

IASA 9/27/19 - Firewalls!

Don't forget to sign in 😊

Agenda



1. Sign in, get pizzas
2. Go over quickly how firewall rules work
3. See some firewall setup in Linux
4. See firewall setup in Windows

Note: Commands are now in **orange** text 📡

Firewall Concepts 🔥

- Firewalls control network traffic in and out of a device
- Can be local software based or physical network devices
- Some routing
- Rules go in chronological order
- Interface with the core (kernel) of the OS

What is the Kernel of an OS?

So "the kernel" of an operating system is the **minimum needed to run the various hardware**, the minimum needed to get programs into and out of memory, and the minimum needed to let programs ask the kernel to operate the hardware for them (instead of needing the programs to operate the hardware themselves).

https://www.reddit.com/r/explainlikeimfive/comments/5u2nkx/eli5_what_is_a_linux_kernel/

Firewall Concepts (cont) 🔥

- Example of a rule:
 - **ALLOW ANY ANY**
 - **DROP ANY ANY**
- Why is this a bad rule?

IPTables

1. Advantages

- a. **Extremely** versatile
- b. Closest kernel-level control you can get
- c. Extensive documentation and examples
- d. Can become Linux Kernel Firewall Jedi if you master IPTables 🙏

2. Disadvantages

- a. Complex
- b. No GUI
- c. Not forgiving

Using IPTables

- **NOTE:** Because you are working directly with the Linux Kernel, all commands need to be run as **sudo**
- You can check if **iptables** is installed by typing
 - *which iptables*
 - You should get something like */sbin/iptables* or */usr/sbin/iptables*
 - This means the actual application is in the */sbin/* directory
- Also **NOTE:**
 - Iptables rules are **ephemeral**, which means they **need to be manually saved** for them to persist after a reboot.
 - Install **CLEAN** persistent IPTables:
 - *sudo apt-get remove iptables iptables-persistent*
 - *sudo apt-get install iptables iptables-persistent*

Using IPTables

- How to check current rules?
 - **sudo iptables --list**
 - Remember, to use sudo if you see something like this:

```
cmeyer25_emich_edu@ubuntu-east-1:~$ iptables --list
iptables v1.6.1: can't initialize iptables table `filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
cmeyer25_emich_edu@ubuntu-east-1:~$ █
```


Using IPTables

- IPTables

Components

- **INPUT = Inbound**

Connections

- Ex. I ssh to your box

- **FORWARD = For packets**

Not destined for you device, but are passing through it. Think like a middleman rule, like a mini router.

- **OUTPUT = Outbound**

- I wanna go to facebook and watch cat videos





```
cmeyer25_emich_edu@ubuntu-east-1:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
```

Blocking Incoming IP Addresses

- Have the person next to you run check the External IP of their VM, and have them ping your external IP. It *should* work.
 - **ping 35.243.245.42**

Filter VM instances							Columns
<input type="checkbox"/> Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect	
<input checked="" type="checkbox"/>  ubuntu-east-1	us-east1-b			10.142.15.213 (nic0)	35.243.245.42	SSH	⋮
<input type="checkbox"/>  ubuntu-east-2	us-east1-b			10.142.15.212 (nic0)	35.185.81.165	SSH	⋮
<input type="checkbox"/>  ubuntu-east-3	us-east1-b			10.142.15.211 (nic0)	35.231.251.43	SSH	⋮
<input type="checkbox"/>  ubuntu-east-4	us-east1-b			10.142.15.214 (nic0)	35.231.38.222	SSH	⋮

Blocking Incoming IP Addresses

- To DROP an incoming IP address:
 - `iptables -A INPUT -s IP.Address.Here. -j DROP`
- Example, blocking Inbound Google DNS
 - `iptables -A INPUT -s 8.8.8.8 -j DROP`

Breaking down the command

- **iptables -A INPUT -s 8.8.8.8 -j DROP**
- **iptables**
 - The program you are using
- **-A**
 - Append argument. This will add the rule to the bottom of your rule list
- **INPUT**
 - Setting this to the **INBOUND** chain
- **-s**
 - Add IP address to the chain. This is the “what” we’re working with

Breaking down the command

- **iptables -A INPUT -s 8.8.8.8 -j DROP**
 - 8.8.8.8
 - IP address or range of IP addresses you want to interact with
 - -j DROP
 - Specifies what to do with the IP address. Here, we are saying to DROP, or discard the packet.
- This means that **ANY incoming** connections from **Google's DNS** will be **DROPPED**

Verify The Rules Were Applied

- **iptables --list**
 - This will list all current rules
- If you see the rule, you now need to **SAVE** the rule
 - **sudo iptables-save**
 - **/etc/sysconfig/iptables**
- Now have your friend **ping** your IP address again
 - If you did this properly, they should not be able to ping it anymore

```
cmeyer25_emich_edu@ubuntu-east-2:~$ sudo iptables-save
# Generated by iptables-save v1.6.1 on Fri Sep 27 19:06:08 2019
*filter
:INPUT ACCEPT [486:40838]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [324:33408]
:sshguard - [0:0]
-A INPUT -j sshguard
-A INPUT -s 8.8.8.8/32 -j DROP
COMMIT
# Completed on Fri Sep 27 19:06:08 2019
cmeyer25_emich_edu@ubuntu-east-2:~$
```

Why this is so important

1. This is one of the most rock-solid ways to secure a device
 - a. If you cannot communicate with a device, you can't really exploit it...
2. Consistent
 - a. Installed on **MOST** Linux distros across the board
 - b. Commands are extremely similar if not the same no matter which OS
3. Can be scripted!
4. Very good skill to know

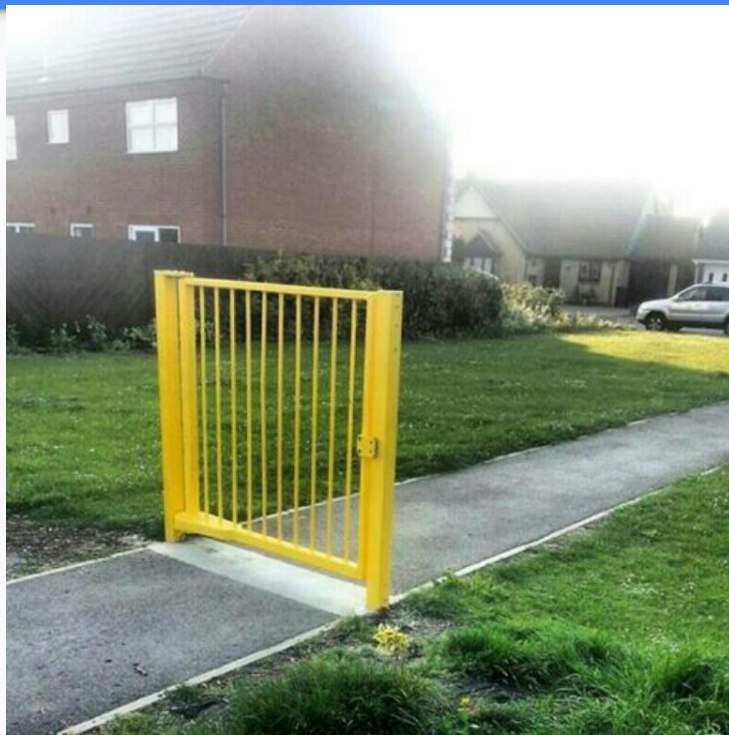
Windows Firewall

Why use Windows Firewall?

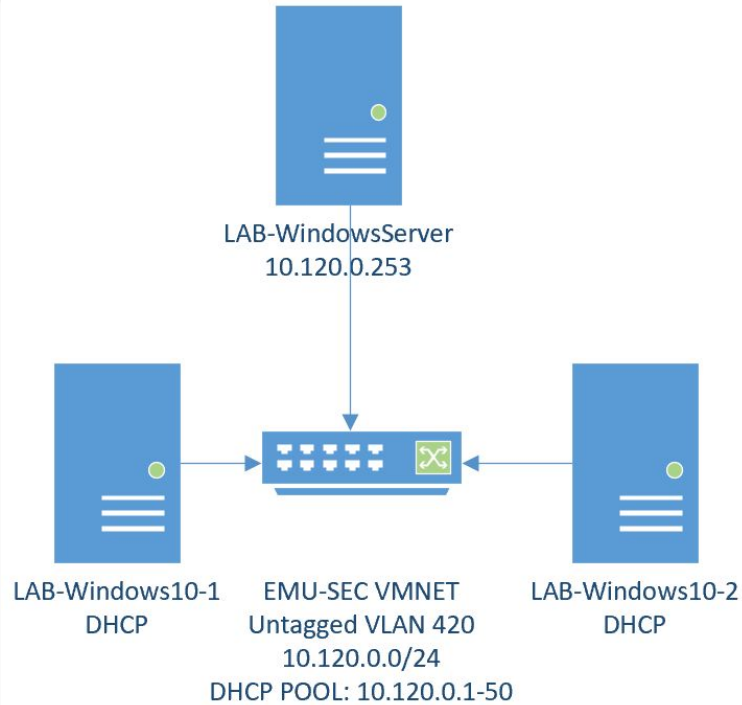
- It's Free
- It's pre installed and useful in environments you don't have network access
- *It's better than nothing*



In-Production Deployment



Demo Topology



Types of Windows Firewall

Domain Networks - This setting is applied when the computer is connected to a domain controller, which is controlling a Windows domain.

Private Networks - This setting is applied when a connection to a network for which the computer's account is not associated with. This can be a different domain or home network. A computer can only be joined to one domain at a time, so if the computer is not joined to the Domain network, it can only be joined to a Private or Public network. It is suggested that the Private network profile of settings be more restrictive than the Domain network profile of settings.

Public Networks - This setting is applied when a connection to a domain is made through a public network, such as at an airport, hotel, or coffee shop. Since the security of these networks is unknown and not really controlled by the user running the computer, it is suggested that the Public network profile of settings be more restrictive than either the Domain network or Private network.

Why Deploy With Group Policy

- Base Security Template can be deployed quickly
 - Time is valuable in competition environments
- Malicious IPs can be blocked on any joined machine quickly.
 - Reduces time, eliminates the need to login to every box

Where do I deploy this?

In Windows Server 2003, 2008, 2012, 2016, 2019 You can find the GPO object Here:

Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security

Demo