Cyber Defense Organization

Fall 2018 - Firewalls

Goals

1. Introduction to Pfsense Firewalls and rule creation
2. Basic firewall concepts
3. Introduction to hardening

I know who's got my vote!

About Me

- Jonathan Matza
- Sophmore majoring in Digital Forensics and Accounting
- IT-CTO

What are firewalls

- The gods of the network
- Filters outgoing and ingoing packets based on a set of rules
- Most firewalls double as a router

What we will be using

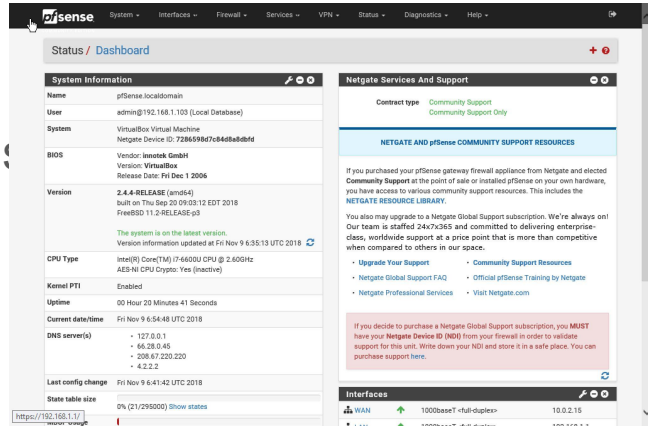
- Open Source, FreeBSD firewall called pfsense
- Extremely versatile
- Command shell is kind of like linux (a couple of different commands)

Start those VMS!

- Open up firewall workshop and firewall workshop 2 (windows server and pfsense)
- Password (for windows): bb123#123
- Pfsense webgui: username: admin password: pfsense
- Why did I choose windows to connect to firewall?

WebGUI

- The place to go to more easily navigate the firewall
- Uses
  - Rule Creation
  - User management
  - Package installation
  - Log analysis
  - Much More
- How do you access the web gui?
- Important tabs: System, Firewall, and status
- Default gateway: Destination of all traffic that is not s
  on the same network as the sender



Hardening using the web gui

- Big problem: password protection for firewall shell is not a default
- What users are on your firewall
- Analyzing logs helps with:
  - Knowing who is logging into your firewall (including the ip address)
  - Knowing what changes were implemented on firewall
  - Traffic the firewall rules deny

ANY QUESTIONS??

White lists vs black lists

- White lists: Only allow traffic that is explicitly allowed
- Blacklists: Allows all traffic unless it is explicitly blocked

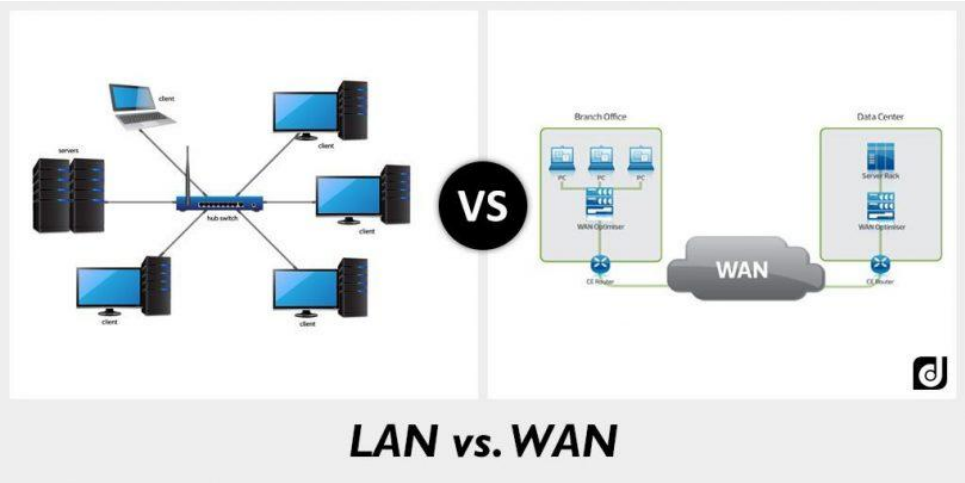
Blacklisting

Whitelisting

	Pros	Cons
Blacklists	• Scale • Quick to deploy	• Quickly out of date • Resource intensive • Will eventually fail to protect
Whitelists	• Every site is vetted • Safer • Less frequent updates	• Every site needs to be vetted • Scale

Lan vs Wan

- Lan: local area network: think of the room your in
- Wan: wide area network: internet is one big wan



Rule Placement

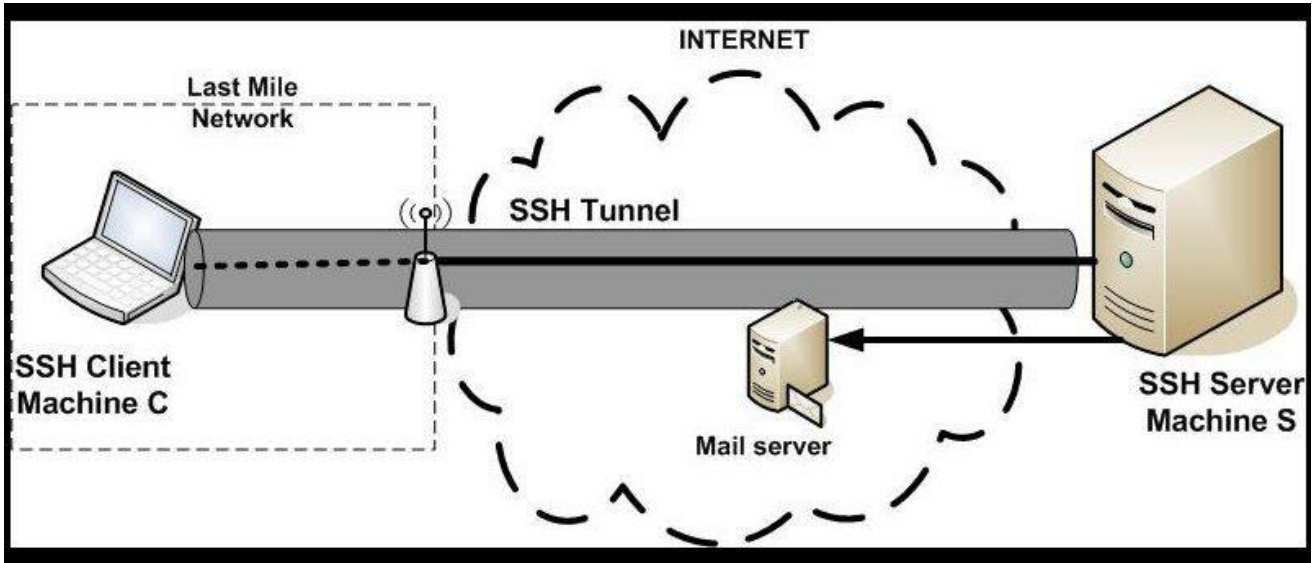
- Think of where traffic originates
- What is an example of Lan? Wan?

Order of precedence

- The order in which firewalls read rules
- Goes first to last
- Example of firewall without order of precedence: Windows Defender

SSH rule Creation

- Lets allow the default port of ssh from all computers
- What is a port? - Think of it as a unique ID # of a service
- What is ssh (Secure Shell)- think remote access
- Default port: 22

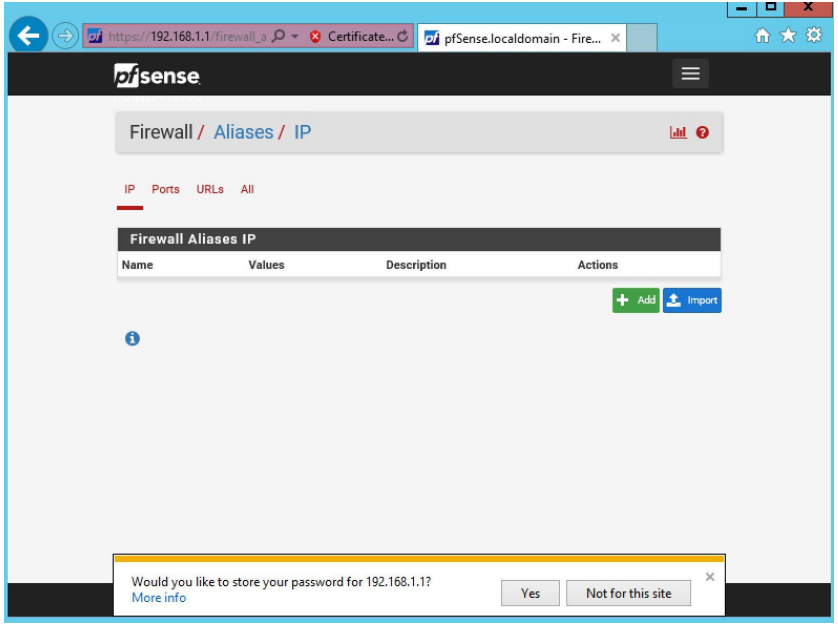


Let's create the core rule for a whitelist

- The deny any any rule!
- Why doesn’t this overrule your allow rules?
- Always put on bottom (order of precedence)

Aliases

- Allows you to incorporate multiple ports, Ip addresses, etc into one rule
- Good for organization
- Follow along while I create an alias for the internet



ANY QUESTIONS??

Do it yourself!

- Allow these services:
  - Pop (hint there are two)
  - IMAP (hint there are two)
- I didn’t give you the ports: Google it!

If we have time

- Lets block a website
- Situation: people are constantly going on reddit at work
- How do we solve that? Firewall rules!
- Disclaimer: There are better ways than firewall rules to do this

reddit

Cya Next week!

Thank you to everyone who filled out the survey!

We made a discord! Keep an eye on email.

Follow us on Twitter? Add on myInvolvement?

Email us if you have an idea for the sweatshirt design!

CCDC! - Monday 7:30

BB123 (Check email).

The Cloud

- **Friday 3pm BB123**