Introduction to Firewalls

- Creates a single chokepoint that all data must flow through before reaching the LAN
- All inbound and outbound network traffic passes through firewall
- Used in Virtual Private Networks (VPNs)
- An engine with a well defined rule set
  - Firewalls look at incoming packets and based on the rule set, will either forward the packet through, or drop the packet
  - Not possible to have a rule for every possible combination of source and destination IP address
  - The rules implement access control at the packet level
  - Firewall searches through table of policies and look for a match
  - If no match can be made default policy is used
- If a package is encrypted, it can bypass firewall rules (ex: if an IP address is masqueraded it can bypass the firewall)
- If using a wireless network, it is difficult to define a single chokepoint for packages to go through. Therefore, firewalls can also be defined at the wireless level.
- Limitations of Firewalls:
  - They do not solve/prevent Denial of Service attacks.
  - The rules for firewalls are not easy to define.
  - If a firewall designer does not understand the protocol, it might be a poor-quality firewall. The protocol is not necessarily easy to understand.
  - Can not prevent attacks that exploit bugs in the firewall
  - Can not detect insider attacks
  - Firewalls have limited logging functionality, not keeping track of the packets passing through

Types of Firewalls (Four total)

- Packet Filtering Firewall - resides in the transport layer and looks in every file in a packet to make a decision on whether the packet will pass the firewall.
  - Simple and fast
  - Firewall makes a decision on per-packet basis - stateless
- Looks at the destination IP, source IP, destination port and source port, does a matching to determine whether to allow the packet to pass, or to drop the packet
- Policies:
  - Default policy – allow a packet to go through or drop the packet
  - Discard policy: more conservative, as it’s cautious about what to do with the packet, less user friendly
  - Forward policy: more liberal, less secure, more usable; even if you don’t know where the packet is coming from, you may still let it go through.
- Packet Filtering Weaknesses
  - Does not keep track of which packets have come through, analyzes a packet, then immediately forgets what was in that packet after the decision has been made
  - “Tiny fragment attack”, if fragment size is small it is possible to force part of the TCP header into another packet
    - Example: IP address gets chopped up between two packets the firewall will not recognize it
- Problem with stateless filtering
  - Server should be allowed to send outgoing packets by default
  - There is no verification of a valid connection, server no way to know if it’s making a valid response to a request
- Stateful Inspection Firewall
  - Reviews packet header info similar to Packet Filtering
  - It keeps track of state information - it remembers which packets it has already seen
- Application-Level Gateway
  - Operates on the Application layer, which is a layer that is able to do filtering
  - Built for a specific application, http, email, etc.
    - Use different protocols for different applications
  - Can prevent tiny-packet attacks
  - More overhead because we are not only looking at packet headers, we are also looking inside the packet
  - Only allows certain addresses to go through (i.e. https)
  - Strength - More secure than packet filters
  - Weakness - must have a proxy code
    - This leads to high overhead as every application needs to be re-engineered to work through a proxy
- Circuit-Level Gateway
  - Designed to filter all of the different types of proxies
  - A compromise to the Application-Level Gateway (lower overhead)
- Operates on all TCP protocols
- Most client/server applications use TCP
- Hardware based, relays TCP segments without examining contents
- Only checks if TCP connection is allowed
  - Similar to an application-level gateway except it works on all applications that use the TCP protocol
- Firewall Basing
  - Firewalls are located on routers
  - Bastion Host
    - Only running essential services
    - Located in a no-man’s land, a DMZ (Demilitarized Zone) between two firewalls
    - Can be used to host/run a honeypot
  - Host-Based Firewall
    - Used to secure individual hosts, such as Servers
    - These can be based at the network interface layer
    - Can configured to a specific host’s needs
    - Can provide protection from internal and external attacks
  - Personal Firewall
    - Mostly for personal use, rather than corporate use
    - Less protection/functionality/complexity than a Host-Based Firewall
    - Mostly used to deny access to unauthorized parties

**Virtual Private Networks**
- Virtual Private Networks (VPN)
  - These allow for secure communication between multiple networks
  - User has a different IP address not associated with network
  - Network firewall may be configured to only allow in network traffic
  - Are used to resolve a specific problem
    - A user is working from a different network than an organization
    - IP Security protocol: authentication and encryption
    - A VPN takes packets generated by a corporate machine and puts them into a different IP packet that has IP address of the corporate network.
    - The machine will be running a VPN client that’s been configured by the corporate manager to repackage the IP packet that’s generated by the remote machine.
    - After it gets past a firewall, a packet that’s passed through a VPN connection will act like any other packet.
Firewall Limitations

- If firewall goes down network goes down
- Does not protect against buggy software, misconfiguration, or bad protocol design
- Not a solution for most DoS attacks
- Does not protect against insider attacks

Intrusion Prevention Systems

- Recent addition to security products that operates in front of a firewall using IDS functionality
- Can block network traffic just like a firewall
  - Host-Based IPS
    - This can be made to work for certain platforms
    - This can also be made to use a sandbox for protected execution
  - Network-based IPS
    - SNORT is a widely used and well-known Network-based IPS

Lecture Summary:

- Firewalls look into packets and use a rule set to decide what packets are allowed through and which ones are dropped.
- The packets that are allowed through depends on how much security a firewall can provide.
- Firewalls have very simple designs and are products that are easy to build.

Socratic Questions

Q1: Can you give more information about what is expected for the poster presentation?

If you haven’t received feedback on your topic, that means that your topic will work and that’s the one that you’ll present. It should be interesting and technical poster that fits the scope of what you have learned in this class.

Q2: How do firewalls compensate for Tor where next node destination ip addresses are encrypted?

Hang on to this discussion until we talk about VPN. Tor client has an address for various Tor routers. The packet goes to various routers in the Tor network. There is an encryption of the IP address and there are substitutions so the user does not know where the address came from.
Q3: Could a packet-filtering firewall be used to combat or prevent a SYN-flood attack?

A SYN Flood needs the firewall to keep track of the state of this particular connection. With enough information, a firewall can detect a SYN Flood

Q4: With the extra monitoring, does a firewall slow down internet performance?

The firewall will have some effect on the components on the network. A network without a firewall will be faster than one that has one. Modern day firewalls are very fast. You can have a fast processor implementing the firewall.

Q5: Is it possible for malware to perform a man in the middle attack and spoof false input coming from what looks like the correct port?

A man in the middle can spoof false input and it can spoof the IP addresses. The answer is yes, but you have to be more specific.

Q6: What will be on the final?

More emphasis will be on what has been covered after the midterm, but some will be from before.

Q7: Are most firewalls implemented on routers and servers or on local machines? (windows firewall vs Router firewall)

We will be coming to this in just a second. Many firewalls are implemented on routers.

Q8: If a firewall goes down, is all traffic allowed through or is everything blocked until it is restored?

A firewall acts as a single chokepoint, so the packets will get dropped until the firewall is back up again, no traffic passes. Everything fails if the firewall is attacked and goes down until it is restored.

Q9: So a VPN is more secure for hiding network activity because it encrypts the IP address the activity is coming from?

Yes, and it can also encrypt the data. That is what makes it more secure. When you use a VPN, traffic going from one machine all the way to the other is encrypted.
Q10: Could firewalls exacerbate some DDoS attacks or is it at worst neutral?

The firewall is a simple chokepoint. I mean, DDos attacks create an availability problem. If there is a single path that everything must go through, it could definitely make it worse.

Q11: If a firewall goes down, is all traffic allowed through or is everything blocked until it is restored?

If the firewall is acting like a single chokepoint and the firewall goes down then all network traffic is stopped. This is a problem with firewalls, if the firewall is attacked then usability and security may be compromised. If there is more than one firewall some points of the network may still be accessible.