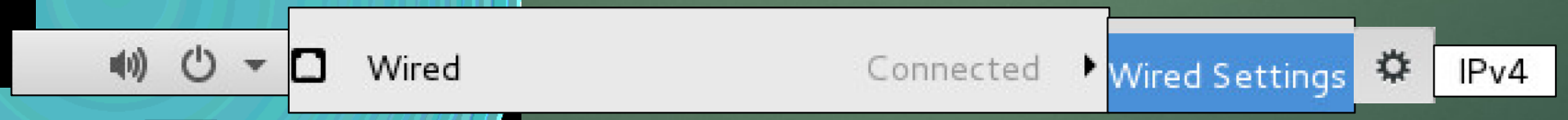
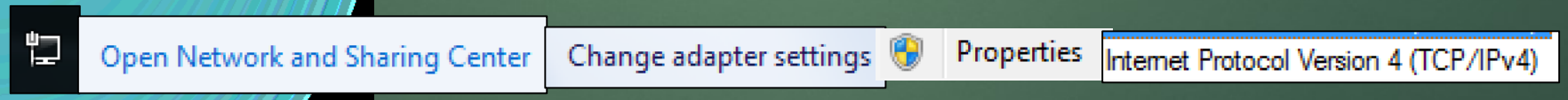
Networking Exercise

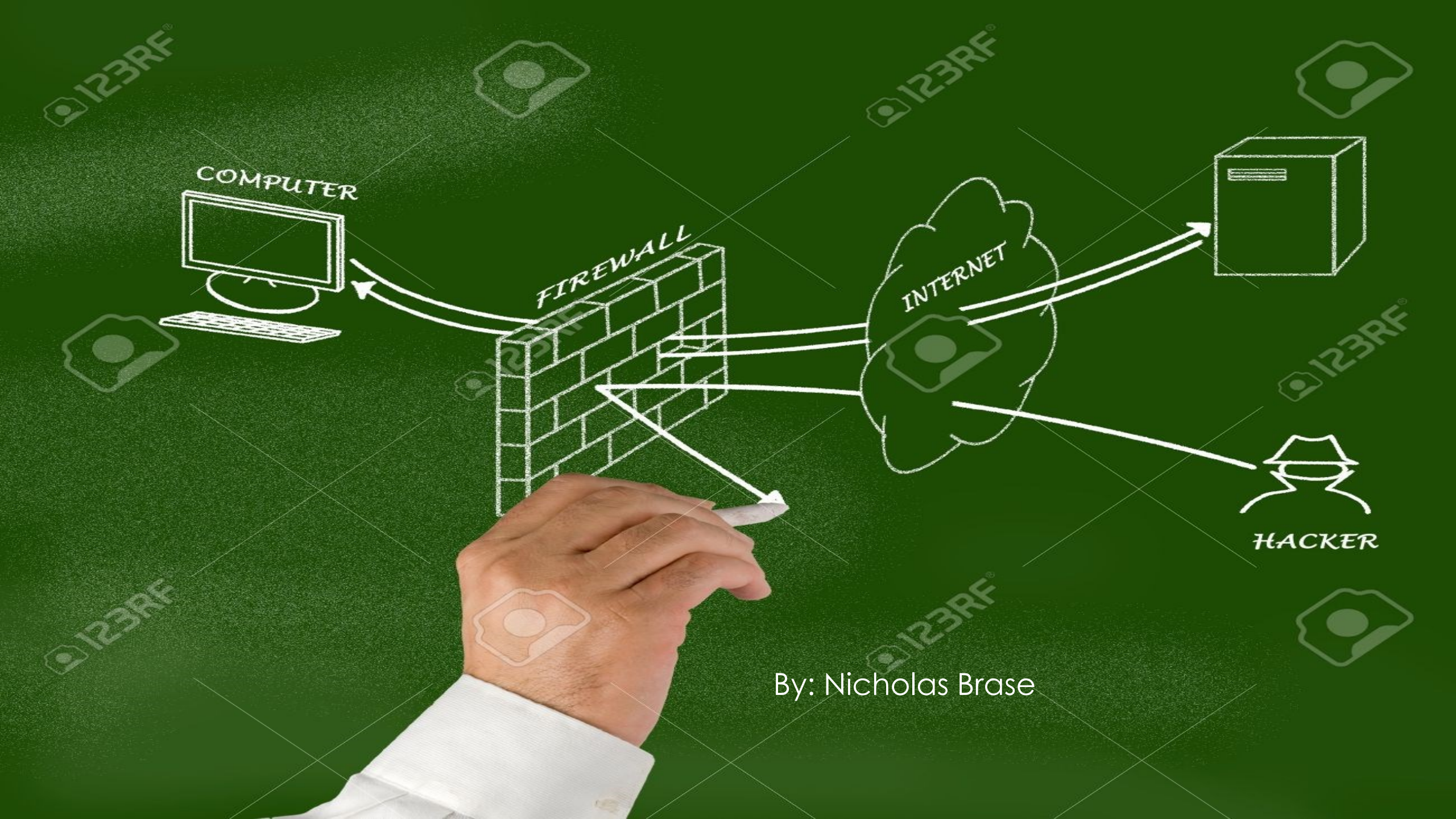
- Currently: 10.42.X.X
- pfSense: 10.42.X.1
- Linux Server: 10.42.X.3
- Ubuntu ClientA: ~~10.42.X.2~~ → 10.42.X.110
- Ubuntu ClientB: ~~10.42.X.2~~ → 10.42.X.111
- Windows Server: 10.42.X.4
- Windows ClientA: ~~10.42.X.5~~ → 10.42.X.120
- Windows ClientB: ~~10.42.X.5~~ → 10.42.X.121

Linux:



Windows:

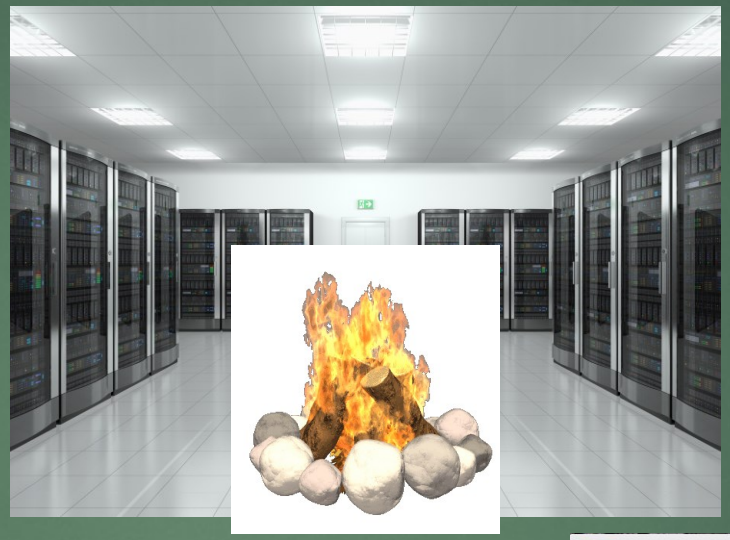


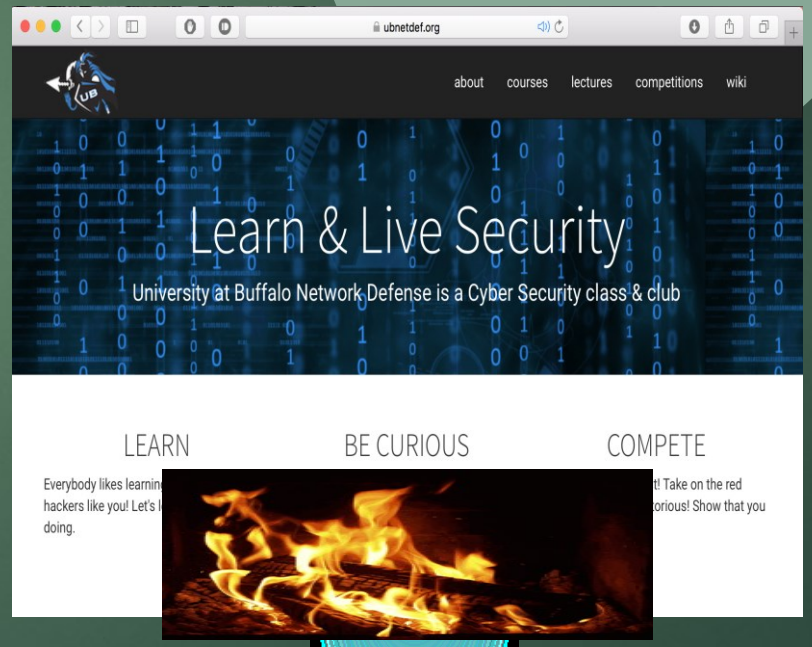


By: Nicholas Brase

Power of Firewalls

- What they do:
  - Block Fires in a network
- What type of fires:
  - Hackers
  - Websites





What happens without them?

- Things burn down
- People get annoyed

```
[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain (Mon Mar  6 17:10:34 2017):

dank memes

[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain (Mon Mar  6 17:10:42 2017):

dank memes

[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain (Mon Mar  6 17:10:49 2017):

dank memes

[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain (Mon Mar  6 17:11:38 2017):

dank memes

Broadcast message from SysSec@localhost.localdomain (Mon Mar  6 17:11:44 2017):

dank memes
```

Types of firewalls

- IP tables --linux

```
[root@node01 ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.21 on Tue Apr 28 18:41:14 2015
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [262:28166]
-A INPUT -p tcp -m state --state NEW -m tcp --dport 7790 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 7789 -j ACCEPT
-A INPUT -m addrtype --dst-type MULTICAST -j ACCEPT
-A INPUT -p igmp -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 2224 -j ACCEPT
-A INPUT -p udp -m state --state NEW -m multiport --dports 5404,5405 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Tue Apr 28 18:41:14 2015
[root@node01 ~]#
```

http://www.tecmint.com

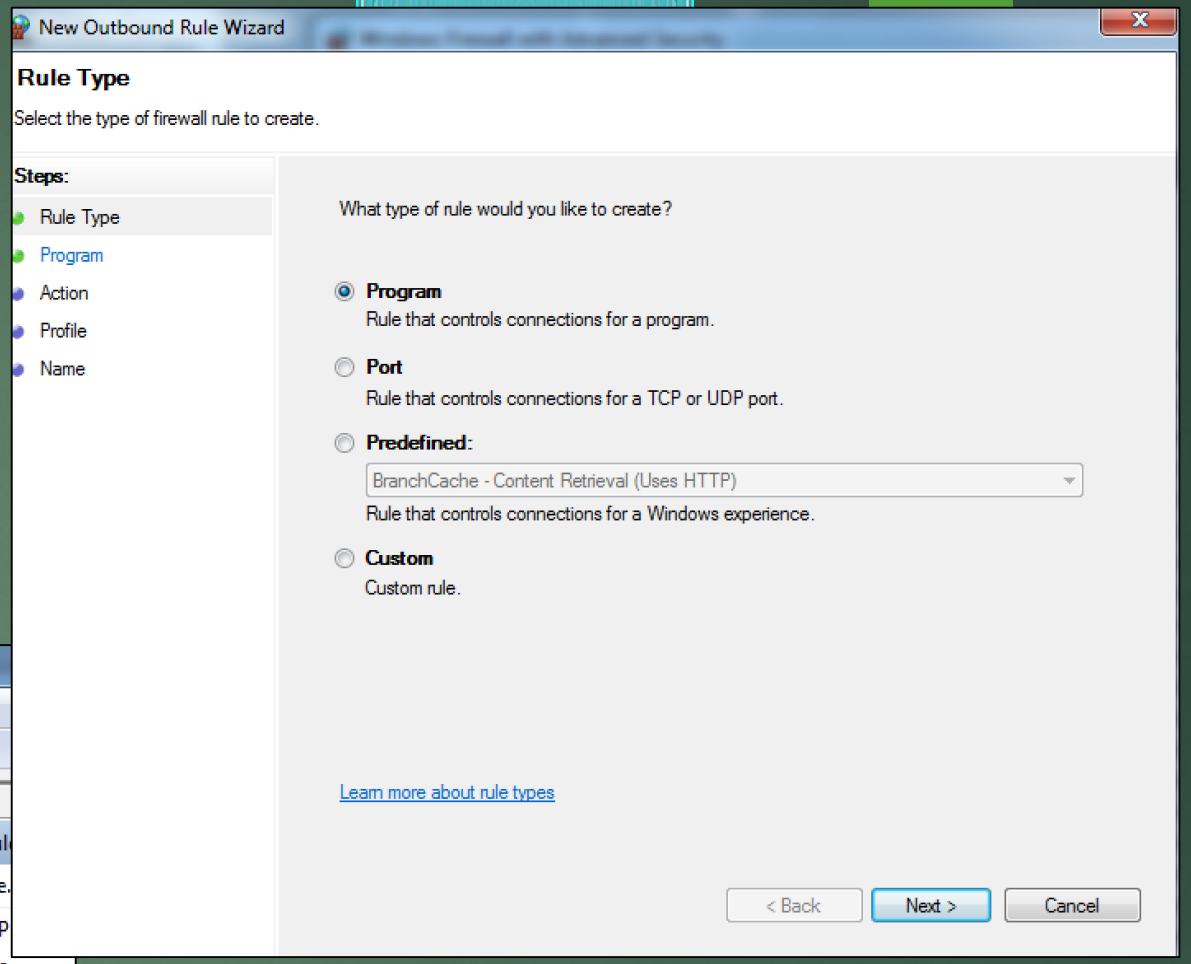
Types of firewalls

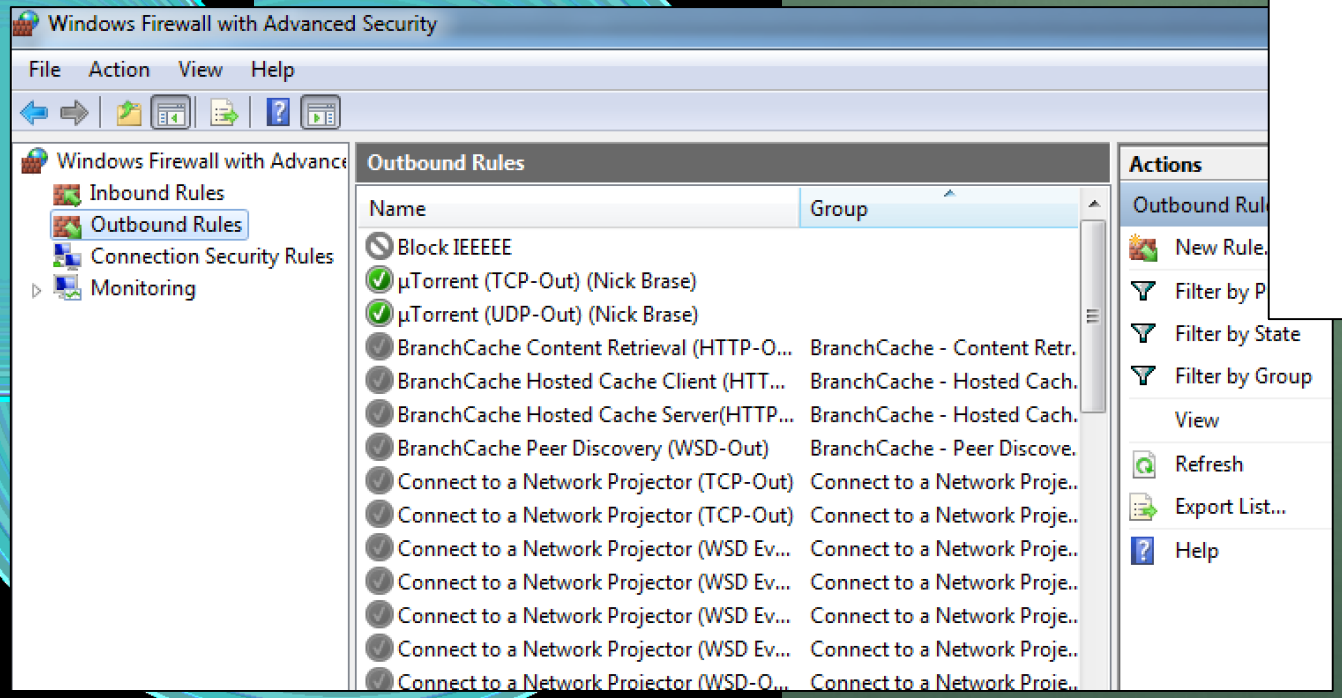
- IP tables --Linux
- UFW --Linux

```
root@ubuntu:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 53                         ALLOW IN    192.168.1.50
[ 2] 22/tcp                     ALLOW IN    192.168.1.50
[ 3] 21/tcp                     ALLOW IN    192.168.1.10
[ 4] 22/tcp                     ALLOW IN    192.168.1.10

root@ubuntu:~# ufw delete 2
Deleting:
 allow from 192.168.1.50 to any port 22 proto tcp
Proceed with operation (y|n)? y
Rule deleted
root@ubuntu:~#
```

Types of firewalls

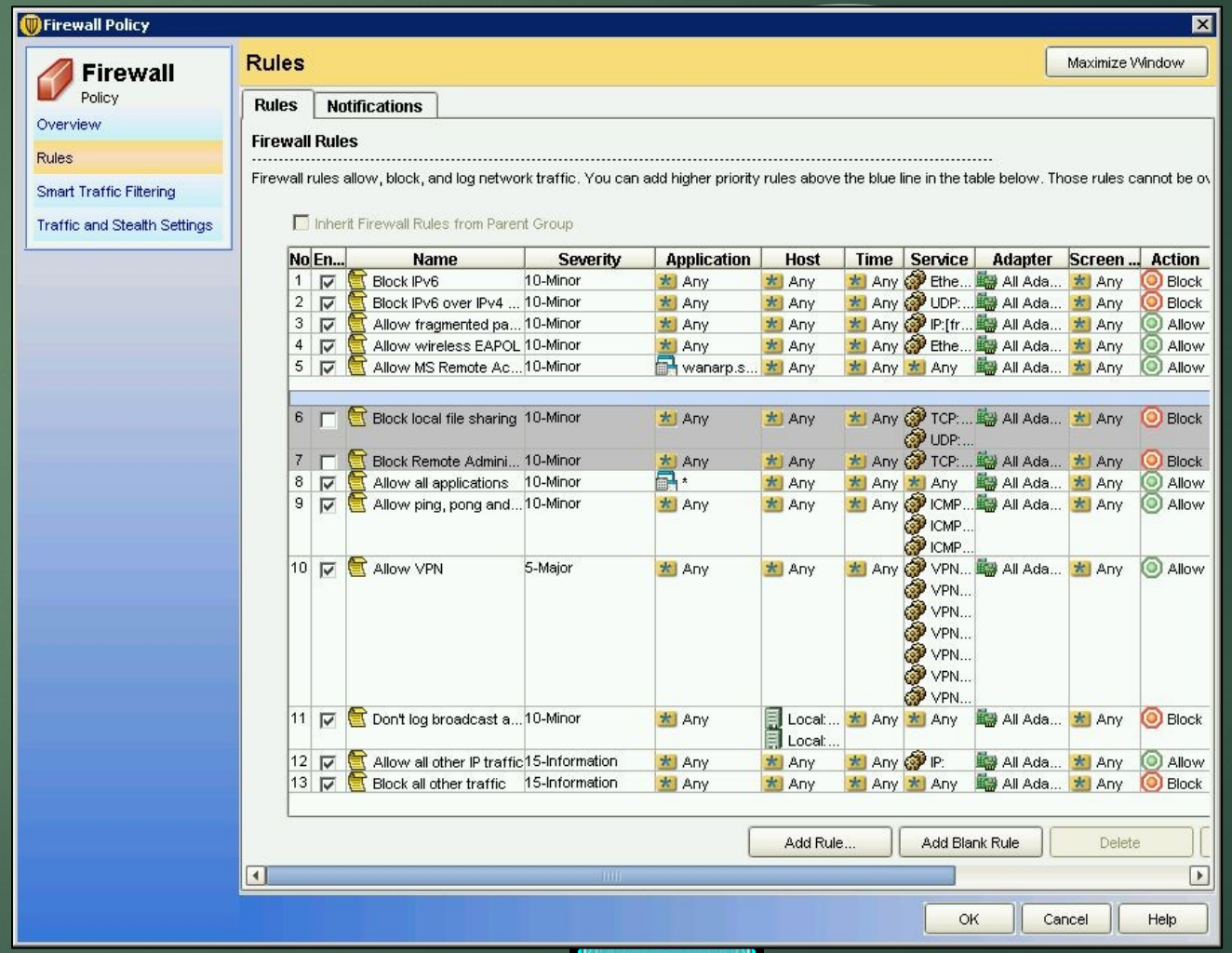
- IP tables --linux
- UFW --linux
- Windows Firewall --Windows





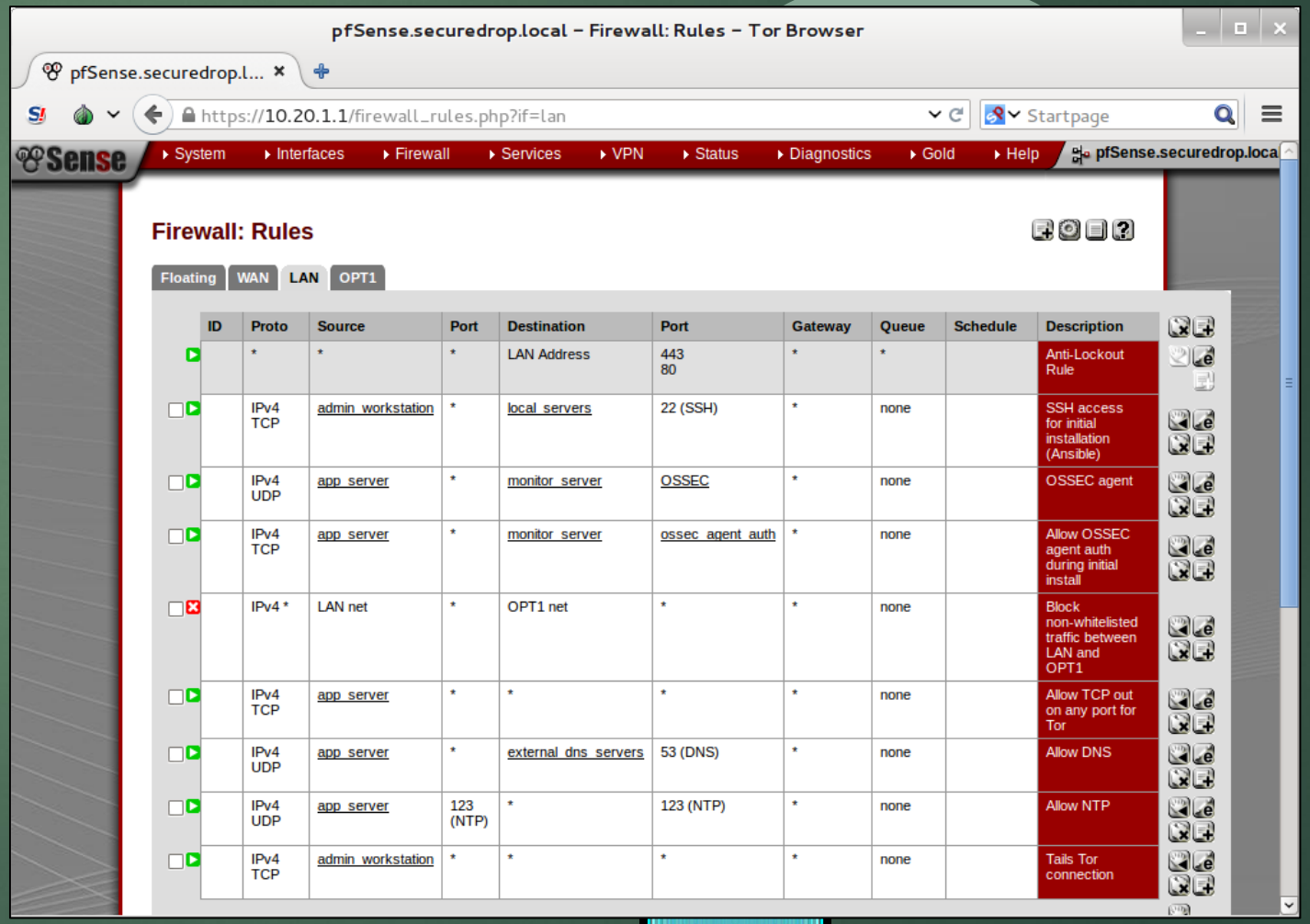
Types of firewalls

- IP tables --linux
- UFW --linux
- Windows Firewall --Windows
- Symantec --antivirus with firewalls



Types of firewalls

- IP tables --linux
- UFW --linux
- Windows Firewall --Windows
- Symantec --antivirus with firewalls
- pfSense --router with firewalls



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
	IPv4 TCP	admin_workstation	*	local_servers	22 (SSH)	*	none		SSH access for initial installation (Ansible)
	IPv4 UDP	app_server	*	monitor_server	OSSEC	*	none		OSSEC agent
	IPv4 TCP	app_server	*	monitor_server	ossec_agent_auth	*	none		Allow OSSEC agent auth during initial install
	IPv4 *	LAN net	*	OPT1 net	*	*	none		Block non-whitelisted traffic between LAN and OPT1
	IPv4 TCP	app_server	*	*	*	*	none		Allow TCP out on any port for Tor
	IPv4 UDP	app_server	*	external_dns_servers	53 (DNS)	*	none		Allow DNS
	IPv4 UDP	app_server	123 (NTP)	*	123 (NTP)	*	none		Allow NTP
	IPv4 TCP	admin_workstation	*	*	*	*	none		Tails Tor connection

Types of firewalls

- IP tables --linux
- UFW --linux
- Windows Firewall --Windows
- Symantec --antivirus with firewalls
- PF sense --router with firewalls
- Cisco --more for enterprise environment (router with firewalls)

Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name Voice

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

Types of firewalls

- IP tables
- UFW
- Windows Fi
- Symantec
- PF sense
- Cisco
- Juniper

--Who knows? The documentation costs money so we don't

Enable | Disable | Filter Rules | Show All Devices Policy | Show Invalid Rules

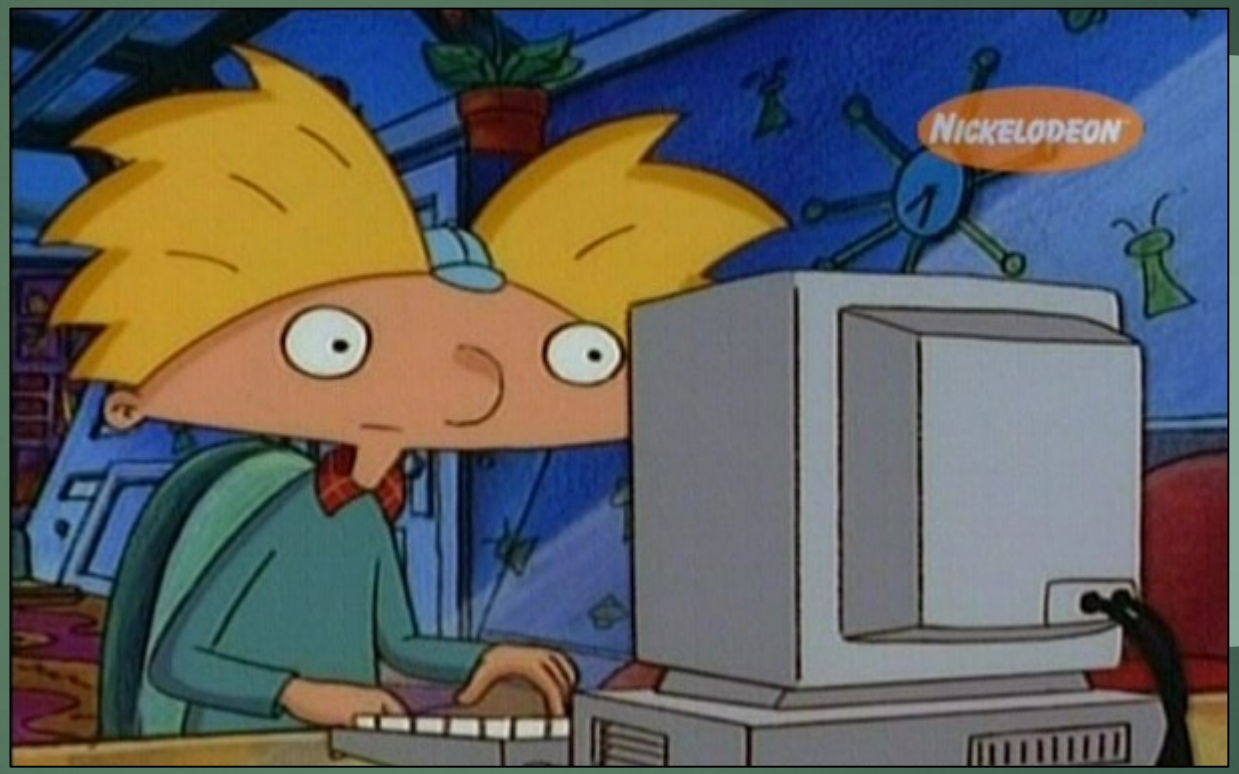
S.No.	Name	Source			Destination		Service	Action	AppFW	Profile
		Zone	Address	Source Identity	Zone	Address				
	Zone (40 rules)									
	All Devices Pre Rules (10 rules)									
	Device Rules (20 rules)									
1	Device-Zone-1	trust	Any		untrust	Any	Any	Tunnel (SRX220-b_tets)	-	
2	Device-Zone-2	trust	Any		untrust	Any	Any	Tunnel (SRX220-b_tets)	-	
3	Device-Zone-3	trust	Any		untrust	Any	Any	Deny	-	
4	Device-Zone-4	trust	Any		untrust	Any	Any	Deny	-	
	test1 (7 rules)									
12	Device-Zone-5	trust	Any		untrust	Any	Any		-	
13	Grp1-Zone-Pre-3	trust	Any		untrust	Any	Any		-	
14	Grp1-Zone-Pre-4	trust	Any		untrust	Any	Any		-	
15	Grp1-Zone-Pre-5	trust	Any		untrust	Any	Any	(SRX220-b_tets)		
16	Grp1-Zone-Pre-6	trust	Any		untrust	Any	Any	Deny	-	
17	Grp1-Zone-Pre-7	trust	Any		untrust	Any	Any	Deny	-	
18	Grp1-Zone-Pre-8	trust	Any		untrust	Any	Any	Tunnel (SRX220-b_tets)	-	
19	Device-Zone-6	trust	Any		untrust	Any	Any	Deny	-	
20	Device-Zone-14	trust	Any		untrust	Any	Any	Deny	-	
	All Devices Post Rules (10 rules)									

Permit
Deny
Reject
Tunnel ▸ Select VPN...

Linux Scenario

Meet Arnold:

- CS major
- Tired
- Constantly coding
- Girl who picks on him
- Frustrated



Linux Scenario

- Arnold just wants to code.
- But he is getting bugged by Helga

```
[SysSec@localhost ~]$ echo dank memes |wall
[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain

dank memes
echo dank memes |wall
[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain

dank memes
```

```
a = 0
while a < 15:
    print 'I am coding a lot for homework',
newline.
    if a == 10:
        print "made it to ten!!"
    a = a + 1
Broadcast message from SysSec@localhost.localdomain
~
dank memes
~
Broadcast message from SysSec@localhost.localdomain
~
dank memes
~
Broadcast message from SysSec@localhost.localdomain
~
dank memes
~
~
```

Linux Scenario

- How did Helga get in?
  - SSH into his box.

```
[SysSec@localhost ~]$ ssh 10.42.x.7
SysSec@10.42.x.7's password:
Last login: Mon Mar  6 16:39:46 2017 from 10.42.x.2
[SysSec@localhost ~]$
```

Linux Scenario

- Arnold is getting annoyed

```
[SysSec@localhost ~]$ echo dank memes |wall
[SysSec@localhost ~]$
Broadcast message from SysSec@localhost.localdomain

dank memes

Broadcast message from SysSec@localhost.localdomain

dank memes
echo dank memes |wall

Broadcast message from SysSec@localhost.localdomain

dank memes
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!

```
root@LB-VM:~/Desktop# iptables -L
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
root@LB-VM:~/Desktop#
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!
- Lets create some
  - Blocking IP addresses

```
root@LB-VM:~/Desktop# iptables -A INPUT -s 10.42.X.XXX -j DROP
```

  - Blocking Ports

```
root@LB-VM:~/Desktop# iptables -A INPUT -s 10.42.X.XXX -p tcp --destination-po
rt 80 -j DROP
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!
- Lets create some
- Now lets view the iptable rules

```
root@LB-VM:~/Desktop# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 10.42.1.110/32
-A INPUT -s 10.42.2.110/32 -j DROP
-A INPUT -s 10.42.3.110/32 -j DROP
-A INPUT -s 10.42.4.110/32 -j DROP
-A INPUT -s 10.42.5.110/32 -j DROP
-A INPUT -s 10.42.6.110/32 -j DROP
-A INPUT -s 10.42.7.110/32 -j DROP
-A INPUT -s 10.42.8.110/32 -j DROP
-A INPUT -s 10.42.9.110/32 -j DROP
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!
- Lets create some
- Now lets view the iptable rules
- There is something wrong…

```
root@LB-VM:~/Desktop# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 10.42.1.110/32
-A INPUT -s 10.42.2.110/32 -j DROP
-A INPUT -s 10.42.3.110/32 -j DROP
-A INPUT -s 10.42.4.110/32 -j DROP
-A INPUT -s 10.42.5.110/32 -j DROP
-A INPUT -s 10.42.6.110/32 -j DROP
-A INPUT -s 10.42.7.110/32 -j DROP
-A INPUT -s 10.42.8.110/32 -j DROP
-A INPUT -s 10.42.9.110/32 -j DROP
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!
- Lets create some
- Now lets view the iptable rules
- There is something wrong…
- Lets fix it

```
root@LB-VM:~/Desktop# iptables -D INPUT -s 10.42.X.XXX -j DROP
```

Linux Scenario

- So he wants to block her with IP tables
  - But there are none there!
- Lets create some
- Now lets view the iptable rules
- There is something wrong…
- Lets fix it
- Don't forget to save

```
root@LB-VM:~/Desktop# iptables-save
```

Linux Scenario

- Next he finds her to kick her out

```
root@LB-VM:~/Desktop# ps aux

root       3638  0.0  0.5  44160  5020 pts/6    S+   03:37   0:00 ssh helga@19
root       3639  0.0  0.7 126136  7068 ?        Ss   03:37   0:00 sshd: helga
helga      3698  0.0  0.4 126136  4356 ?        S    03:37   0:00 sshd: helga@
helga      3699  0.0  0.0   4448   692 pts/2    Ss+  03:37   0:00 -sh
root       3716  0.0  0.3  28268  3876 pts/8    Ss   03:37   0:00 bash
root       3741  0.0  0.2  25636  2536 pts/8    R+   03:38   0:00 ps aux
root@LB-VM:~/Desktop#
```

- To limit the ps aux output use the grep command

```
root@LB-VM:~/Desktop# ps aux |grep ssh
```

Linux Scenario

- Now time to kill the connection

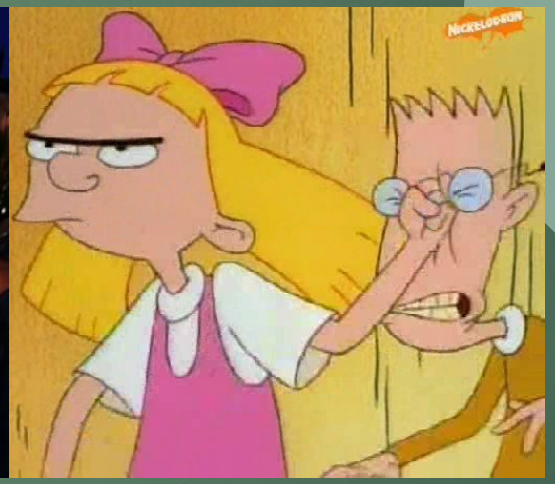
```
root       3638  0.0  0.5  44160  5020 pts/6    S+   03:37   0:00 ssh helga@19
root       3639  0.0  0.7 126136  7068 ?        Ss   03:37   0:00 sshd: helga
helga      3698  0.0  0.4 126136  4356 ?        S    03:37   0:00 sshd: helga@
helga      3699  0.0  0.0   4448   692 pts/2    Ss+  03:37   0:00 -sh
root       3716  0.0  0.3  28268  3876 pts/8    Ss   03:37   0:00 bash
root       3741  0.0  0.2  25636  2536 pts/8    R+   03:38   0:00 ps aux
root@LB-VM:~/Desktop#
```

```
root@LB-VM:~/Desktop# kill -9 3638
```

```
$ Killed
```

Linux Scenario

- Now what stands between Helga and Arnold is a wall on fire.



Try it:

- Log onto a Ubuntu client, A or B.
- Find another person in the room not on your team of the opposite letter
- Letter A will ping B
- Letter B will write an iptable rule to block their ip (.111)
- Don't forget to kill the process
- Now switch

  Hint1: #todo
  Hint2: ps aux is your friend
  Hint3: | grep ssh might help
  Now switch roles

Windows Scenario

- You are now an IT professional:

Windows Scenario

- Your boss's boss of the boss who bosses your boss to boss you told them that people have been using ubnetdef.org at work. One of those boss's doesn't like it so now you should probably block it.





Windows Scenario

- Knowing how to block IP addresses, how can we get the ubnetdef.org ip address?
- nslookup ubnetdef.org

```
C:\Windows\system32>nslookup ubnetdef.org
Server:  ns.buffalo.edu
Address:  128.205.1.2

Non-authoritative answer:
Name:    ubnetdef.org
Address:  128.205.44.157
```

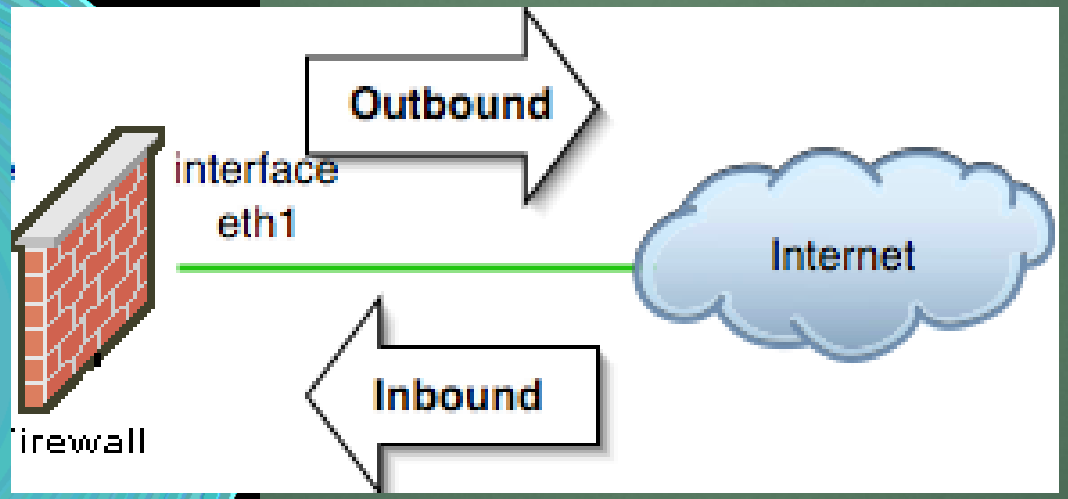
Windows Scenario

- Time to test it.

```
C:\Windows\system32>ping 128.205.44.157

Pinging 128.205.44.157 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 128.205.44.157:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
```

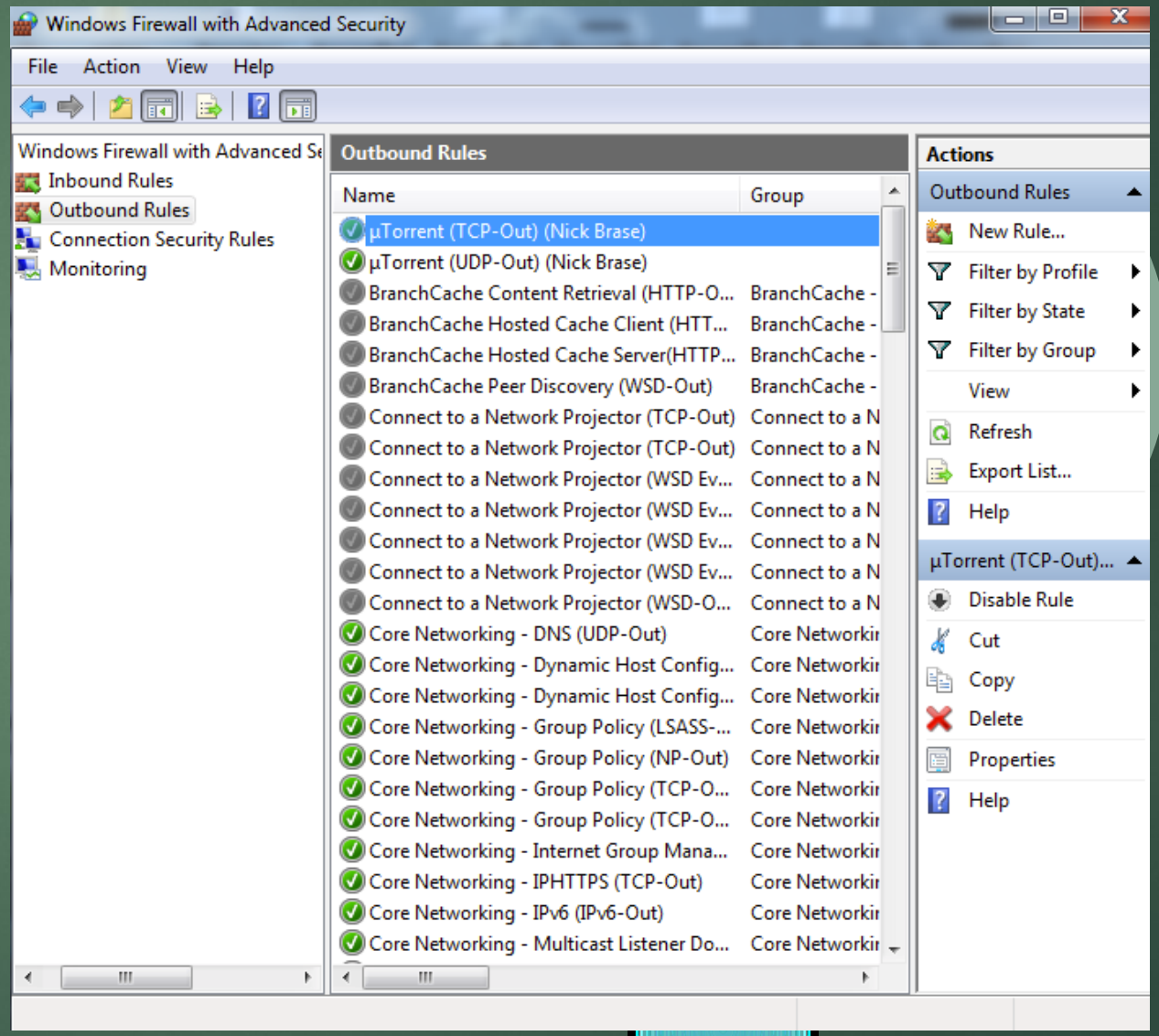
Windows Scenario

- The Linux Scenario Arnold blocked Helgas _____traffic.
- Now the IT professional will block _____traffic.



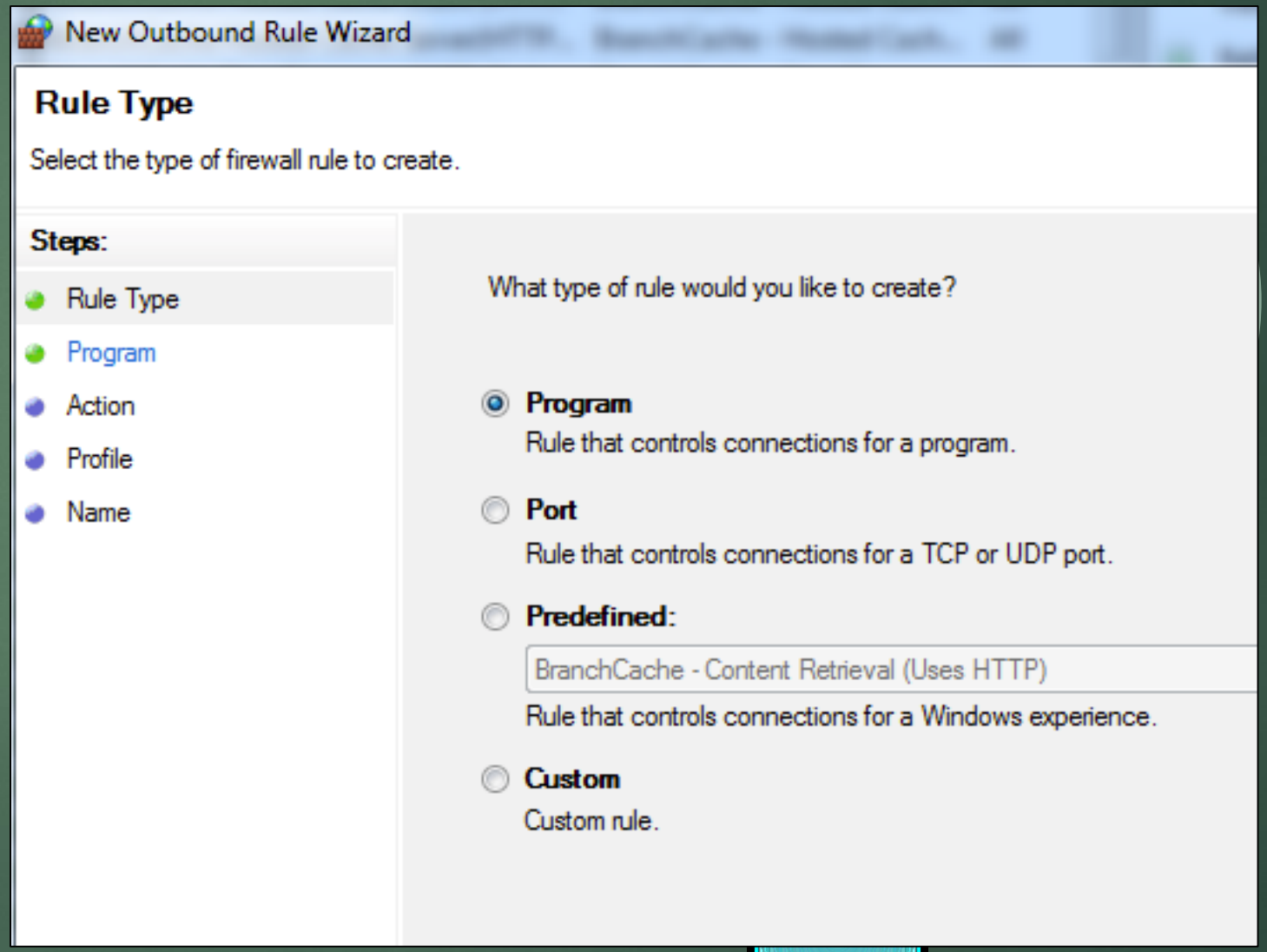
Windows Scenario

- Now lets block outbound traffic going to ubnetdef.org



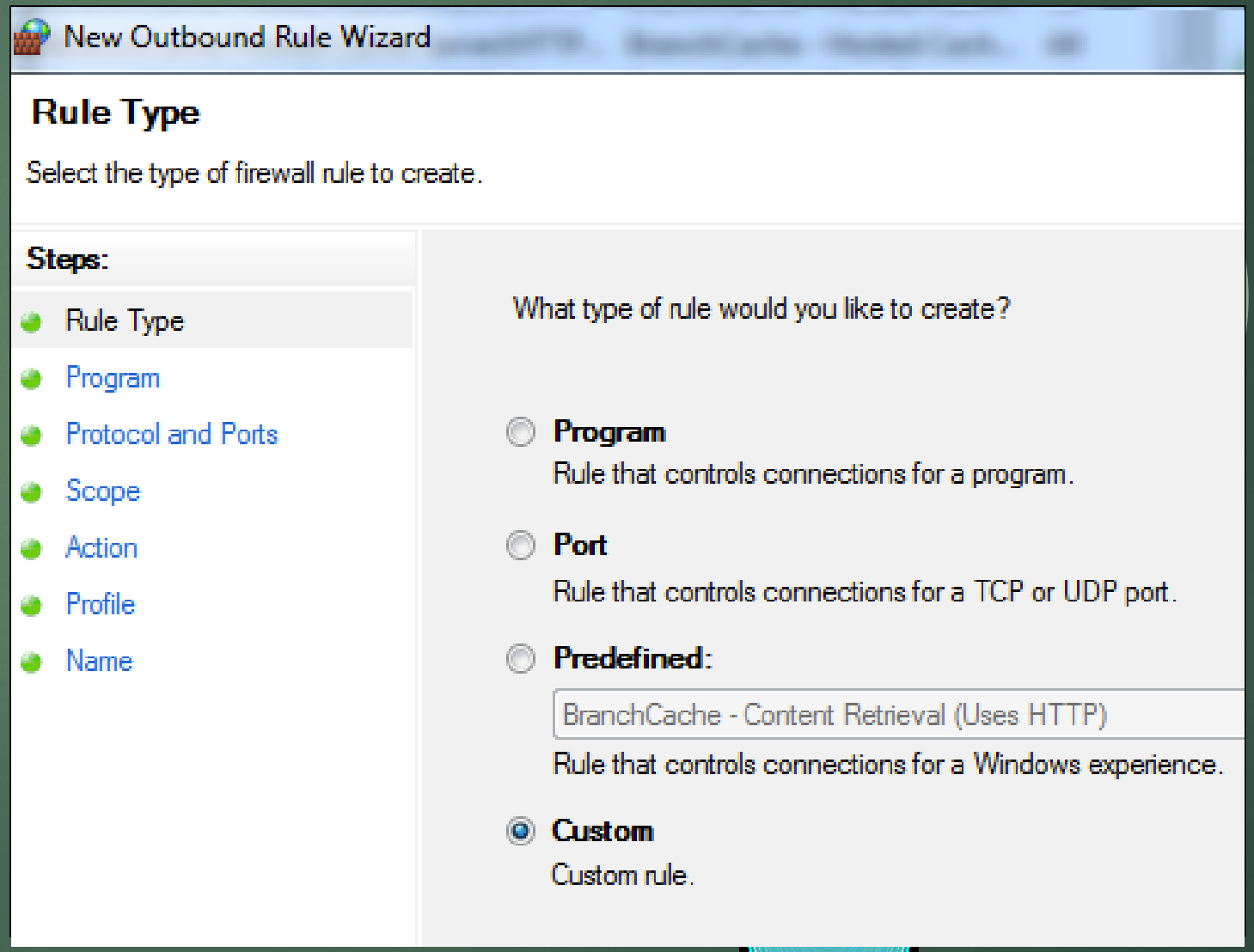
Windows Scenario

- What type of rule?



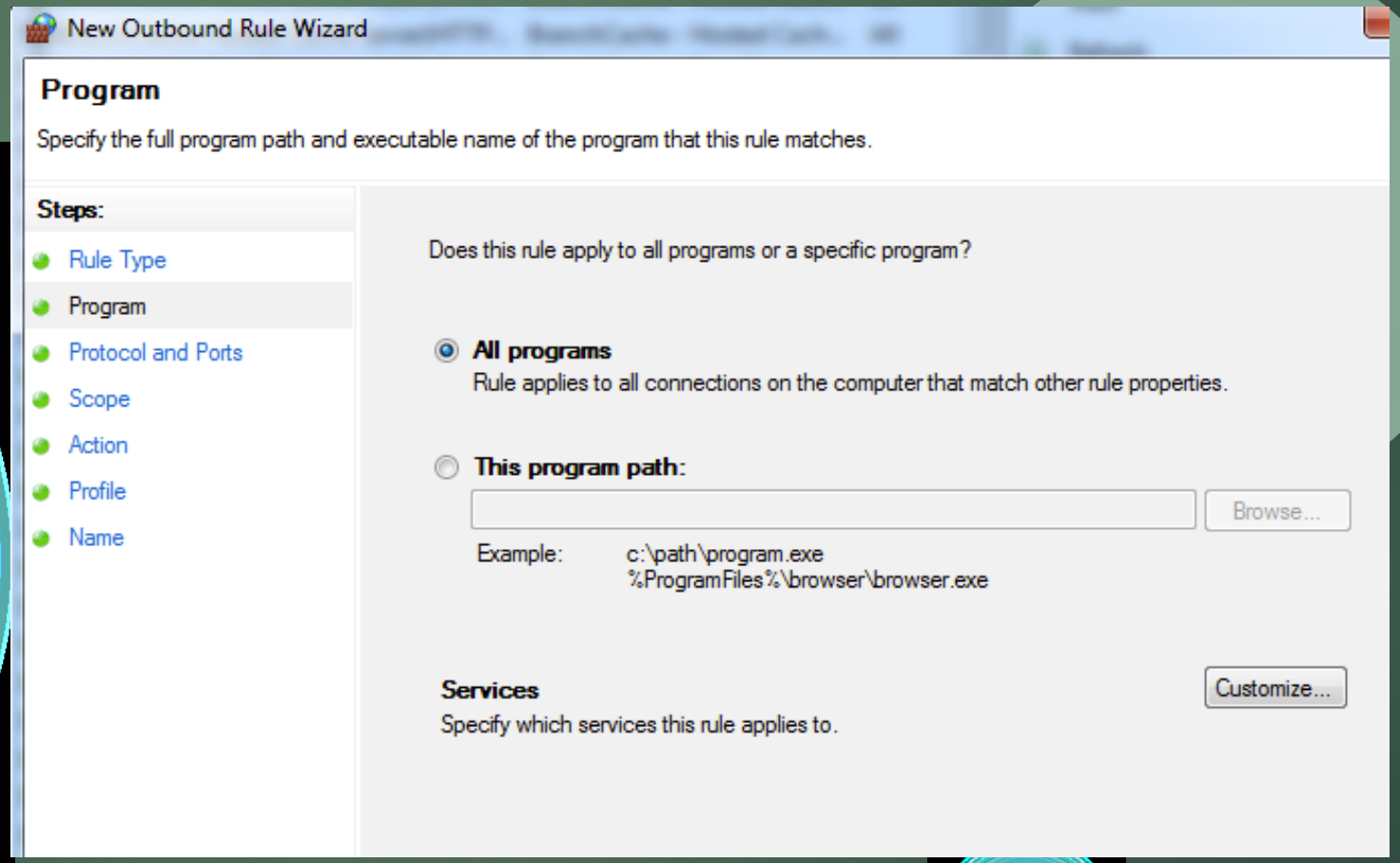
Windows Scenario

- What type of rule?



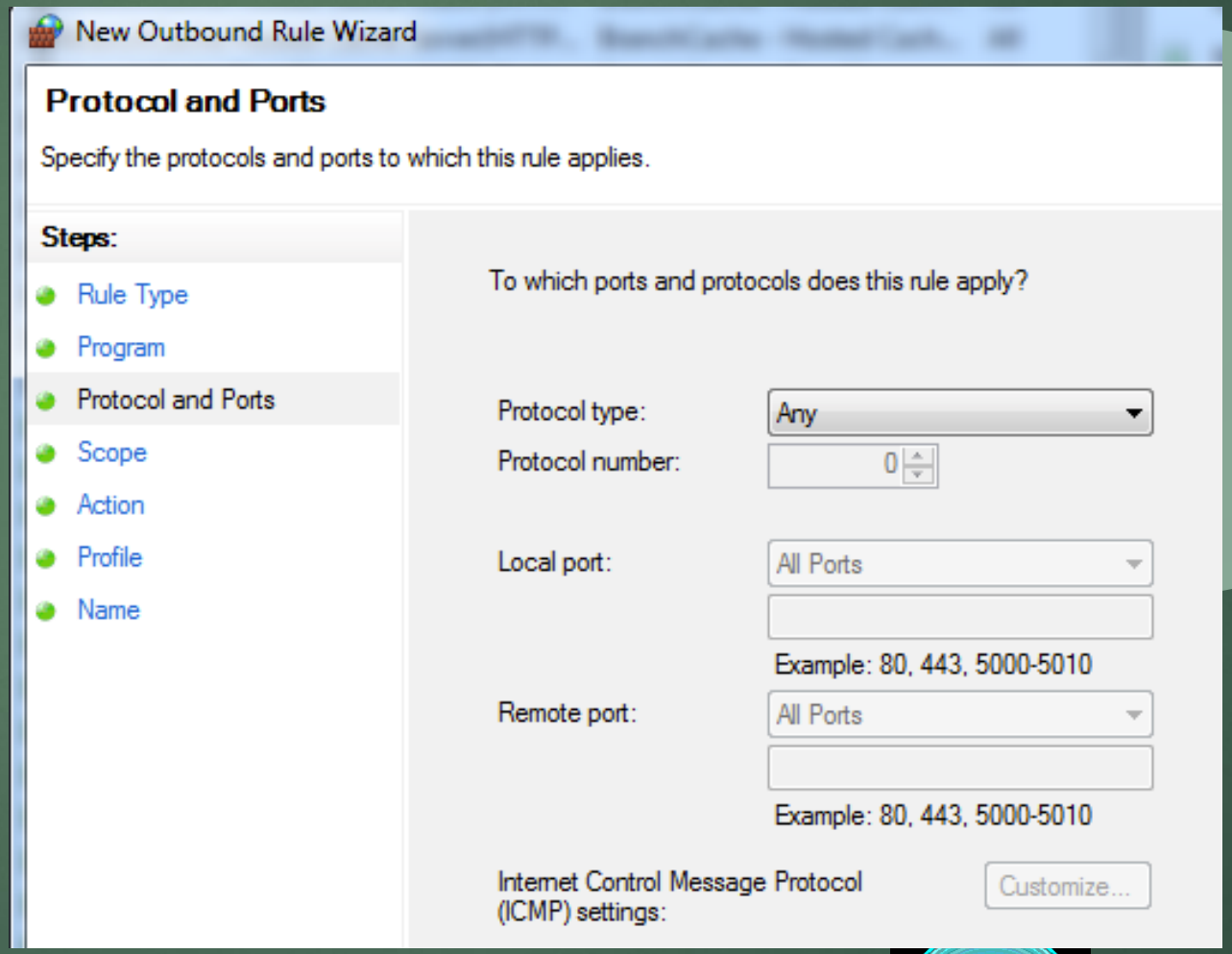
Windows Scenario

- Program?



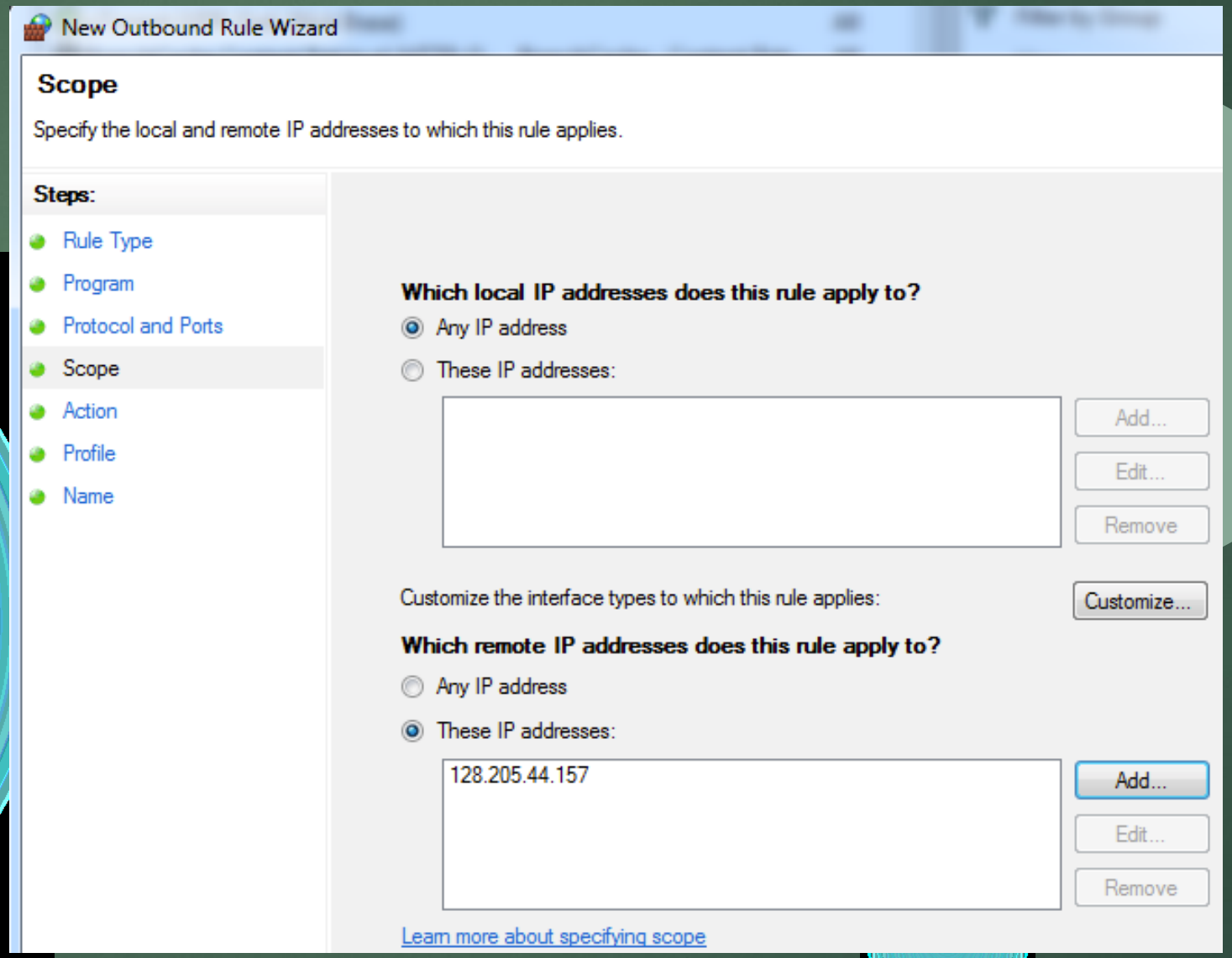
Windows Scenario

- Protocol?



Windows Scenario

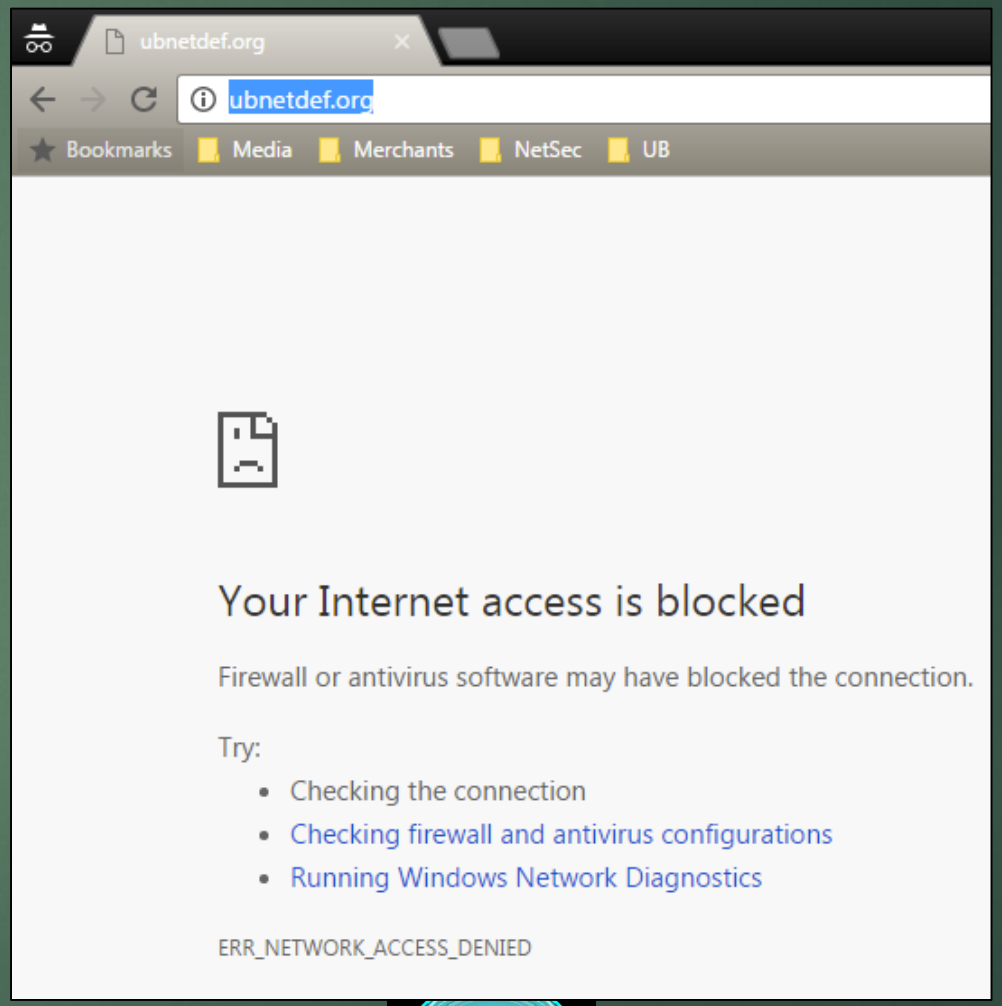
- Scope?



Windows Scenario

- Time to test it.

```
C:\Windows\system32>ping 128.205.44.157

Pinging 128.205.44.157 with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 128.205.44.157:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



Try it:

- Log onto Windows client, A or B.
- Block RDP (remote desktop) going outbound
- Try to RDP into another windows machine (use IP address)

Hint1: #todo
Hint2: RDP seems like a protocol
Hint3:
Now switch roles

Homework / Beginning of project

- So far you have a LAN
  - Linux server, 3 x Linux client, 2 x Windows client, Windows server
- Your goal:
  - White list all of the clients to the servers
    - Add rules to allow connection from only the clients on your LAN access to the servers
  - Set up an FTP server on your Linux server
- Extra:
  - If you're feeling froggy, then leap.
    - Leap into your pfSense box and set up firewall rules there
      - Lookup best practices for firewall rules on a router to protect your LAN