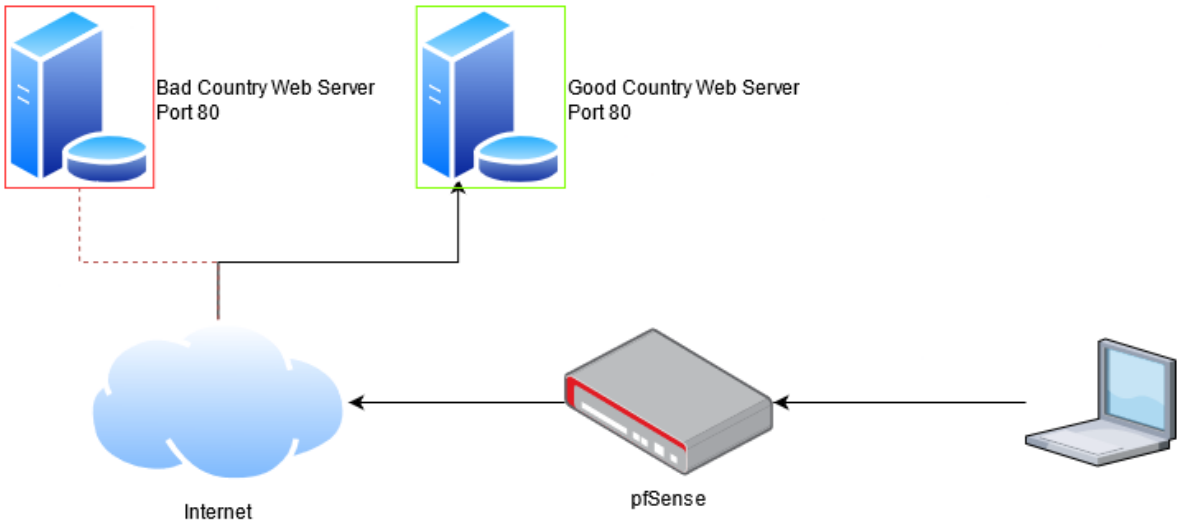


pfBlocker-NG

pfBlocker-NG is a popular add-on for pfSense. It's free (you need a free license) and you can easily install it using the pfSense package manager. Once installed, you can do advanced firewalling such as filtering traffic based on country and filtering DNS based on back or white lists. pfBlocker is an excellent tool to help protect against ransomware by preventing unwanted communications with countries that you don't need to communicate with - thereby preventing malware from communicating back to the criminals. Additionally, back-door software (malware) that would otherwise allow remote attackers to plant spyware on your network would not be able to receive communications back as the firewall would block it - if the attacker is in a blocked country.

Resources:

1. Video: Learn to Configure pfBlocker-NG on pfSense 21.x
    a. https://youtu.be/OQEt2ciWvgE
2. Diagram:



Captive portals

pfSense supports captive portals. Captive portals allow you to prevent people from surfing the web until they meet certain conditions such as agreeing to your terms and conditions or providing valid credentials. Hotels and schools often use this facility.

Resources:

1. Video: Learn to Configure a Captive Portal on pfSense 21.x
    a. https://youtu.be/aZUrpWWrKoo

HAProxy

HAProxy is the de facto standard for load-balancing technology. It allows you to create a cluster of web servers (for example) and make them available to the Internet as a single server. HAProxy also allows you to terminate the SSL/TLS connection which simplifies your back-end server management. The lab in this course is simplified but you can use the documentation (tutorial) in the Resources section to go much further if you are interested to learn more. HAProxy can be installed as an add-on using the pfSense package manager.

Resources:

1. Video: Learn to Configure HAProxy on pfSense 21.x
    a. https://youtu.be/VEx4AVogXCU
2. Documentation: https://www.agix.com.au/configure-haproxy-on-pfsense-with-letsencrypt-ssl-https-termination/

Network Management

Multi-WAN

Some organisations have multiple Internet connections (Multi-WAN) for one of two reasons; first, they might want to load-balance to increase total bandwidth. Or second, they might want to have a secondary Internet connection just in case the primary goes down. pfSense supports this in both modes.

Resources:

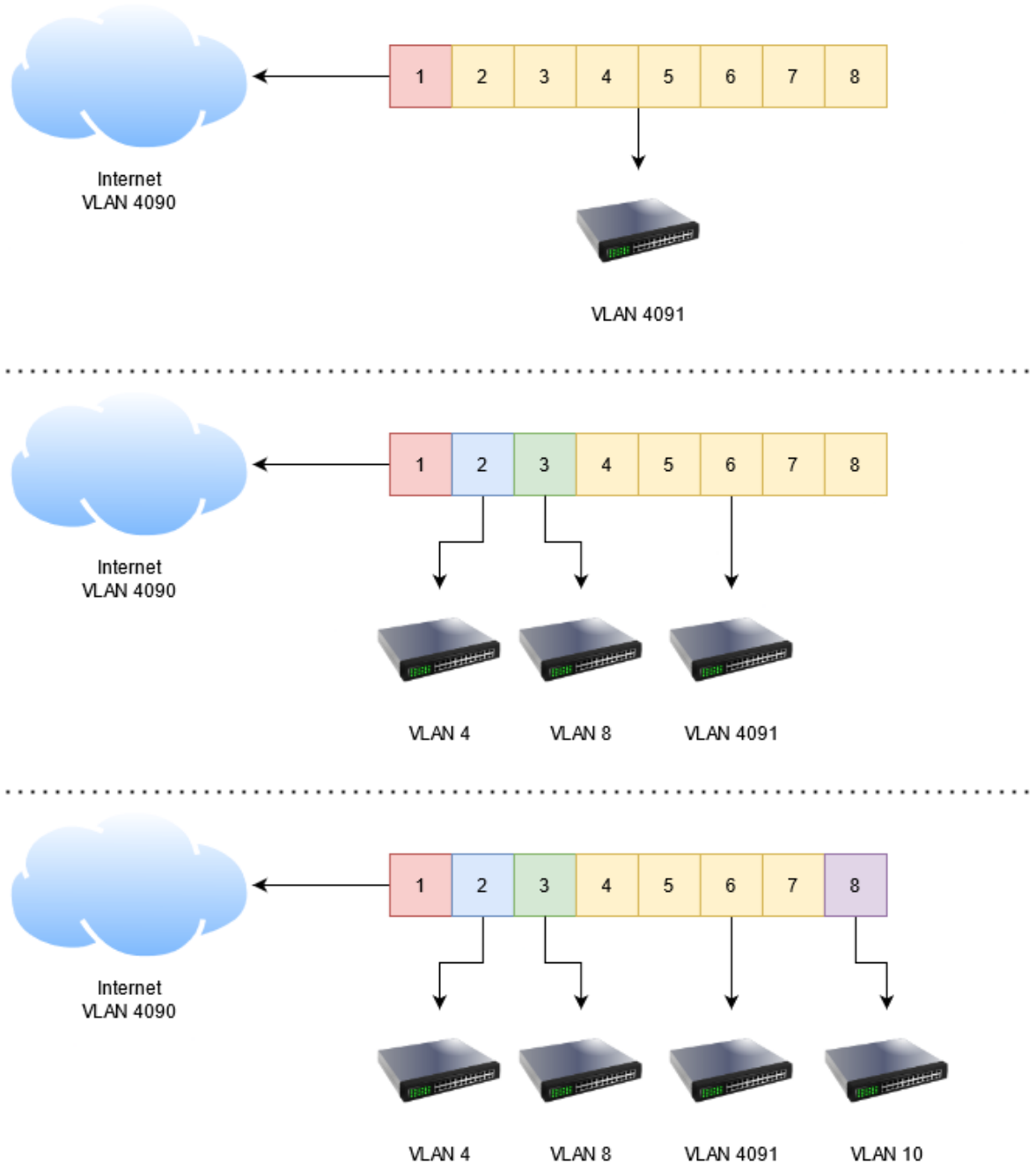
1. Video: Learn to Configure Multi-WAN on pfSense 21.x
    a. https://youtu.be/T0kQMB-mMNc

VLANs (switch-port tagging)

pfSense supports trunking and switch-port VLANs. This lab demonstrates assigning an Ethernet port on the pfSense appliance to a VLAN. Using VLANs, you can segment the network and keep different departments or companies from communicating with each other. You can even allow different VLANs at different speeds to and from the Internet. We have a lab for that (traffic shaping) in this course.

Resources:

1. Video: Learn how to configure VLANs with pfSense 21.x
    a. https://youtu.be/izmJtNQuzNs
2. Diagram:



Traffic Shaping

pfSense allows you to limit the speed (to and from the Internet) for different VLANs. This is useful when you want to allow one department (or company) faster Internet access than another.

Resources:

1. Video: Learn Traffic Shaping with pfSense 21.x
    a. https://youtu.be/72wFjU-wuAM

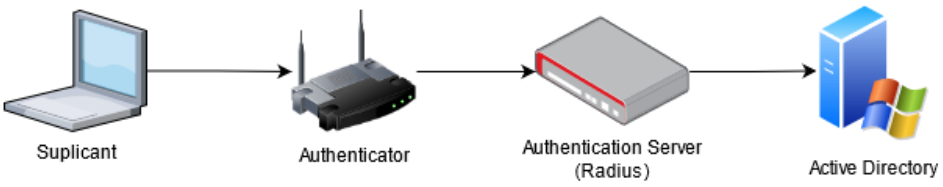
Remote Access

Radius

One of the most commonly used (and old) authentication protocols for remote authentication is Radius. Radius stands for “Remote Authentication Dial in User Service”. It’s a well supported means for devices to authenticate back to a central authentication server. Consider the diagram below in the Resource section: The user with a laptop wants to connect to the WIFI. The user's computer discovers the network and the user submits their credentials to the Access Point (AP). The AP sends the users credentials to the Radius server (Authentication server) which then forwards the credentials to the Active Directory (AD) server. If the user’s credentials are correct (according to the AD server), the Radius server will send back an “Accepted” message to the AP which then permits the user to join the WIFI.

Resources:

1. Video: Learn to Configure Radius on pfSense 21.x
    a. https://youtu.be/77vW9V6-224
2. Diagram:



OpenVPN

pfSense supports OpenVPN for both Remote Access VPNs (remote workers) and Site to Site VPNs. OpenVPN was initially released in 2001. It uses the OpenSSL libraries. It’s supported (through addon software) on Mac, Windows and Linux and IOS and Android devices. It can support 2FA provided that the authenticator (Radius) supports it. However, in its simplest form, it can authenticate users against the pfSense’s internal user database or use SSL certificates and/or PSK (pre-shared keys).

OpenVPN Remote Access

In this lab, we will create a Remote Access VPN which could be used to allow remote workers to access the corporate network while on the road or from home.

Resources:

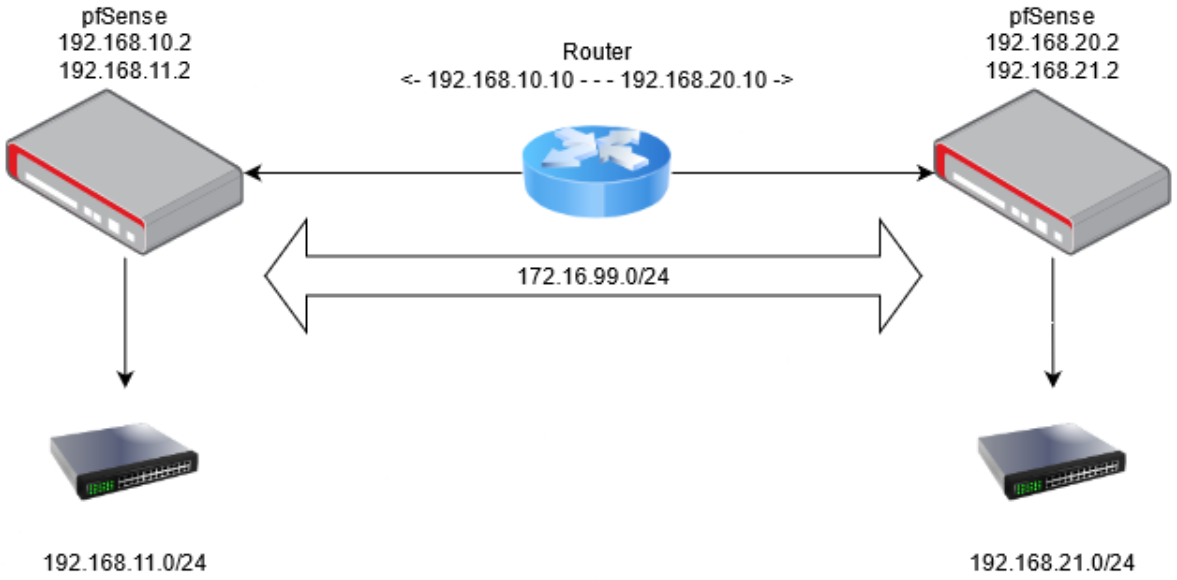
1. Video: Learn how to configure OpenVPN Remote-Access VPNs with pfSense 21.x
    a. https://youtu.be/QLyMAtVxcTY

OpenVPN Site to Site

In this lab, we will create a Site to Site VPN which could be used to join two geographically separate networks together. Unlock IPSec, OpenVPN relies on the server/client model. Ie, one side is the server, and the other is the client.

Resources:

1. Video: Learn how to configure OpenVPN Site-to-Site VPNs with pfSense 21.x
    a. https://youtu.be/oEANSHefFiM
2. Diagram:

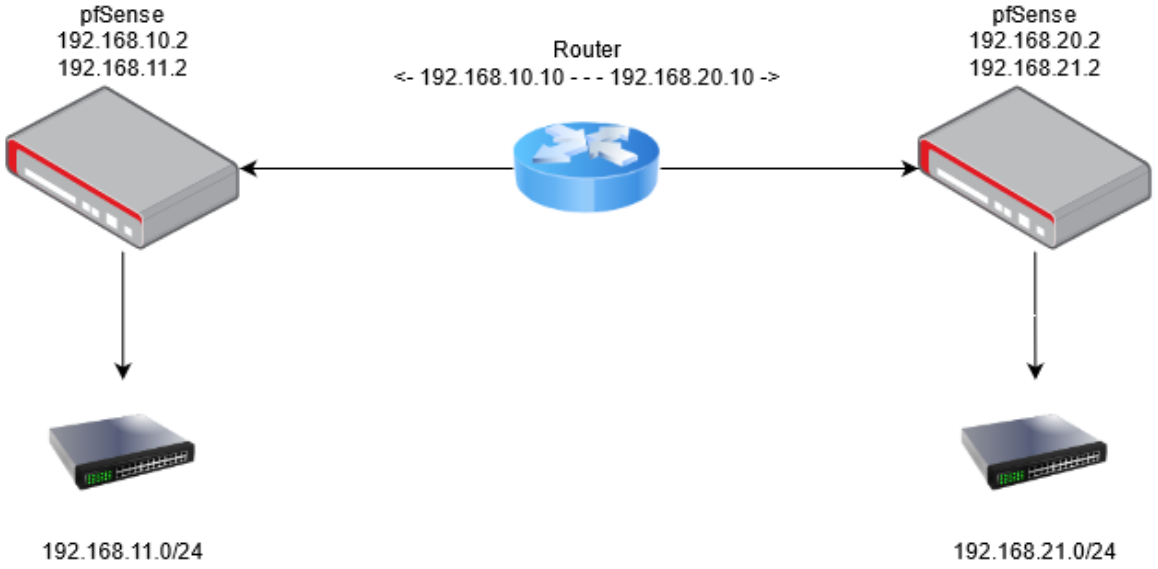


IPSec

pfSense supports IPSec. IPSec has been around since the early 90's. It's a suite of security tools. It works in both Tunnel mode and Transport mode. Tunnel mode is the Site to Site VPN mode. Transport mode is used to secure transmission between two or more computers on a LAN. IPSec is probably the most common Site to Site VPN technology in use today.

Resources:

1. Video: context-ipsec
    a. https://youtu.be/SqiCdg4RB8U
2. Diagram:



IPSec Site to Site

In this lab, we create a Site to Site VPN which could be used to join two geographically separate networks together. Unlock OpenVPN, IPSec doesn't rely on a server/client model.

Resources:

1. Video: Learn to Configure IPSec on pfSense 21.x
    a. https://youtu.be/SqiCdg4RB8U

Summary

Course summary

This course has taken us through all major topics that I (the trainer) deal with on a daily basis. There's plenty more that a pfSense firewall can do, but what you've learned in this course is most of what you'll need to do as a firewall administrator.