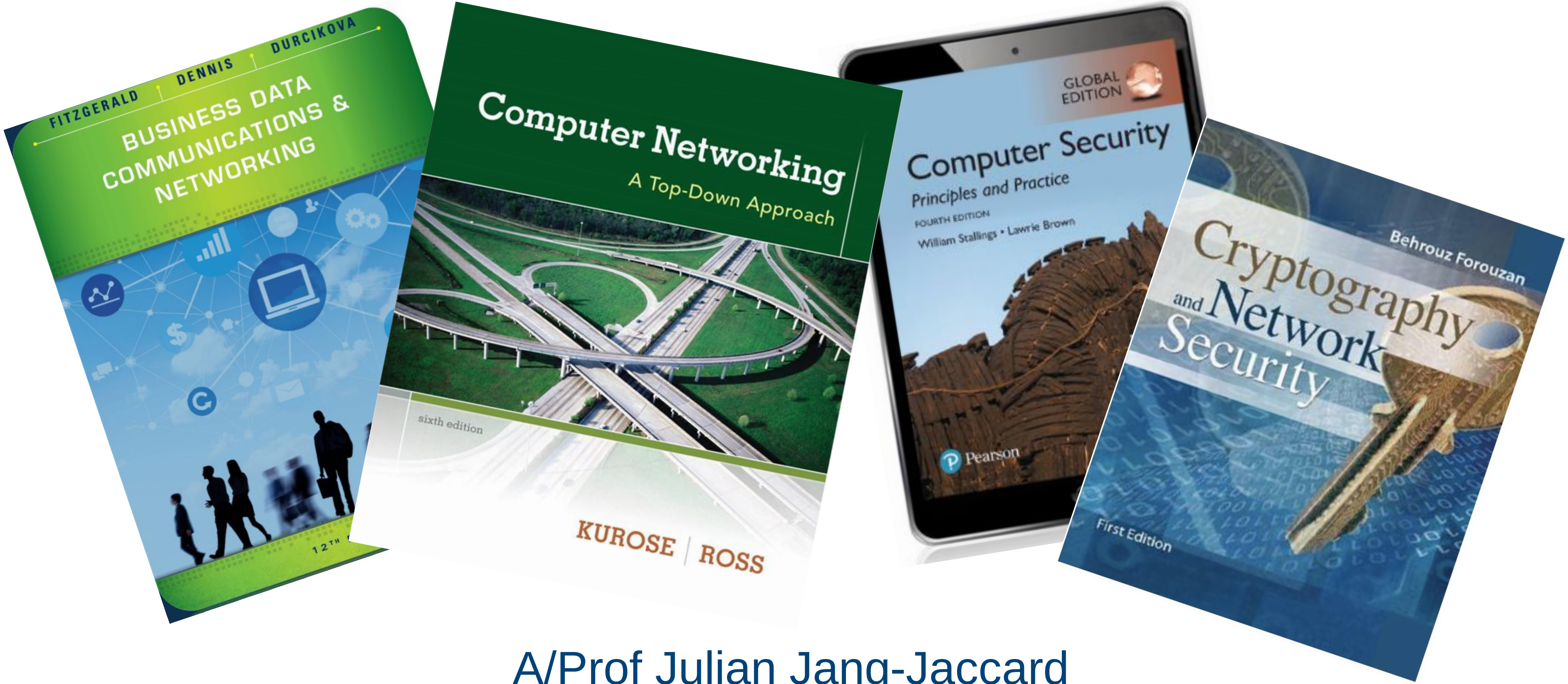
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

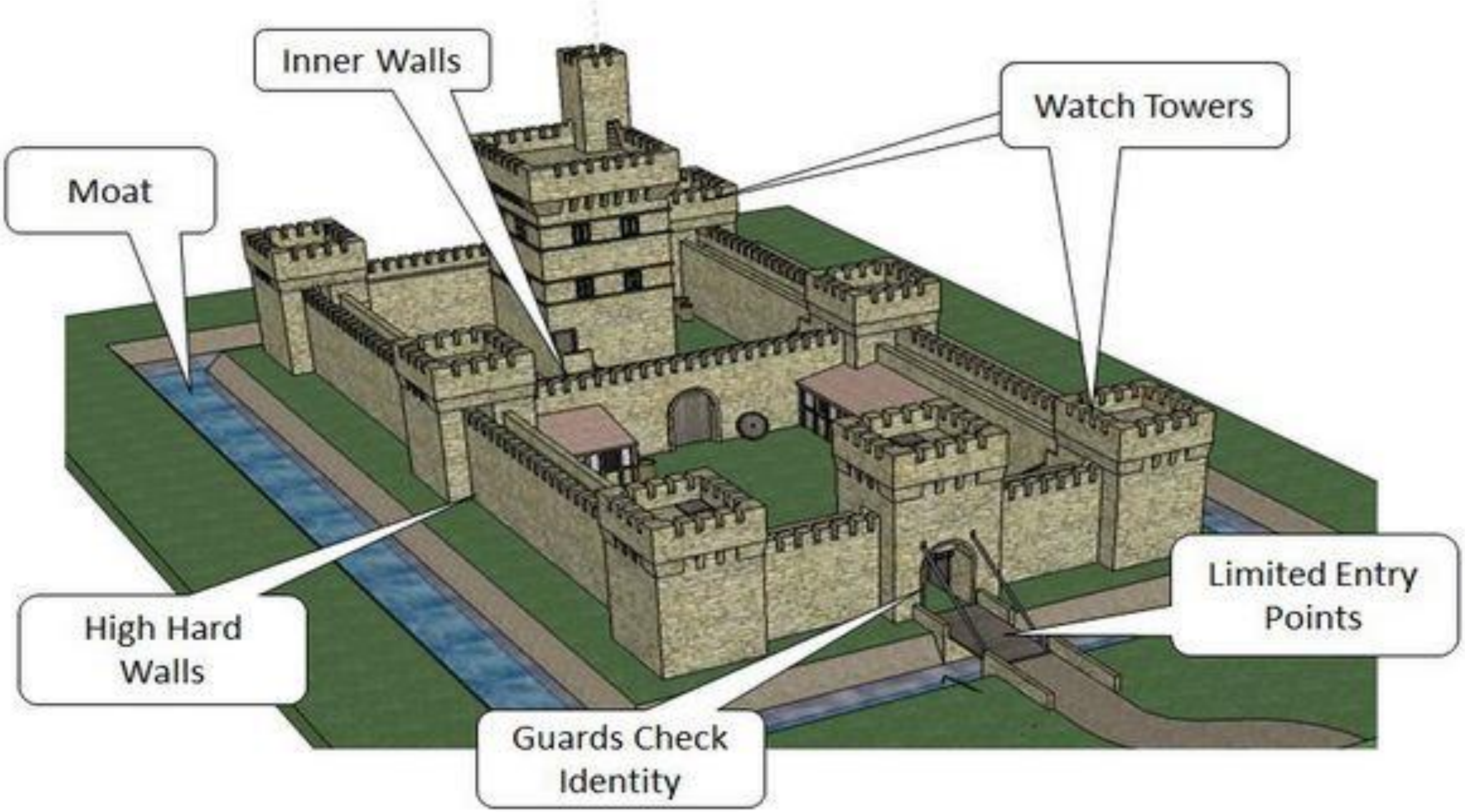
Network, Security and Privacy

158.235



A/Prof Julian Jang-Jaccard

Perimeter Defense: Castle



Securing Network Perimeter

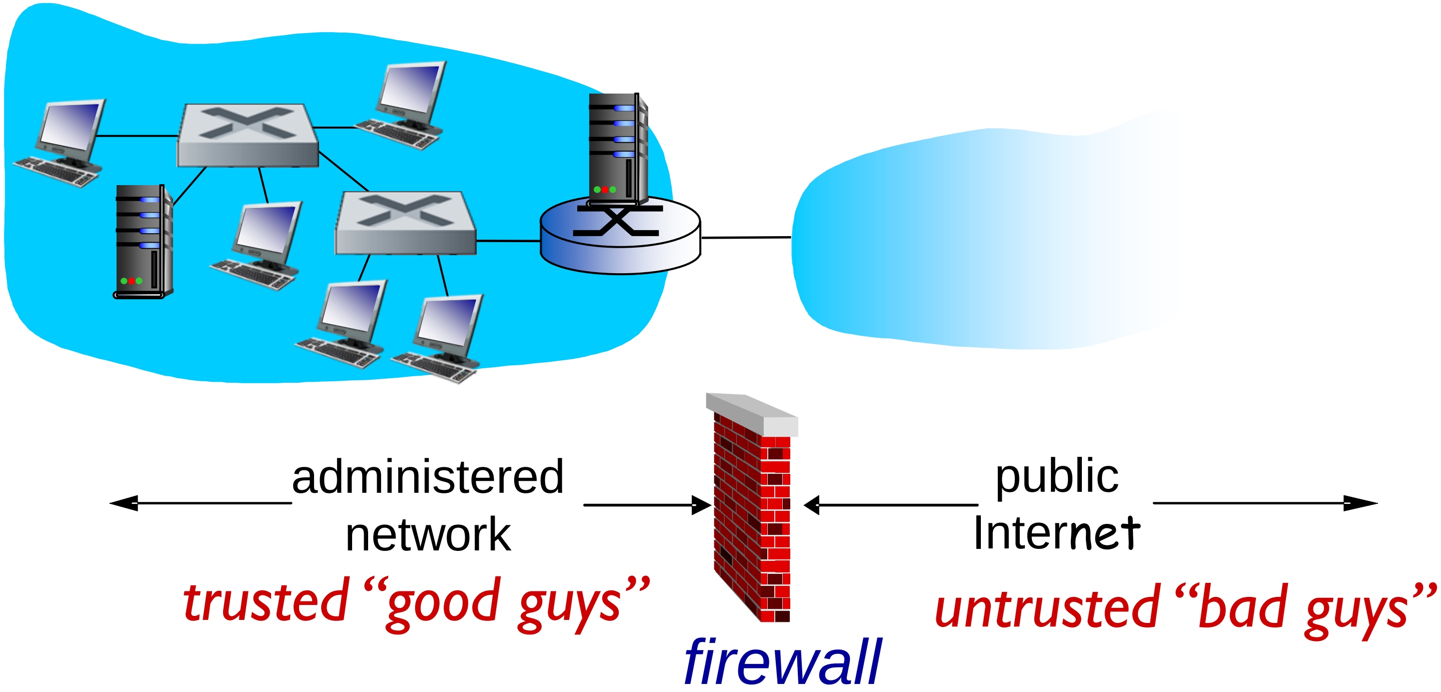
- Basic access points into a network
  - LANs inside the organization (public-facing services, e.g. servers)
  - Facilitated via Internet (most attacks come in this way)
- Basic elements in preventing access
  - Firewalls
  - Intrusion Detection Systems (IDS)
  - Network Address Translation (NAT)

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Firewall

Firewalls

- Isolates organization’s internal networks from larger Internet, allowing some packets to pass, blocking others



administered network

public Internet

trusted “good guys”

untrusted “bad guys”

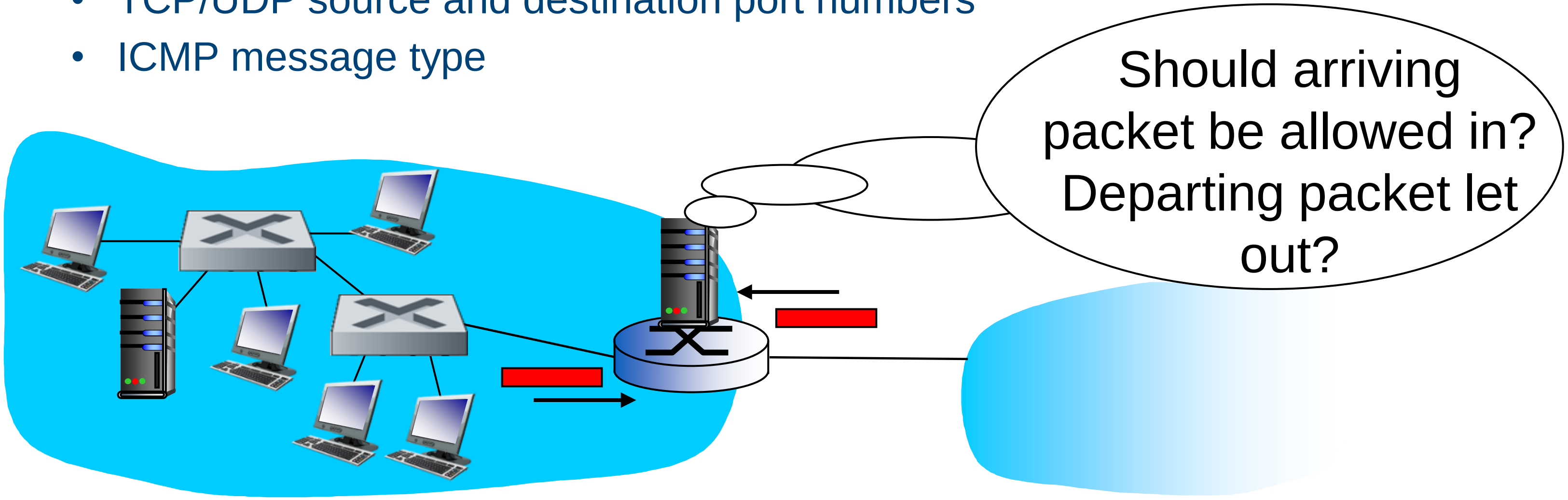
firewall

Firewalls: Why?

- Prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections
- Prevent illegal modification/access of internal data
  - e.g., attacker replaces CIA’s homepage with something else
- Allow only authorized access to inside network
  - set of authenticated users/hosts
- Three types of firewalls:
  - stateless packet filters
  - stateful packet filters
  - application gateways

Stateless packet filtering

- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type



Should arriving packet be allowed in? Departing packet let out?

Stateless packet filtering: example

- *example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23*
  - *result:* all incoming, outgoing UDP flows and telnet connections are blocked
- *example 2: block inbound TCP segments with ACK=0.*
  - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).

Access Control Lists

- ACL: table of rules, applied top to bottom to incoming packets: (action, condition) pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

- stateless packet filter: heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- Stateful packet filter: track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

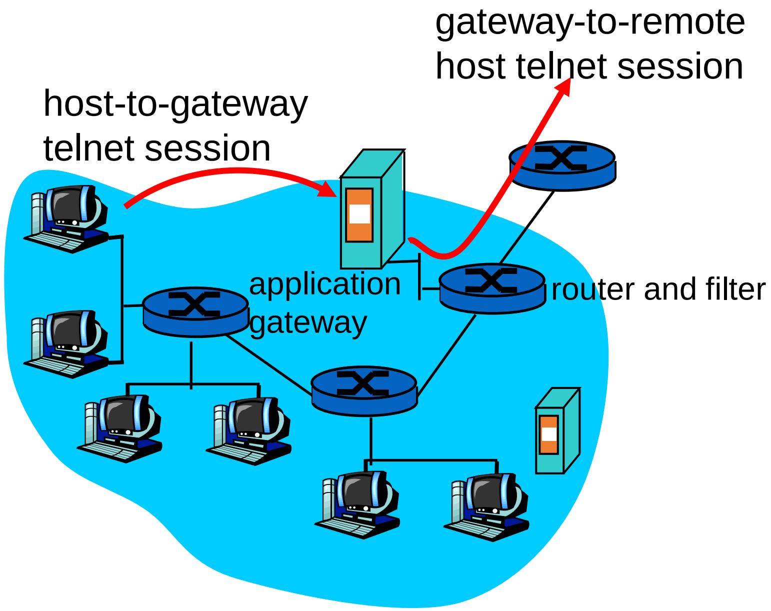
Stateful packet filtering

- ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conn
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	x
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	x
deny	all	all	all	all	all	all	

Application gateways

- filters packets on application data as well as on IP/TCP/UDP fields.
- example: allow select internal users to telnet outside.
  1. require all telnet users to telnet through gateway.
  2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
  3. router filter blocks all telnet connections not originating from gateway.


gateway-to-remote host telnet session
host-to-gateway telnet session
application gateway
router and filter

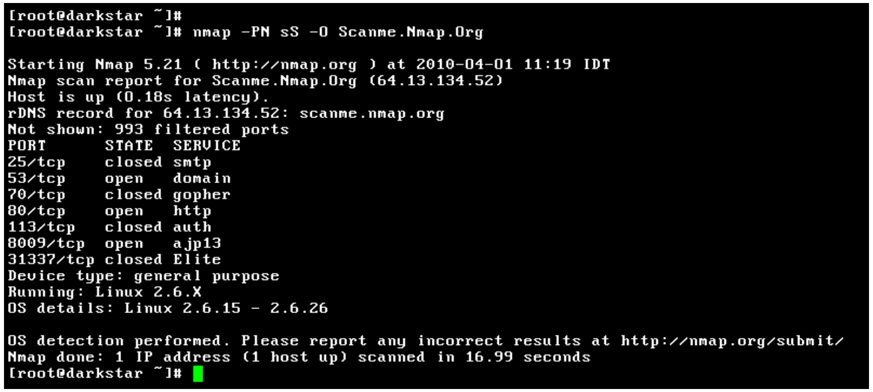
Limitations of firewalls, gateways

- *IP spoofing:* router can't know if data "really" comes from claimed source
- if multiple app's need special treatment, each has own app. gateway
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP
- *tradeoff:* degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks

Intrusion Detection Systems

Intrusion detection systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

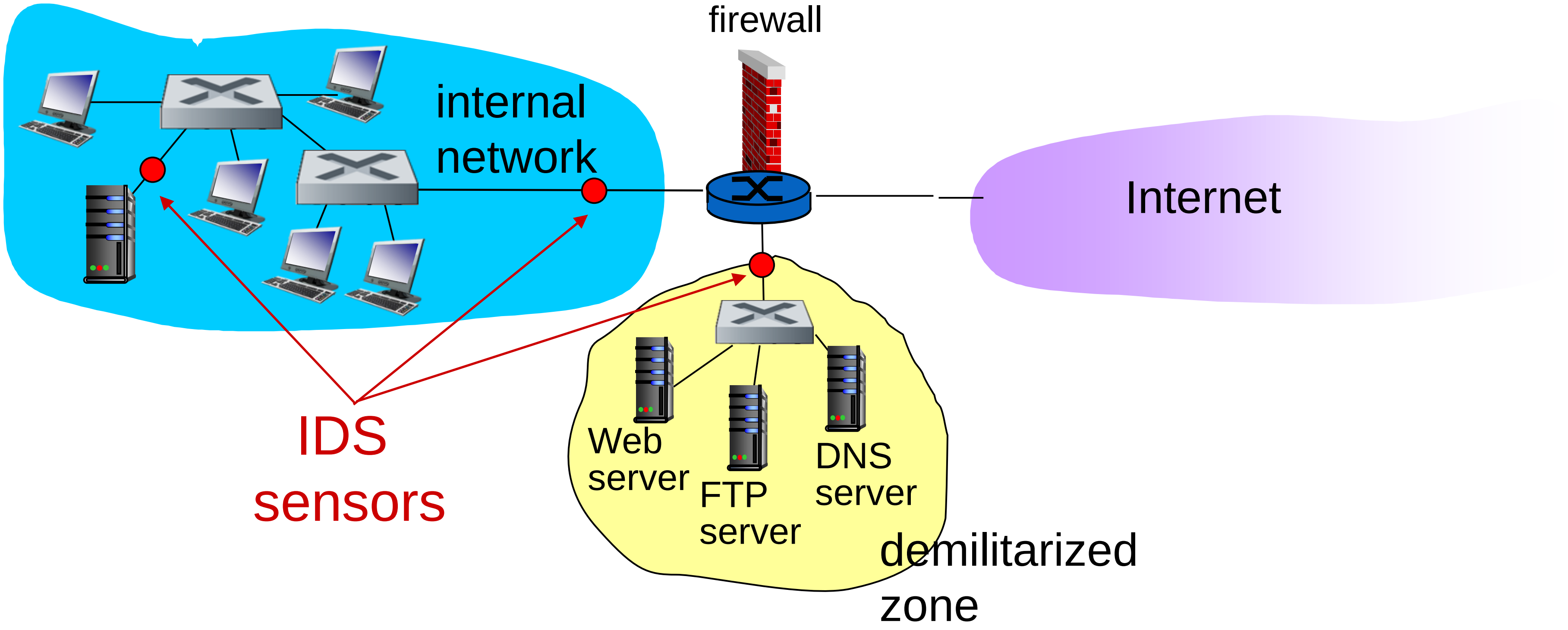


```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN sS -O Scanme.Nmap.Org

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]# █
```

Example: Port scanning by Nmap

Intrusion detection systems

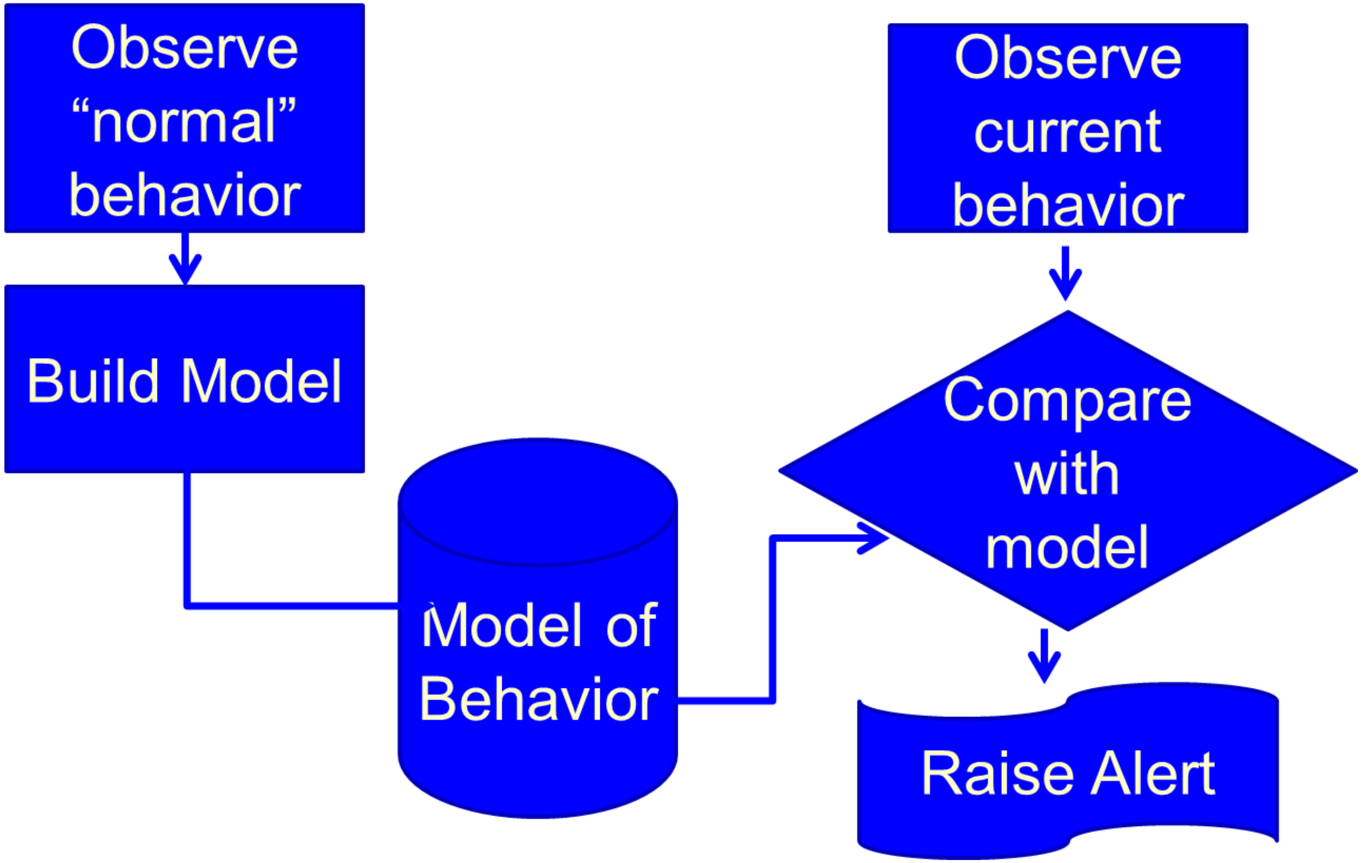
- multiple IDSs: different types of checking at different locations



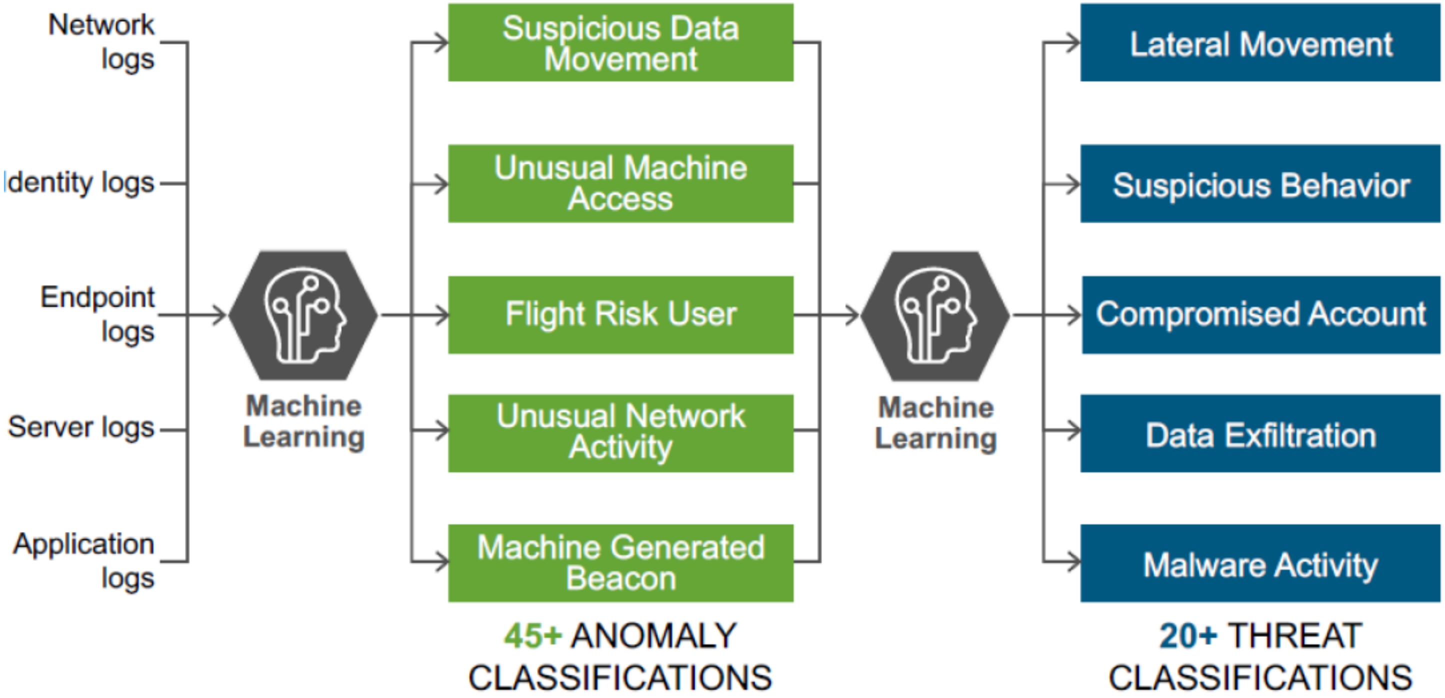
Anomaly Detection-based Filtering

- Model of expected “normal” behaviour.
- Attacks assumed to exhibit different pattern.
- Able to detect unknown attacks.
- Example of “normal”:
  - User logs on every weekday 9am.
  - Accesses supplier websites.
  - Logs off at 5pm.
- Example of “suspicious”:
  - User logs on at 3am.
  - Installs new software.
- Weakness –potential for false alarms

Anomaly Detection-based Filtering



Example: Splunk

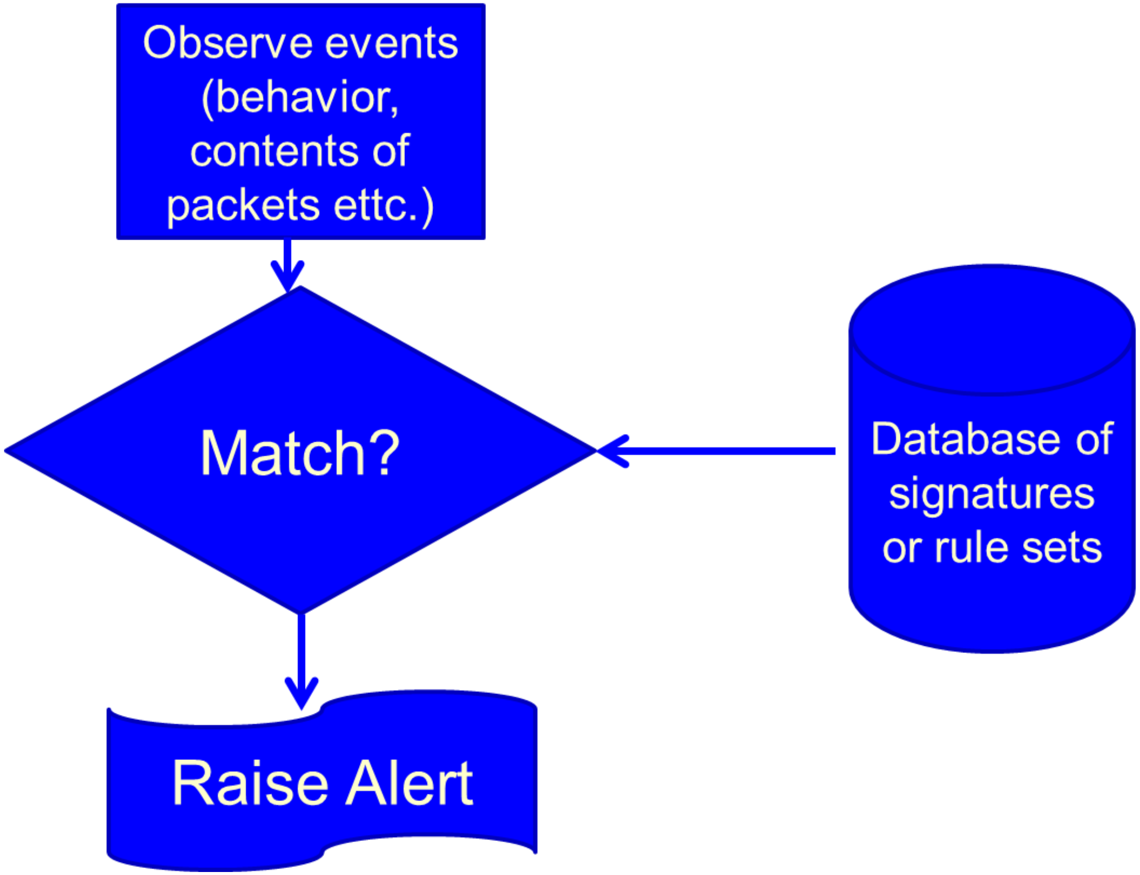


https://www.splunk.com/en_us/software/user-behavior-analytics.html

Misuse based Detection

- Attack patterns of “signatures”.
- Configured by an administrator.
- Identify user behaviour that matches.
- Strength –minimises occurrence of legitimate activity mis-identified.
- Weakness –only can identify known attacks and requires regular updates.

Misuse based Detection



Observe events (behavior, contents of packets ettc.)

Match?

Database of signatures or rule sets

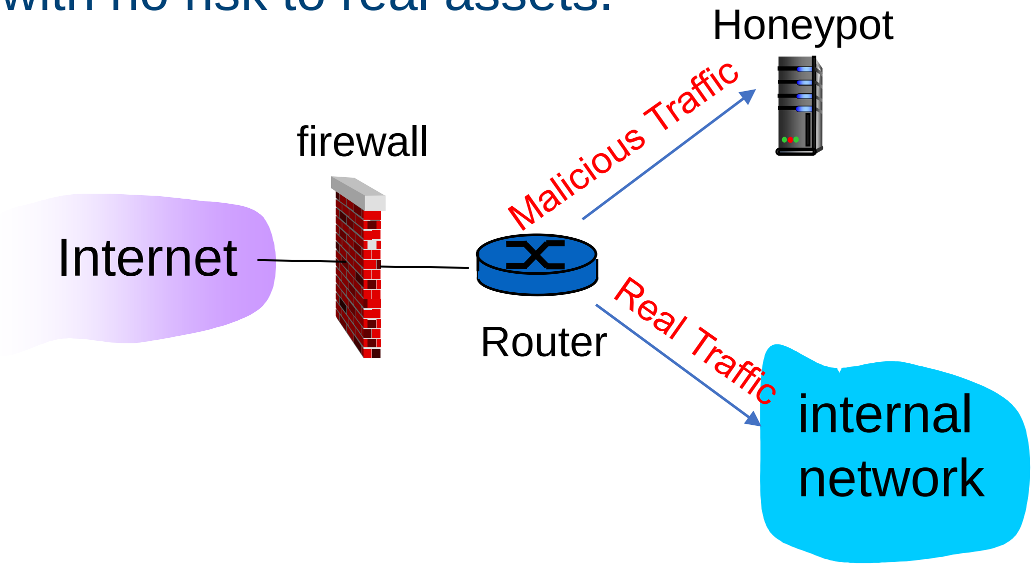
Raise Alert

Example: Snort

- Lightweight IDS system capable of performing real-time traffic analysis and packet logging
- Snort has three primary uses. It can be used as:
  1. a packet sniffer like tcpdump
  2. a packet logger (useful for network traffic debugging, etc)
  3. a full network intrusion detection system

Honeypots

- Computer or network appearing legitimate.
- Actually, a trap known as a honeypot.
- Used to study attacks or draw an attacker out.
- Monitor attacker behaviour with no risk to real assets.



MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Network Address Translation

Revisiting IP Addresses

- Most IP addresses are public
  - they uniquely identify a node in the ‘Internet’, i.e. known to the outside world
  - can be routed in the Internet
- Certain groups of IP addresses are private
  - not known to the outside world (e.g. outside of an organization or a private home network)
  - cannot be routed in the ‘Internet’

Private IP Addresses

- Private IP address ranges (IPv4):
    - 10.0.0.0/8
        - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0/12
        - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0/16
        - 192.168.0.0 – 192.168.255.255
- If you assign a node with any one of these addresses, they are not meant to be ‘seen’ by the outside world

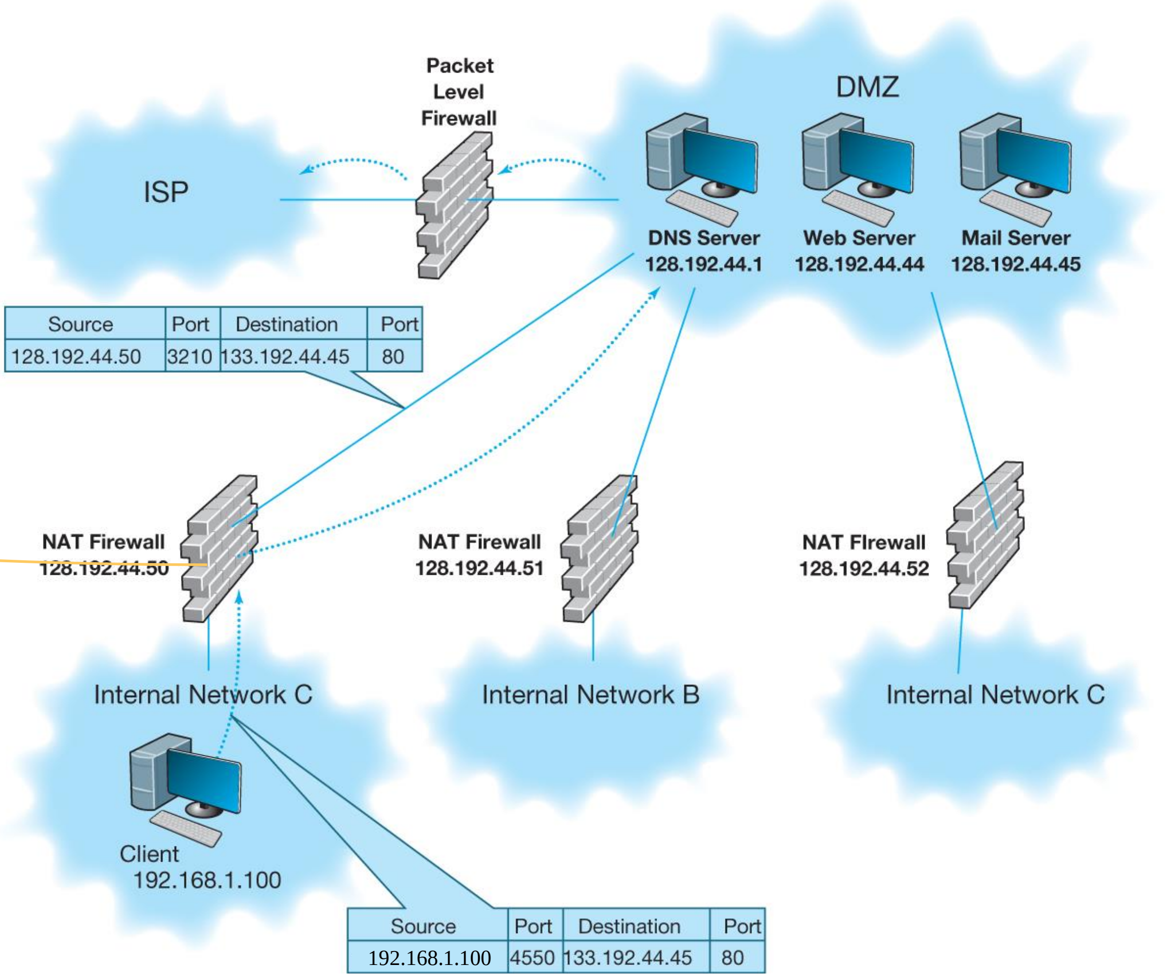
Network Address Translation (NAT)

- Used by most firewalls to shield a private network from public network
  - Translates between private addresses inside a network and public addresses outside the network
  - Done transparently, internal IP addresses remain hidden
- Performed by NAT proxy servers/router
  - Uses an address table to do translations, e.g.
    - one-to-one mapping: replace a private ‘internal’ address with public ‘outside’ address
    - one-to-many mapping: map multiple private hosts to one publicly exposed IP address
    - Performs reverse operations for response packets

Network with NAT

Port Address Translation for NAT Firewall C

Original IP	Original Source	Mapped IP	Mapped Source
192.168.1.100	4550	128.192.44.50	3210
192.168.1.101	8764	128.192.44.50	3215



Source	Port	Destination	Port
128.192.44.50	3210	133.192.44.45	80

Source	Port	Destination	Port
192.168.1.100	4550	133.192.44.45	80

Using Private Addresses with NAT

- Used to provide additional security
- Assigns private IP addresses to devices inside the network
    - Even if they are discovered, no packets with these addresses will be delivered (publicly illegal IP address)
    - Example: Assigned public address: 128.192.55.xx
        - Assign to NAT proxy server: 128.192.55.1
        - Assign to internal computers: 10.3.3.xx
            - 10.x.x.x is never used on Internet
        - Private address hidden from outside world
- Additional benefit is that it gives ability to have more internal IP addresses for an organization
    - Save IPv4 address exhaustion

END