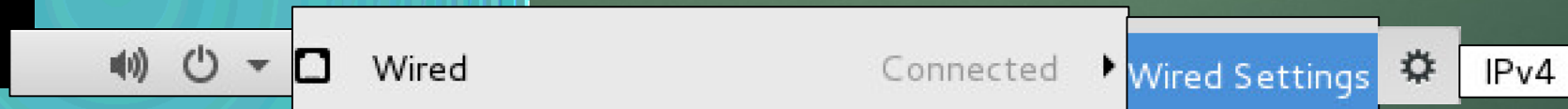


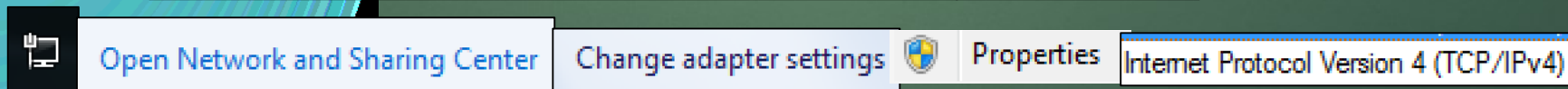
# Networking Exercise

- ▶ 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

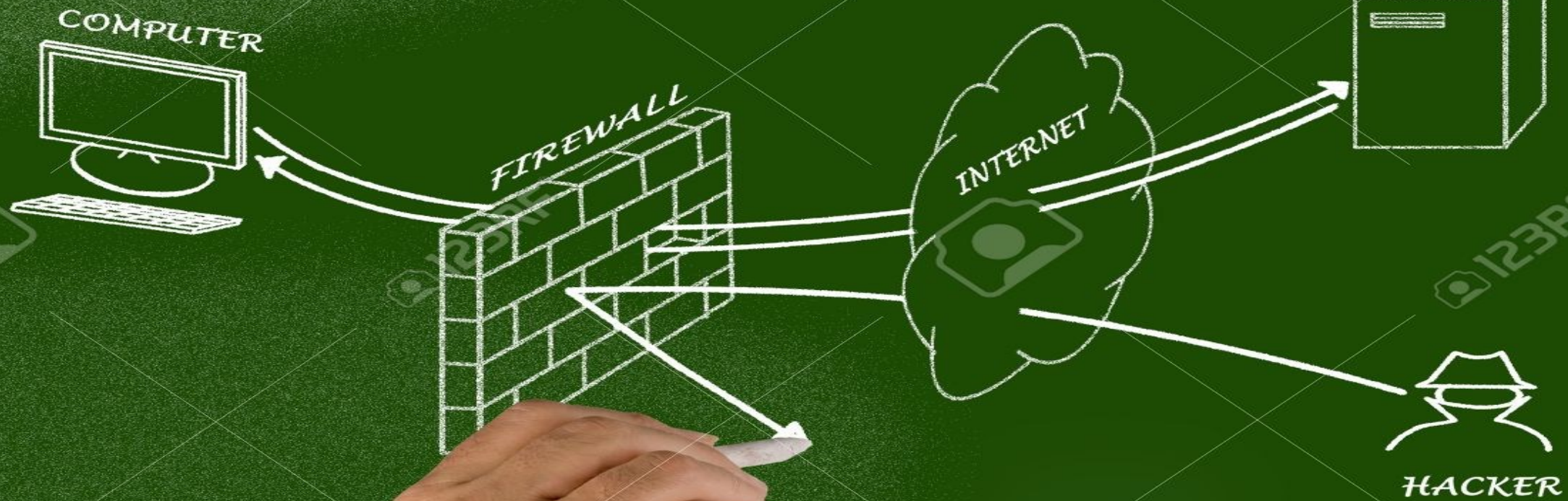
Linux:



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

```

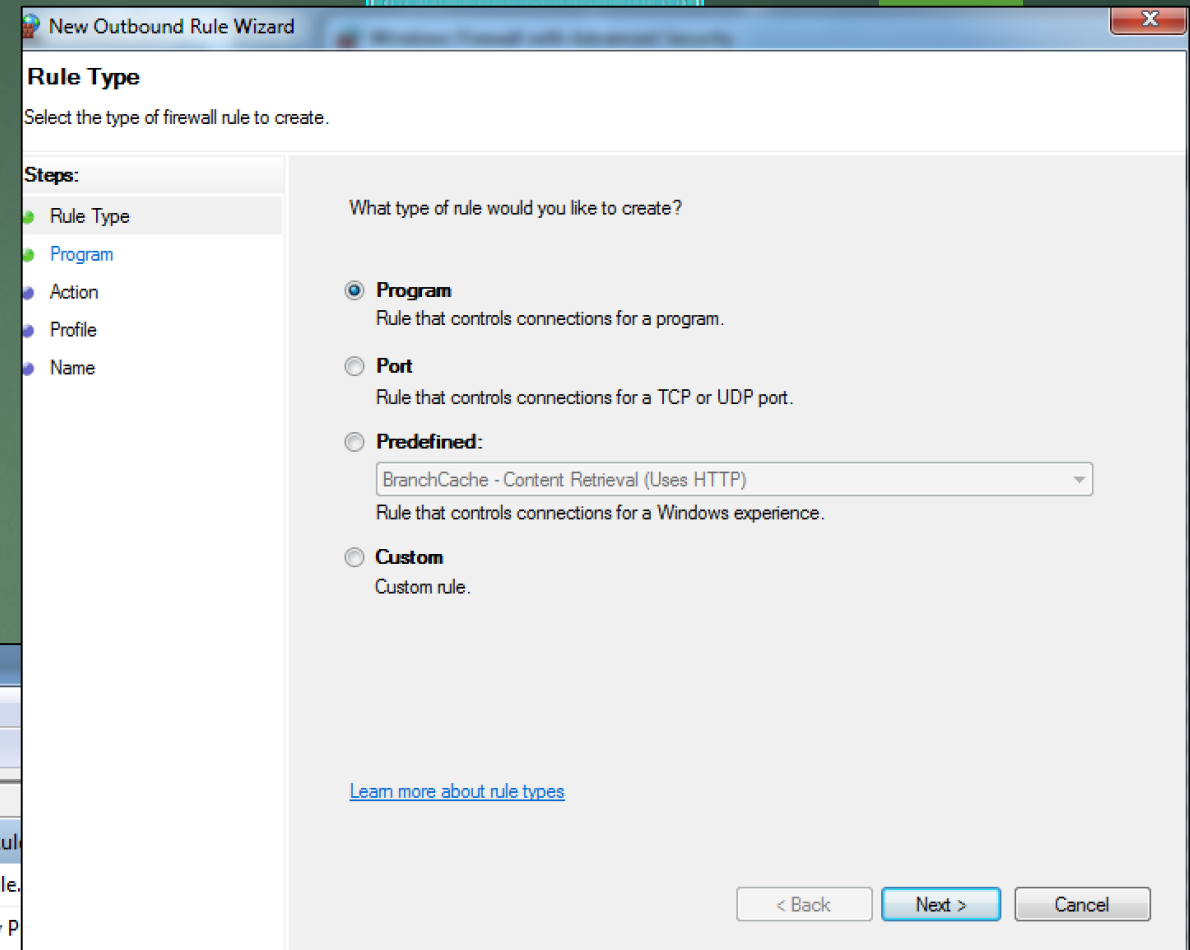
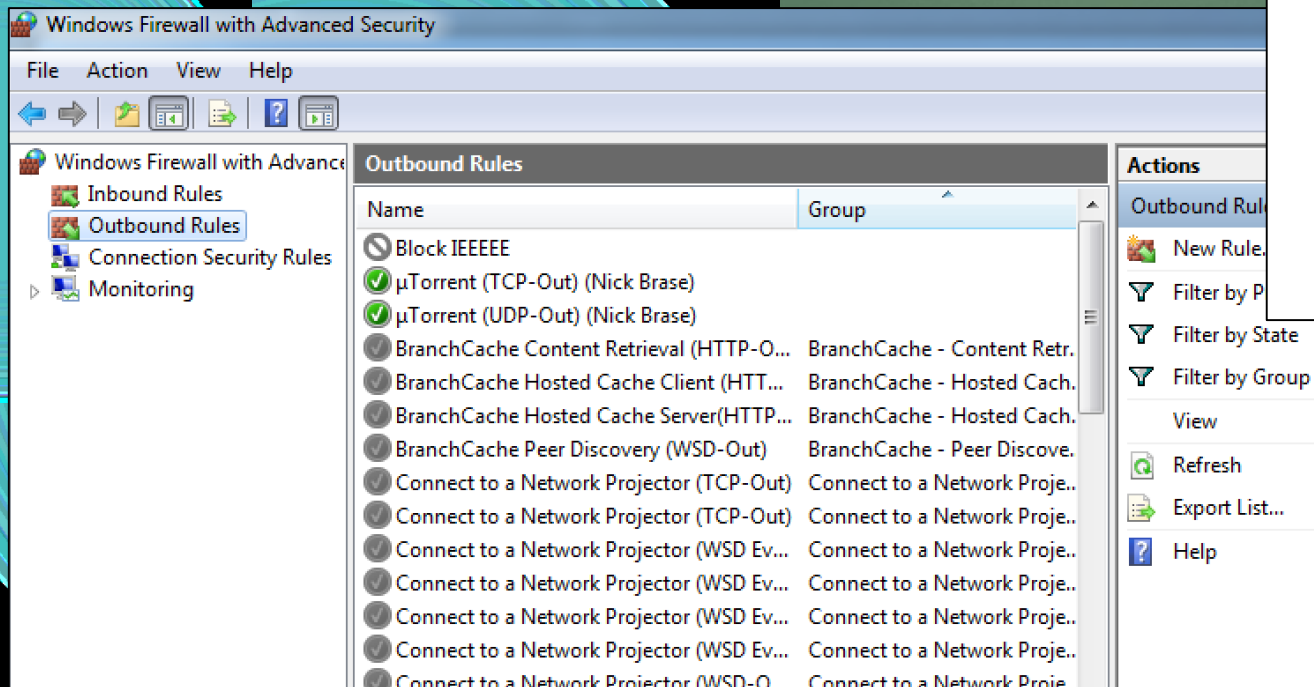
root@ubuntu:~# ufw delete 2
Deleting:
  allow from 192.168.1.50 to any port 22 proto tcp
Proceed with operation (y|n)? y
Rule deleted
root@ubuntu:~# █
```

# Types of firewalls

▶ IP tables --linux

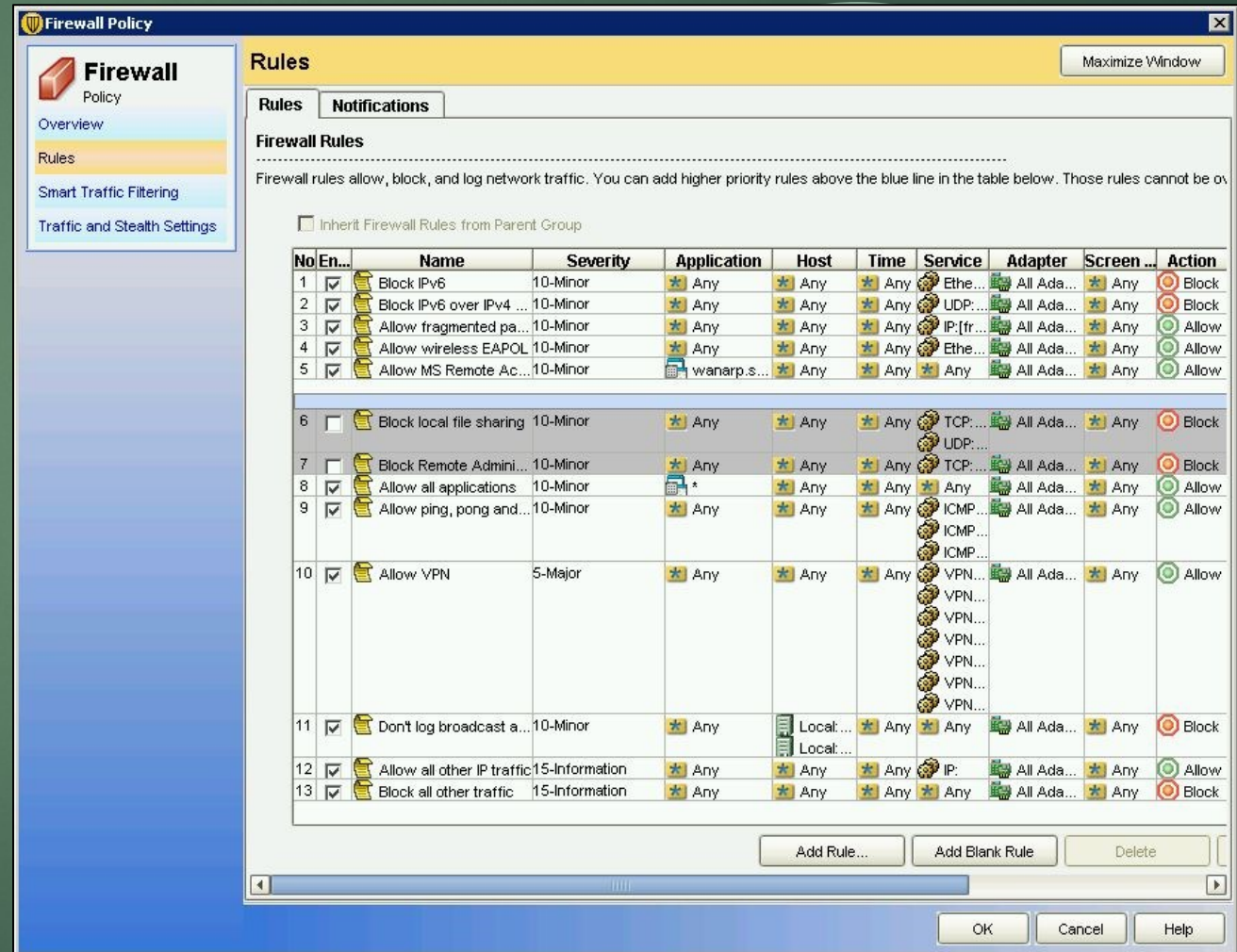
▶ UFW --linux

▶ 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

pfSense.securedrop.local - Firewall: Rules - Tor Browser

pfSense.securedrop.local... x

https://10.20.1.1/firewall\_rules.php?if=lan

Startpage

pfSense

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

### Firewall: Rules

Floating WAN LAN OPT1

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	▶	IPv4 TCP	admin_workstation	*	local_servers	22 (SSH)	*	none		SSH access for initial installation (Ansible)
<input type="checkbox"/>	▶	IPv4 UDP	app_server	*	monitor_server	OSSEC	*	none		OSSEC agent
<input type="checkbox"/>	▶	IPv4 TCP	app_server	*	monitor_server	ossec_agent_auth	*	none		Allow OSSEC agent auth during initial install
<input type="checkbox"/>	✗	IPv4 *	LAN net	*	OPT1 net	*	*	none		Block non-whitelisted traffic between LAN and OPT1
<input type="checkbox"/>	▶	IPv4 TCP	app_server	*	*	*	*	none		Allow TCP out on any port for Tor
<input type="checkbox"/>	▶	IPv4 UDP	app_server	*	external_dns_servers	53 (DNS)	*	none		Allow DNS
<input type="checkbox"/>	▶	IPv4 UDP	app_server	123 (NTP)	*	123 (NTP)	*	none		Allow NTP
<input type="checkbox"/>	▶	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		<a href="#">Edit</a> <a href="#">Remove</a>
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound		<a href="#">Edit</a> <a href="#">Remove</a>
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound		<a href="#">Edit</a> <a href="#">Remove</a>
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound		<a href="#">Edit</a> <a href="#">Remove</a>
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound		<a href="#">Edit</a> <a href="#">Remove</a>
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound		<a href="#">Edit</a> <a href="#">Remove</a>
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound		<a href="#">Edit</a> <a href="#">Remove</a>
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		<a href="#">Edit</a> <a href="#">Remove</a>
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		<a href="#">Edit</a> <a href="#">Remove</a>



# Types of firewalls

► IP tables

► UFW

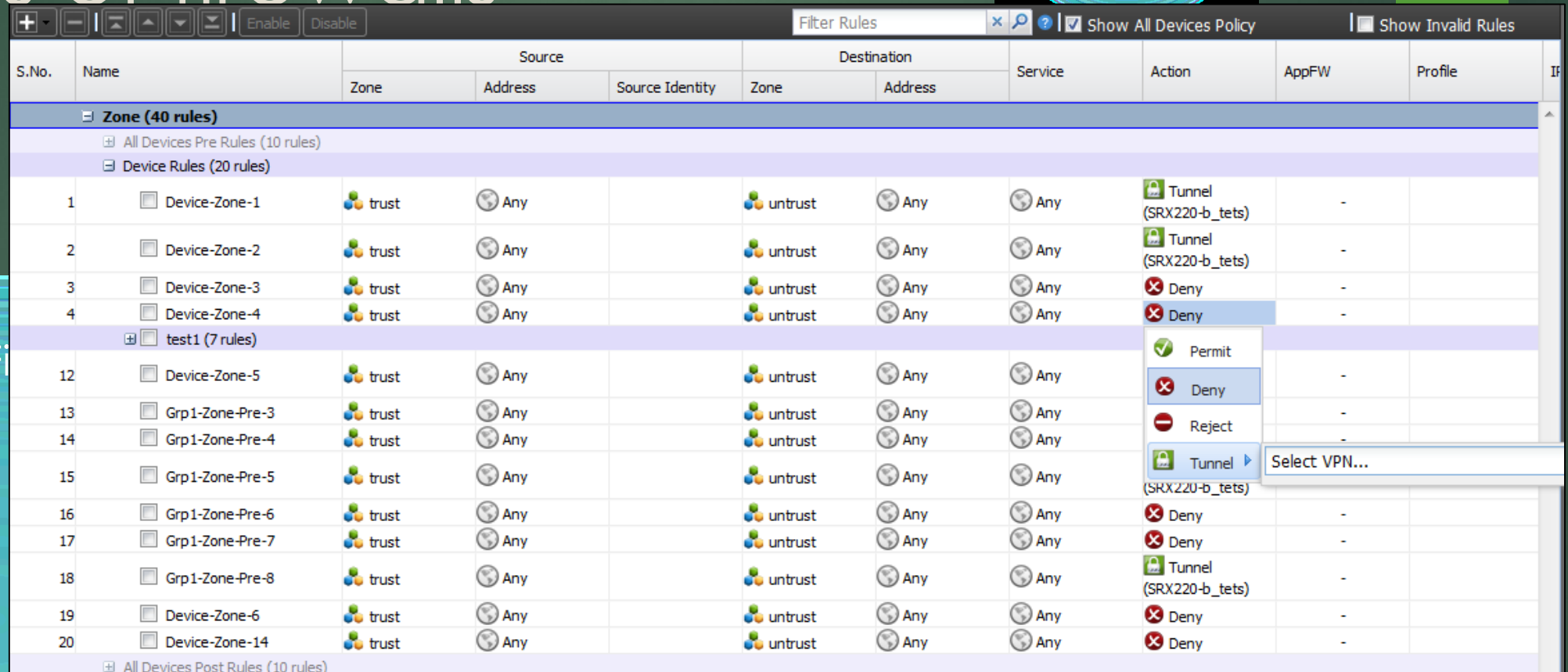
► Windows Firewall

► Symantec

► PF sense

► Cisco

► Juniper

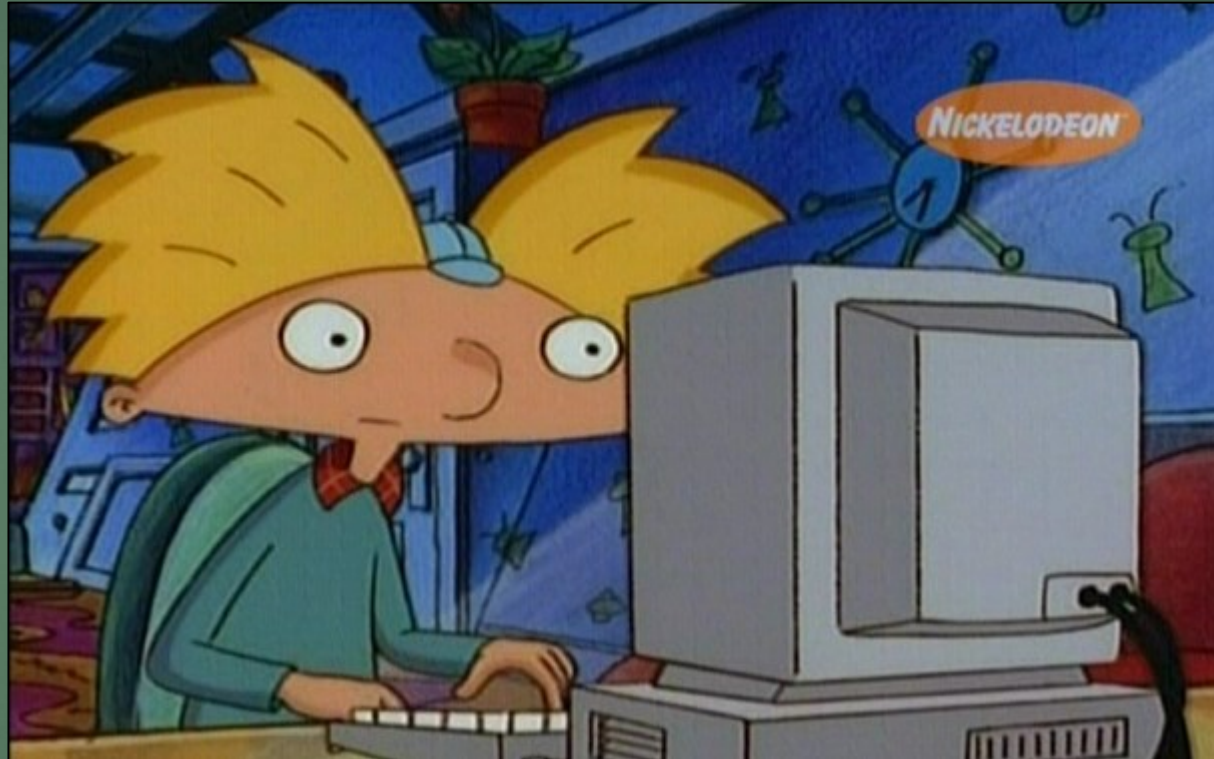


S.No.	Name	Source			Destination		Service	Action	AppFW	Profile
		Zone	Address	Source Identity	Zone	Address				
<b>Zone (40 rules)</b>										
All Devices Pre Rules (10 rules)										
Device Rules (20 rules)										
1	Device-Zone-1	trust	Any		untrust	Any	Any	Tunnel (SRX220-b_tets)	-	
2	Device-Zone-2	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		-	
16	Grp1-Zone-Pre-6	trust	Any		untrust	Any	Any		-	
17	Grp1-Zone-Pre-7	trust	Any		untrust	Any	Any		-	
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)										

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

# 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.x7'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-port 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

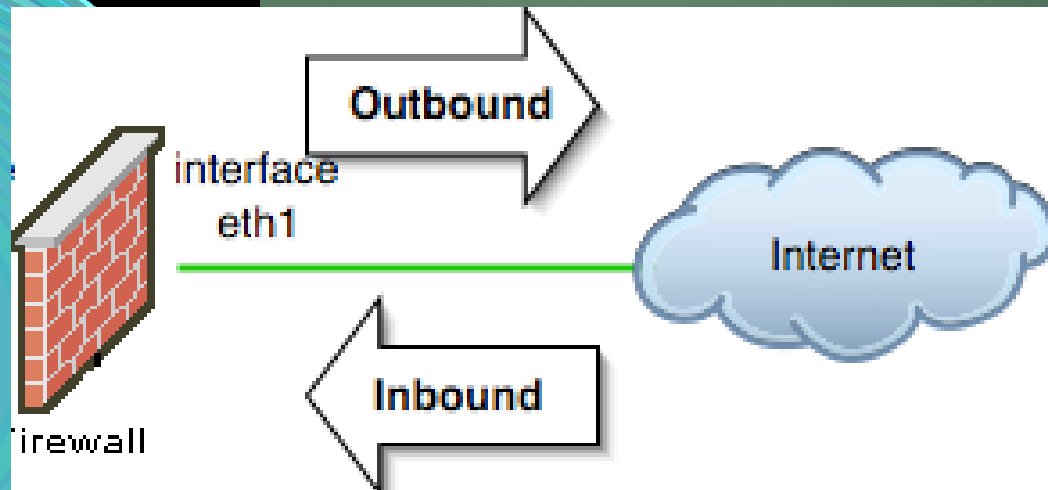
Pinging 128.205.44.157 with 32 bytes of data:
Request timed out.
Request timed out.

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

A screenshot of a web browser displaying the UBNetDef website. The browser's address bar shows the URL 'https://ubnetdef.org'. The website has a dark header with a logo on the left and navigation links ('about', 'courses', 'lectures', 'competitions', 'wiki') on the right. The main content area features a large banner with the text 'Learn & Live Security' and 'University at Buffalo Network Defense is a Cyber Security class & club' over a background of binary code. Below the banner, there are three sections: 'LEARN' with the text 'Everybody likes learning! Even super hackers like you! Let's learn together by doing.', 'BE CURIOUS' with the text 'Test, Break, Repeat. This is your mantra. Find new 0days, figure out better ways to secure an organization, or finally protect humans from themselves.', and 'COMPETE' with the text 'Prove you are the best! Take on the red team and emerge victorious! Show that you are truly the best.'

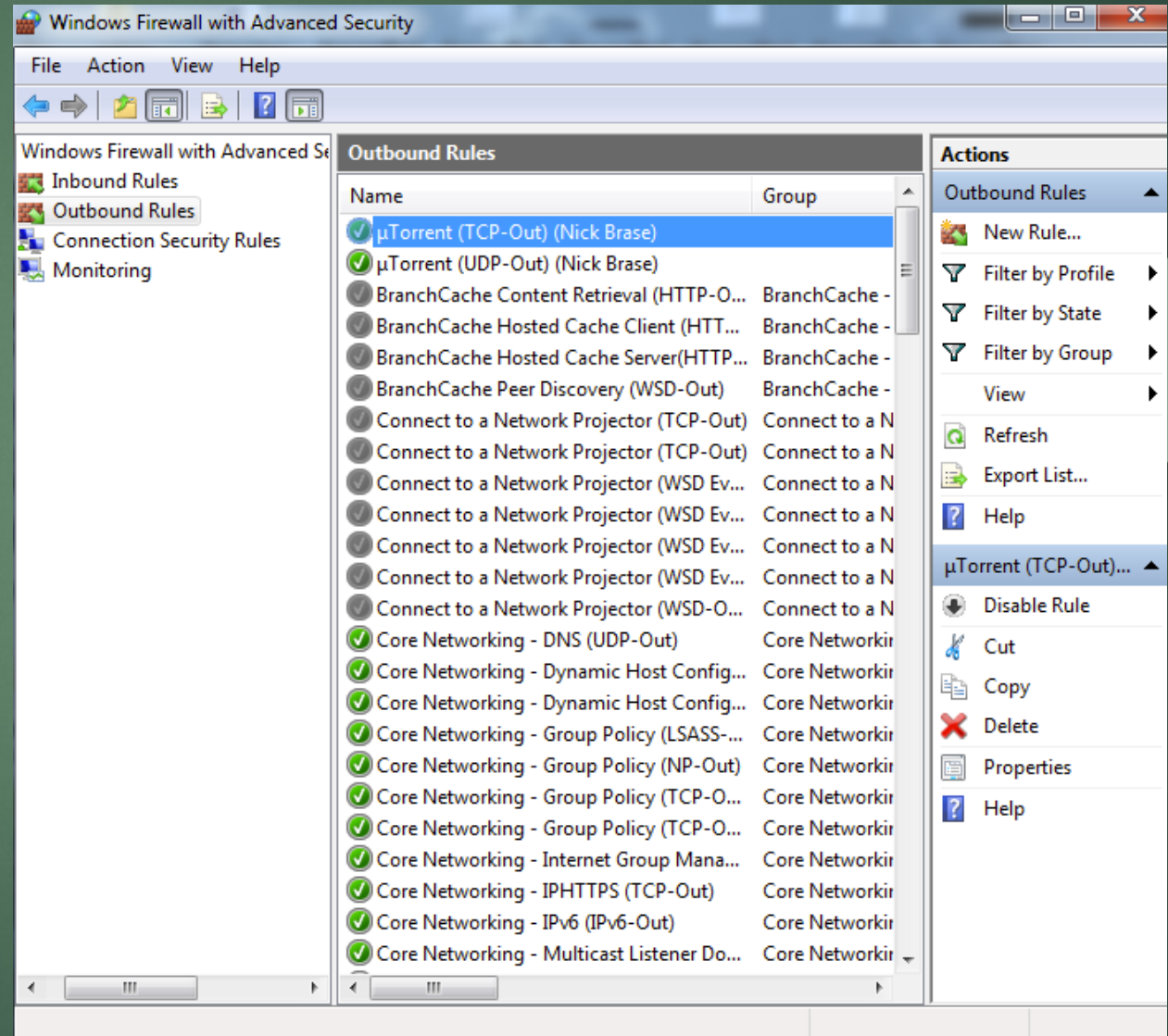
# Windows Scenario

- ▶ The Linux Scenario Arnold blocked Helgas \_\_\_\_\_ traffic.
- ▶ Now the IT professional will block \_\_\_\_\_ traffic.



# Windows Scenario

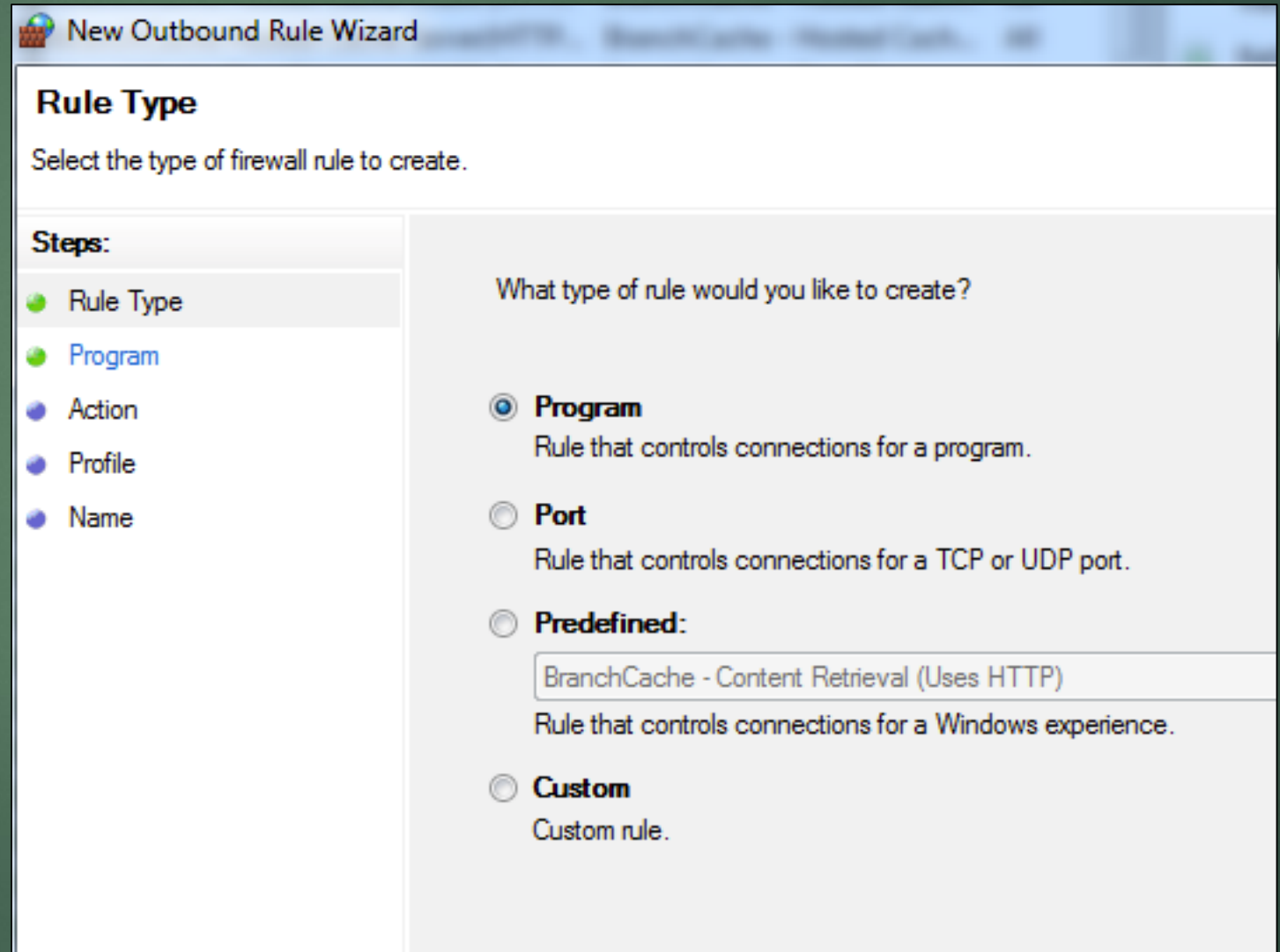
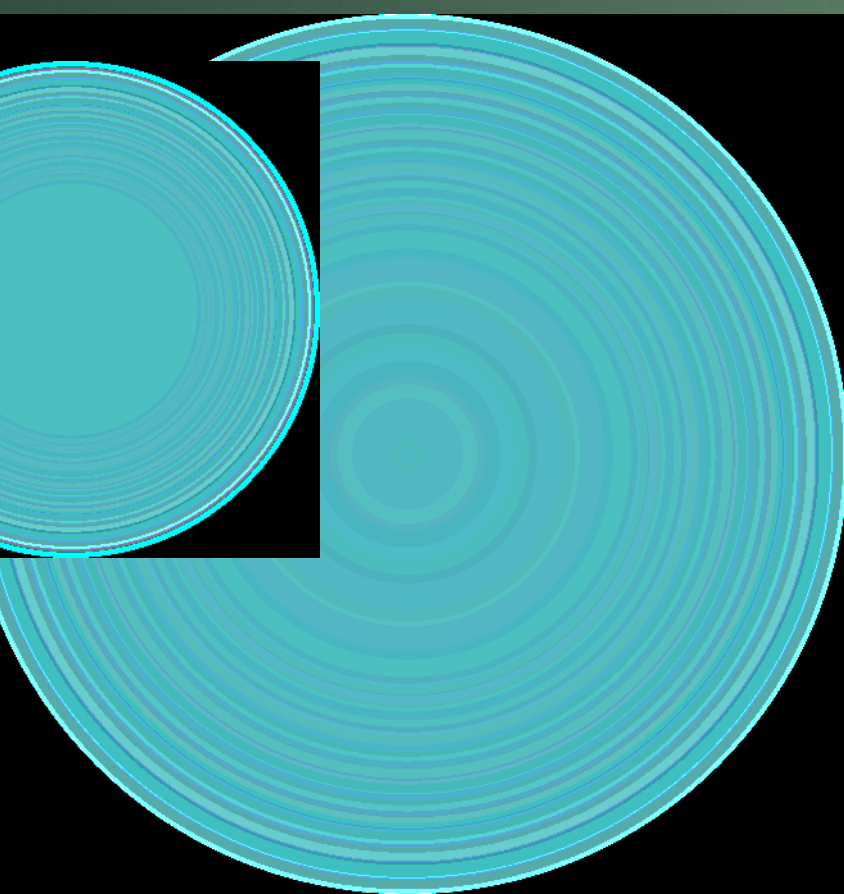
- Now lets block outbound traffic going to ubnetdef.org





# Windows Scenario

► What type of rule?



New Outbound Rule Wizard

## Rule Type

Select the type of firewall rule to create.

**Steps:**

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

☒ **Program**  
Rule that controls connections for a program.

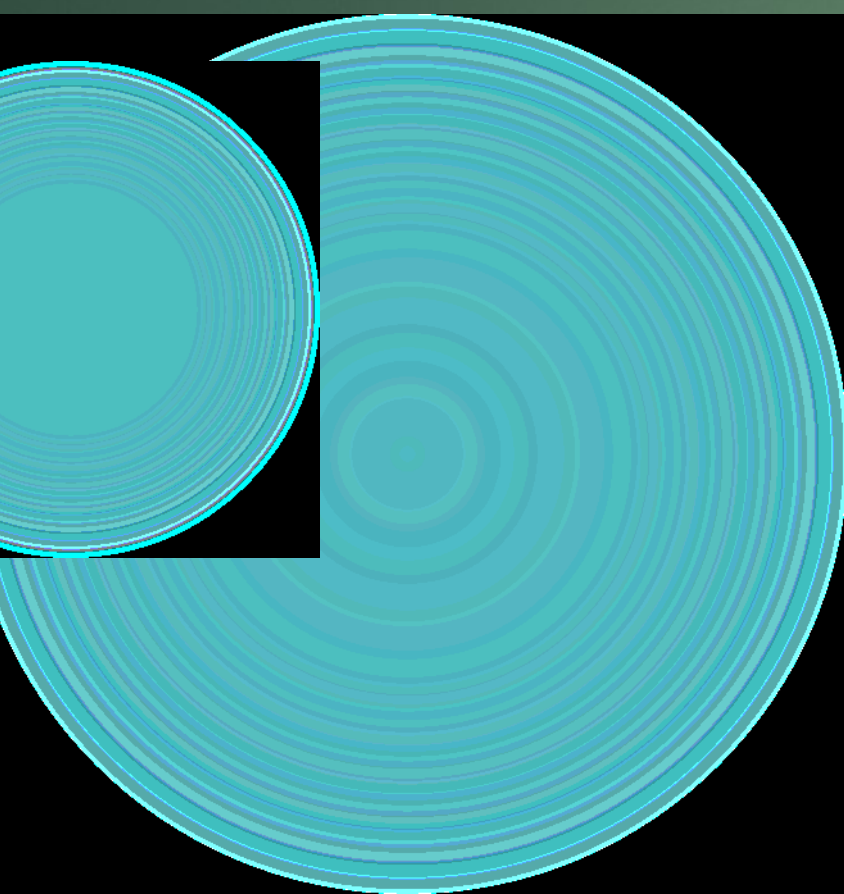
☐ **Port**  
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**  
BranchCache - Content Retrieval (Uses HTTP)  
Rule that controls connections for a Windows experience.

☐ **Custom**  
Custom rule.

# Windows Scenario

► What type of rule?



New Outbound Rule Wizard

### Rule Type

Select the type of firewall rule to create.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**  
Rule that controls connections for a program.

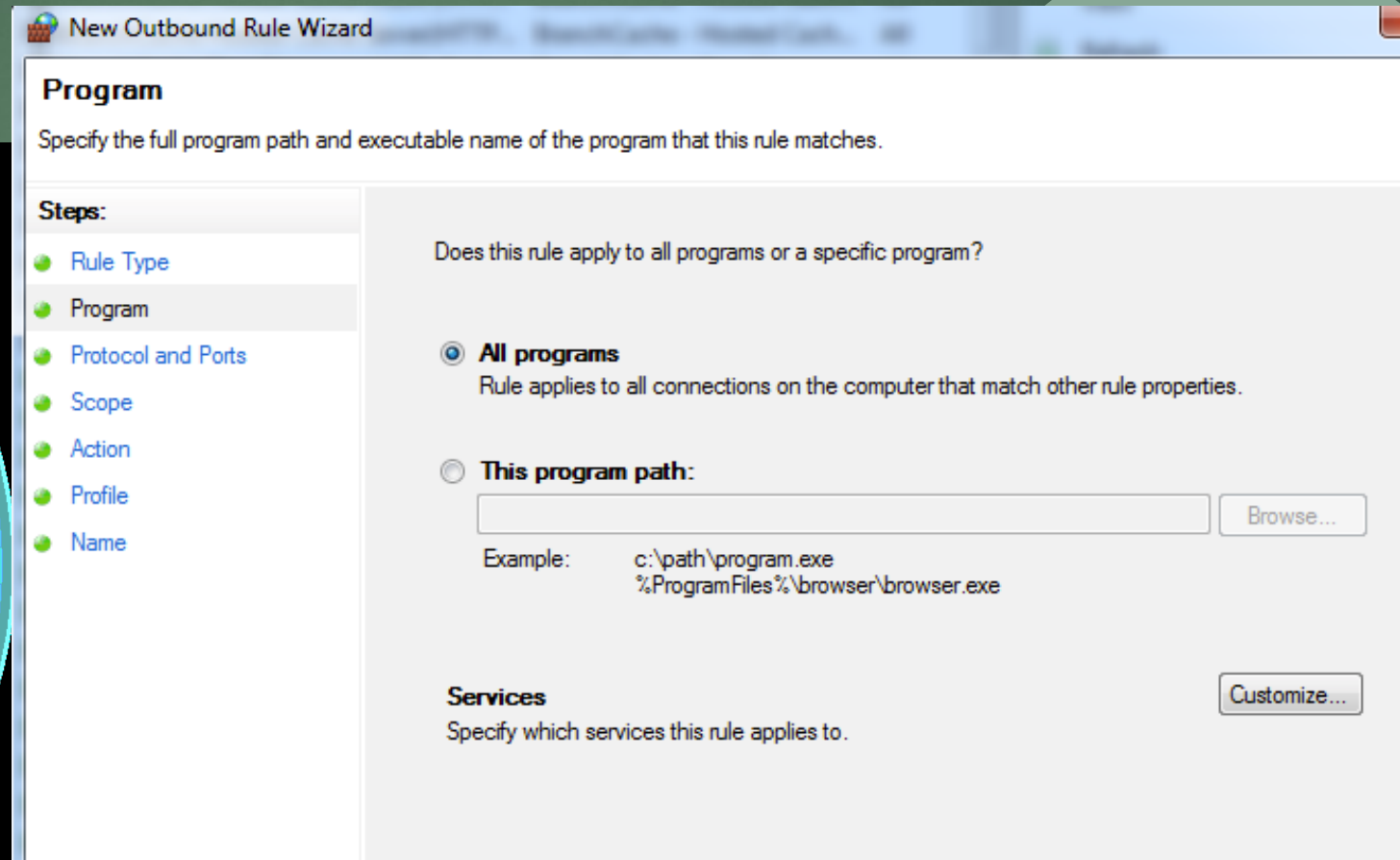
☐ **Port**  
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**  
BranchCache - Content Retrieval (Uses HTTP)  
Rule that controls connections for a Windows experience.

☒ **Custom**  
Custom rule.

# Windows Scenario

## ► Program?



The image shows a screenshot of the 'New Outbound Rule Wizard' window in Windows Firewall. The window title is 'New Outbound Rule Wizard'. The current step is 'Program', which is highlighted in the 'Steps' list on the left. The 'Steps' list includes: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area of the wizard asks 'Does this rule apply to all programs or a specific program?'. There are two radio button options: 'All programs' (selected) and 'This program path:'. The 'All programs' option has a description: 'Rule applies to all connections on the computer that match other rule properties.' The 'This program path:' option has a text input field and a 'Browse...' button. Below the input field, there are example paths: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom of the wizard, there is a 'Services' section with the text 'Specify which services this rule applies to.' and a 'Customize...' button.

**Program**

Specify the full program path and executable name of the program that this rule matches.

**Steps:**

- Rule Type
- Program**
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

☒ **All programs**  
Rule applies to all connections on the computer that match other rule properties.

☐ **This program path:**

Example: c:\path\program.exe  
%ProgramFiles%\browser\browser.exe

**Services**  
Specify which services this rule applies to.



# Windows Scenario

## ► Protocol?

New Outbound Rule Wizard

### Protocol and Ports

Specify the protocols and ports to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports**
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type:

Protocol number:

Local port:

Example: 80, 443, 5000-5010

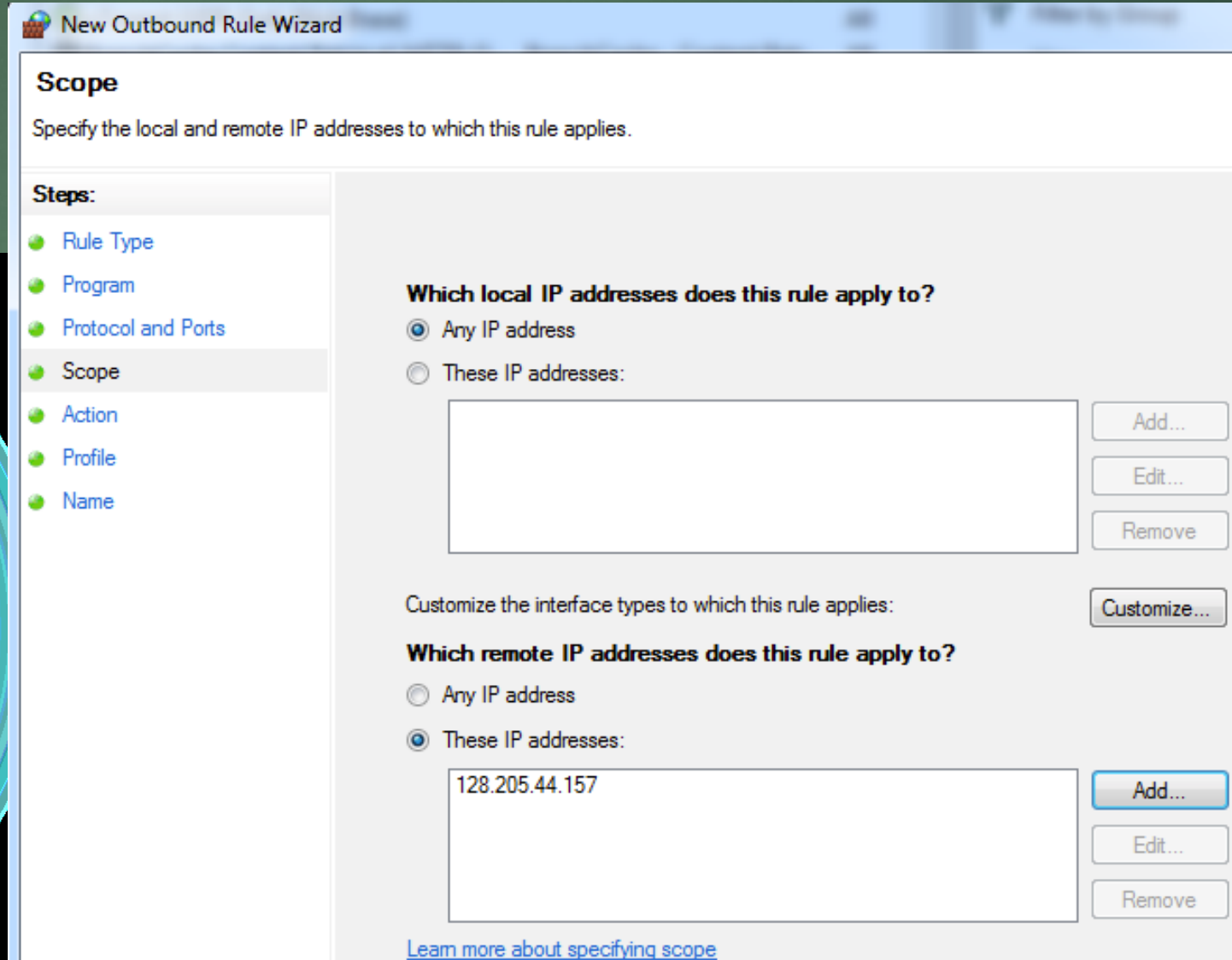
Remote port:

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

# Windows Scenario

► Scope?



The image shows a screenshot of the 'New Outbound Rule Wizard' window in Windows Firewall. The 'Scope' step is selected in the left-hand 'Steps' list. The main area is titled 'Scope' and contains the instruction 'Specify the local and remote IP addresses to which this rule applies.' Under the heading 'Which local IP addresses does this rule apply to?', the 'Any IP address' radio button is selected. Below this is an empty text box for specifying IP addresses, with 'Add...', 'Edit...', and 'Remove' buttons to its right. Further down, there is a 'Customize the interface types to which this rule applies:' section with a 'Customize...' button. Under the heading 'Which remote IP addresses does this rule apply to?', the 'These IP addresses:' radio button is selected. Below this is a text box containing the IP address '128.205.44.157', with 'Add...', 'Edit...', and 'Remove' buttons to its right. At the bottom, there is a link that says 'Learn more about specifying scope'.

New Outbound Rule Wizard

**Scope**  
Specify the local and remote IP addresses to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**Which local IP addresses does this rule apply to?**

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

**Which remote IP addresses does this rule apply to?**

☐ Any IP address

☒ These IP addresses:

128.205.44.157

Add... Edit... Remove

[Learn more about specifying scope](#)

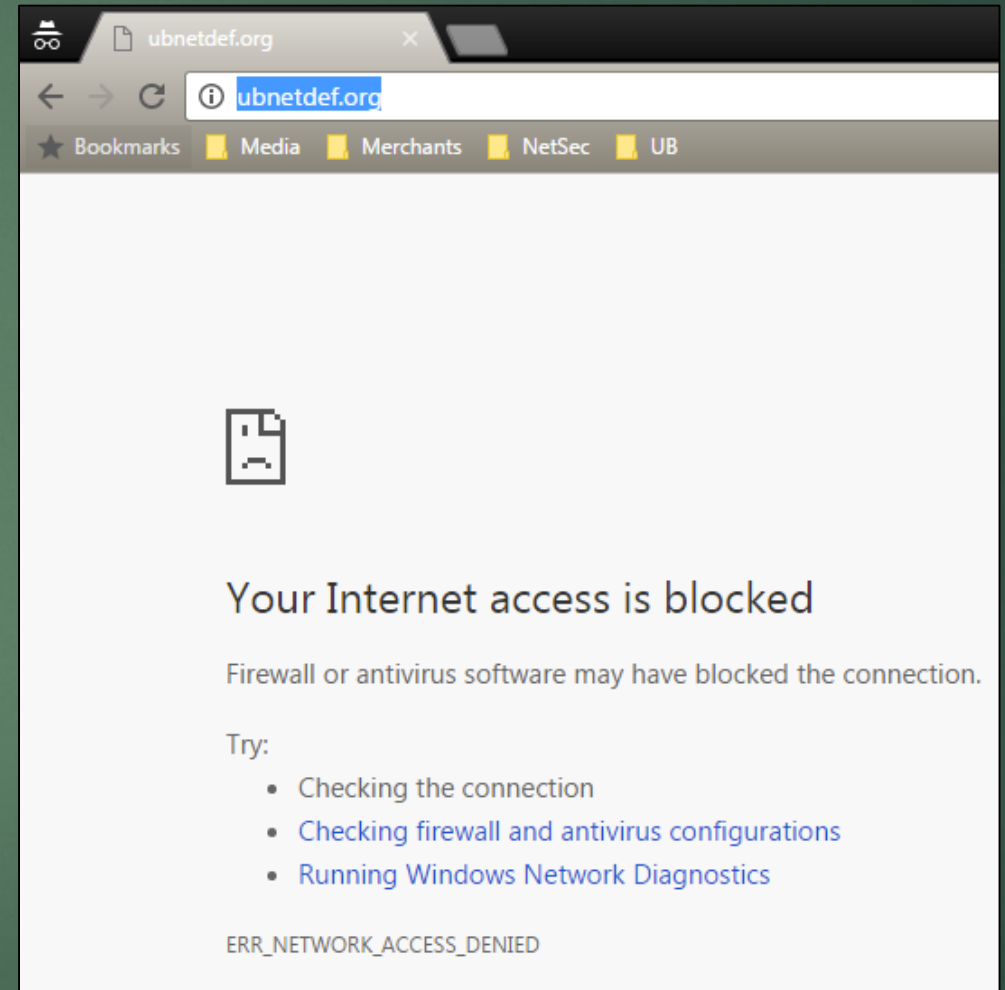
# Windows Scenario

► 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