SI110
Networking – Firewalls

Major Brian Hawkins, USMC

U.S. Naval Academy

Fall AY 2018

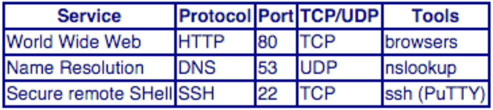
Outline

1. Services Over a Network
    - Disabling Services
2. Firewalls & ACLs
    - Firewall Location

Services over a network

Review from Pillars Lecture

- Tension between *services* and *security*
  - House with no doors or windows. . .
  - . . . offering a service (listening on a port)
  - gives attackers an entry point
- What are some vulnerabilities of providing the below services?



Service	Protocol	Port	TCP/UDP	Tools
World Wide Web	HTTP	80	TCP	browsers
Name Resolution	DNS	53	UDP	nslookup
Secure remote SHell	SSH	22	TCP	ssh (PuTTY)

Disabling Services

Pretend you're a server administrator.... . .

How could you disable your host from being a "web server"?

- Don't run the process that facilitates that service
- Don't allow any data to be sent to the port number associated with the service

Pretend you're a network/domain administrator.... . .

How could you disable web browsing for your client hosts?

- Block outbound network traffic destined for port 80
- ...but what if there's a web server NOT running on port 80?

Disabling Services

Pretend you're a server administrator.... . .

How could you disable your host from being a "web server"?

- Don't run the process that facilitates that service
- Don't allow any data to be sent to the port number associated with the service

Pretend you're a network/domain administrator.... . .

How could you disable web browsing for your client hosts?

- Block outbound network traffic destined for port 80
- ...but what if there's a web server NOT running on port 80?

Disabling Services

Pretend you’re a server administrator.... . .

How could you disable your host from being a ”web server”?

- Don’t run the process that facilitates that service
- Don’t allow any data to be sent to the port number associated with the service

Pretend you’re a network/domain administrator.... . .

How could you disable web browsing for your client hosts?

- Block outbound network traffic destined for port 80
- ...but what if there’s a web server NOT running on port 80?

Disabling Services – Continued

Moral of the story: we can can block access to a service by throwing out packets that are destined for the port number associated with it. This is called *filtering* traffic.

What if we want to offer a service, but only to certain hosts?

- What information could we use to *filter* network traffic?
- We've seen that we can use source and destination port numbers.
- What about source and destination IP addresses?
- What about protocol – e.g. TCP/UDP?

All of the above

If we only wanted users in the 1.1.1.0/24 network to access our website, we could allow only TCP traffic from IP addresses in the 1.1.1.0/24 network to send traffic to port 80, and deny all other traffic to port 80.

Disabling Services – Continued

Moral of the story: we can can block access to a service by throwing out packets that are destined for the port number associated with it. This is called *filtering* traffic.

What if we want to offer a service, but only to certain hosts?

- What information could we use to *filter* network traffic?
- We've seen that we can use source and destination port numbers.
- What about source and destination IP addresses?
- What about protocol – e.g. TCP/UDP?

All of the above

If we only wanted users in the `1.1.1.0/24` network to access our website, we could allow only TCP traffic from IP addresses in the `1.1.1.0/24` network to send traffic to port 80, and deny all other traffic to port 80.

Disabling Services – Continued

Moral of the story: we can can block access to a service by throwing out packets that are destined for the port number associated with it. This is called *filtering* traffic.

What if we want to offer a service, but only to certain hosts?

- What information could we use to *filter* network traffic?
- We've seen that we can use source and destination port numbers.
- What about source and destination IP addresses?
- What about protocol – e.g. TCP/UDP?

All of the above

If we only wanted users in the `1.1.1.0/24` network to access our website, we could allow only TCP traffic from IP addresses in the `1.1.1.0/24` network to send traffic to port 80, and deny all other traffic to port 80.

Enter – the *firewall*!

What is it?

- Either a **device** or a **program** that filters network traffic in order to **control access to services**.

  Could be a standalone, separate device – or, it could be a set of rules on a router

- Configured with a set of rules, called an **Access Control List** (ACL) that it uses to determine whether a packet should be forwarded to its destination or not
- ACL rules can forward or drop a packet based on S/D IP address, protocol, and S/D port numbers
  - **Important!** – ACL rules are checked from top to bottom, in order – once one matches, that action is taken. Order matters!
- **Firewalls allow us to implement our security decisions** – what services can be accessed or provided, and by whom or to whom they may be accessed

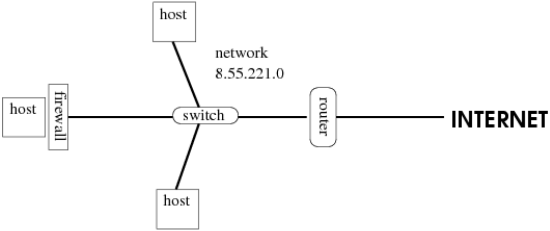
Firewall Location

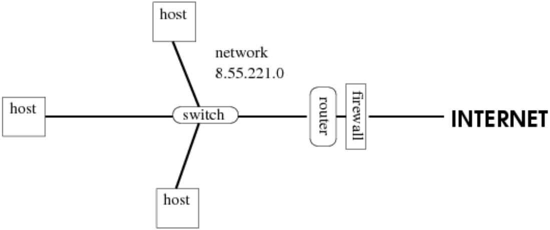
Where in the network should a firewall be located?

Firewall placement

- Firewalls can be implemented on your machine in the Operating System
- Windows 10 has a firewall – so there's a firewall implemented in your Operating System
  - This filters the traffic in and out of your PC!
  - Let's take a look at some of the ACL rules on your machine
- Firewalls can also be placed at the ingress point to our network
  - If it is a device, usually immediately "before" the router, or if it is in software, as a set of ACL rules in the router itself

Firewall Location – Continued





Exercise

http://rona.academy.usna.edu/~sy110/resources/firewall/firewall.html

Questions

Questions?