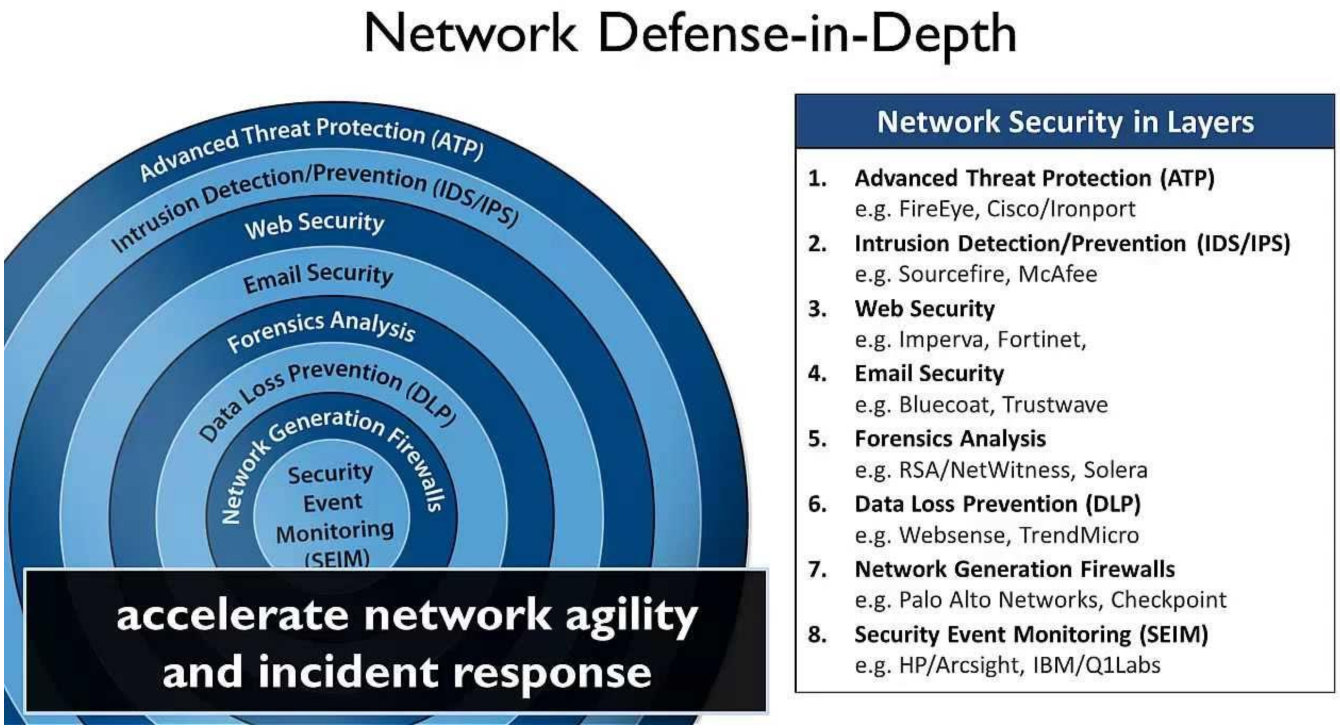
Cyber Security Fundamentals
Dr Peter Loh

Cyber Security Fundamentals

Network Security

Introduction to Network Defence: Firewalls

Network Defence


Network Defense-in-Depth
Advanced Threat Protection (ATP)
Intrusion Detection/Prevention (IDS/IPS)
Web Security
Email Security
Forensics Analysis
Data Loss Prevention (DLP)
Network Generation Firewalls
Security Event Monitoring (SEIM)
accelerate network agility and incident response

Network Security in Layers

1. **Advanced Threat Protection (ATP)**
   e.g. FireEye, Cisco/Ironport
2. **Intrusion Detection/Prevention (IDS/IPS)**
   e.g. Sourcefire, McAfee
3. **Web Security**
   e.g. Imperva, Fortinet,
4. **Email Security**
   e.g. Bluecoat, Trustwave
5. **Forensics Analysis**
   e.g. RSA/NetWitness, Solera
6. **Data Loss Prevention (DLP)**
   e.g. Websense, TrendMicro
7. **Network Generation Firewalls**
   e.g. Palo Alto Networks, Checkpoint
8. **Security Event Monitoring (SEIM)**
   e.g. HP/Arcsight, IBM/Q1Labs

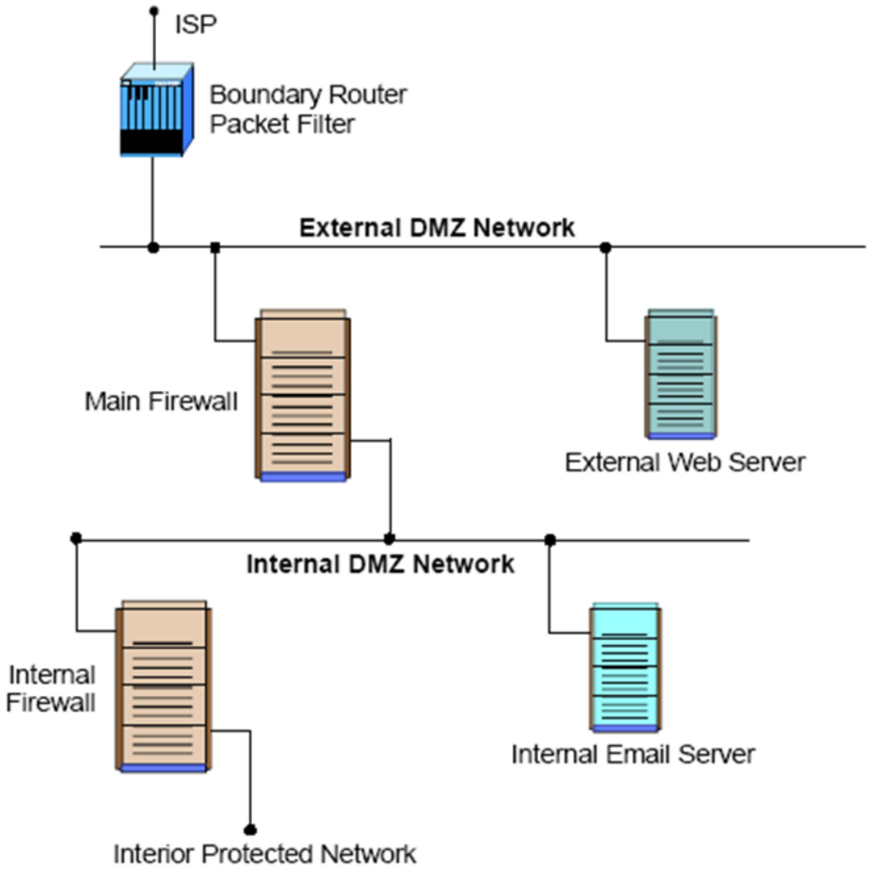
Concept of perimeter is eroding – eg. mobile employees, tele-commuting

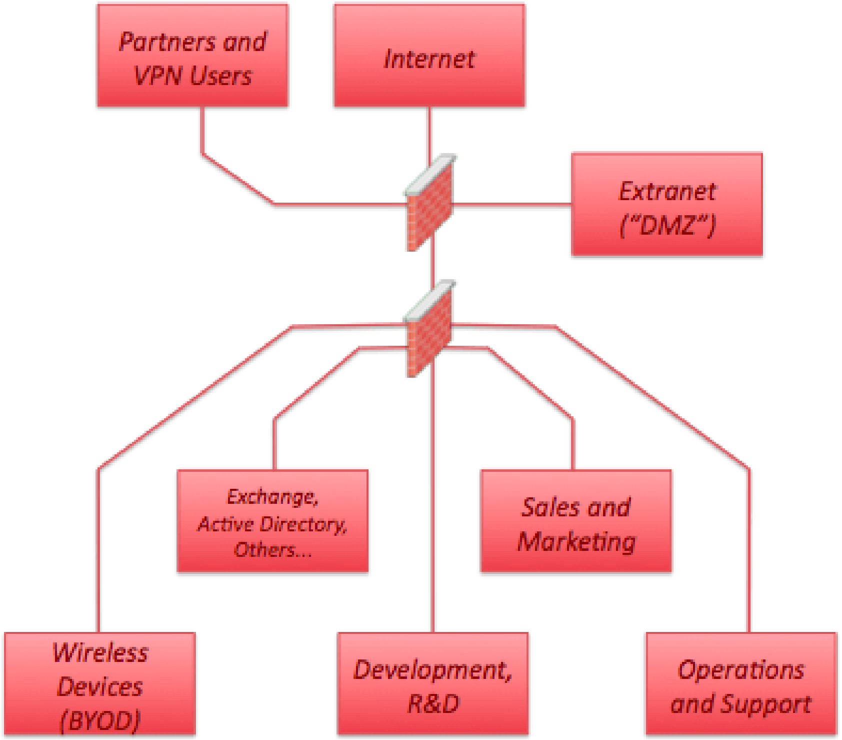
SEIM or SIEM

- Defense in depth – defences are layered, main objective to delay the attack’s progress rather than to stop it at the onset.
- First level – Firewalls and proxies control access to and from unauthorized networks and will allow or block traffic based on a set of security rules.
- Second level – Intrusion detection/protection systems detect (and protect) against malicious network activity; typically signature-based.
- Third level – VPN provides encryption over a public IP network

Firewalls

- Can be implemented as hardware or software appliance
- Monitors and filters network traffic – DMZ, zone segregation
- Combination of security mechanisms (e.g. packet filters, proxies)
- Can support Virtual Private Networks

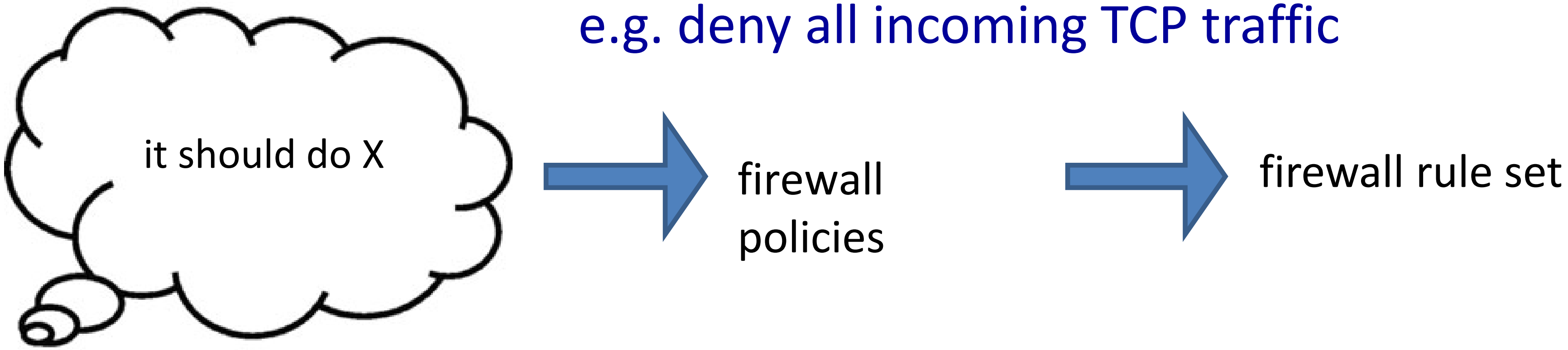




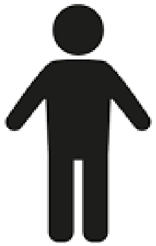
Zero Trust Model

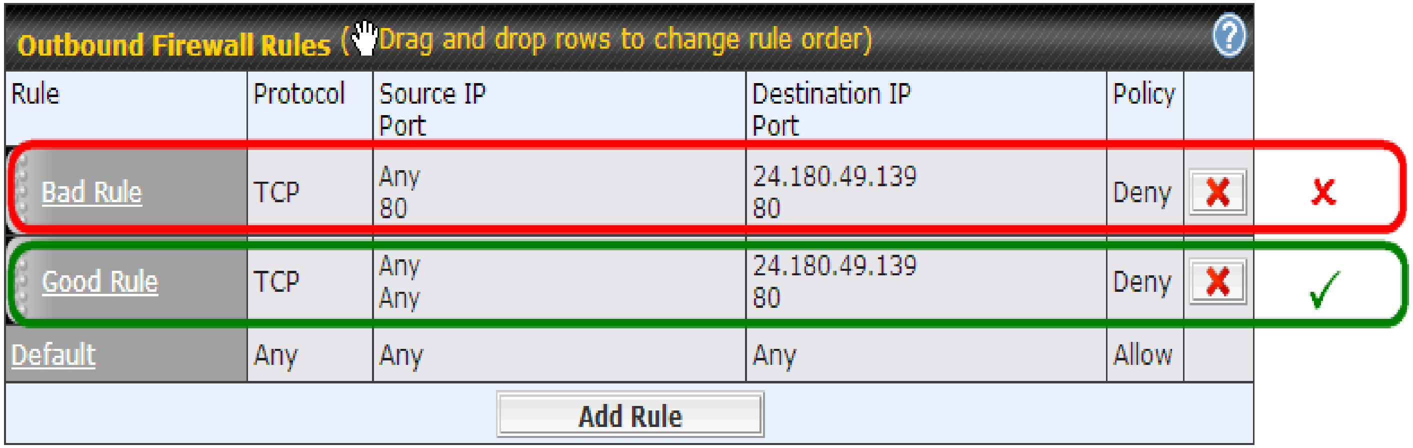
Cyber Security Fundamentals
Dr Peter Loh

Firewall policies and rule sets



e.g. deny all incoming TCP traffic





Outbound Firewall Rules (Drag and drop rows to change rule order)

Rule	Protocol	Source IP Port	Destination IP Port	Policy		
Bad Rule	TCP	Any 80	24.180.49.139 80	Deny	☒	✗
Good Rule	TCP	Any Any	24.180.49.139 80	Deny	☒	✓
Default	Any	Any	Any	Allow		

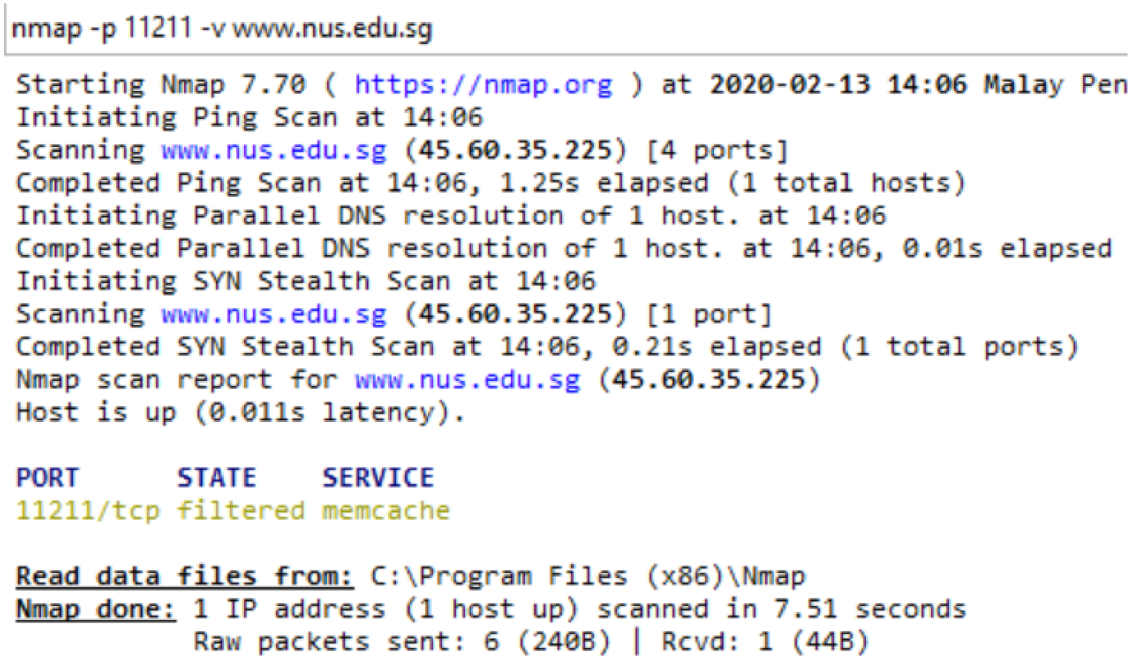
- The bad one only looks for requests from port 80 to port 80, but we could have HTTP requests from any port between 1024-65535 so traffic could still be let through.

What attacks does a firewall mitigate?

- Port scanning will have limited results, as can lock down access to ports
- Could use it to stop war driving, requests allowed only from specific IP addresses
- Limited help with DoS /DDoS – stop a lot of requests from unwanted sources but cannot protect against complex DDoS eg. Reflection DDoS
- Cannot protect against bypass attacks – eg. dial-up server behind firewall

Reflection occurs when an attacker forges the source address of request packets, pretending to be the victim. Servers are unable to distinguish legitimate from spoofed requests when UDP is used – WHY?

Attack caused exploited memcached servers to send huge amounts of traffic to the victim.



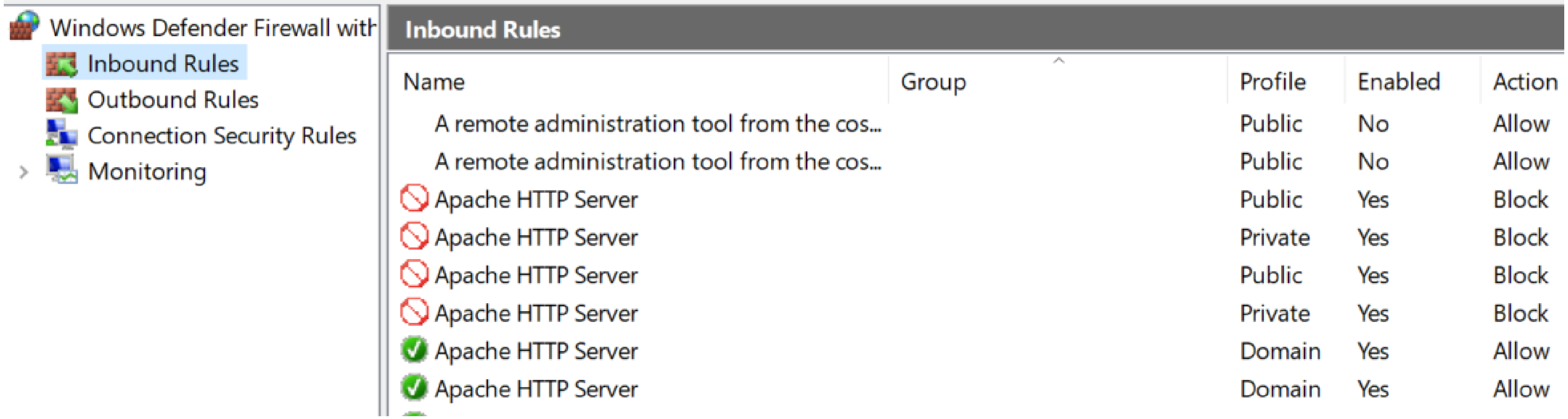
```
nmap -p 11211 -v www.nus.edu.sg

Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-13 14:06 Malay Pen
Initiating Ping Scan at 14:06
Scanning www.nus.edu.sg (45.60.35.225) [4 ports]
Completed Ping Scan at 14:06, 1.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:06
Completed Parallel DNS resolution of 1 host. at 14:06, 0.01s elapsed
Initiating SYN Stealth Scan at 14:06
Scanning www.nus.edu.sg (45.60.35.225) [1 port]
Completed SYN Stealth Scan at 14:06, 0.21s elapsed (1 total ports)
Nmap scan report for www.nus.edu.sg (45.60.35.225)
Host is up (0.011s latency).

PORT      STATE    SERVICE
11211/tcp filtered memcache

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds
           Raw packets sent: 6 (240B) | Rcvd: 1 (44B)
```

Packet Filtering



Windows Defender Firewall with
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

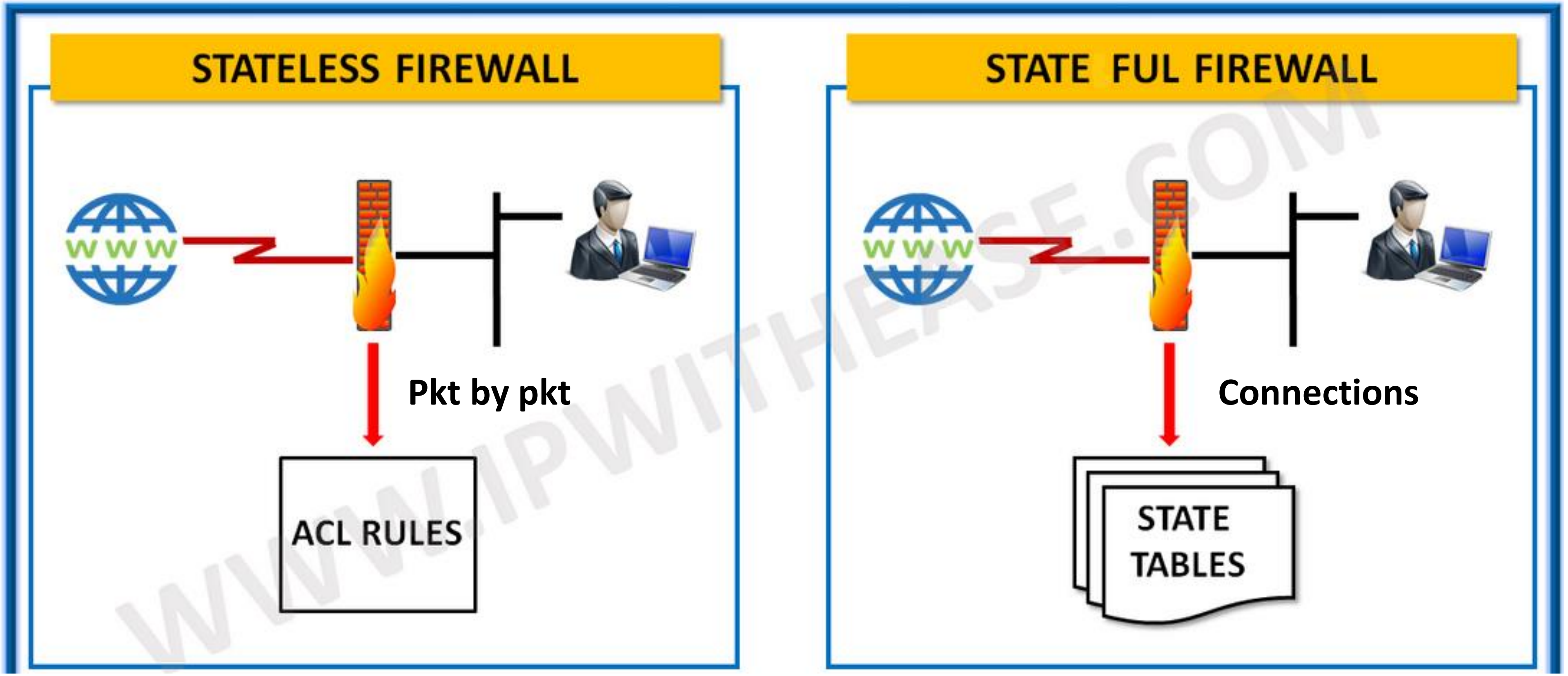
Inbound Rules

Name	Group	Profile	Enabled	Action
A remote administration tool from the cos...		Public	No	Allow
A remote administration tool from the cos...		Public	No	Allow
⊘ Apache HTTP Server		Public	Yes	Block
⊘ Apache HTTP Server		Private	Yes	Block
⊘ Apache HTTP Server		Public	Yes	Block
⊘ Apache HTTP Server		Private	Yes	Block
✓ Apache HTTP Server		Domain	Yes	Allow
✓ Apache HTTP Server		Domain	Yes	Allow

Intel 82599 Packet Filter

- A **packet filtering firewall** tests each packet that crosses the firewall according to a set of user-defined rules.
- Most common type of firewall
- Security rules pass/block/filter traffic based on eg. port, IP address and IP protocol
- Hardware and software packet filtering
- In addition, compare **Stateless vs Stateful**

[redacted]



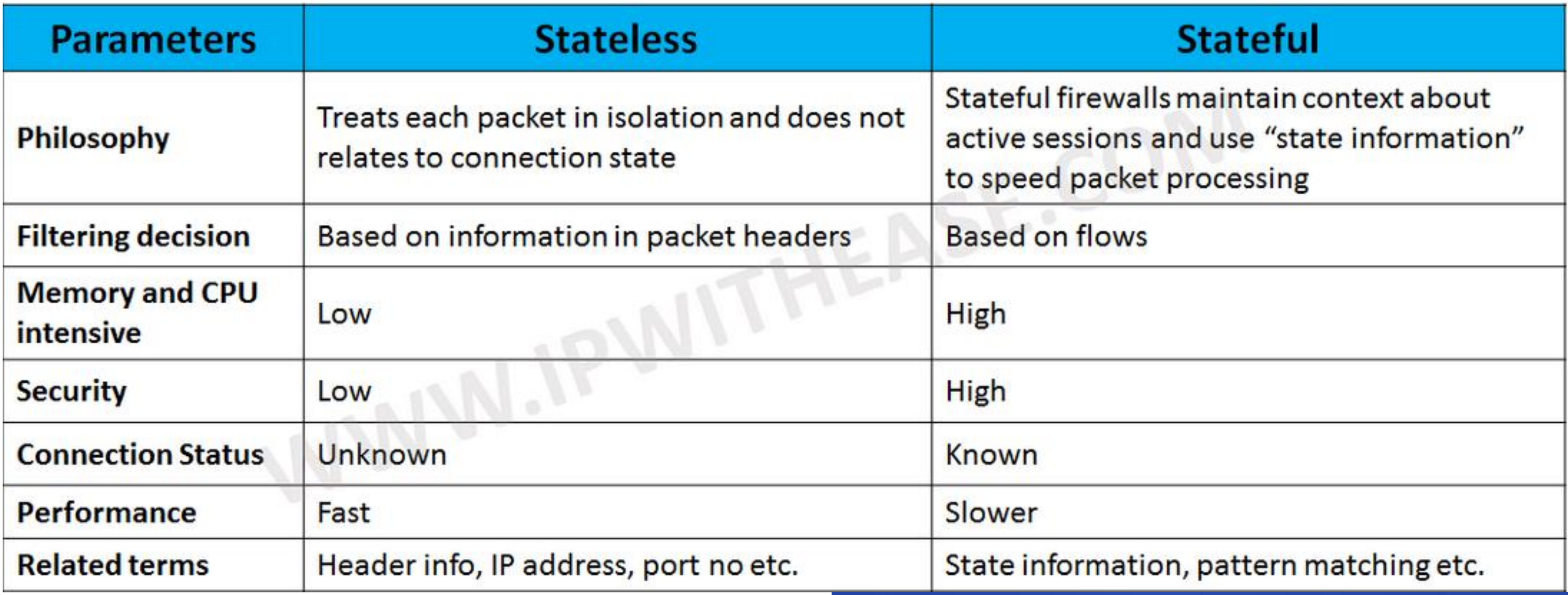
- Stateless packet filter - Does not look at the state of connections but just at the packets themselves. An example is the Extended Access Control Lists on Cisco IOS Routers.

- Stateful packet filter - aware of the connections that pass through it. It adds and maintains information about a user's connections in a state table. It then uses this table to implement the security policies for users connections. Examples: PIX, ASA, Checkpoint.

[redacted]

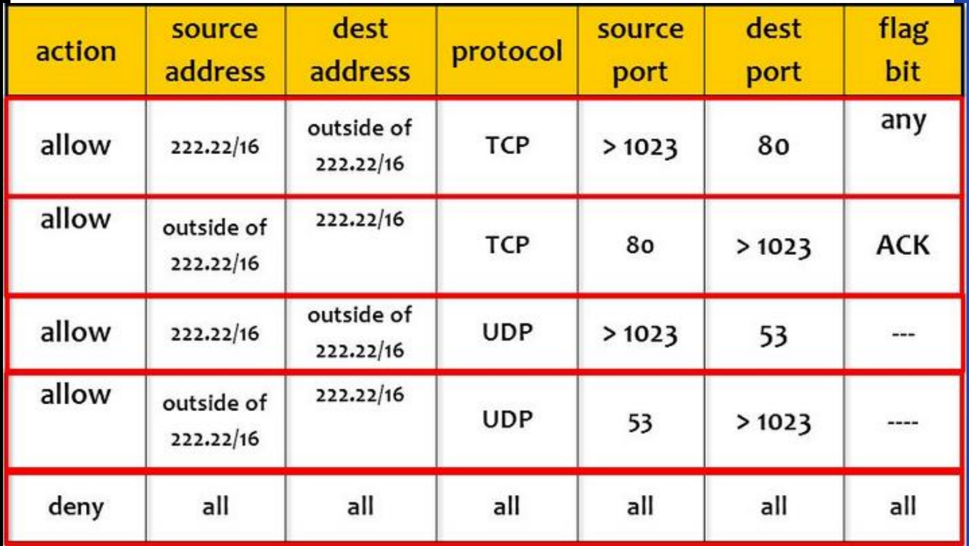
Cyber Security Fundamentals
Dr Peter Loh

Stateless vs Stateful Packet Filtering



Parameters	Stateless	Stateful
Philosophy	Treats each packet in isolation and does not relates to connection state	Stateful firewalls maintain context about active sessions and use "state information" to speed packet processing
Filtering decision	Based on information in packet headers	Based on flows
Memory and CPU intensive	Low	High
Security	Low	High
Connection Status	Unknown	Known
Performance	Fast	Slower
Related terms	Header info, IP address, port no etc.	State information, pattern matching etc.

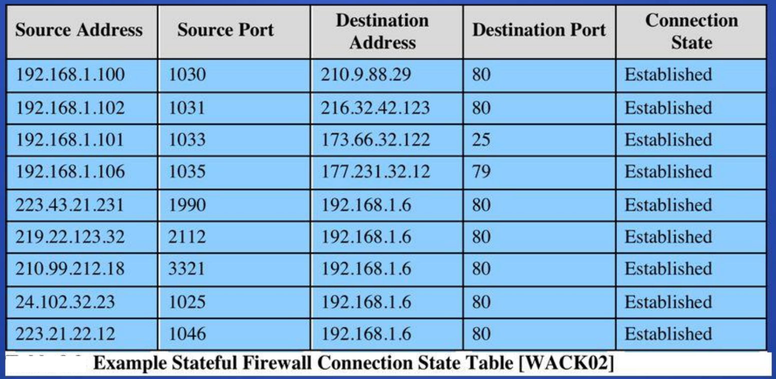
Access Control List (Stateless)



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

Example

Stateful Firewall Connection State Table



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Example Stateful Firewall Connection State Table [WACK02]

Firewall Configuration Exercise

Rules	Permission	Protocol	Source	Destination	Port
1	ALLOW/DENY	IP/TCP/UDP			
2	ALLOW/DENY	IP/TCP/UDP			
3	ALLOW/DENY	IP/TCP/UDP			
4	ALLOW/DENY	IP/TCP/UDP			
5	ALLOW/DENY	IP/TCP/UDP			
6	ALLOW/DENY	IP/TCP/UDP			

NOTES:

- **Permission:** ALLOW allows the traffic. Use DENY to block the traffic.
- **Protocol:** For both TCP and UDP traffic using the same port, you can use IP instead.
- **Source:** Set specific IP address to allow or block, or ANY to include all addresses.
- **Destination:** Set specific IP address to allow or block, or ANY to include all addresses.
- **Port:** State port number of destination server

Firewall Configuration Exercise

Rules	Permission	Protocol	Source	Destination	Port
1	ALLOW	TCP	ANY	192.168.1.174	80
2	ALLOW	TCP	ANY	192.168.1.174	443
3	ALLOW	UDP	ANY	192.168.1.100	53
4	DENY	TCP	ANY	ANY	53
5	DENY	IP	ANY	ANY	53
6	DENY		ANY	ANY	

CONFIGURE THE FIREWALL TO:

1. Allow all TCP traffic to a web server with an IP of 192.168.1.174:80.
2. Allow all HTTPS traffic to a web server with an IP of 192.168.1.174.
3. Allow DNS name queries (UDP) to a computer with an IP of 192.168.1.100.
4. Block DNS zone transfer traffic (TCP) from any source to any destination.
5. Block all DNS traffic from any source to any destination.
6. Implement implicit deny – **Any rules optimization possible here?**

Cyber Security Fundamentals
Dr Peter Loh

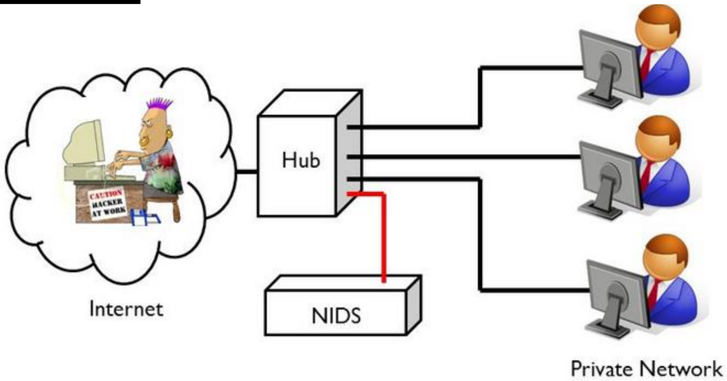
Network Security

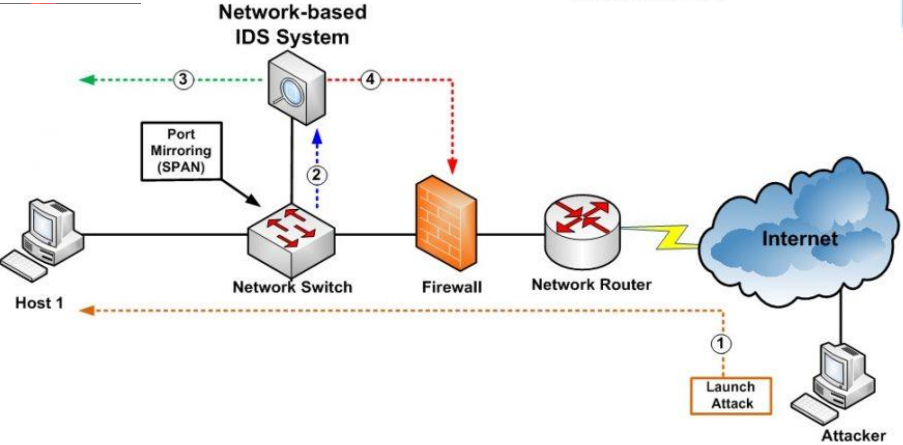
Introduction to Network Defence:

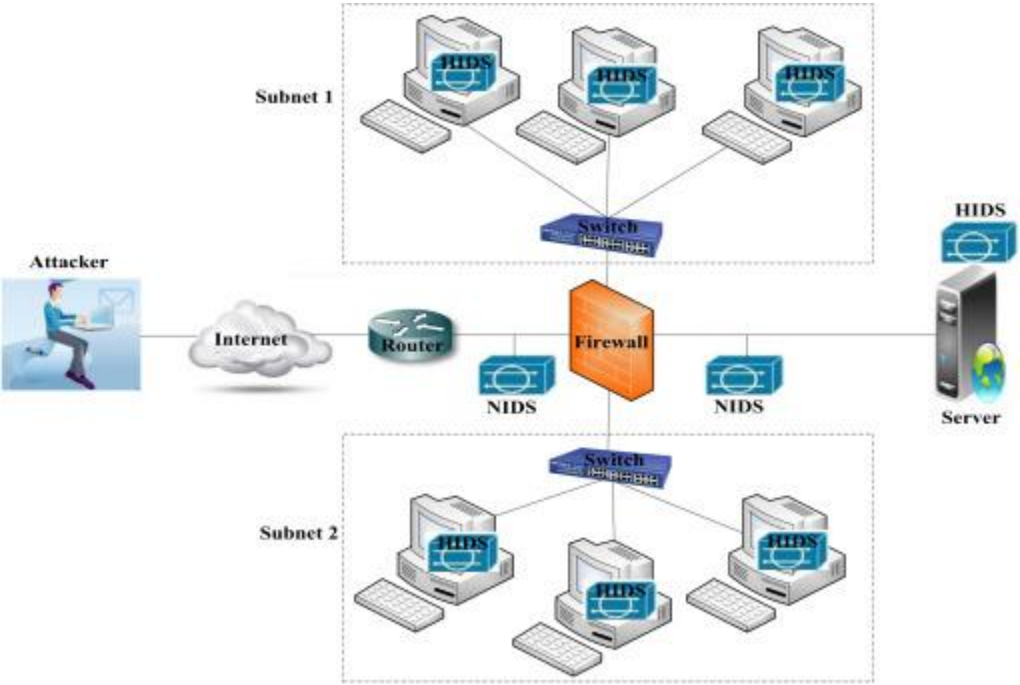
Intrusion Detection Systems (IDS)

Intrusion Prevention Systems (IPS)

Intrusion Detection Systems – 1/2





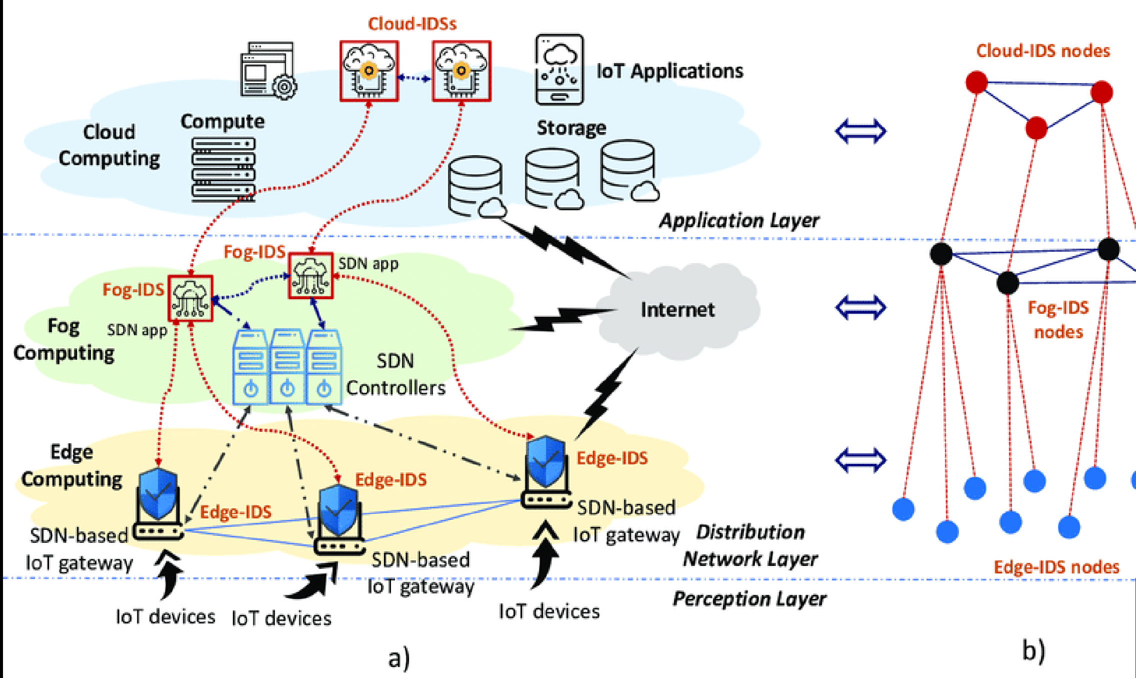


- Network Intrusion Detection System (NIDS) detects unauthorized access to network and host resources without needing traffic flow through it.

- NIDS can be connected to a Hub-based network in ***promiscuous*** mode or to a Switch-based network via ***port mirroring*** to monitor multiple/different clients.

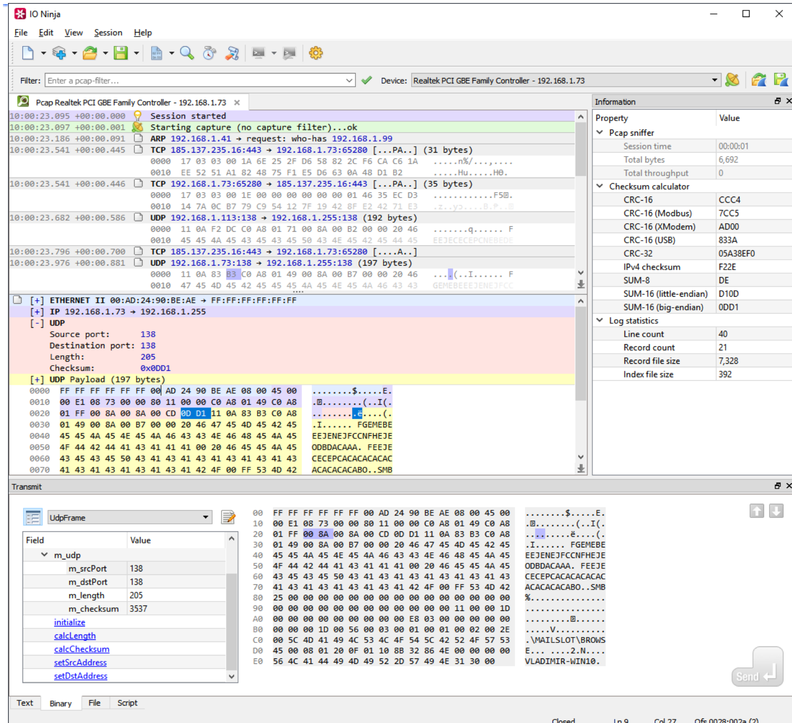
- NIDS monitoring can be extended via Host-based IDS (HIDS) or agents to cover a larger network scope (eg. SolarWinds Security Event Manager).

Intrusion Detection Systems – 2/2



- HIDS can monitor more flexibly and cover a large scope compared to a firewall.
- Able to support monitoring of IoT networks via gateway-installed agents.

- Supports deep packet inspection (DPI) – examines both header and data sections of packet; in greater detail than just packet filtering
- Signature-based or statistical anomaly-based detection techniques
- Can be used as part of IPS


IO Ninja
File Edit View Session Help
Filter: Enter a pcap-filter...
Device: Realtek PCI GBE Family Controller - 192.168.1.73
Pcap Realtek PCI GBE Family Controller - 192.168.1.73
Information
Transmit
UdpFrame
Text Binary File Script
Send

```
10:00:23.095 +00:00.000   Session started
10:00:23.097 +00:00.001   Starting capture (no capture filter)...ok
10:00:23.186 +00:00.091   ARP 192.168.1.41 → request: who-has 192.168.1.99
10:00:23.541 +00:00.445   TCP 185.137.235.16:443 → 192.168.1.73:65280 [...PA..] (31 bytes)
                          0000  17 03 03 00 1A 6E 25 2F D6 58 82 2C F6 CA C6 1A   .....n%/...,....
                          0010  EE 52 51 A1 82 48 75 F1 E5 D6 63 0A 48 D1 B2      .....Hu.....H0.
10:00:23.541 +00:00.446   TCP 192.168.1.73:65280 → 185.137.235.16:443 [...PA..] (35 bytes)
                          0000  17 03 03 00 1E 00 00 00 00 00 00 01 46 35 EC D3   ............F5.
                          0010  14 7A 0C B7 79 C9 54 12 7F 19 42 8F E2 42 71 E3   .z..y.....B...
10:00:23.682 +00:00.586   UDP 192.168.1.113:138 → 192.168.1.255:138 (192 bytes)
                          0000  11 0A F2 DC C0 A8 01 71 00 8A 00 B2 00 00 20 46   .......q...... F
                          0010  45 45 4A 45 43 45 43 45 50 43 4E 45 42 45 44 45   EEJECECEPCNEBEDE
10:00:23.796 +00:00.700   TCP 185.137.235.16:443 → 192.168.1.73:65280 [....A..]
10:00:23.976 +00:00.881   UDP 192.168.1.73:138 → 192.168.1.255:138 (197 bytes)
                          0000  11 0A 83 B3 C0 A8 01 49 00 8A 00 B7 00 00 20 46   ....(..I...... F
                          0010  47 45 4D 45 42 45 45 45 4A 45 4E 45 4A 46 43 43   GEMEBEEEJENEJFCC

[+] ETHERNET II 00:AD:24:90:BE:AE → FF:FF:FF:FF:FF:FF
  [+] IP 192.168.1.73 → 192.168.1.255
  [-] UDP
      Source port:      138
      Destination port: 138
      Length:           205
      Checksum:         0x0DD1
  [+] UDP Payload (197 bytes)
   0000  FF FF FF FF FF FF 00 AD 24 90 BE AE 08 00 45 00   ........$.....E.
   0010  00 E1 08 73 00 00 80 11 00 00 C0 A8 01 49 C0 A8   ..........(..I(.
   0020  01 FF 00 8A 00 8A 00 CD 0D D1 11 0A 83 B3 C0 A8   .........ë....(.
   0030  01 49 00 8A 00 B7 00 00 20 46 47 45 4D 45 42 45   .I...... FGEMEBE
   0040  45 45 4A 45 4E 45 4A 46 43 43 4E 46 48 45 4A 45   EEJENEJFCCNFHEJE
   0050  4F 44 42 44 41 43 41 41 41 00 20 46 45 45 4A 45   ODBDACAAA. FEEJE
   0060  43 45 43 45 50 43 41 43 41 43 41 43 41 43 41 43   CECEPCACACACACAC
   0070  41 43 41 43 41 43 41 43 41 42 4F 00 FF 53 4D 42   ACACACACABO..SMB
```

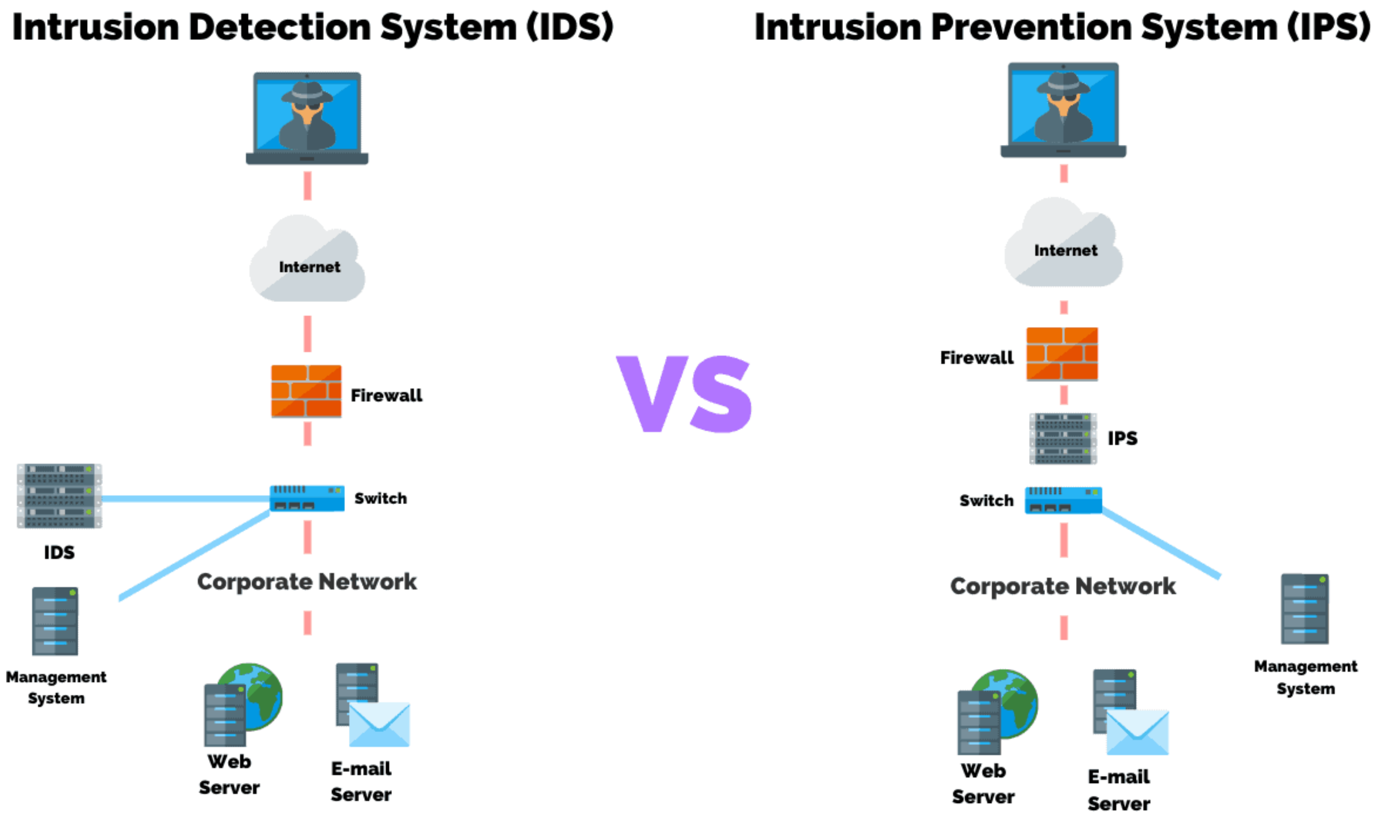
Property	Value
Pcap sniffer	
Session time	00:00:01
Total bytes	6,692
Total throughput	0
Checksum calculator	
CRC-16	CCC4
CRC-16 (Modbus)	7CC5
CRC-16 (XModem)	AD00
CRC-16 (USB)	833A
CRC-32	05A38EF0
IPv4 checksum	F22E
SUM-8	DE
SUM-16 (little-endian)	D10D
SUM-16 (big-endian)	0DD1
Log statistics	
Line count	40
Record count	21
Record file size	7,328
Index file size	392

Field	Value
m_udp	
m_srcPort	138
m_dstPort	138
m_length	205
m_checksum	3537
initialize	
calcLength	
calcChecksum	
setSrcAddress	
setDstAddress	

```
00  FF FF FF FF FF FF 00 AD 24 90 BE AE 08 00 45 00   ........$.....E.
10  00 E1 08 73 00 00 80 11 00 00 C0 A8 01 49 C0 A8   ..........(..I(.
20  01 FF 00 8A 00 8A 00 CD 0D D1 11 0A 83 B3 C0 A8   .........ë....(.
30  01 49 00 8A 00 B7 00 00 20 46 47 45 4D 45 42 45   .I...... FGEMEBE
40  45 45 4A 45 4E 45 4A 46 43 43 4E 46 48 45 4A 45   EEJENEJFCCNFHEJE
50  4F 44 42 44 41 43 41 41 41 00 20 46 45 45 4A 45   ODBDACAAA. FEEJE
60  43 45 43 45 50 43 41 43 41 43 41 43 41 43 41 43   CECEPCACACACACAC
70  41 43 41 43 41 43 41 43 41 42 4F 00 FF 53 4D 42   ACACACACABO..SMB
80  25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   %...............
90  00 00 00 00 00 00 00 00 00 00 00 11 00 00 1D      ................
A0  00 00 00 00 00 00 00 00 00 E8 03 00 00 00 00 00   ................
B0  00 00 00 1D 00 56 00 03 00 01 00 01 00 02 00 2E   .....V..........
C0  00 5C 4D 41 49 4C 53 4C 4F 54 5C 42 52 4F 57 53   .\MAILSLOT\BROWS
D0  45 00 08 01 20 0F 01 10 8B 32 86 4E 00 00 00 00   E... .....2.N....
E0  56 4C 41 44 49 4D 49 52 2D 57 49 4E 31 30 00      VLADIMIR-WIN10.
```

Closed Ln 9 Col 27 Ofs 0028:002a (2)

Intrusion Protection Systems



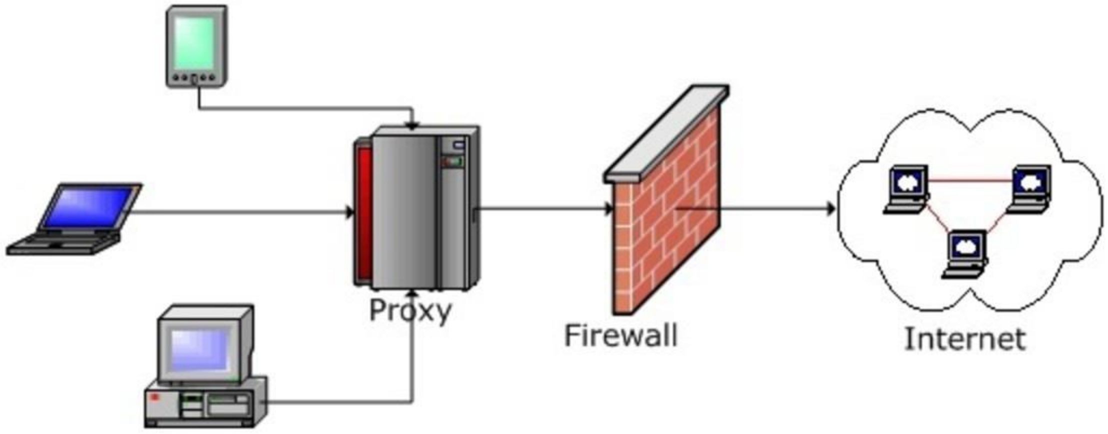
- A Network Intrusion Prevention System (NIPS) does what a NIDS does plus automated responses to block intrusions, protect against system hijacking and data theft (including changing firewall settings).
- NIPS is usually located inline between the firewall and the protected network and thus requires greater logging capacity and ability to respond in real-time.

Network Security

Introduction to Network Defence

Proxies

Proxies – 1/2

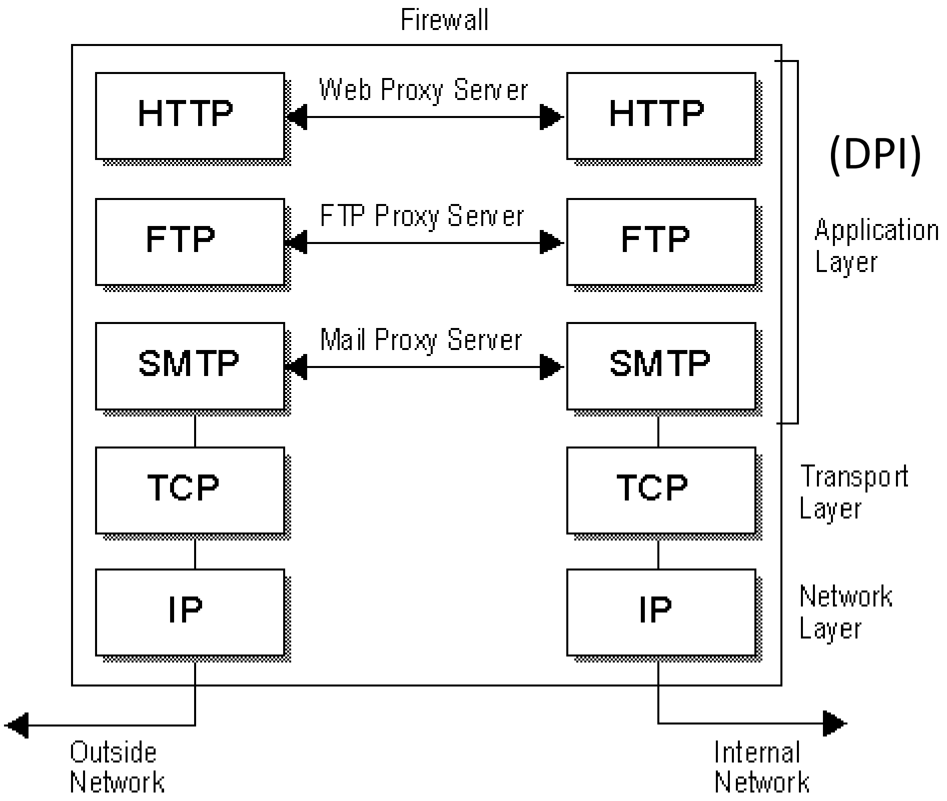


Makes application-level connections to external hosts on behalf of internal hosts to completely break the network connection between internal and external hosts

- A proxy firewall, or application gateway, protects network resources by re-directing web requests at the application layer (no direct connections with external servers).
- Scans incoming traffic for layer 7 protocols like FTP and HTTP and also offers deep packet inspection of the incoming data packets for possible maliciousness.
- Functioning at high level in the OSI stack enable them to detect and address spoofing and other sophisticated attacks;
- Examines the data for content that is not allowed; can limit applications supported by network.
- Provides private or anonymous Internet access (hides IP address).

Proxies – 2/2

A proxy service must be run for each type of Internet application the firewall will support -- a Simple Mail Transport Protocol (SMTP) proxy for e-mail, an HTTP proxy for Web services etc.



Examples:
Symantec Advanced Security and Gateway ProxySG

- Have extensive logging capabilities due to ability to examine contents of the entire network packet rather than just addresses and ports.
- It can also cache frequently accessed web pages to reduce network traffic – improved network performance.
- May not be well suited for real-time or high-bandwidth applications.

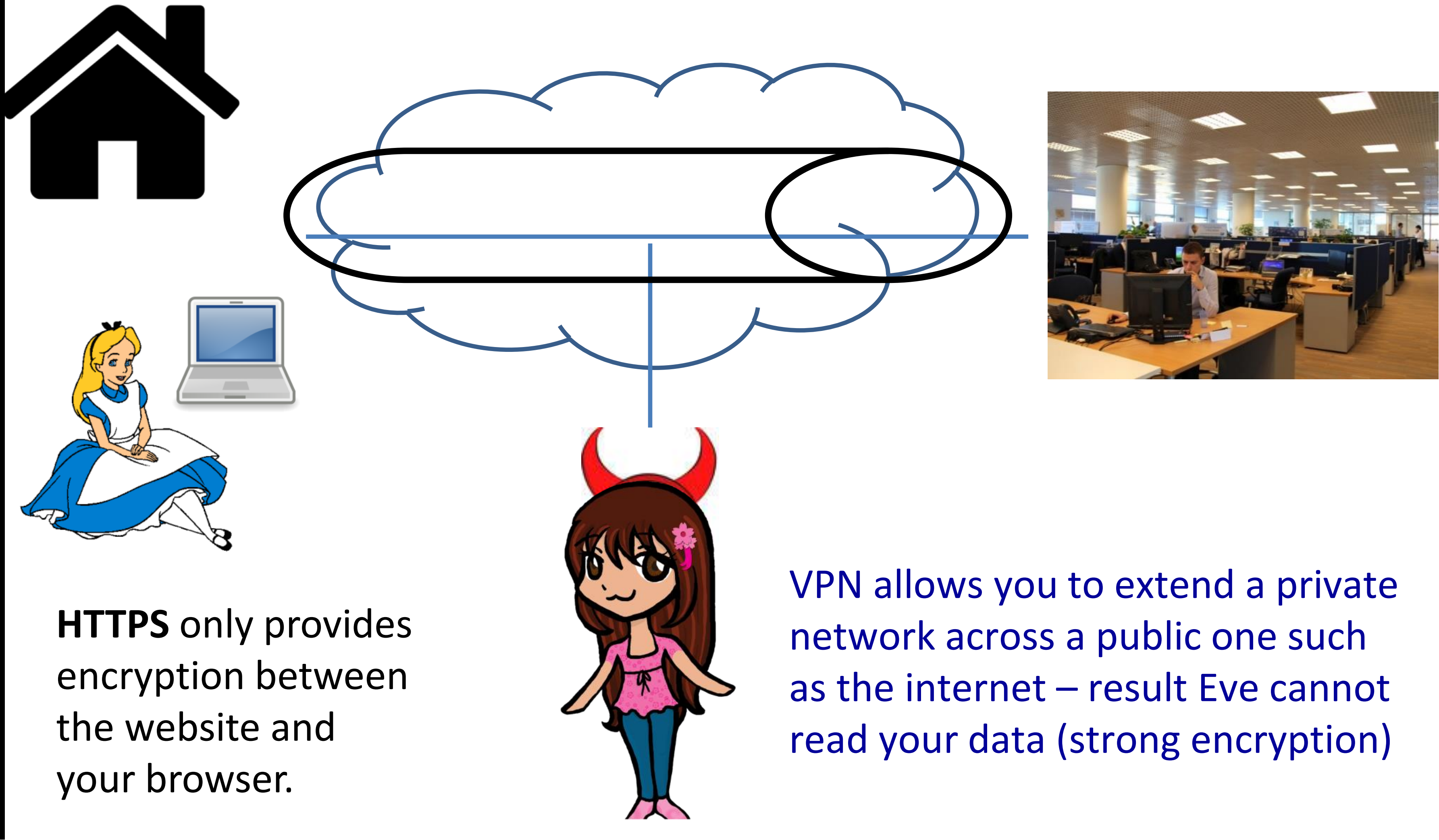
Network Security

Introduction to Network Defence:

Virtual Private Networks

Virtual Private Networks (VPNs)

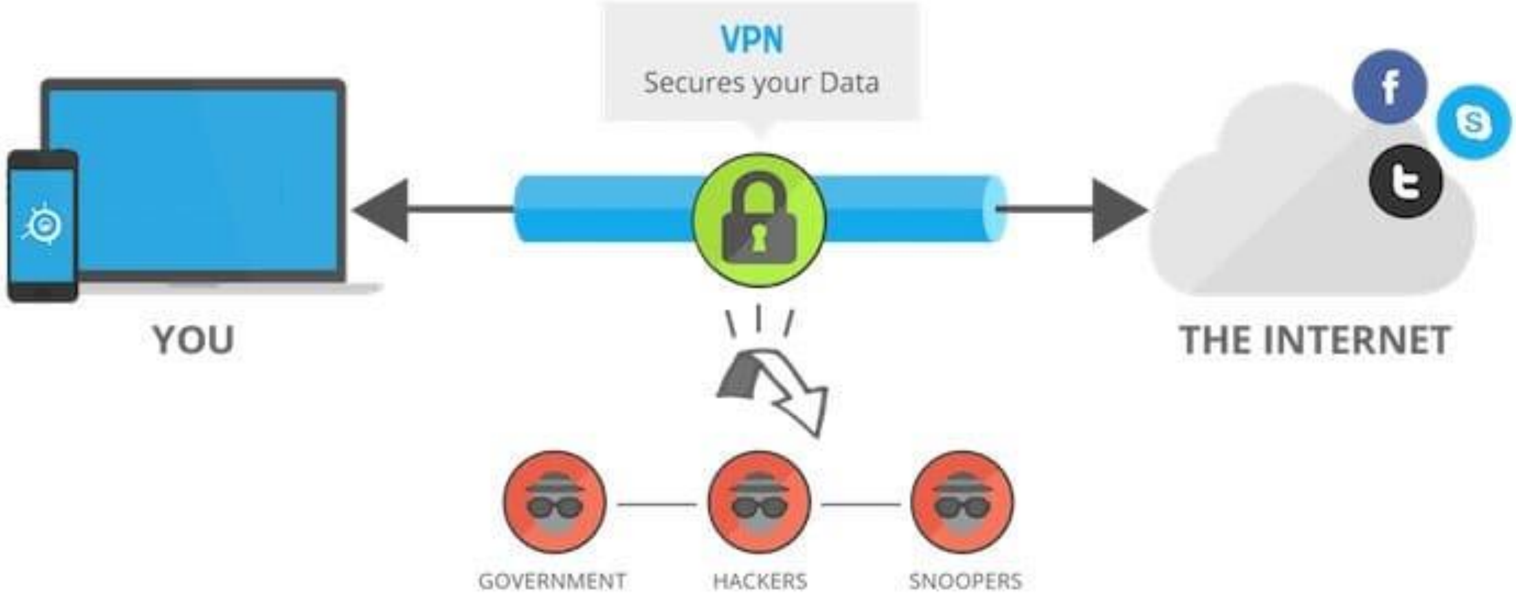
Extend corporate networks to remote offices, mobile users, telecommuters and other extranet partners



HTTPS only provides encryption between the website and your browser.

VPN allows you to extend a private network across a public one such as the internet – result Eve cannot read your data (strong encryption)

VPN Sub-Systems

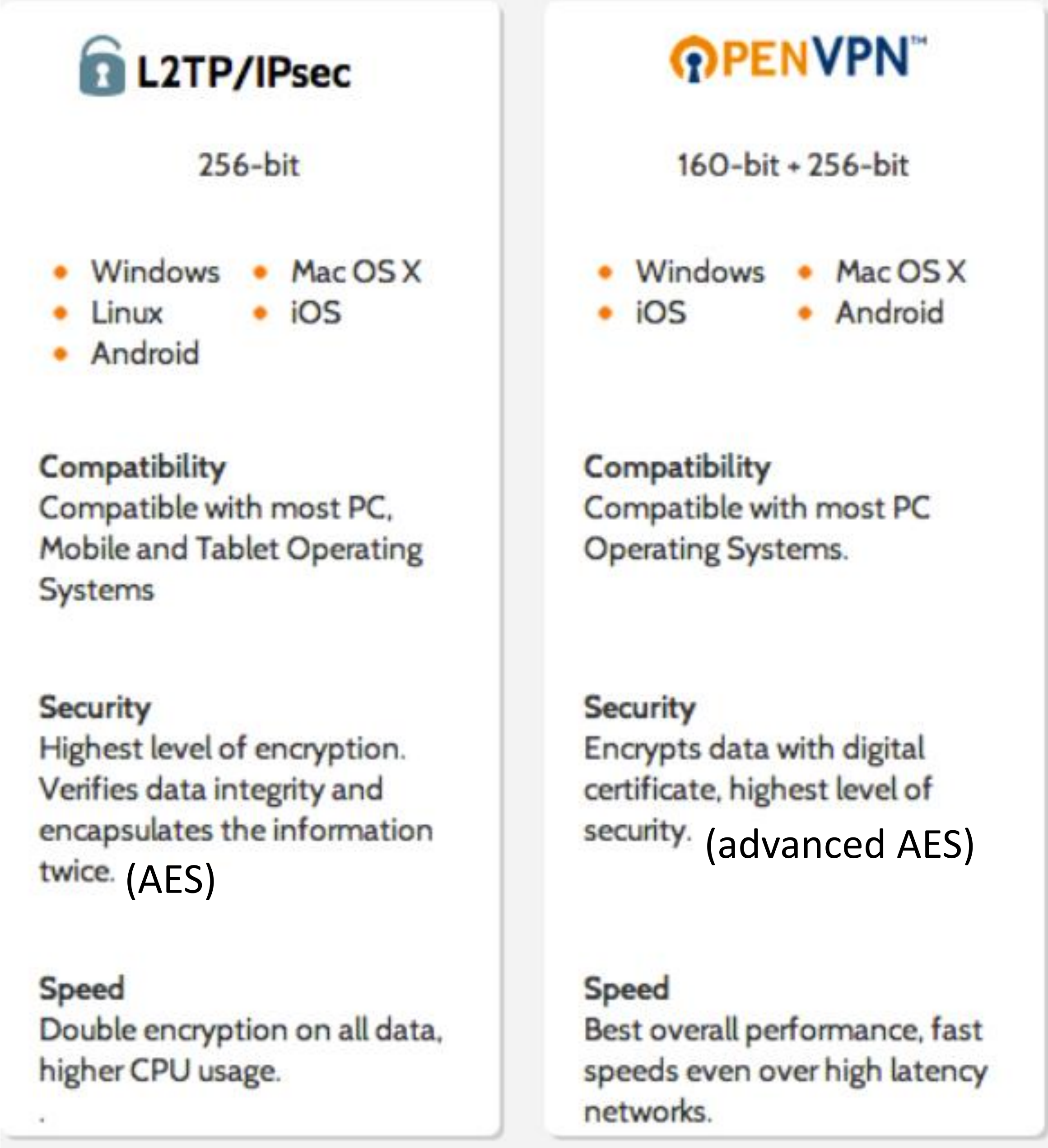


Internet Protocol Security (IPSec) and Transport Layer Security (TLS)

- Authentication – users must be authenticated before secure tunnel is established.
- Tunnelling – encapsulation of one type of protocol packet within the datagram of a different protocol; A tunnel management protocol is used as the mechanism to create, maintain, and terminate the tunnel.
- Encryption – to protect data travelling thru tunnel.

IPSec VPN vs TLS VPN (Security)

- Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol implemented with IPsec for security
- OpenVPN is an open source s/w implementing VPN techniques and uses Transport Layer Security (TLS) for key exchange



L2TP/IPsec	OPENVPN™
256-bit	160-bit + 256-bit
• Windows • Mac OS X • Linux • iOS • Android	• Windows • Mac OS X • iOS • Android
Compatibility Compatible with most PC, Mobile and Tablet Operating Systems	**Compatibility** Compatible with most PC Operating Systems.
Security Highest level of encryption. Verifies data integrity and encapsulates the information twice. (AES)	**Security** Encrypts data with digital certificate, highest level of security. (advanced AES)
Speed Double encryption on all data, higher CPU usage.	**Speed** Best overall performance, fast speeds even over high latency networks.

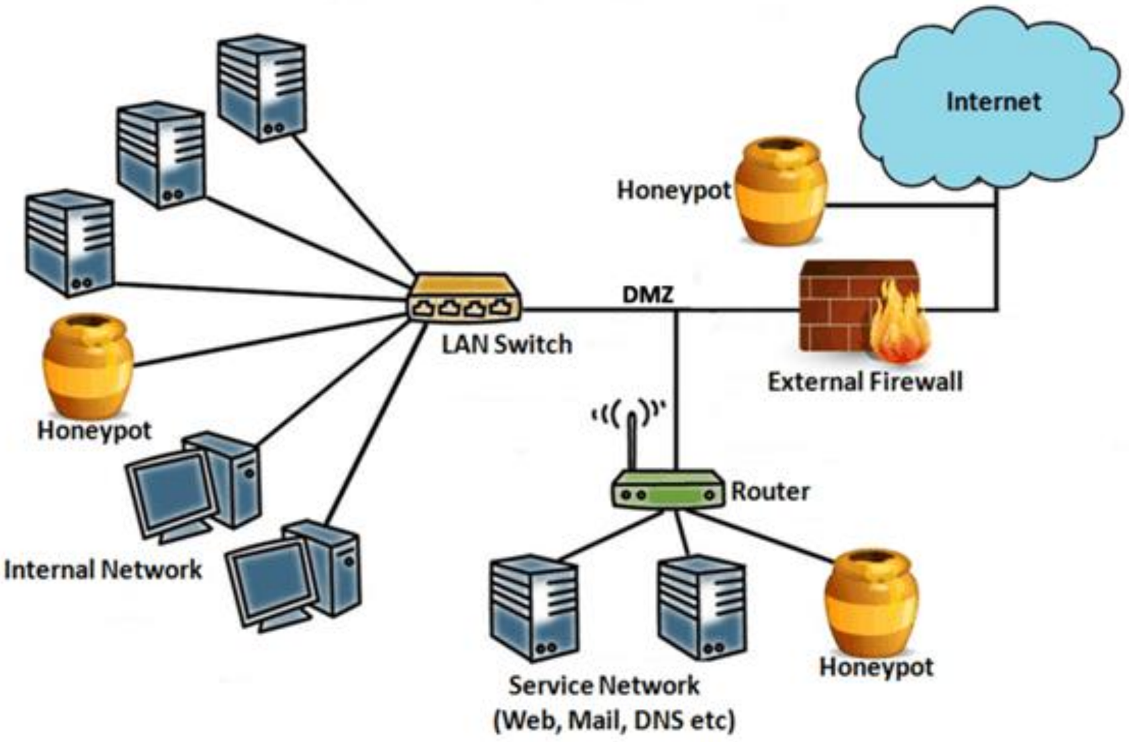
Cyber Security Fundamentals
Dr Peter Loh

Network Security

Introduction to Network Defence:

Honeypots (Optional/Additional Level of Defence)

Honeypots in the Network



Attivo Networks – Adaptive Honeypots (with ML)

Dynamically learns from attacks; preparation for 0-days

- A honeypot acts as a decoy – often set up in a VM or cloud server connected to a network, but isolated and monitored
- Honeypots are designed to be intentionally vulnerable, with weaknesses that get detected by a port scanner who will then try to exploit
- A properly configured honeypot should have many of the same features of your production system – attacker should not be put on alert of its presence

Cyber Security Fundamentals
Dr Peter Loh

Summary

- Overview of Network Security and Defence-in-Depth
- Firewalls – configuring rules, stateless vs stateful packet filtering.
- Network Intrusion Detection vs Prevention System
- Proxies – Proxy Firewall as application gateway
- VPN – Authentication, Tunnelling and Encryption
- VPN Protocols – IPSec and OpenVPN
- OpenVPN has better security and performance over IPsec.
- (Smart) Honeypots as an additional level of (adaptive) defence.
- **Next Lecture – Network Vulnerabilities and Exploits**