Protecting the Network – Firewalls

INFO-6078 – Managing Enterprise Networks

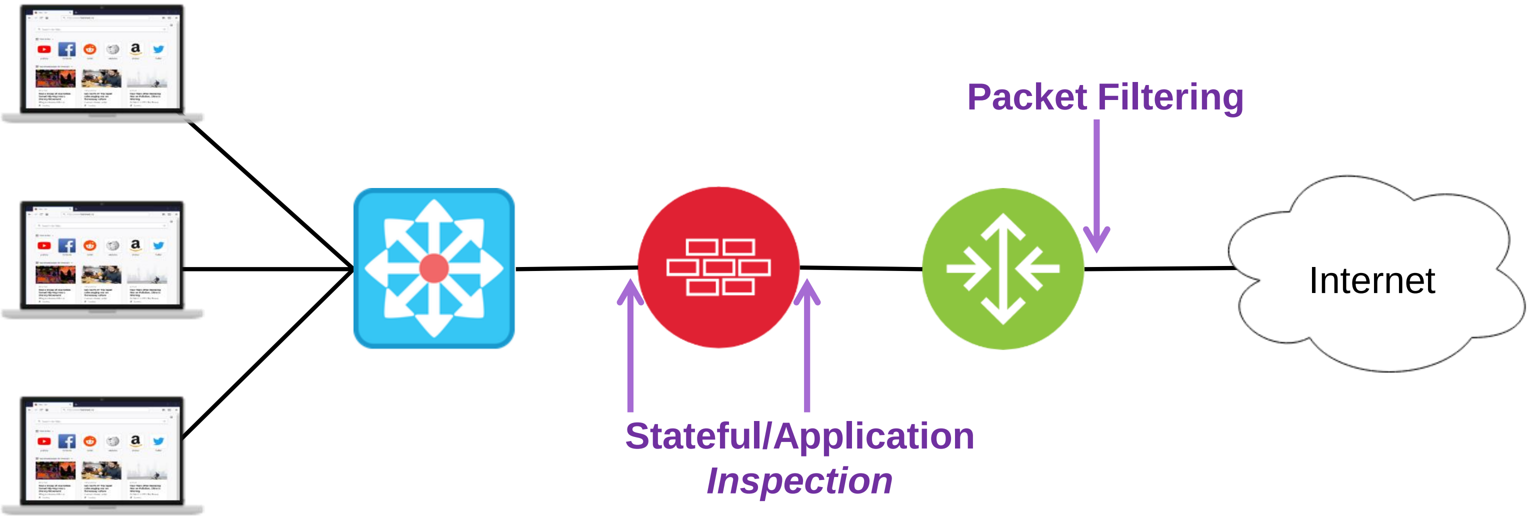
FANSHAWE

Protecting the Network

- As information systems have developed, so has our reliance on the technologies used to maintain them
- Today, much of the services we rely on in our everyday lives rely on computers and networking at the core of their service
- The networks that support these services hold much of our personal information, which needs to be protected from falling into the wrong hands
- Firewalls were developed as an impenetrable barrier to protect these hosts and networks

Firewall Technologies

- Firewalls control what traffic is allowed to flow thorough the device and into the networks that are connected to it
- A firewall is often placed at the edge of a network, or at a network boundary, as a barrier to protect the internal hosts from external threats



Firewall Types

- Firewalls are commonly classified as being either a network firewall or a host firewall
- **Network Firewall**
  - Filters traffic moving between two networks
  - May be implemented as a dedicated device, incorporated into a router or security appliance, or as a component of an operating system in a VM
- **Host Firewall**
  - A software filter that authorizes or denies traffic entering or leaving a specific host machine

Firewall Generations – Packet Filters

- The original firewalls were simple packet filtering devices that discarded traffic based on a set of rules
- Packet filtering was usually restricted to layer 3 and sometimes layer 4 of the OSI model
- The packet could be silently dropped, or an ICMP notification could be generated
- Packet filtering firewalls are also known as stateless firewalls
- Packet filtering is still used as a component of overall network security today

Firewall Generations – Packet Filters

- Packet filter firewalls are less resource intense and can normally be combined with existing routing hardware
- As only simple filtering can occur, rule generation is relatively easy and lowers administrative burden
- Often used to reduce the “noise” at the network perimeter

Firewall Generations – Stateful Filters

- Stateful firewalls added the ability to track individual communication sessions that pass through the device
- By analyzing TCP and UDP source and destination port numbers, stateful firewalls can determine if a session was requested by one of its users
- Individual TCP sessions are analyzed for context of session state (connection, data transfer, closure) and this information is tracked in the state table
- Stateful firewalls dynamically adjust allow rules to accept incoming traffic for established sessions

Firewall Generations – Application Layer

- Aware of protocols in operation from layers 3-7 of the OSI model
  - Has the ability to read and respond to messages from well-know protocols such as DNS, HTTP, and Telnet as long as the data is unencrypted
  - Can identify if a well-know protocol is masquerading as another service to bypass firewall restrictions

Firewall Generations – Next-Generation

- Next-generation firewalls combine traditional firewalls with additional features such as:
  - Intrusion prevention systems
  - SSL interception
  - Antivirus inspection
  - Reputation-based filtering
  - VPN services

Access Control Lists

- Access control lists (ALCs) are used in all aspects of IT to classify and control access to resources
- In relation to networking, ACLs can identify traffic that is allowed or denied access to hosts or network devices based on a set of rules defined by the administrator
- ACLs can filter network traffic based on identifiers found in layers 2, 3, 4 and 7 of the OSI model
- ACLs are also used to classify a particular type of traffic for non-security related functions

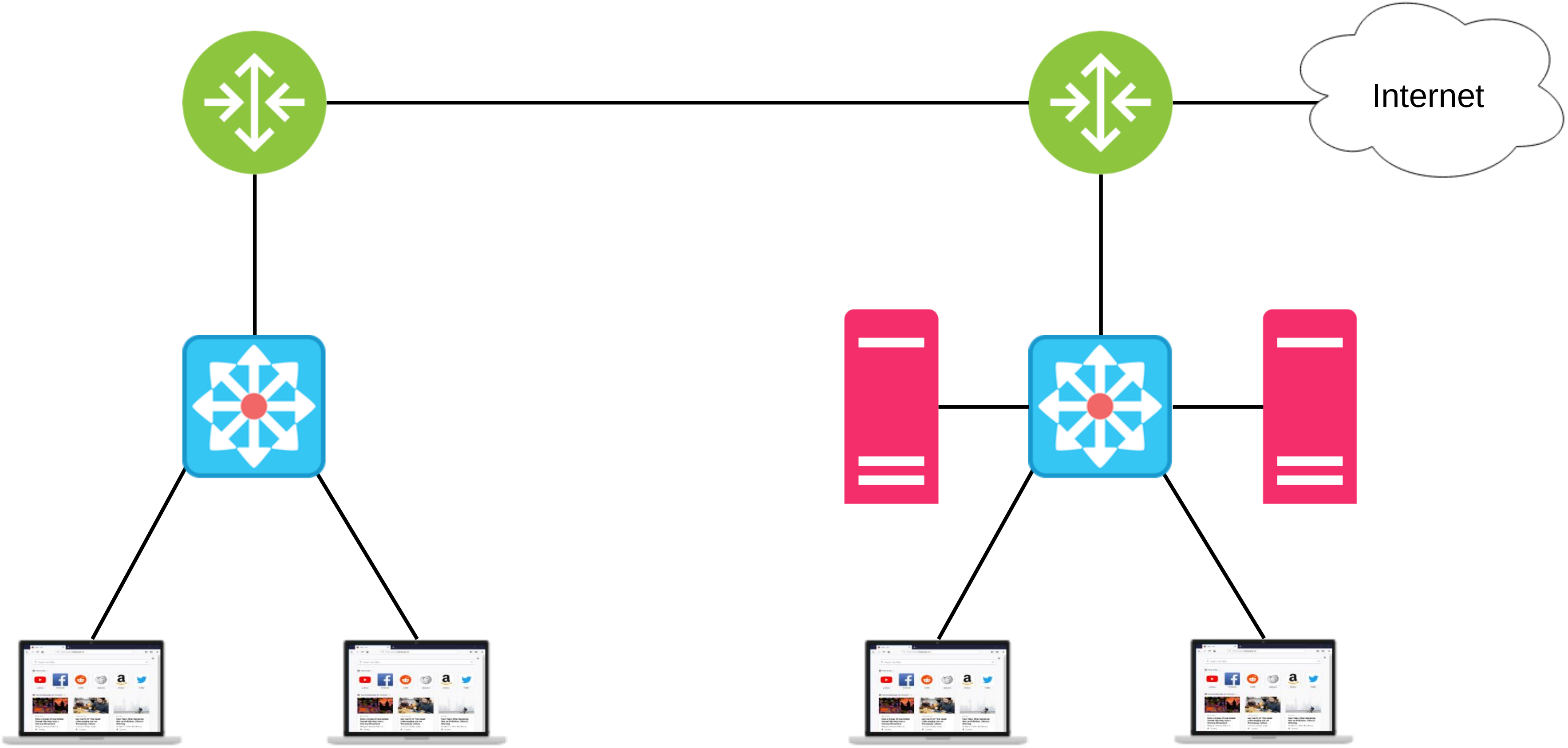
Access Control Lists

- An ACL is a collection of statements called access control entries (ACEs), which define the individual rules used to shape the network traffic
- When traffic is subject to an ACL, the packet is evaluated against each ACE in sequence until a match is found
- ACE should be arranged so that general traffic types are evaluated before specific traffic type to maintain network performance
- In most implementations of ACLs, an implicit deny all statement exists at the end of the ACL
  - If a specific permit statement does not exist, the traffic will be dropped

Access Control Lists

- ACEs can evaluate traffic based on the following criteria:
  - Source MAC address
  - Source or destination IP address/subnet
  - Protocol
  - Layer 4 source or destination port number
  - Established session
  - Time of day
  - Session length

ACL Example



ACL Placement

- ACLs should be placed on EVERY interface to verify ingress traffic on the interface
- On edge interfaces, ACLs should also sanitize egress traffic leaving the organization
- Cisco ACLs come in two different types:
  - Standard ACL
    - Filters based on the source IP address
    - Should be placed close to the traffic destination
  - Extended ACL
    - Filters based on source/destination IP address, protocol, port
    - Should be placed close to the traffic source

ACL Protection Examples

- ACLs can provide an effective first step to mitigating simple attacks in lower network layers
- Some attack types that ACLs can help prevent:
  - IP/MAC address spoofing
  - Denial-of-Service (DoS) attacks
  - ICMP manipulation attacks
  - IP subnet scanning

ACL Example – IP Spoofing

- On edge interfaces, ACLs should prevent the following traffic source ranges from entering the organizations network:
  - **Special Use Addresses**
    - All zeros (0.0.0.0/32)
    - Loopback (127.0.0.0/8)
    - Documentation (192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24)
    - IP Multicast (224.0.0.0/4)
    - Broadcast (255.255.255.255/32)
  - **Private IP Addresses (RFC 1918)**
    - Class A (10.0.0.0/8)
    - Class B (172.16.0.0/12)
    - Class C (192.168.0.0/16)
  - **Any public addressing used within the network boundary**

ACL Example – ICMP Manipulation

- Edge interfaces should strictly control the types of ICMP traffic that are allowed to enter the organization
- ICMP is required for normal operation of the network, but can be abused to subvert routing tables, deny access to resources or scan internal hosts as a part of network enumeration
- ICMP messages required for normal operation:
  - **Echo/Echo Reply**
    - Allows internal hosts to ping external hosts
    - External hosts should be prevented from pinging internal hosts

ACL Example – ICMP Manipulation

- **Unreachable**
  - Informs a host requested resources are unavailable
- **Fragmentation Required/Packet Too Big**
  - Informs the source that the message cannot be delivered as it exceeds the MTU of a link en-route to the destination
- **Time Exceeded**
  - Informs the source that the message could not be delivered due to the IP TTL expiring in transit
  - Required for the operation of traceroute

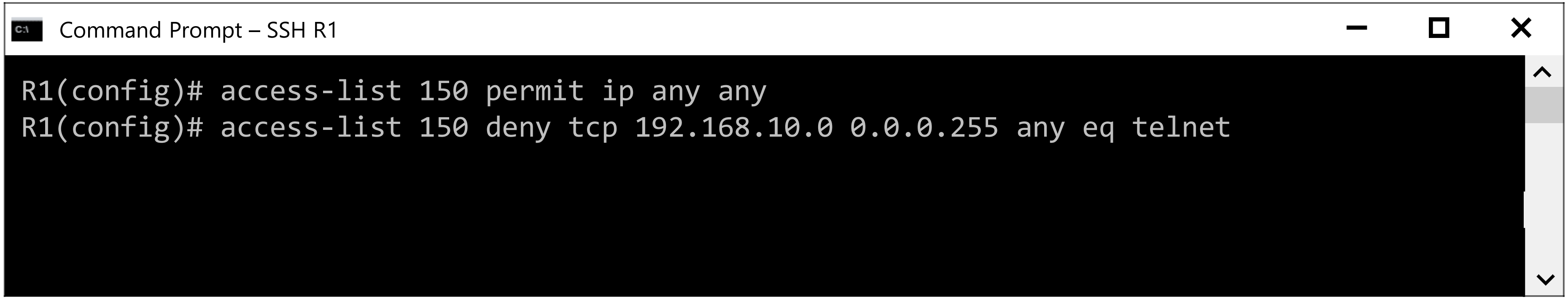
- All allowed ICMP traffic should be rate limited to prevent protocol abuse

*** ICMP source quench depreciated in RFC 6633 (2012)**

ACL Evaluation

- ACLs filter traffic based on rules, but if the configured rules contain incorrect logic, the ACL can have unintended effects on the network

What is the result of the following ACL?



```
R1(config)# access-list 150 permit ip any any
R1(config)# access-list 150 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```