

Week 9 - Network Security

Firewalls



THE UNIVERSITY OF
SYDNEY

Dr. Suranga Seneviratne

School of Computer Science, The University of Sydney

Agenda

- Basics of Firewalls
- Stateful Firewalls
- Stateless Firewalls
- Common Firewall Configurations and Mistakes

1. Network Firewalls - Overview

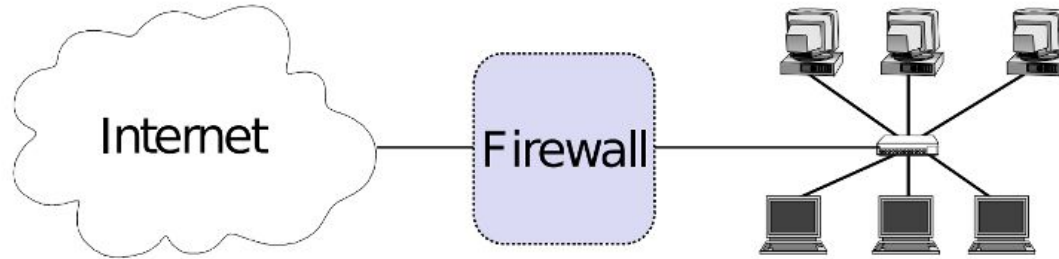


Network Firewalls - Overview

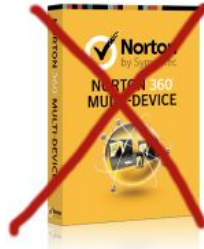
- **Story of firewall**
 - Building construction
 - Keep a fire from spreading from one part of the building to another
 - Network: Better compared to a moat of a medieval castle
 - Restricts people to enter at one carefully controlled point
 - Prevents attackers from getting close to other defenses
 - Restricts people to leave at one carefully controlled point



Network Firewalls - Overview

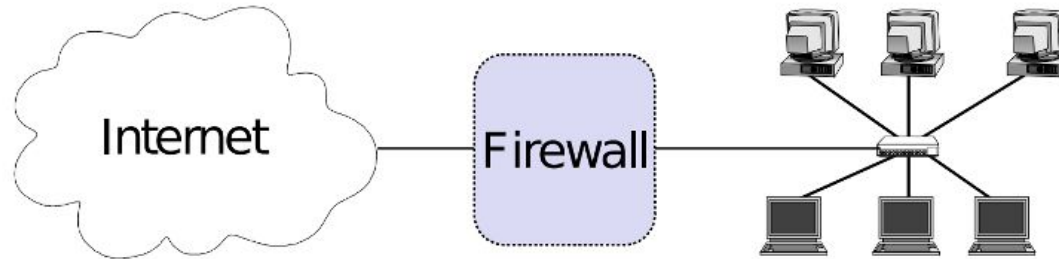


Do not get confused with host-based firewalls



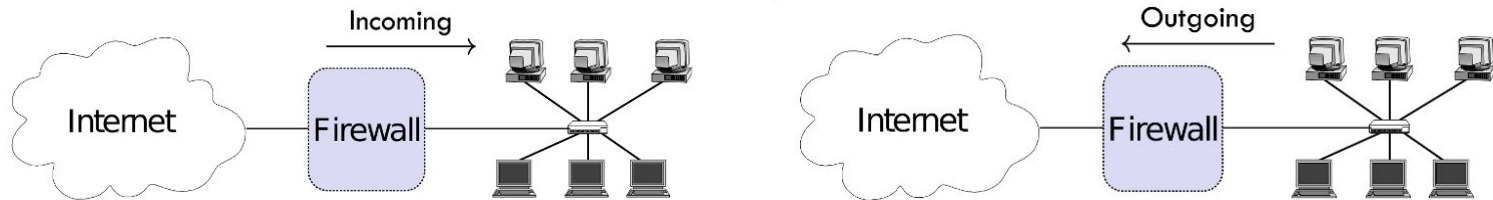
Network Firewalls - Overview

- **Controlled Access** at the network level
- Install where a protected subnetwork is connected to a less trusted network
- If not specified otherwise, we assume
 - Firewall is placed between Internet and local network



Network Firewalls - Principles

- We need to define what incoming and outgoing means in the context of the networks we deal with.
- This is dependent on where you view the packets from.
- **Example - View 1: Viewpoint of an admin of the LAN**

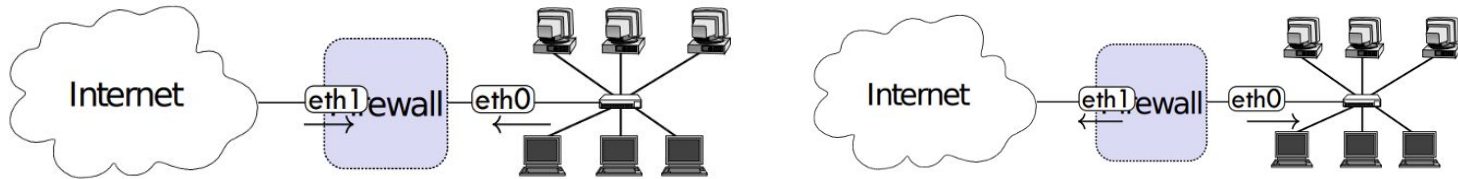


Incoming: from the Internet to the local network

Outgoing: from the local network to the Internet

Network Firewalls - Principles

- We need to define what incoming and outgoing means in the context of the networks we deal with.
- This is dependent on where you view the packets from.
- **Example - View 2: Right in the middle of the firewall, say the man page.**



On each interface, there are incoming and outgoing packets

2. Network Firewalls - Basic Configurations



Firewall Configuration

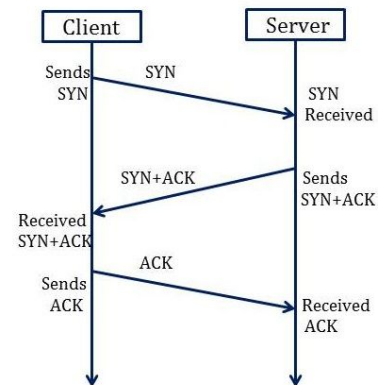
Firewalls need configuration.

- **Whitelisting**
 - Default deny strategy: Everything not explicitly permitted is denied
 - Increased security
- **Blacklisting**
 - Default permit strategy: Everything not explicitly forbidden is permitted
 - Less hassle with users
- **Best Practice:** Whitelisting. But may not be practical in many situations

Firewall Configuration - Example

Rule	Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

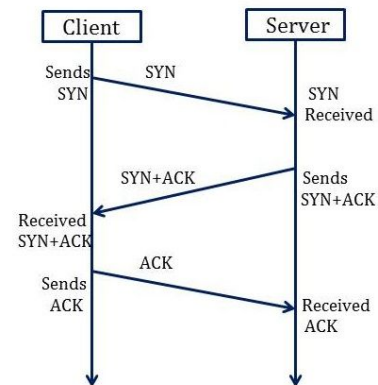
- **Policy: Allow outgoing HTTP (TCP port 80), deny the rest**
- LAN can initiate outgoing HTTP connections
 - Example: SYN
- The Internet may respond to established connections
 - Example: SYN,ACK
- LAN may use established connections
 - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
 - Example: DNS



Firewall Configuration - Example

Rule	Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

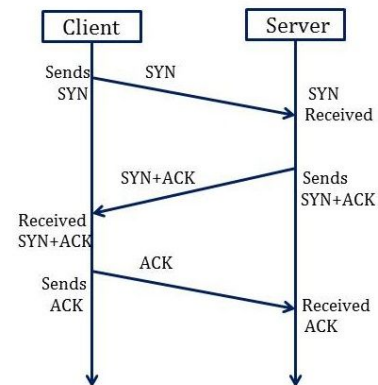
- **Policy: Allow outgoing HTTP (TCP port 80), deny the rest**
- LAN can initiate outgoing HTTP connections
 - Example: SYN
- The Internet may respond to established connections
 - Example: SYN,ACK
- LAN may use established connections
 - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
 - Example: DNS



Firewall Configuration - Example

Rule	Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

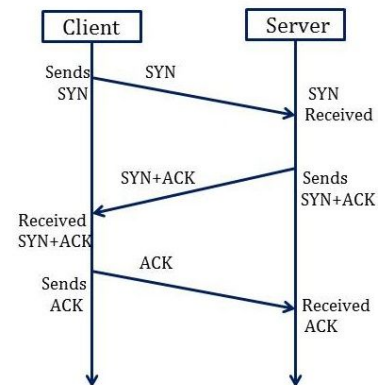
- **Policy: Allow outgoing HTTP (TCP port 80), deny the rest**
- LAN can initiate outgoing HTTP connections
 - Example: SYN
- **The Internet may respond to established connections**
 - Example: SYN,ACK
- LAN may use established connections
 - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
 - Example: DNS



Firewall Configuration - Example

Rule	Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

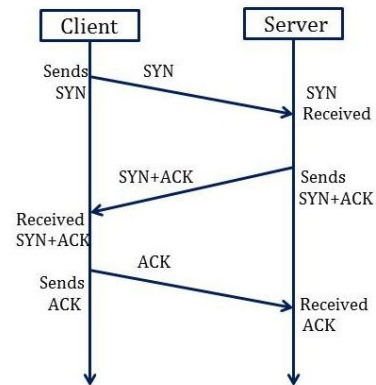
- **Policy: Allow outgoing HTTP (TCP port 80), deny the rest**
- LAN can initiate outgoing HTTP connections
 - Example: SYN
- The Internet may respond to established connections
 - Example: SYN,ACK
- LAN may use established connections
 - Example: ACK, HTTP GET / HTTP/1.0
- Everything else is prohibited
 - Example: DNS



Firewall Configuration - Example

Rule	Interface	Source IP	Destination IP	Protocol	Source Port	Destination Port	State	Action
A	lan	192.168.0.0/16	0.0.0.0/0	TCP	> 1023	80	New,Est.	Accept
B	inet	0.0.0.0/0	192.168.0.0/16	TCP	80	> 1023	Est.	Accept
C	*	0.0.0.0/0	0.0.0.0/0	*	*	*	*	Drop

- **Policy: Allow outgoing HTTP (TCP port 80), deny the rest**
- LAN can initiate outgoing HTTP connections
 - Example: SYN
- The Internet may respond to established connections
 - Example: SYN,ACK
- LAN may use established connections
 - Example: ACK, HTTP GET / HTTP/1.0
- **Everything else is prohibited**
 - Example: DNS



Firewall Configuration

- A firewall is configured by a list of rules
- For every packet, the ruleset is processed sequentially until a matching rule is found
- A rule consists of
 - Match condition
 - Action

Firewall Configuration: Rules

- Actions

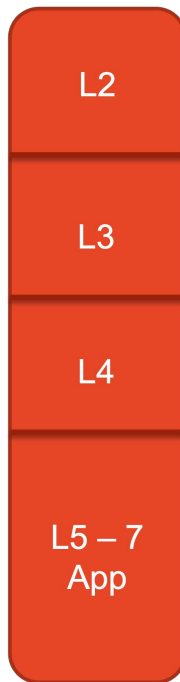
- Accept
- Drop, Reject
- Log
- ...

- Match Conditions

- Incoming interface
- All Layer 2
- Layer 4 packet fields
- MAC addresses, IP addresses, protocol, ports, flags, ...
- Stateful matches
- The firewall tracks connections for you
- Further advanced conditions - rate limits etc.

Firewall Configuration: Commonly Used Fields

- Link Layer (L2) - Ethernet
 - Often: Ethernet MAC Address
 - Easily spoofable
 - `# ifconfig eth0 hw ether de:ad:be:ef:de:ad`
- Network Layer (L3) - IPv4
 - IP addresses
 - Transport protocol
 - TCP, UDP, ICMP, ...



Firewall Configuration: Commonly Used Fields

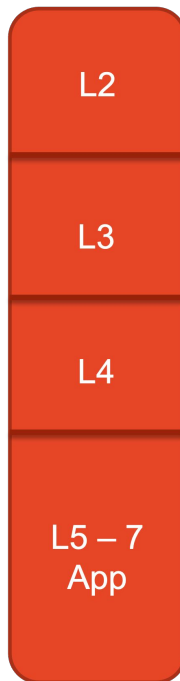
- Transport Layer (I4) - TCP/UDP

- **Ports**

- Determine the sending / receiving application.
 - Well-Known Ports (0-1023): E.g. HTTP (80), DNS (53), HTTPS (443).
 - Registered Ports (1024-49151) E.g. IRC (6667), BitTorrent tracker (6969), ...
 - Ephemeral Ports (49152-65535)

- **Flags**

- ACK: set in every segment of a connection except first
 - SYN: only set in the first two segments
 - RST: ungraceful close of a connection



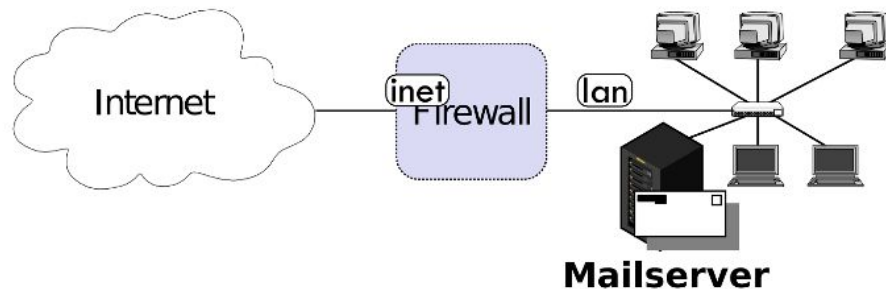
3. Stateful Matching



Statefull Matching

- Arriving packets may generate state in the firewall.
- Connection tracking with the IP-5-tuple
 - (Src IP, Dst IP, Proto, Src Port, Dst Port)
- States of a connection
 - NEW: First packet of a connection
 - ESTABLISHED: All following packets
- Note: UDP connection tracking is always an approximation.

Stateful Example: A LAN with a Mail Server



- **Security policy**

- Incoming and outgoing email should be the only allowed traffic into and out of a protected network
- Email is SMTP, TCP port 25
- Anyone in the internal network can send out emails to arbitrary mail servers on the Internet
- Incoming emails must only arrive at the Mail server

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)

Stateful Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	inet	external	mailserver	TCP	*	25	New	Accept
B	lan	internal	external	TCP	*	25	New	Accept
C	*	*	*	TCP	*	*	Est.	Accept
D	*	*	*	*	*	*	*	Drop

- Rule A allows new incoming SMTP (TCP port 25) connections to establish a connection with the internal Mail server
- Rule B allows establishing SMTP connection from the internal network to the Internet
- Rule C allows all established connections. Only with rule A and B, a connection can be in the ESTABLISHED state.
- Rule D denies the rest (whitelisting)



Only TCP can into to Established State (Specifically only incoming and outgoing TCP connections related to email can get into established state).

Firewall Tuning

- Firewall rules are matched sequentially. Rule order has huge impact on performance.
- Many packets will use an established connection
- Move rule C to the front - hit earlier
- We also set source port to > 1023 - clients rarely use well-known ports (they are for root-run services) - for extra security

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
C	*	*	*	TCP	*	*	Est.	Accept
A	inet	external	mailserver	TCP	> 1023	25	New	Accept
B	lan	internal	external	TCP	> 1023	25	New	Accept
D	*	*	*	*	*	*	*	Drop

4. Stateless Matching



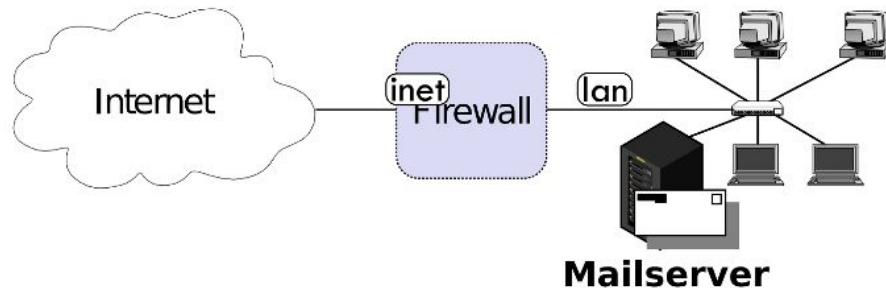
Stateless Matching

- Only operates on the rules and each individual packet.
- No state information is generated when processing a packet.
- Keeping state is expensive and needs fast memory.
- Only few rules: stateless filtering may be faster.
- Many rules: stateful filtering may be faster.
- Majority matches first rule.
- Rule of thumb: stateless is harder to configure! Mistakes more likely.

TCP Handshake and Flags

- **TCP handshake** is essentially this:
 - Client sends a packet with SYN flag
 - Server sends back one with SYN/ACK
 - Client confirms with a third one, with only ACK
- All packets during data transmission have ACK set
- Attackers could, of course, send SYN/ACK in a first packet to trick the firewall - but hosts would ignore that
- **UDP** has no state information (it's **stateless**) - always set ACK to *
- Also means we cannot differentiate between sender and responder with UDP.

Stateless Example: A LAN with a Mail Server



- **Security policy**

- Incoming and outgoing email should be the only allowed traffic into and out of a protected network
- Email is SMTP, TCP port 25
- Anyone in the internal network can send out emails to arbitrary mail servers on the Internet
- Incoming emails must only arrive at the Mail server

Stateless Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A ₁	inet	external	mailserver	TCP	*	25	*	Accept
A ₂	lan	mailserver	external	TCP	*	> 1023	Yes	Accept
B ₁	lan	internal	external	TCP	*	25	*	Accept
B ₂	inet	external	internal	TCP	*	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- Rule A₁ allows incoming email to enter the network.
- Rule A₂ allows the mail server's answers to exit the network.
- Rules B₁ and B₂ are analogous for outgoing email.
- Rule C denies all other traffic.

Stateless Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A_1	inet	external	mailserver	TCP	*	25	*	Accept
A_2	lan	mailserver	external	TCP	*	> 1023	Yes	Accept
B_1	lan	internal	external	TCP	*	25	*	Accept
B_2	inet	external	internal	TCP	*	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- Rule A_1 allows incoming email to enter the network.
- Rule A_2 allows the mail server's answers to exit the network.
- Rules B_1 and B_2 are analogous for outgoing email.
- Rule C denies all other traffic.

Stateless Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A ₁	inet	external	mailserver	TCP	*	25	*	Accept
A ₂	lan	mailserver	external	TCP	*	> 1023	Yes	Accept
B ₁	lan	internal	external	TCP	*	25	*	Accept
B ₂	inet	external	internal	TCP	*	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- Rule A₁ allows incoming email to enter the network.
- Rule A₂ allows the mail server's answers to exit the network.
- Rules B₁ and B₂ are analogous for outgoing email.
- Rule C denies all other traffic.

Stateless Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A ₁	inet	external	mailserver	TCP	*	25	*	Accept
A ₂	lan	mailserver	external	TCP	*	> 1023	Yes	Accept
B ₁	lan	internal	external	TCP	*	25	*	Accept
B ₂	inet	external	internal	TCP	*	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- Rule A₁ allows incoming email to enter the network.
- Rule A₂ allows the mail server's answers to exit the network.
- Rules B₁ and B₂ are analogous for outgoing email.
- Rule C denies all other traffic.

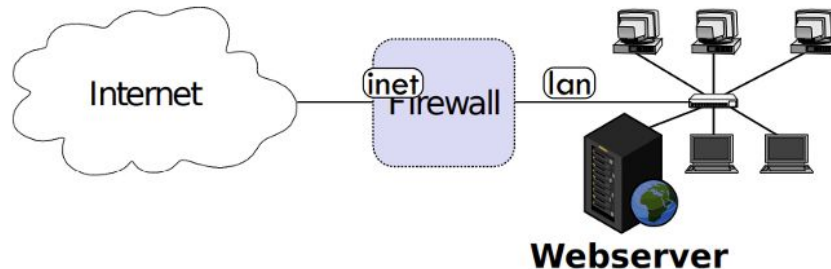
Stateless Example: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
A ₁	inet	external	mailserver	TCP	*	25	*	Accept
A ₂	lan	mailserver	external	TCP	*	> 1023	Yes	Accept
B ₁	lan	internal	external	TCP	*	25	*	Accept
B ₂	inet	external	internal	TCP	*	> 1023	Yes	Accept
C	*	*	*	*	*	*	*	Drop

- **What about spoofing?**

- Inbound packets must have an external source address
- Rules A₁ and B₂ → successfully blocked
- Same for outbound packets; Rules A₂ and B₁

Stateless Example: A LAN with a Web Server



- **Security policy**

- Allow HTTP traffic initiated by external hosts to the web server
- Allow internal hosts to initiate HTTP and DNS
- HTTP: TCP port 80; DNS: UDP port 53
- Do not allow other communication, in particular no communication initiated by external hosts to the local hosts other than the web server.

Stateful Firewall: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	State	Action
A	*	*	*	*	*	*	Est.	Accept
B	inet	external	webserver	TCP	> 1023	80	New	Accept
C	lan	internal	external	TCP	> 1023	80	New	Accept
D	lan	internal	external	UDP	> 1023	53	New	Accept
E	*	*	*	*	*	*	*	Drop

Stateless Firewall: Rules

Rule	Iface	Src IP	Dst IP	Protocol	Src Port	Dst Port	Ack	Action
B ₁	inet	external	webserver	TCP	> 1023	80	*	Accept
B ₂	lan	webserver	external	TCP	80	> 1023	Yes	Accept
C ₁	lan	internal	external	TCP	> 1023	80	*	Accept
C ₂	inet	external	internal	TCP	80	> 1023	Yes	Accept
D ₁	lan	internal	external	UDP	> 1023	53	-	Accept
D ₂	inet	external	internal	UDP	53	> 1023	-	Accept
E	*	*	*	*	*	*	*	Drop

5. Firewall Configuration - Precautions



Spoofing Protection



IP spoofing is when an attacker falsifies the source IP address in network packets to make them appear as if they're coming from a trusted or legitimate source. This technique is commonly used in DDoS attacks and to bypass security controls. Spoofing protection is a firewall security measure that validates source IP addresses to prevent spoofed traffic from entering or leaving a network.

- **Outgoing (to the Internet)**
 - Only allow source IPs that belong to you
 - Don't be an operator who facilitates spoofed DOS attacks on the Internet!
- **Incoming (from the Internet)**
 - Only allow 'valid' source IPs
 - For a varying definition of 'valid'
 - IPs which belong to you are not valid
 - Local and special purpose IPs are not valid

Spoofing Protection: Example

- Assume your institution owns 129.78.0.0/16
- And you also want to drop traffic relating to private IP addresses

Rule	Iface	Src IP	Dst IP	Action
A	lan	!129.78.0.0/16	*	Drop
B	inet	129.78.0.0/16	*	Drop
C	inet	192.168.0.0/16	*	Drop
D	inet	10.0.0.0/8	*	Drop
E	inet	172.16.0.0/12	*	Drop
F	*	*	*	Accept

Common Firewall Mistakes

- How is your firewall management interface reachable?
 - From the Internet? From the complete internal network?
- What is allowed over the Internet?
- Do you use IPv4 and IPv6?
 - Are the rules the same?
- Outbound rule ANY? (c.f. spoofing)

Common Firewall Mistakes: Shadowing



Shadowing refers to the case where all the packets one rule intends to deny (accept) have been accepted (denied) by preceding rules

Rule	Iface	Src IP	Dst IP	Action
A	*	*	192.168.0.0/16	Accept
B	*	*	192.168.42.0/24	Drop

- When rules are sequentially matched, **Rule B will never match.**

Limitations of Firewalls

- **A firewall**
 - Cannot protect against malicious insiders
 - Cannot protect against connections that don't go through it
 - Cannot protect against completely new threats
 - Cannot fully protect against viruses (e.g. if viruses are spread through emails, and the email service is allowed through the firewall, which is typically the case)
 - Does not perform cryptographic operations, e.g. message authentication (however, firewalls are often co-located with VPN endpoints)
- Cannot set itself up correctly

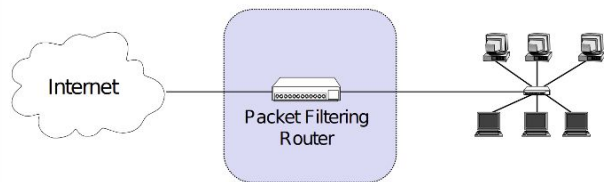
6. Common Firewall Setups



Simple Packet Filter Architecture



Definition: A single packet-filtering router or firewall that sits between the internal network and the Internet, inspecting and filtering traffic based on predefined rules.



Architecture:

- Single point of entry/exit between Internet and internal network
- Router/firewall has two network interfaces (Internet-facing and internal-facing)

Characteristics:

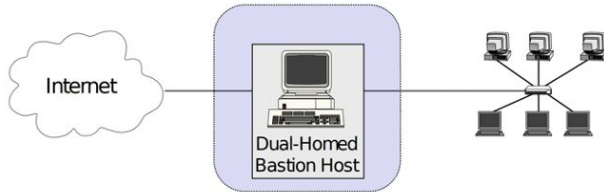
- Simplest and most cost-effective firewall setup
- Makes filtering decisions based on packet headers (IP addresses, ports, protocols)
- Stateless or stateful filtering depending on device capabilities
- Single point of failure - if compromised, entire network is exposed

Best for: Small networks, home offices, or settings with limited security requirements

Dual-Host Architecture



Definition: A dedicated host computer with two network interface cards (NICs) that acts as a gateway between two networks, functioning as both a firewall and application proxy.



Architecture:

- Dual-Homed Host is part of two separate networks simultaneously
- One interface connects to the Internet, the other to the internal network
- IP forwarding is disabled, preventing direct packet routing between networks
- All traffic must be explicitly processed by the host

Two Common Implementations:

1. Basic Dual-Homed Firewall:

- Host runs firewall software only
- Filters packets based on rules
- May forward allowed packets between interfaces

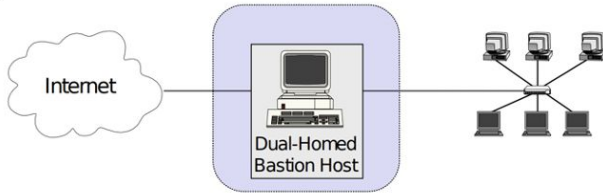
2. Bastion Host (Firewall + Application Proxy):

- More secure implementation
- Acts as both firewall AND application proxy
- Forces all traffic through application-layer proxies

Dual-Host Architecture



Definition: A dedicated host computer with two network interface cards (NICs) that acts as a gateway between two networks, functioning as both a firewall and application proxy.



Characteristics:

- Provides application-layer filtering and proxy services (bastion host)
- Can inspect and filter traffic at a deeper level than simple packet filters
- Single device controls all traffic flow

Drawbacks:

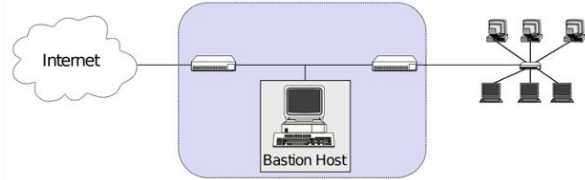
- Creates a bottleneck: All traffic is processed by a single machine
- If attackers gain control of the host, they have direct access to both networks

Best for: Medium-sized networks requiring application-layer inspection

Screened Subnet Architecture - DMZ



Definition: A network architecture that places publicly accessible servers in an isolated network segment (DMZ) between two firewalls, providing defense-in-depth protection for the internal network.



Architecture:

- Demilitarized Zone (DMZ): A perimeter network that isolates public-facing servers
- Dual firewall design: External firewall protects DMZ from Internet, internal firewall protects internal network from DMZ
- Hosts Bastion Host (Proxy) and publicly accessible servers in the DMZ
- Creates three security zones: Internet, DMZ, and Internal Network

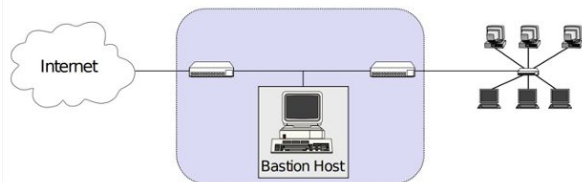
Characteristics:

- Secondary protection : If DMZ is breached, internal network remains protected
- Public services exposed in DMZ with restricted access to internal resources
- Requires two firewalls or one firewall with at least 3 network cards
- Most secure common architecture - provides layered defense

Screened Subnet Architecture - DMZ



Definition: A network architecture that places publicly accessible servers in an isolated network segment (DMZ) between two firewalls, providing defense-in-depth protection for the internal network.



Security Benefits:

- Limits blast radius of security breaches
- Separates public and private resources
- Allows granular control over traffic between zones

Best for: Organizations hosting public services while protecting sensitive internal resources; enterprises with high security requirements

Recap

- **We discussed:**

- Basics of Firewalls
- Stateful Firewalls
- Stateless Firewalls
- Common Firewall Configurations and Mistakes

