Firewalls

CYBR371: System and Network Security, (2024/T1)

Arman Khouzani, Mohammad Nekooei
Slides modified from "Masood Mansoori"

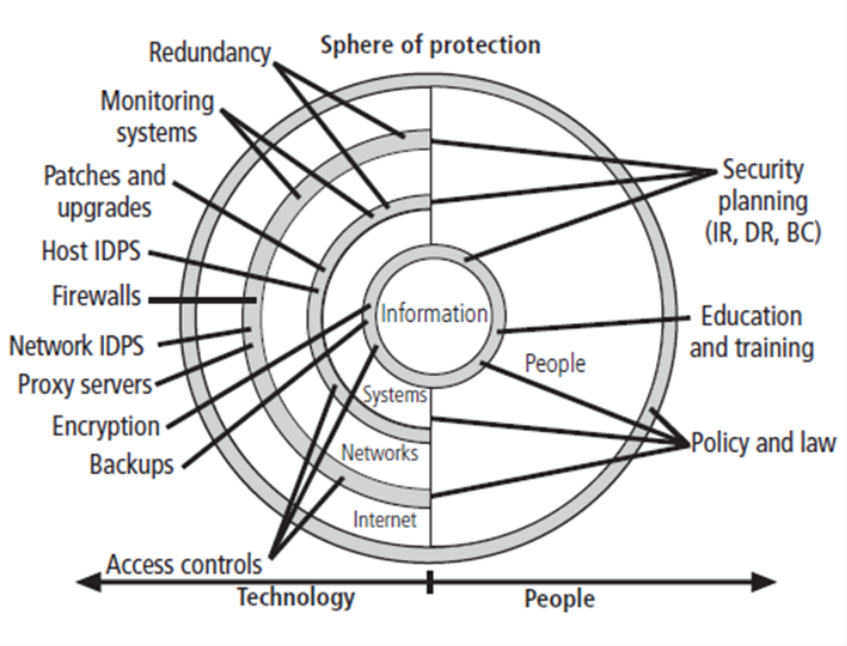
24 April 2024

Victoria University of Wellington – School of Engineering and Computer Science

An Overview of Firewalls

Hardware or software configured to control and block unauthorised network access.

- Provides perimeter defence.
- Imposes restrictions on network services.
  - only authorised traffic is allowed.
  - and Auditing.
- Itself immune to penetration.



An Overview of Firewalls

Firewall cannot protect against:

- malicious insiders.
- connections that do not go through it.

Core functions of firewalls:

- Filtering
- Proxying
- Logging
- Redirection

Types of Firewalls:

- Software-based firewalls
- Hardware-based firewalls

- Packet filtering
- Application gateways
- Circuit-Level Firewalls

Types of Firewalls

Type of firewall	Advantages	Disadvantages
Software—freeware	Small file size; ease of installation	Only minimal features are offered; lack of technical support
Software—commercial personal firewalls	Simple to install; economical; autoconfiguration features help novice users yet give advanced users more fine-tuned control	Not as full-featured as enterprise products and not as robust as hardware appliances; usually installed on single-computer systems, which reduces security
Software—commercial enterprise firewalls	Usually installed on a dedicated host for maximum security; centralized administration available for large networks; real-time monitoring and other administrative features	Can be difficult to install and configure; tend to be more expensive
Hardware appliances	More scalable than software firewalls; offer faster throughput	Can be expensive and difficult to patch if bugs or security alerts require it

Packet Filtering Firewalls

Packet Filtering Firewalls: Uses transport-layer information only

- IP Source Address, Destination Address
- Protocol/Next Header (TCP, UDP, ICMP, SSH, SNMP etc.)
- TCP or UDP source & destination ports
- TCP Flags (SYN, ACK, FIN, RST, PSH, etc.)
- ICMP message type

Example: No incoming port 53 (DNS) packets except known trusted servers

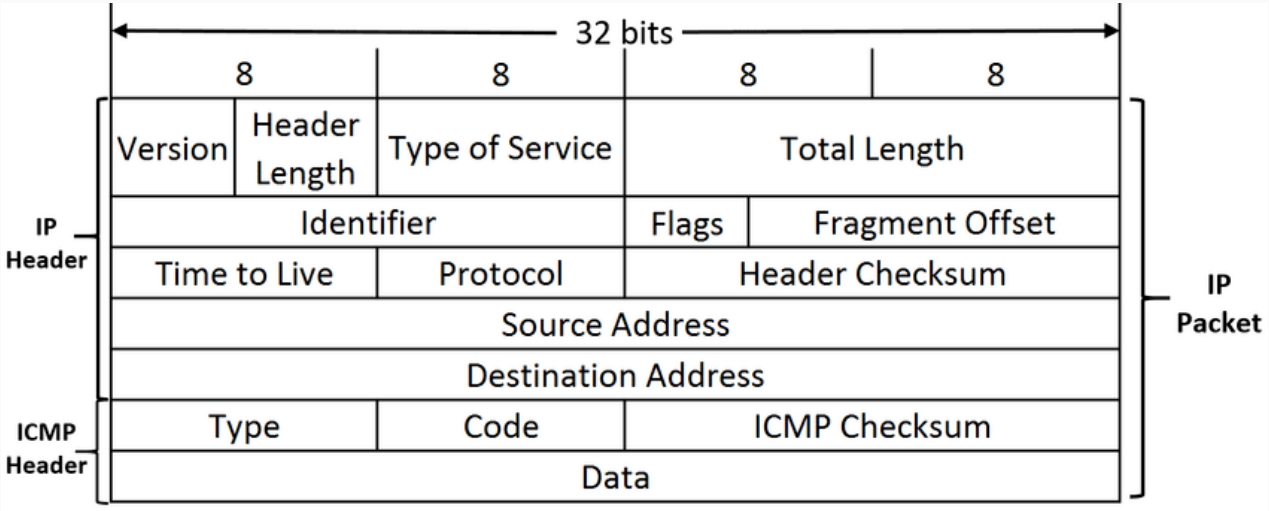
Types of Packet Filtering Firewalls

1. Stateless packet filtering
2. Stateful packet filtering

Stateless packet filtering: Filtering based on common IP header features such as IP address/Subnets and Port numbers.

- Advantage: Inexpensive, fast (really fast!).
- Disadvantages: Intruders can get around these defences, hard to maintain, vulnerable to IP spoofing, and no form of authentication.

Stateless Packet Filtering



Rule	Source IP	Source port	Destination IP	Destination port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny
3	Any	Any	192.168.120.1	Any	Deny
4	192.168.120.0	Any	Any	Any	Allow
5	Any	Any	192.168.120.2	25	Allow
6	Any	Any	192.168.120.3	80	Allow
7	Any	Any	Any	Any	Deny

Stateful Packet Filtering

Maintain a file called a **state table** containing record of all current connections.

- Allows incoming packets to pass through only from external hosts already connected.
- Example?

Source IP	Source port	Destination IP	Destination port	Connection state
192.168.120.101	1037	209.233.19.22	80	Established
192.168.120.104	1022	165.66.28.22	80	Established
192.168.120.107	1010	65.66.122.101	25	Established
192.168.120.102	1035	213.136.87.88	20	Established
223.56.78.11	1899	192.168.120.101	80	Established
206.121.55.8	3558	192.168.120.101	80	Established
224.209.122.1	1079	192.168.120.105	80	Established

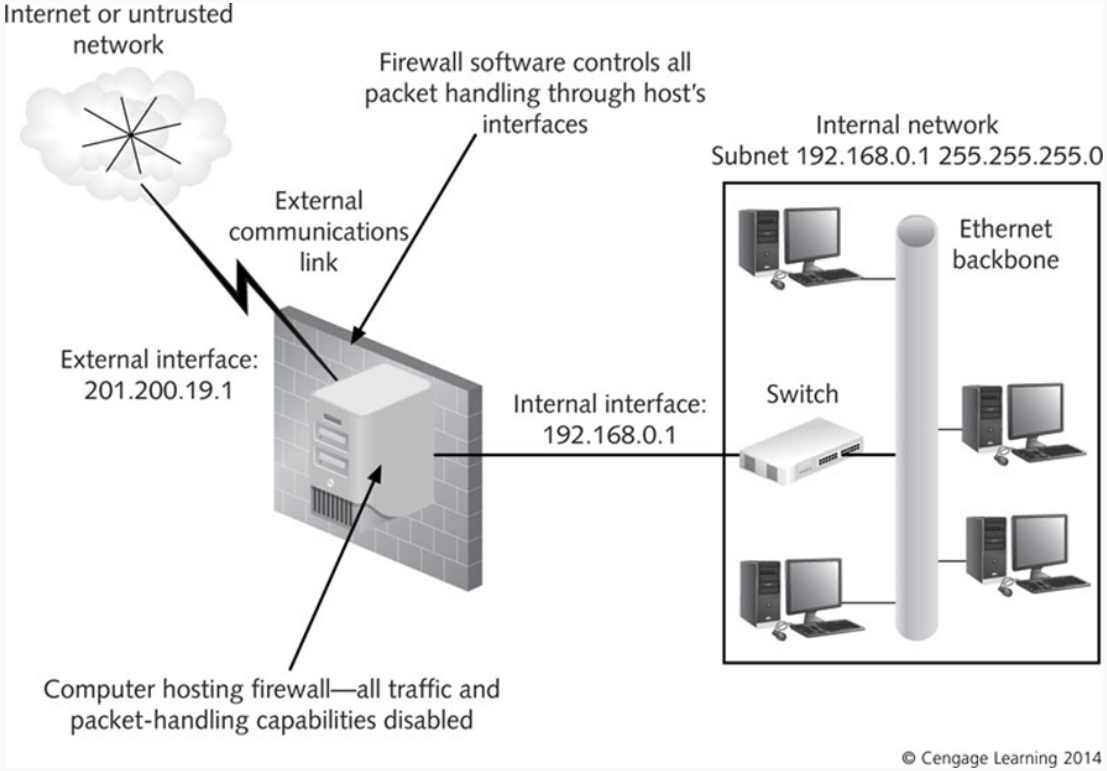
Firewall Configurations

Firewalls can be deployed in several ways

- As part of a screening router
- Dual-homed host
- Screen host
- Screened subnet DMZ
- Multiple DMZs
- Multiple firewalls
- Reverse firewall

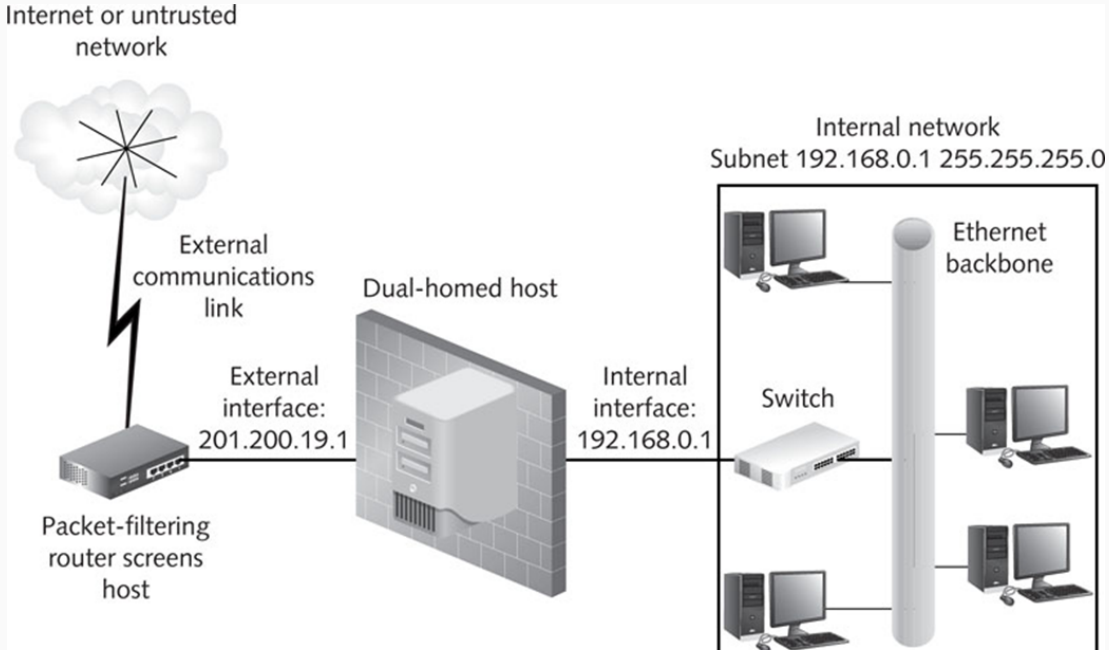
Firewall Configurations: Dual-homed host

- Computer that has been configured with more than one network interface. Only firewall software can forward packets from one interface to another.
- Firewall is placed between the network and the Internet.
- Host serves as a single point of entry to the organisation.
    - Attackers only have to break through 1 layer of protection.



Firewall Configurations: Screened host

- Similar to a dual-homed host except router is added between the host and the Internet to do IP packet filtering.
- Combines a dual-homed host and a screening router.
- Might choose this setup for perimeter security on a corporate network.
- Can function as an application gateway or proxy server.



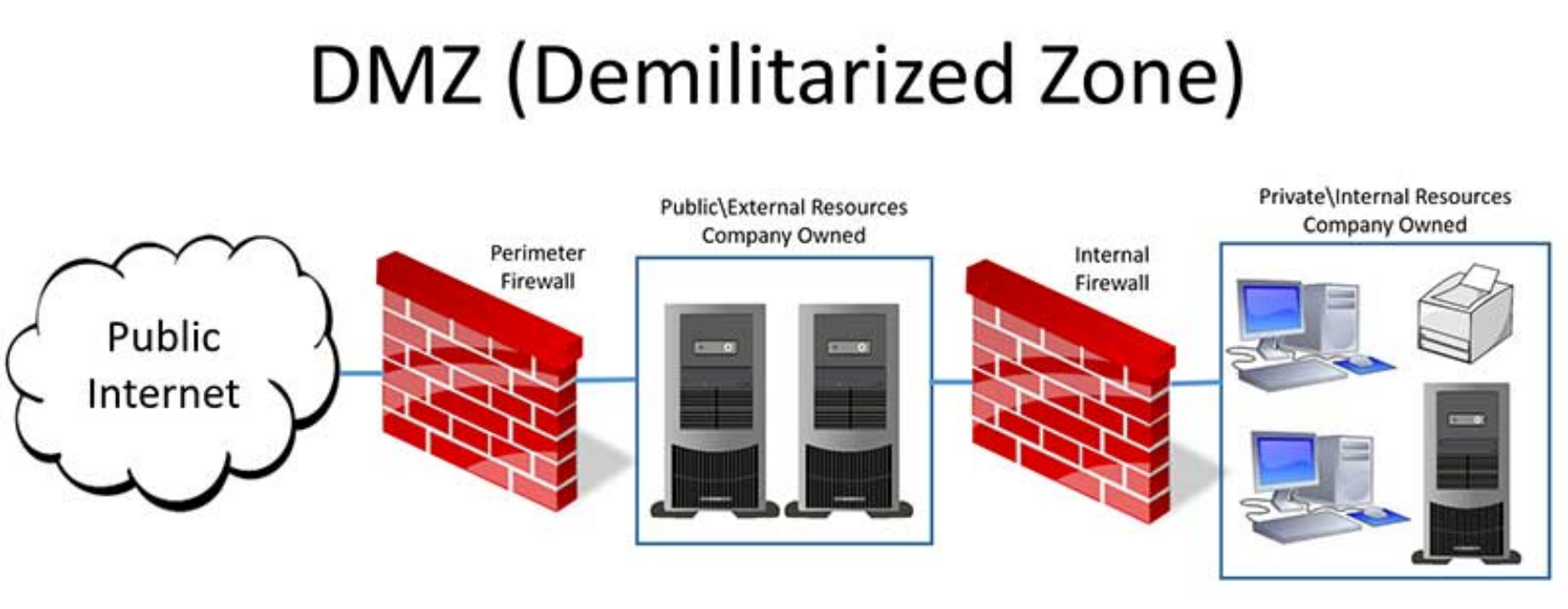
Multiple Firewall Configurations

Many organisations find they need more than one firewall.

Protecting a DMZ with Multiple Firewalls.

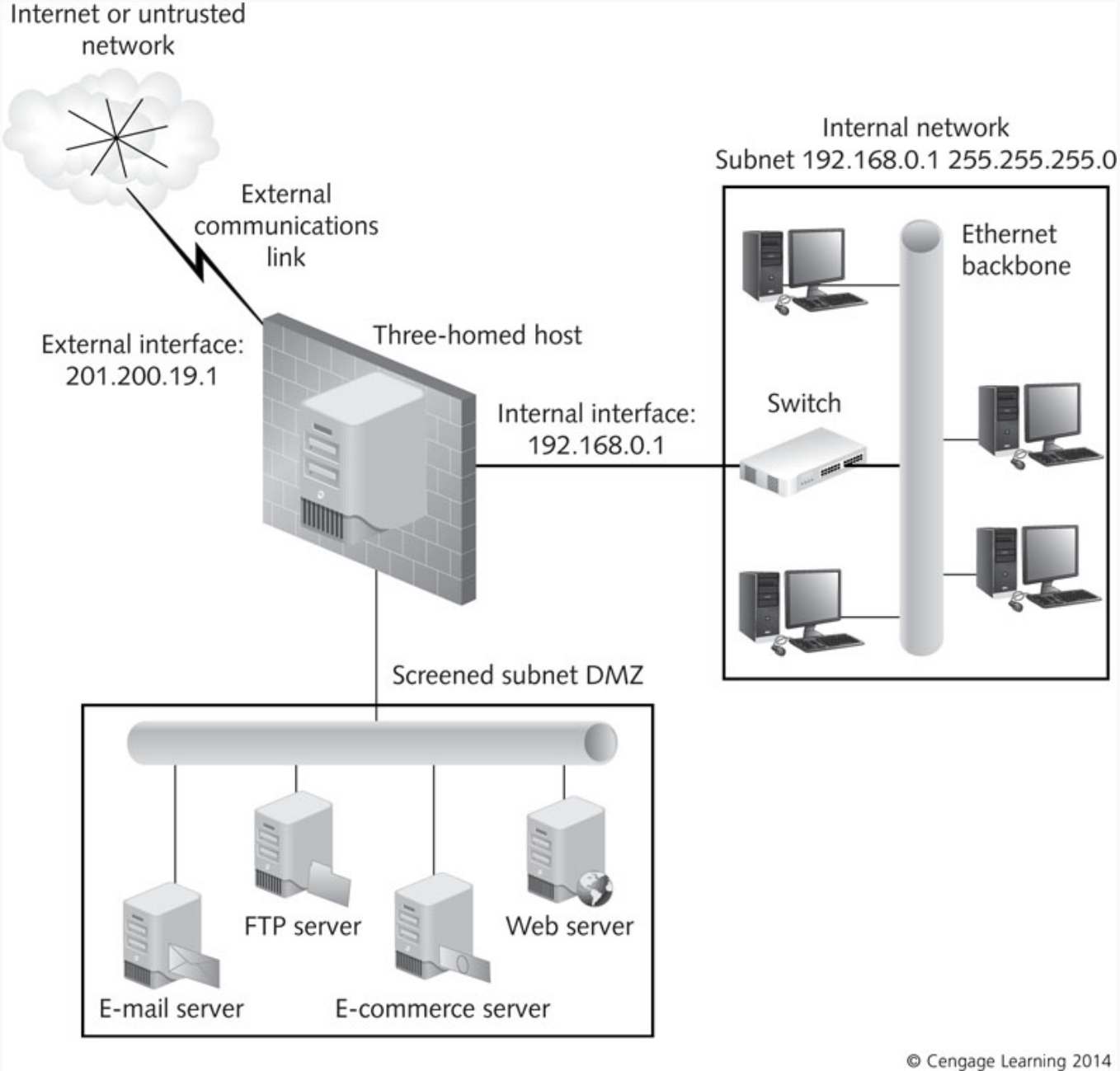
- Must be configured identically and use the same software.
- One firewall controls traffic between DMZ and Internet.
- Second firewall controls traffic between protected network and DMZ.
    - Can also serve as a failover firewall (backup if one fails).

Firewall Configurations: DMZ



- Subnet of publicly accessible servers placed outside the internal LAN
- Firewall that protects the DMZ is connected to the Internet and the internal network

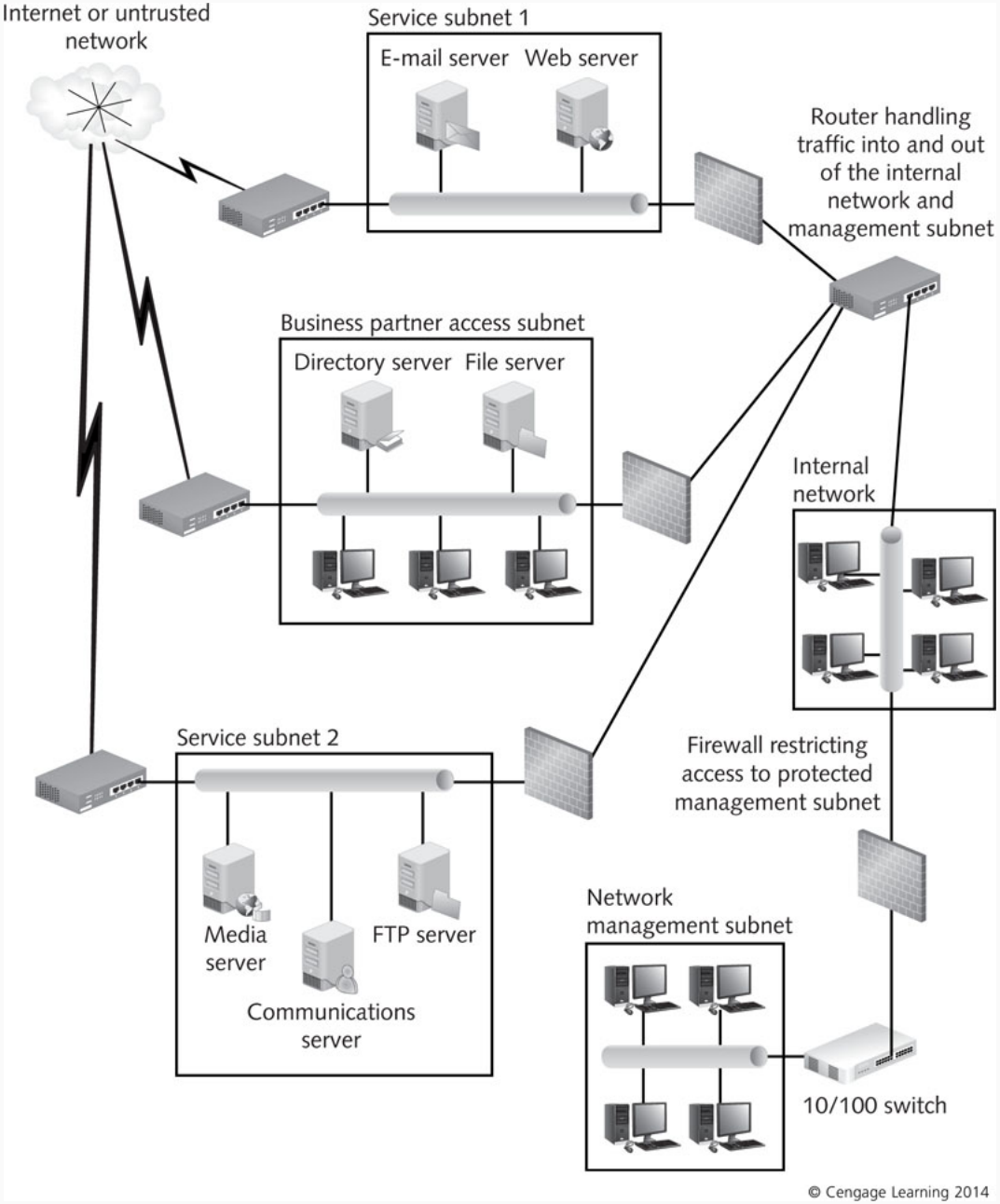
Firewall Configurations: DMZ



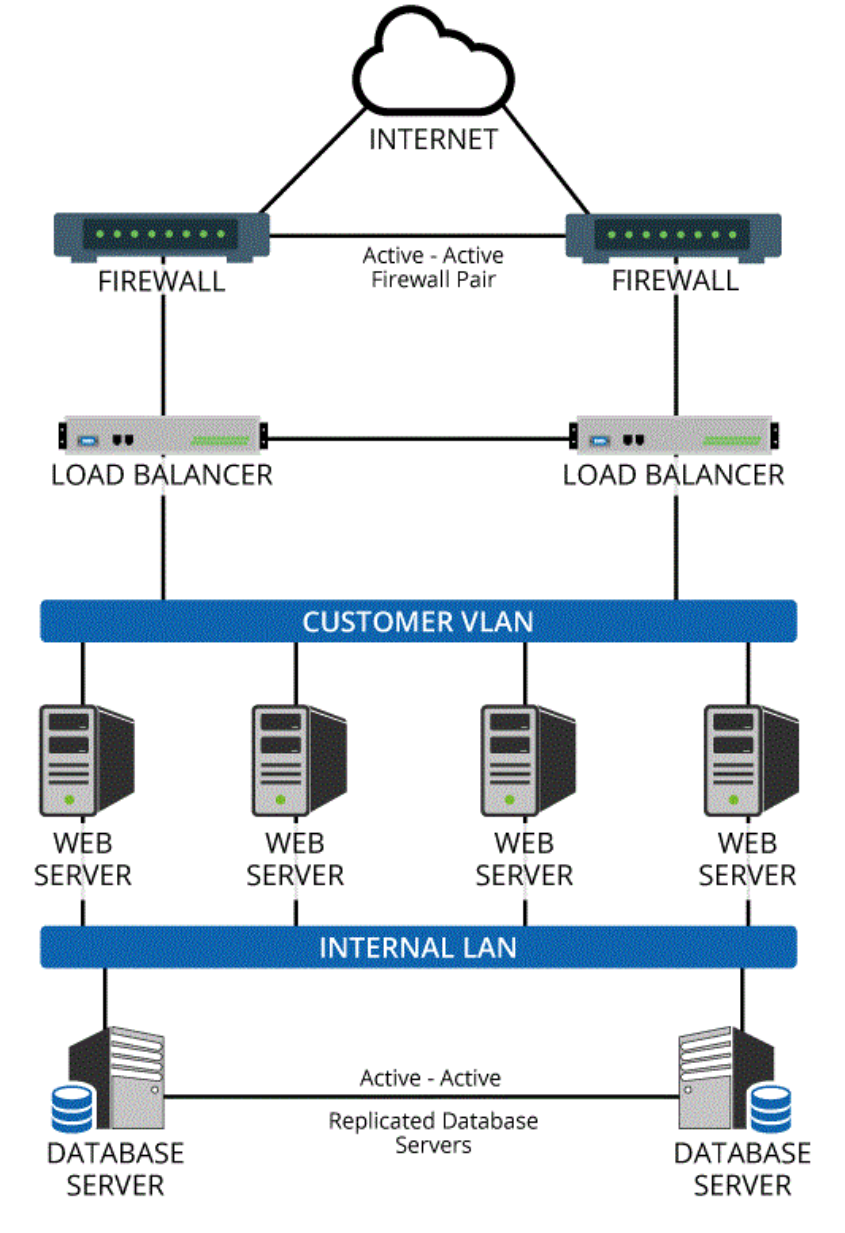
Firewall Configurations: Multiple DMZ/Firewall Configurations

- **Server farm:** Group of servers connected in their own subnet
    - Work together to receive requests with the help of load-balancing software
- Clusters of servers in DMZs help protect the internal network from becoming overloaded
- Each server farm/DMZ can be protected with its own firewall or packet filter

Multiple DMZ/Firewall Configurations



Multiple DMZ/Firewall Configurations with Load Balancing



Reverse Firewalls

- Monitors outgoing connections
- Helps monitor outgoing connection attempts that originates from internal users
    - Filters out unauthorised attempts
    - Block unauthorised sites that are accessed repeatedly

Advantages and disadvantages of firewall configurations

Configuration	Advantages	Disadvantages
Screening router	Simple, inexpensive; good for home applications if a stateful packet filter is used	Provides only minimal protection; viruses, Trojan programs, and some malformed packets might get through
Dual-homed host	Simple, economical; can provide effective protection if configured correctly	Provides a single point of entry (and fault); the firewall depends entirely on the host computer
Screened host	Provides two layers of protection for home and small-business networks	Provides a single point of entry (and fault); the firewall depends on the host computer and the router protecting it
Screened subnet DMZ	Protects public servers by isolating them from the internal network	Servers in the DMZ are highly vulnerable and need to be hardened
Multiple DMZs/firewalls	Provide layers of protection for a business network	Expensive
Single DMZ/two firewalls	Balance traffic load in high-traffic situations	Expensive
Branch offices/multiple firewalls	Provide protection for all offices in a corporate network as well as central administration	Firewalls must be purchased, installed, and configured at each office location
Reverse firewall	Monitors attacks from inside the network; enables organizations to monitor user activity	Can slow down user access to external networks or other parts of the internal network

Firewall Policy

Firewall Policy

Firewall policy (SysSP): Describes how firewalls should handle application traffic.

General steps to create a firewall policy:

- Identify network applications/services that are needed.
- Determine methods for securing application/service traffic.
    - Must balance security, user requirements, and cost.
- Consider all firewalls in your network.
    - Develop a traffic matrix for each location.

Firewall Policy

Application or service	Internal host type	Location	Host security policy	Firewall internal security policy	Firewall external security policy
FTP	Windows	Any	Client only; antivirus	Allow	Deny
FTP	UNIX	Any	Secure Shell (SSH); user ID/password; no anonymous traffic	Allow	Application proxy with user authentication
Telnet	Windows	Any	Client only	Allow	Application proxy with user authentication
Telnet	UNIX	Any	SSH	Allow	Application proxy with user authentication
SMB over IP	Windows	Any	Limit access to shares	Allow local domain only; deny all others	Deny

E-mail Configuration

Setting up firewall rules that permit filtering e-mail is not simple Variety of e-mail protocol that can be used:

- POP3 and IMAP4 for inbound mail transport
- SMTP for outbound mail transport
- Lightweight Directory Access Protocol (LDAP) for looking up email addresses
- HTTP for Web-based email service (HTTPS for secured access)

Email Rules

Rule	Protocol	Transport protocol	Source IP	Source port	Destination IP	Destination port	Action
7	POP3 outbound	TCP	208.177.178.0/24	Any	Any	110	Allow
8	POP3/S outbound	TCP	208.177.178.0/24	Any	Any	995	Allow
9	POP inbound	TCP	Any	Any	208.177.178.0/24	110	Allow
10	POP3/S inbound	TCP	Any	Any	208.177.178.0/24	995	Allow
11	SMTP outbound	TCP	208.177.178.29	Any	Any	25	Allow
12	SMTP/S outbound	TCP	208.177.178.29	Any	Any	465	Allow
13	SMTP inbound	TCP	Any	Any	208.177.178.29	25	Allow
14	SMTP/S inbound	TCP	Any	Any	208.177.178.29	465	Allow

Firewall Rules: General Practices

1. Firewall generally operate on two different default policies:

   - **Blocking nothing:** Provides minimal security by only closing holes you can identify. Blocking nothing provides the least inconvenience to the users.

   - **Blocking everything:** “Deny All” security policy should begin by allowing services selectively as needed. It provides the strongest security but the most inconvenience. Things break and people complain.

Firewall Rules: General Practices

2. No one but administrators should be able to connect to the firewall.

3. Should block direct access from the Internet to any computer behind the firewall.

4. Should permit access to the public servers in the DMZ and enable users to access the Internet.

5. Keep the list of rules as short as possible, about 30 rules (no more than 50).

   - The shorter the rule base, the faster the firewall performs.

6. Firewalls process rules in a particular order.

   - Most important rules should be at the top of the list.
   - Make the last rule a cleanup rule.

Packet Filtering Firewall Capabilities e.g. netfilter (iptables)

iptables Capabilities

1. **Categorisation of traffic** into multiple streams and application of rules tables and associated extensions
2. **Chain-related operations** on the main and user-defined chains (e.g. **`INPUT`**, **`OUTPUT`**, and **`FORWARD`**).
3. **Target disposition** (**`ACCEPT`** or **`DROP`**).
4. **IP header field filtering** and matching operations for TCP, UDP, and ICMP, protocol, source and destination address, input and output interfaces, and fragment handling.
5. **Performing stateful inspection**.
6. **Load balancing**.
7. **Time, quota and connection rate** based filtering and restrictions.
8. ...

Categorisation of traffic

iptables uses the concept of separate rule tables for different packet processing functionality.

- **filter**: The filter table is the default table containing the actual firewall filtering rules.
  - **INPUT**
  - **OUTPUT**
  - **FORWARD**
- **nat**: The nat table contains the rules for Source and Destination Address and Port Translation. The built-in chains include:
  - **PREROUTING (DNAT/REDIRECT)**
  - **OUTPUT (DNAT/REDIRECT)**
  - **POSTROUTING (SNAT/MASQUERADE)**
- **mangle**: The mangle table contains rules for setting specialised packet-routing flags.
  - All five chains mentioned above

netfilter hooks and `iptables` Chains

Five (5) main chain types:

- **`PREROUTING`**: Triggered by **`NF_IP_PRE_ROUTING`** hook.
- **`INPUT`**: Triggered by **`NF_IP_LOCAL_IN`** hook.
- **`FORWARD`**: Triggered by **`NF_IP_FORWARD`** hook.
- **`OUTPUT`**: Triggered by **`NF_IP_LOCAL_OUT`** hook.
- **`POSTROUTING`**: Triggered by **`NF_IP_POST_ROUTING`** hook.

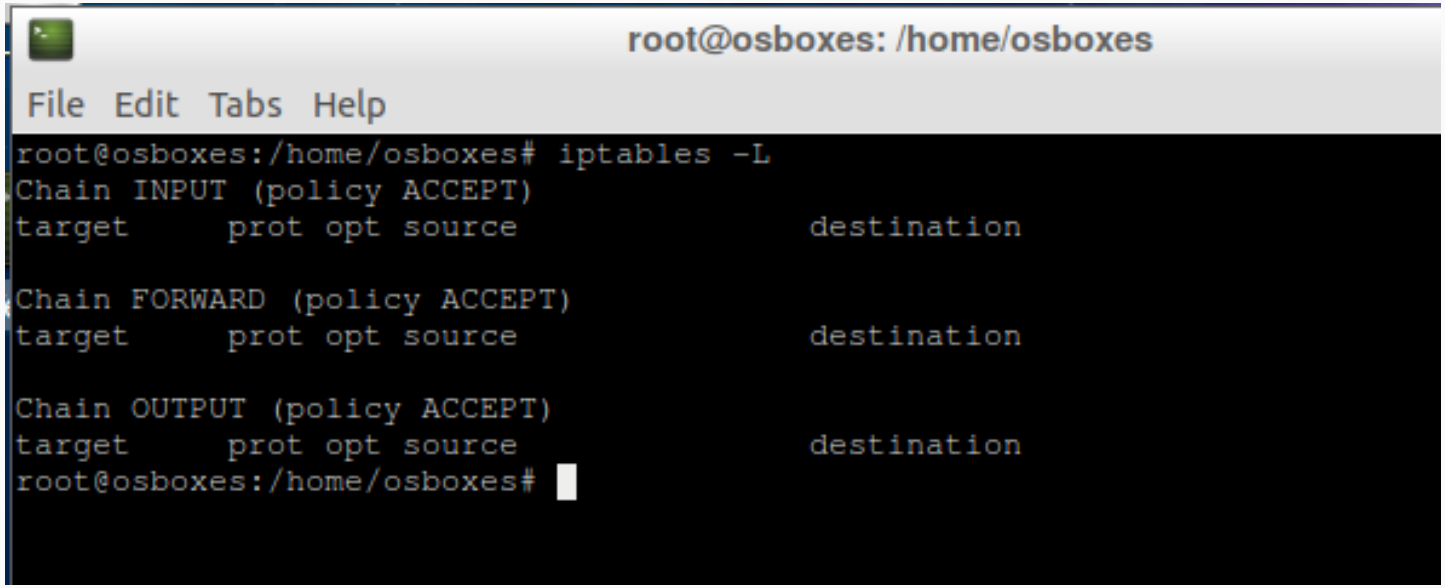
netfilter hooks and iptables Chains

`netfilter`	hook Condition
`NF_IP_PRE_ROUTING`	triggered by any incoming traffic very soon after entering the network stack. This hook is processed before any routing decisions made.
`NF_IP_LOCAL_IN`	triggered after an incoming packet is routed and destined for the local system.
`NF_IP_FORWARD`	triggered after an incoming packet is routed if the packet is to be forwarded to another host.
`NF_IP_LOCAL_OUT`	triggered by any locally created outbound traffic
`NF_IP_POST_ROUTING`	triggered by any outgoing or forwarded traffic after routing has taken place and just before being put out on the wire

Chain-Related Operations

Outlining Default actions on chains of traffic

- **iptables –policy INPUT DROP**
- **iptables –policy OUTPUT DROP**
- **iptables –policy FORWARD DROP**
- **iptables -A INPUT -i lo -j ACCEPT**
- **iptables -A OUTPUT -o eth1 -j ACCEPT**



netfilter hooks and iptables Chains

Additional custom chains can be defined for easier management of traffic. For example:

```
# Define chain to allow particular source addresses
iptables -N chain-incoming-connections
iptables -A chain-incoming-connections -s 192.168.1.101
    -j ACCEPT
iptables -A chain-incoming-connections -s 192.168.1.102
    -j ACCEPT
iptables -A chain-incoming-connections -j DROP
```

Target disposition

- **ACCEPT**
  - iptables stops further processing. The packet is handed over to the end application or the OS for processing.
- **DROP**
  - iptables stops further processing. The packet is blocked.
- **LOG**
  - The packet information is sent to the syslog daemon for logging. iptables continues processing with the next rule in the table.
  - You can't log and drop at the same time ->use two rules.

```
--log-prefix "reason"
```

- **REJECT**
  - Works like the **DROP** target, but will also return an error message to the host sending the packet that the packet was blocked

Target Disposition

- **SNAT**
  - Used to do source network address translation rewriting the source IP address of the packet
  - The source IP address is user defined

```
--to-source <address>[-<address>][:<port>-<port>]
```

- **DNAT**
  - Used to do destination network address translation. ie. rewriting the destination IP address of the packet

```
--to-destination ipaddress
```

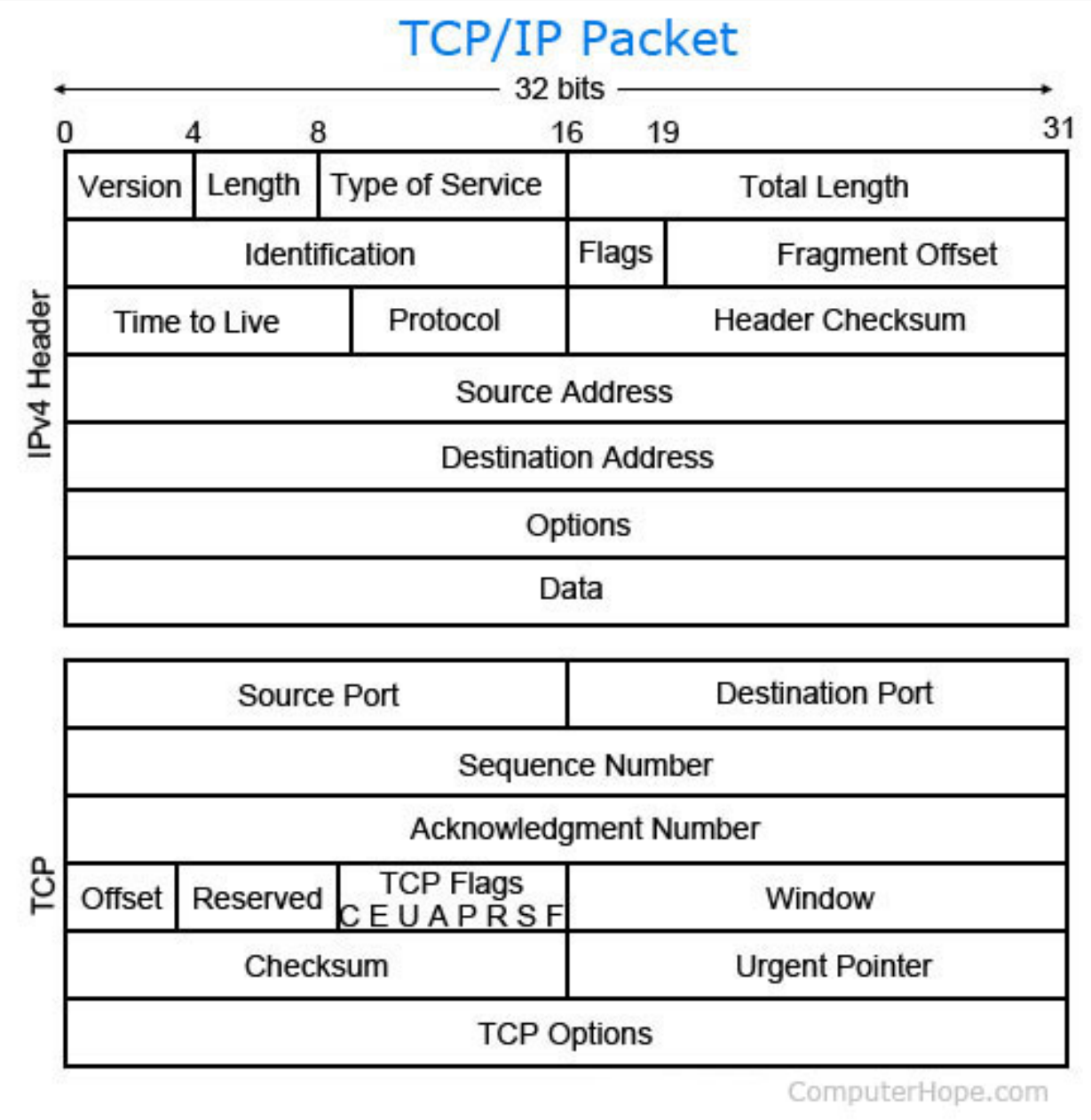
- **MASQUERADE**
  - Used to do Source Network Address Translation (SNAT).
  - By default the source IP address is the same as that used by the firewall's interface.

```
[--to-ports <port>[-<port>]]
```

iptables Header-based Filtering

- The current connection state
- Port lists (supported by the multiport module)
- The hardware Ethernet MAC source address or physical device
- The type of address, link-layer packet type, or range of IP addresses
- The ICMP type
- The length of the packet and/or The time the packet arrived
- Every nth packet or random packets
- The TTL section of the IP header
- Rate-limited packet matching
- ...

iptables Header-based Filtering

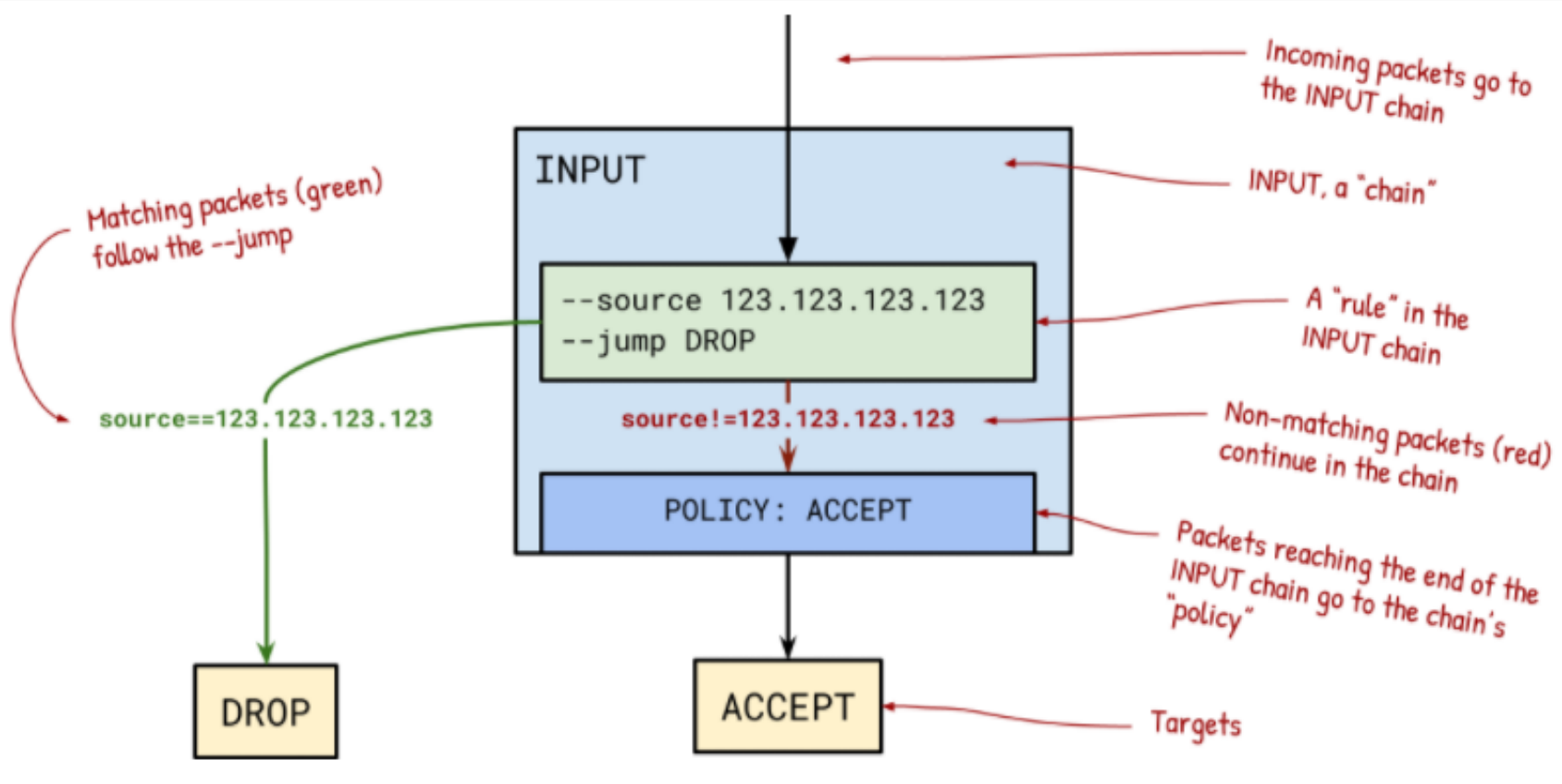


ICMP messages types

Type 0 — Echo Reply
Type 1 — Unassigned
Type 2 — Unassigned
Type 3 — Destination Unreachable
Type 4 — Source Quench (Deprecated)
Type 5 — Redirect
Type 6 — Alternate Host Address (Deprecated)
Type 7 — Unassigned
Type 8 — Echo
Type 9 — Router Advertisement
Type 10 — Router Selection
Type 11 — Time Exceeded
Type 12 — Parameter Problem
Type 13 — Timestamp
Type 14 — Timestamp Reply

iptables Header-based Filtering Examples

```
Syntax: iptables <option> <chain> <matching criteria> <target>
```



iptables Header-based Filtering Examples

```
iptables --append INPUT --source 123.123.123.123 --jump
    DROP
```

Blocking Incoming Traffic

```
iptables -A INPUT -p tcp -s 1.2.3.4 --dport 80 -j DROP
iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --
    dport 80 -j DROP
iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08
    -j DROP
```

Block Outgoing Traffic

```
iptables -A OUTPUT -d 75.126.153.206 -j DROP
iptables -A OUTPUT -d 192.168.1.0/24 -j DROP
iptables -A OUTPUT -o eth1 -d 192.168.1.0/24 -j DROP
```

iptables Stateful Filtering

Keeps track of the state of the connection

- **NEW**: Packet has started a new connection
- **ESTABLISHED**: Packet is associated with a connection which has seen packets in both directions
- **RELATED**: Packet is starting a new connection but is associated with an existing connection.
- **INVALID**: Packet is not associated with an existing connection and isn't appropriate for opening a new connection, cannot be identified/isn't routable, etc.

Example (if default policy is set to DROP):

```
iptables -A OUTPUT -p tcp --dport 22 -m conntrack --
    ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp --sport 22 -m conntrack --
    ctstate ESTABLISHED -j ACCEPT
```

Load Balancing

Load balancing: Uses the iptables **`nth`** extension.

E.g. load balancing the HTTPS traffic to 2 different webservers.

- For every 3th (3rd) packet, it is load balanced to a different server (using the counter 0)

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m
    state --state NEW -m nth --counter 0 --every 3 --
    packet 0 -j DNAT --to-destination 192.168.1.101:443

iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m
    state --state NEW -m nth --counter 0 --every 3 --
    packet 1 -j DNAT --to-destination 192.168.1.102:443
```

Time, Quote Filtering

iptables can match rules based on the time of day and the day of the week using the time module. e.g.:

```
iptables -A FORWARD -p tcp -m multiport --dport http,
    https -o eth0 -i eth1 -m time --timestart 12:30 --
    timestop 13:30 --days Mon,Tue,Wed -j ACCEPT
```

Setting transfer quotas with quota:

```
iptables -A INPUT -p tcp -m quota --quota 2147483648 -j
    ACCEPT
iptables -A INPUT -j DROP
```

The limit matching extension can be used to:

- limit the number of times a rule matches in a given period.
- restrict the number of parallel TCP connections from a particular host or network.

Additional capabilities

Basic payload inspection: The string extension allows one to match a string anywhere in a packet's data payload.

```
iptables -A FORWARD -m string --string '.com' -j DROP
iptables -A FORWARD -m string --string '.exe' -j DROP
```

Packet Matching Based on TTL Values:

```
iptables -A INPUT -s 1.2.3.4 -m ttl --ttl-lt 40 -j
    REJECT
```

Blocking Domains:

```
whois 69.171.228.40 | grep CIDR
> CIDR: 69.171.224.0/19
```

```
iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
iptables -A OUTPUT -p tcp -d facebook.com -j DROP
```

Summary

- Firewall is hardware or software that blocks unauthorised network access
- Firewalls are not a standalone solution
  - Combined with antivirus software, IDPSs, access control, and auditing
- Stateless firewalls filter traffic based on protocol or IP address but are less secure than stateful firewalls
- Stateful firewalls maintain state tables, which are records of connections that are considered trusted
- Firewall rule base should be based on the organisation's security policy, provide rules for how applications can access the Internet, and be as simple and short as possible

References

- https://www.baeldung.com/linux/iptables-packet-rate-limit
- https://man7.org/linux/man-pages/man8/iptables.8.html
- https://help.ubuntu.com/community/IptablesHowTo
- https://phoenixnap.com/kb/iptables-tutorial-linux-firewall
- “Linux *iptables*, Pocket Reference (Firewalls, NAT & Accounting)” by Gregor N Purdy; Safari, an O’Reilly Media Company.; 2004; 1st edition

Next: Network and host-based intrusion detection systems