FIREWALLS 101

CHRIS KLIMEK

https://youtu.be/H3HFOlYba-4

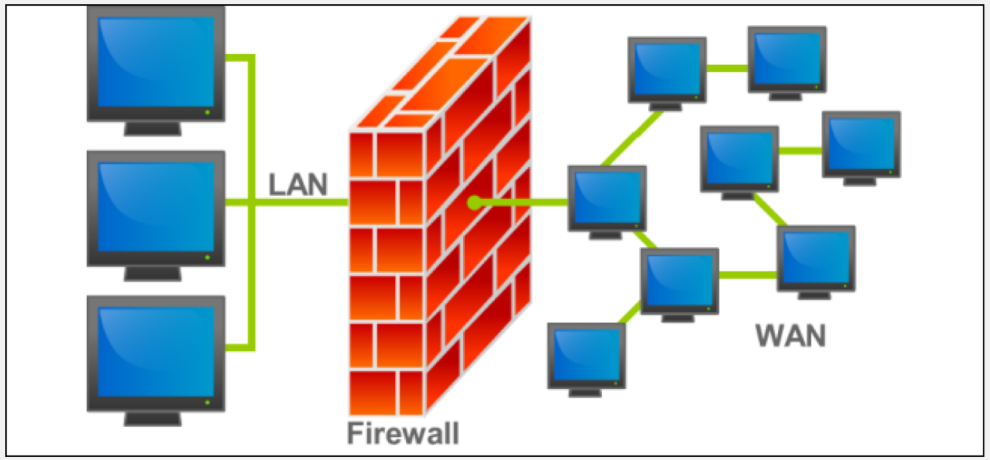
DISCUSSION TOPICS

- General overview
- Types of firewalls
- Implementation
- **More to come….**

WHAT DO THEY DO??

WHAT DO THEY DO??

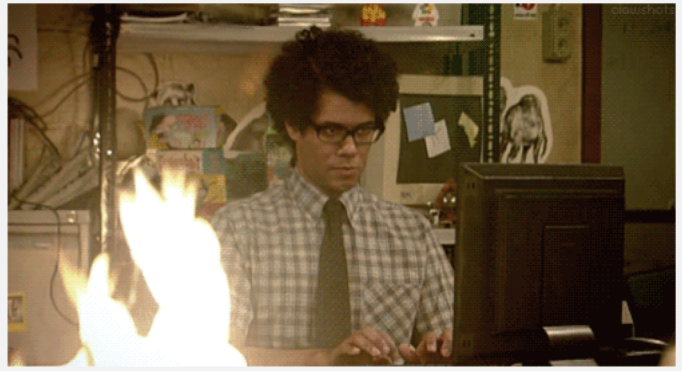
- Controls network connections
- Prevents / allows access to networks



WHAT HAPPENS WITHOUT ONE??

WHAT HAPPENS WITHOUT ONE??

- Fires start
- Unauthorized users can get into your network
- Bad things happen



TYPES OF FIREWALLS

- **Packet layer** – Analyzes traffic at transport protocol layer
- **Circuit level** – Validates that packets are either connection or data packets
- **Application layer** – Ensures data is valid at the application level before connecting
- **Proxy server** – Intercepts messages going in / out of the network

WHAT CAN YOU CONTROL?

WHAT CAN YOU CONTROL?

- Ports
- IP addresses
- MAC addresses

WHERE CAN YOU GET ONE??

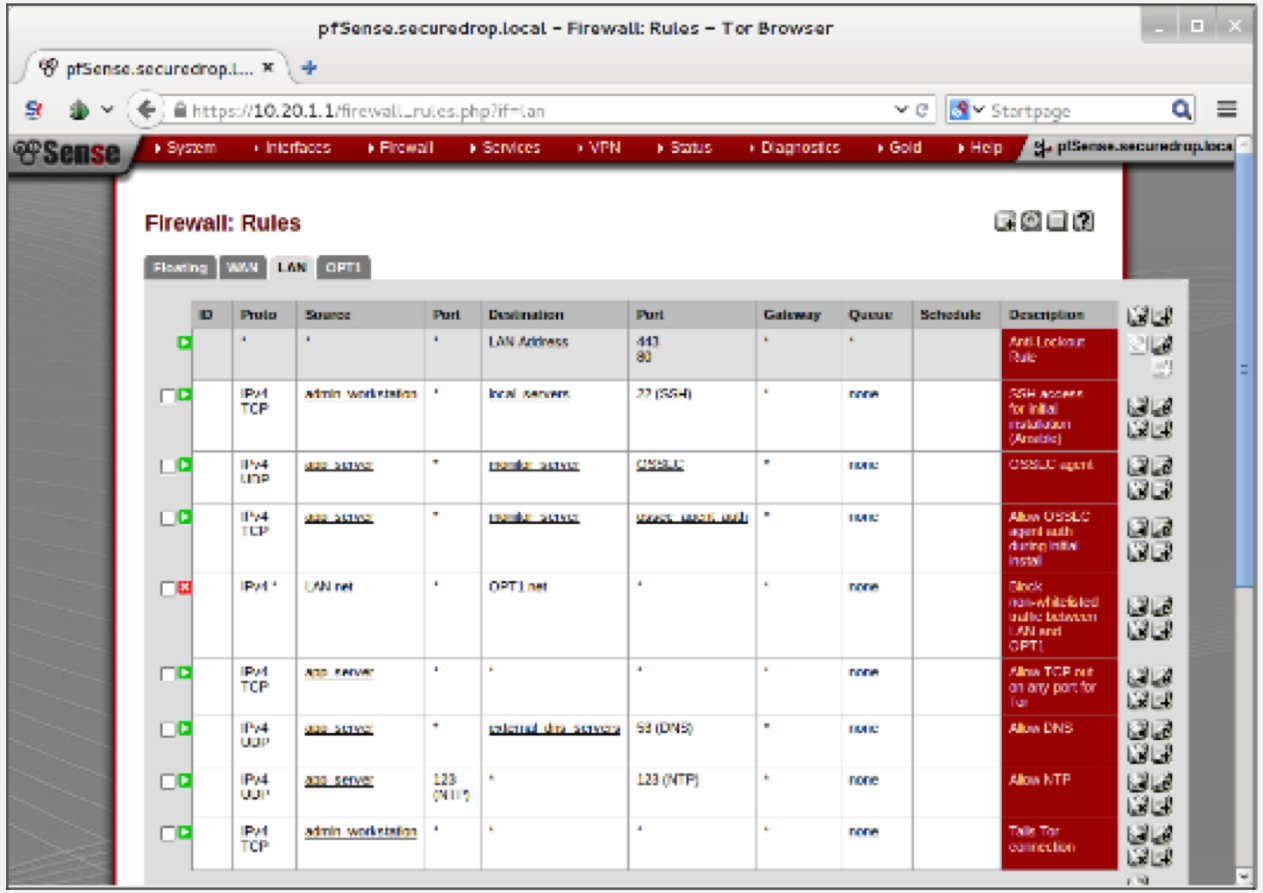
WHERE CAN YOU GET ONE??

- Multiple computers
  - Physical network firewalls
  - Routers
- Single computer
  - Built into OS
  - Additional software

DIFFERENT TYPES

- IP Tables
- UFW
- Windows Firewall
- Symantec
- PF Sense
- Cisco
- Juniper

PF SENSE




```
Block example:
    easyrule block wan 1.2.3.4

Pass example (protocol with port):
    easyrule pass wan tcp 1.2.3.4 192.168.0.4 80

Pass example (protocol without port):
    easyrule pass wan icmp 1.2.3.4 192.168.0.4
```

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 ~]#
```

SOME IP TABLE COMMANDS

- -A : append one or more rules
- -D : delete one or more rules
- -I : insert one or more rules
- -F : flush the selected chain / deleting a rule one by one

- http://ipset.netfilter.org/iptables.man.html

LINUX

- Block an incoming IP address

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

- Block an incoming port

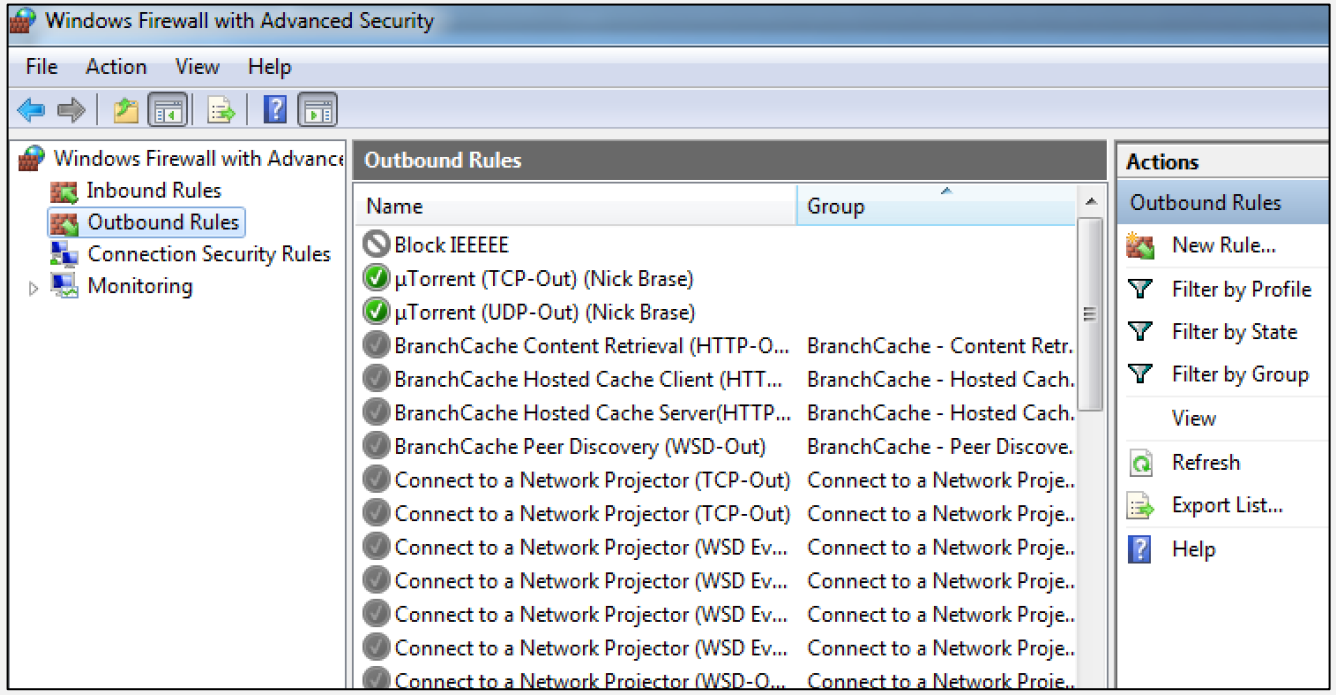
```
root@LB-VM:~/Desktop# iptables -A INPUT -s 10.42.X.XXX -p tcp --destination-po
rt 80 -j DROP
```

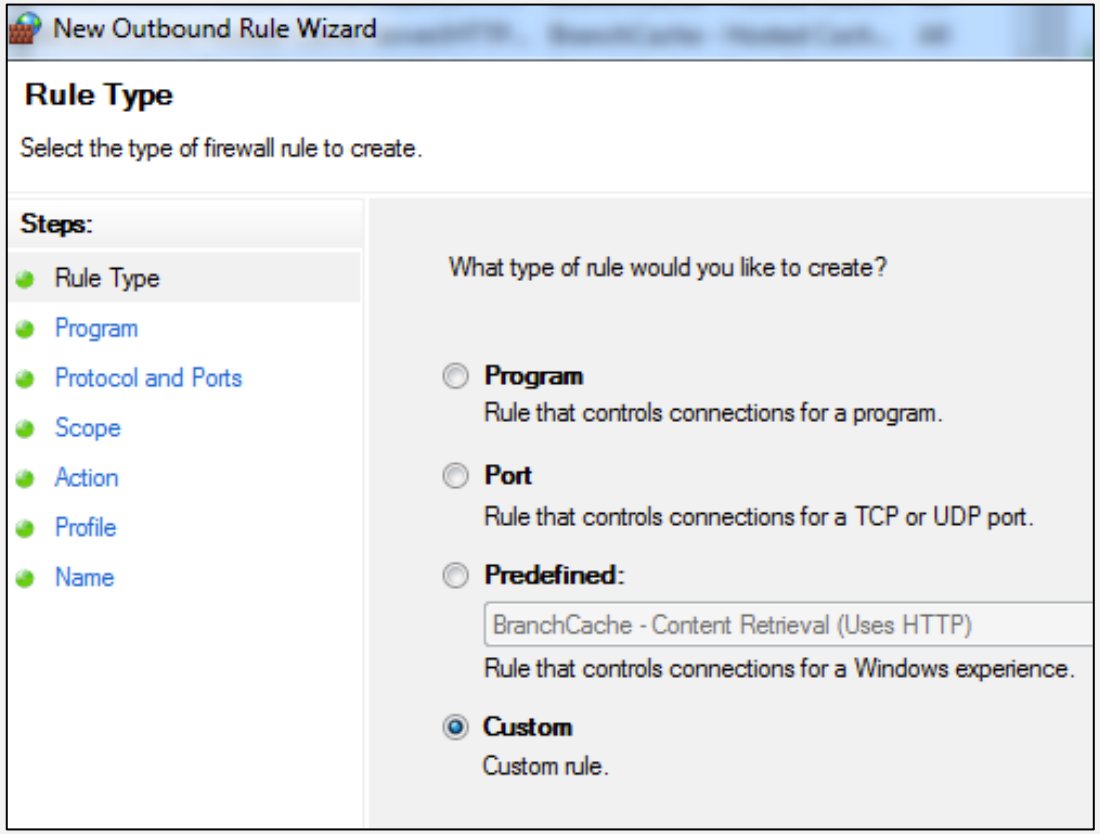
LINUX

- Block an outgoing IP address

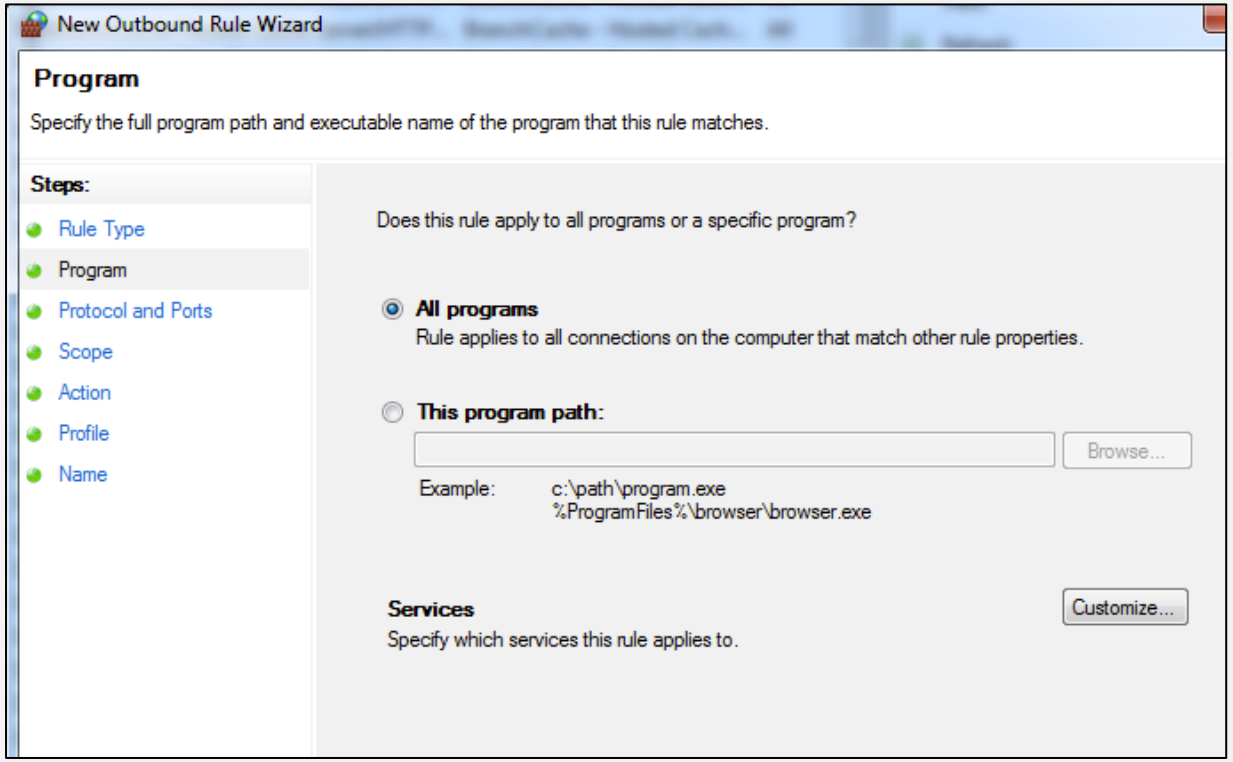
```
# iptables -A OUTPUT -d 75.126.153.206 -j DROP
```

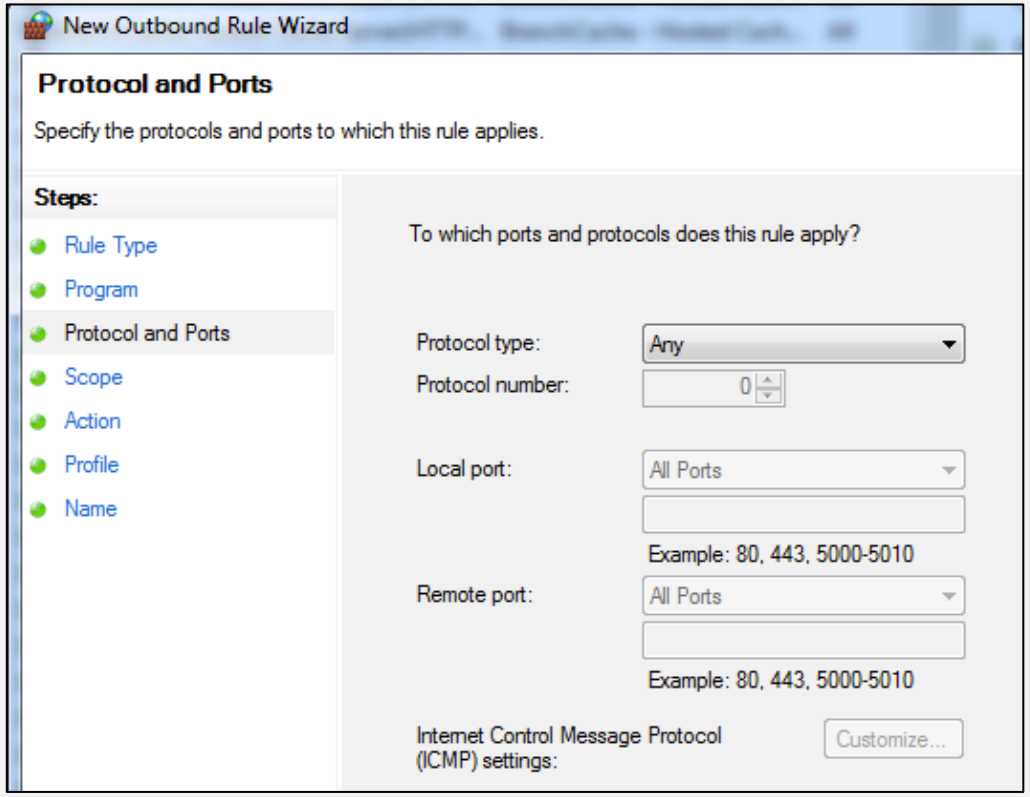
WINDOWS


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Block IEEEEE
µTorrent (TCP-Out) (Nick Brase)
µTorrent (UDP-Out) (Nick Brase)
BranchCache Content Retrieval (HTTP-O... BranchCache - Content Retr.
BranchCache Hosted Cache Client (HTT... BranchCache - Hosted Cach.
BranchCache Hosted Cache Server(HTTP... BranchCache - Hosted Cach.
BranchCache Peer Discovery (WSD-Out) BranchCache - Peer Discove.
Connect to a Network Projector (TCP-Out) Connect to a Network Proje..
Connect to a Network Projector (TCP-Out) Connect to a Network Proje..
Connect to a Network Projector (WSD Ev... Connect to a Network Proje..
Connect to a Network Projector (WSD Ev... Connect to a Network Proje..
Connect to a Network Projector (WSD Ev... Connect to a Network Proje..
Connect to a Network Projector (WSD Ev... Connect to a Network Proje..
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

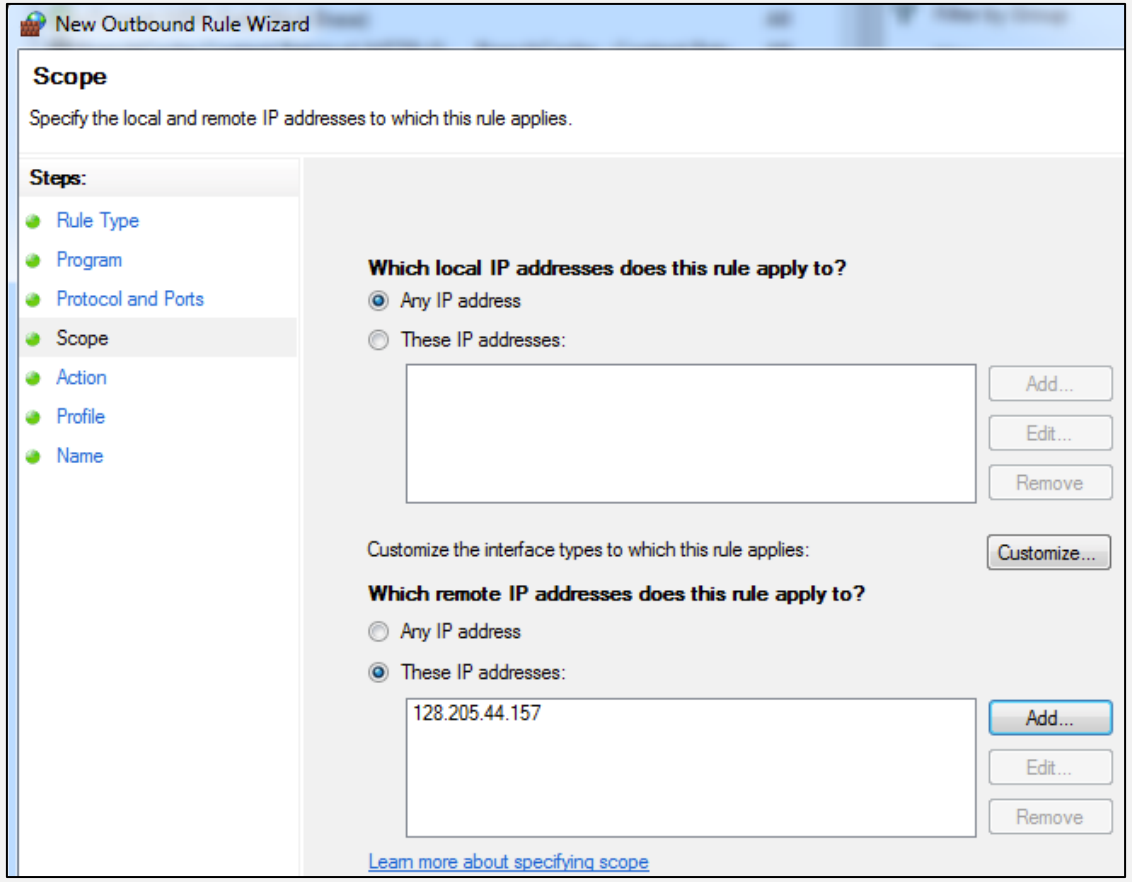

New Outbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.
Custom
Custom rule.

WINDOWS


New Outbound Rule Wizard
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:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...


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:
Any
Protocol number:
0
Local port:
All Ports
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...

WINDOWS


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

BEST PRACTICES

- Drop all connections
- Add connections as needed
- Read from top to bottom

* All of this is very important for competitions and may be a determinant factor in winning!!

TAKEAWAY

- Having a firewall means that you will not be hacked…ever

(THIS IS SARCASM)