Nanyang Polytechnic

Firewalls

Nanyang Polytechnic

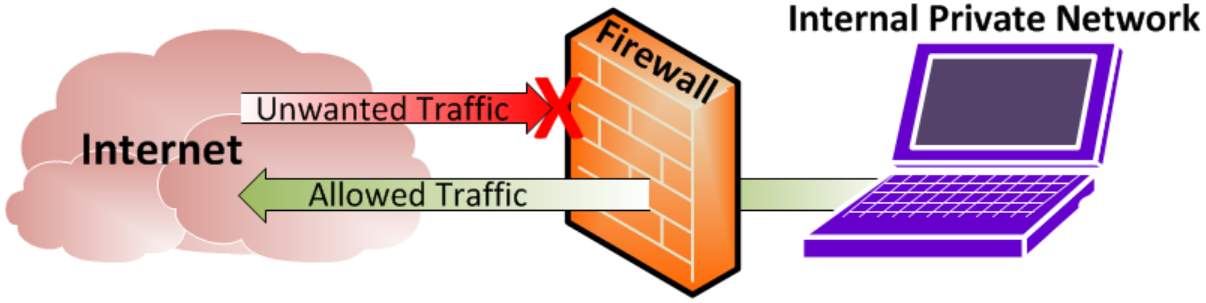
Learning Outcome

After this session, you will be able to describe:

- Types/Architecture of Firewall
- Next Generation Firewall (NGFW)
- How to design firewall Policy
- Firewall Best Practices

Firewall Introduction

A firewall is a system or group of systems used to control access between two networks -- a trusted network (Internal Private Network) & an untrusted network (Internet).



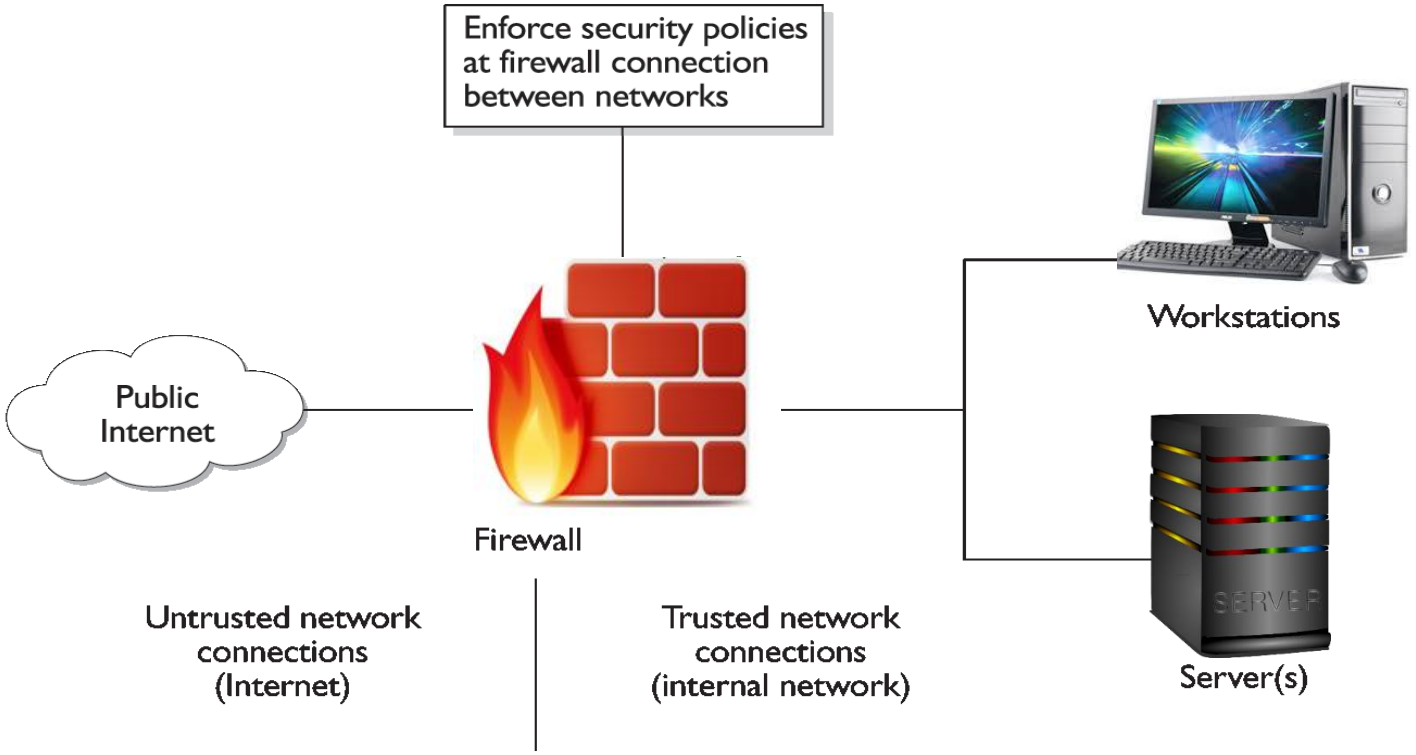
Nanyang Polytechnic

Firewall Introduction

Perimeter Defence

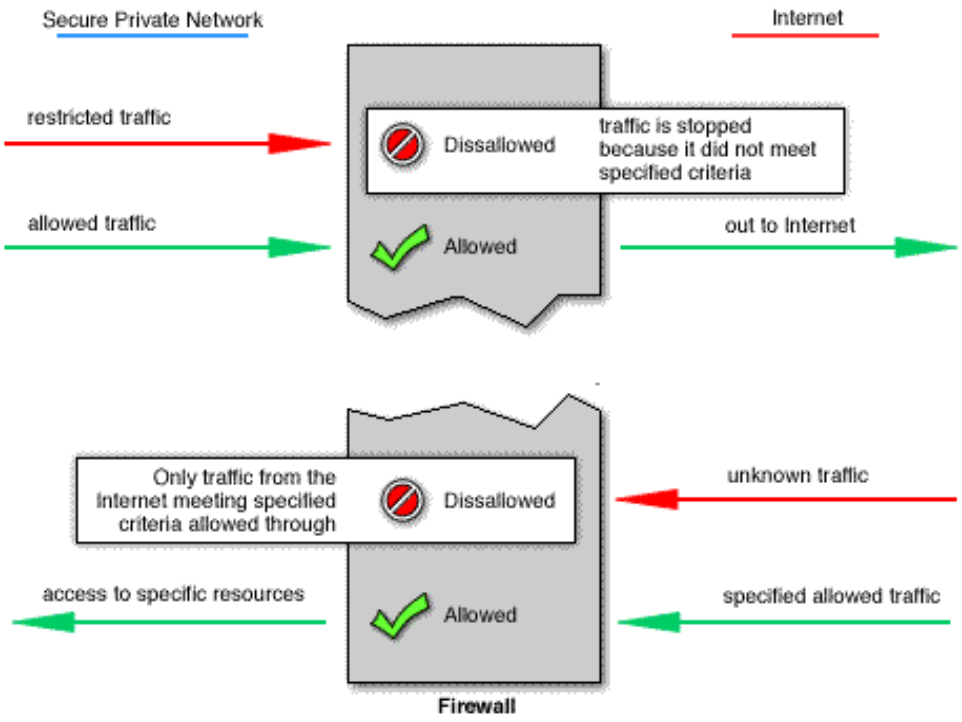
- Intercepts and controls traffic between networks with differing levels of trust, enforced with a network security policy
- Log inter-network activity, and limit the exposure of an organization.

Firewall Introduction



Nanyang Polytechnic

Firewall Introduction



Nanyang Polytechnic

Firewall Introduction

Challenges

- Detecting malware
- Connections that do not go through the firewall
- Unknown threats
- Poorly trained firewall administrator

Nanyang Polytechnic

Firewall Introduction

- Quiz 1

  Can firewalls block malware?

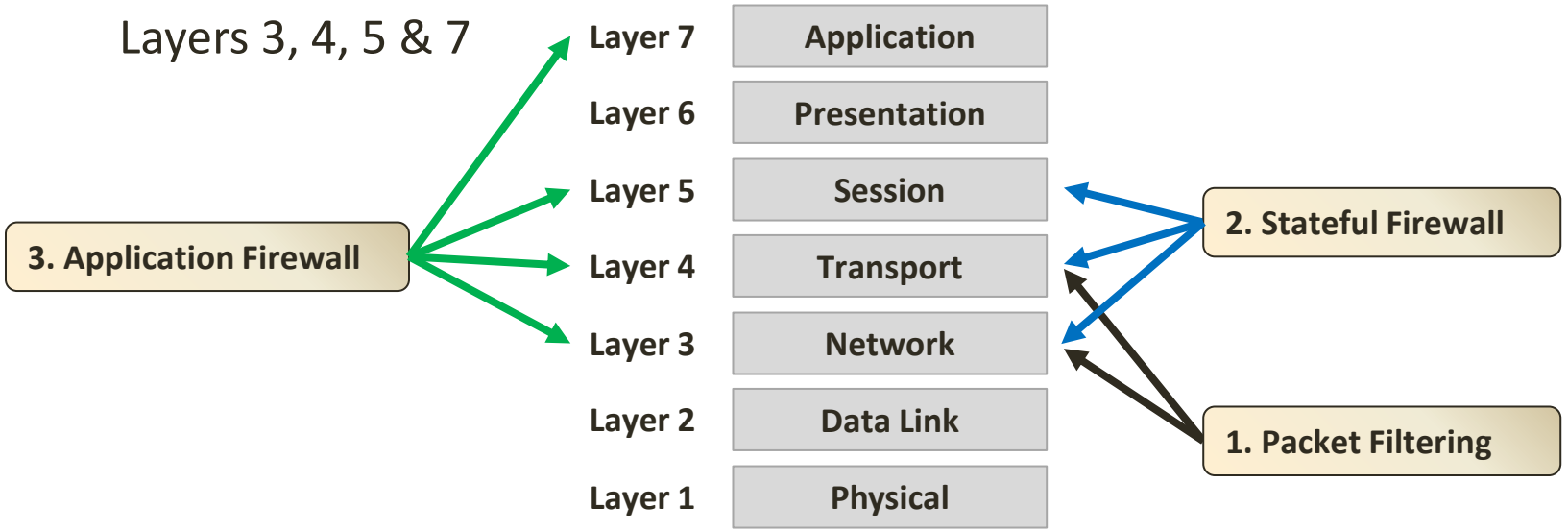
  A) YES

  B) NO

Types/Architecture of Firewall

Nanyang Polytechnic

1. **Packet filtering firewall**
   - Filters packet content, Layer 3 and sometimes Layer 4 information
2. **Stateful firewall**
   - Monitors the state of connections, whether the connection is in an initiation, data transfer, or termination state
3. **Application gateway firewall (proxy firewall)**
   - Filters information at Layers 3, 4, 5 & 7



Nanyang Polytechnic

Types/Architectures of Firewall

Packet Filtering

Vs

Stateful Packet Filtering (Stateful Inspection)

Types/Architectures of Firewall

Packet Filtering

- Firewall makes decision based on packet header
- Stateless

Vs

Stateful Packet Filtering (Stateful Inspection)

- Ensures packet belongs to a valid session
- Keep state information about transactions (Connection)

Types/Architectures of Firewall

Stateful Packet Filtering aka (Stateful Packet Inspection)

- Maintains an entry for each established connection
- Packet filter based on profile of the entries
- Keeps track of TCP sequence numbers to prevent attacks based on sequence numbers
- Inspect data for protocols (FTP, IM, SIP) commands
- Detects and drops packets that overload server
- Disallow packets that has no connection to server

Types/Architectures of Firewall

Stateful Packet Filtering aka (Stateful Inspection)

Drawbacks:

Cannot prevent, Trojan, spyware, adware where an connection has been established from within the network.

Solution?

Types/Architectures of Firewall

Stateful Packet Filtering aka (Stateful Inspection)

Drawbacks:

Cannot prevent, Trojan, spyware, adware where an connection has been established from within the network.

Solution?

Deep Packet Inspection (DPI)

- **Examines also the data part of packet (content)**

Nanyang Polytechnic

Types/Architectures of Firewall

Quiz 2

Can deep packet inspection firewall examine encrypted traffic?

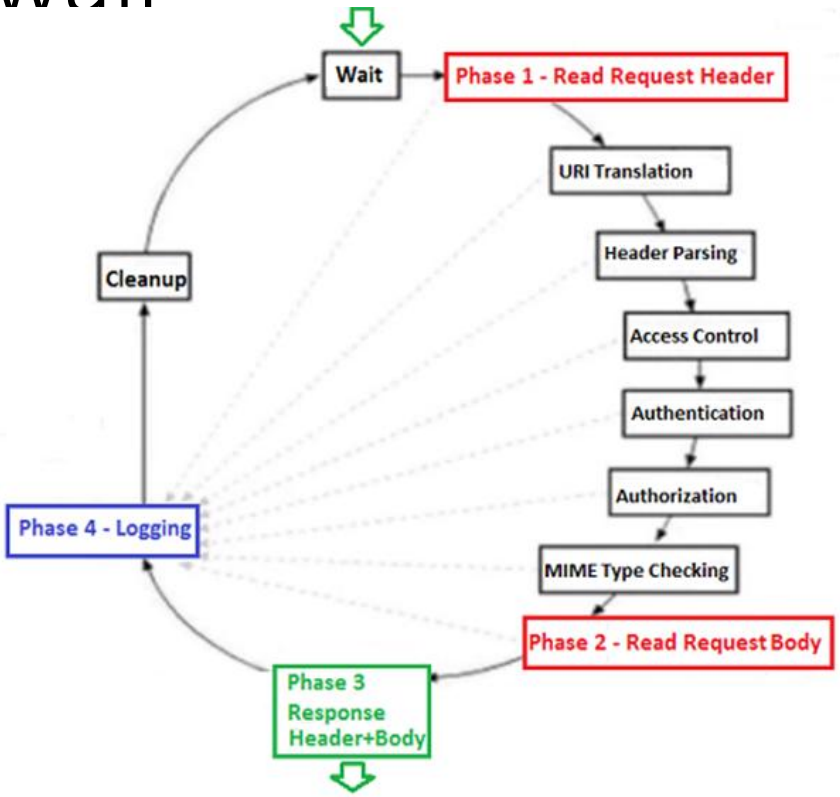
Types/Architectures of Firewall

Web Application Firewall (Example: ModSecurity)

- Act as an inbound proxy to Webserver: Apache, IIS
- Inspect request and response data (including HTTPS)
- Increase information log (Credit card numbers, ID numbers, Passwords, Raw Transaction data)
- OWASP core rule set (Free download)
- Alerts: SQL Injection,XSS,Cookie Tampering,Abnormal Activities, Buffer Overflow etc.
- Commercial rules available from TrustWave

Types/Architectures of Firewall

ModSecu
HTTP/HT
Inspectio
Lifecycle



Types/Architectures of Firewall

Unified Threat Management (UTM)

Consolidates multiple security and networking functions all on one appliance. Popular with SMEs (Small Medium Enterprise)

- Firewall
- IDS/IPS
- SIEM
- Secure Web/Email Gateway
- Remote Access

Types/Architectures of Firewall

Advantages

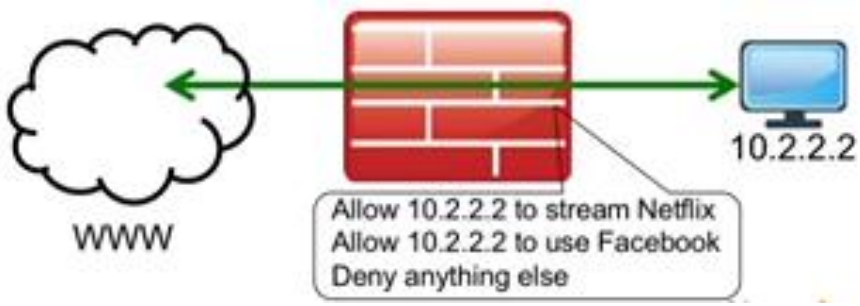
- Browser based management
- Short learning curve for security policy configuration
- Localized software and documentation
  - By 2022, more than 50% of new SMB firewall deployment will tunnel web traffic to a cloud-based secure web gateway, up from less than 10% today.
  - By 2022, 25% of SMBs will use multifunction firewall as an on-premises monitoring and access broker to inventory and control SaaS usage, manage mobile devices, or assess endpoint security posture, up from less than 2% today.
  - By 2022, 10% of new distributed branch offices' firewall deployment will switch to firewall as a service, up from less than 1% today.

Types/Architectures of Firewall

Types/Architectures of Firewall

Application Firewall (Often called NGFW)

All the benefits of packet filtering firewall plus additional capability to block applications like Facebook, Youtube, etc



Nanyang Polytechnic

Types/Architectures of Firewall

Quiz 2

Which of the following firewall does not act on the Application layer of the OSI model?

A) Web Application Firewall

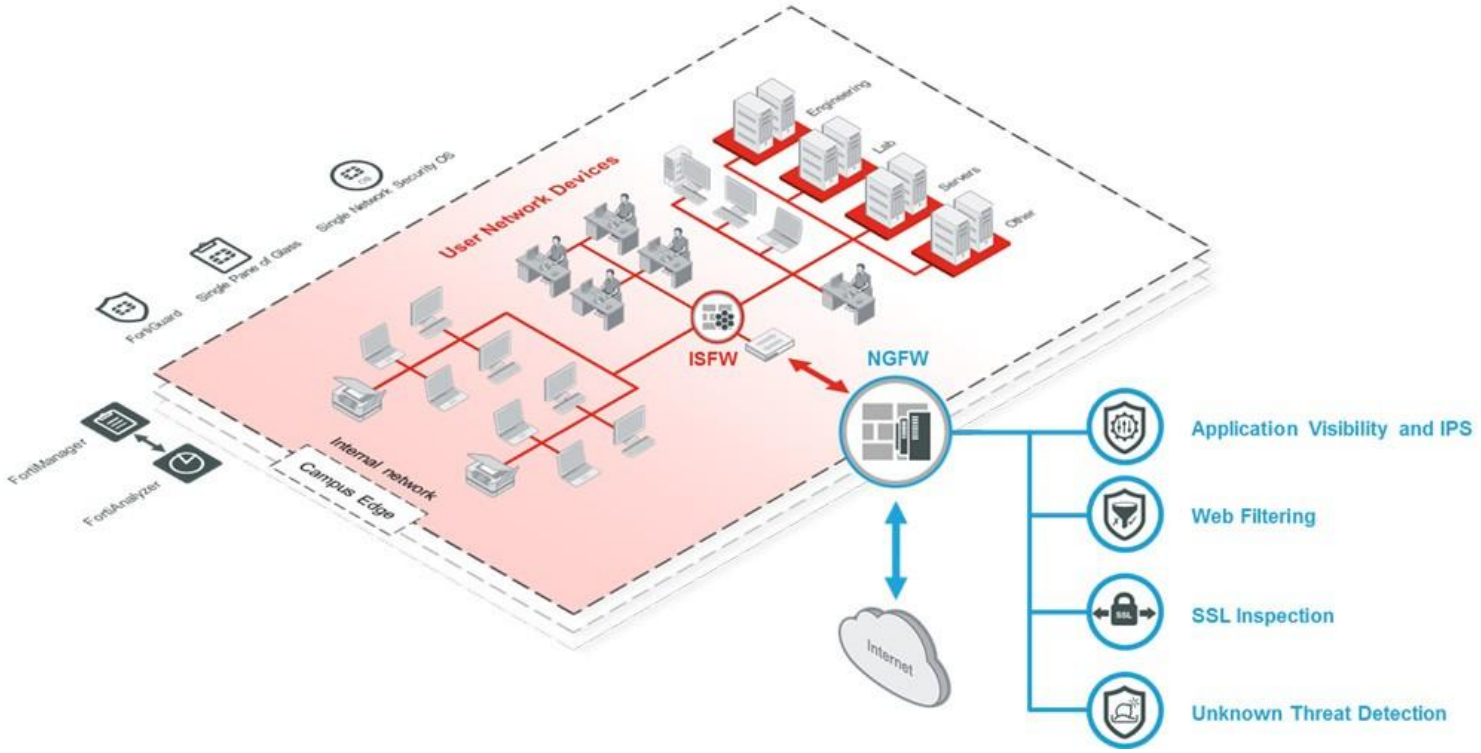
B) Application Firewall

C) Packet Filtering

D) Windows Firewall

Nanyang Polytechnic

Next generation firewall (NGFW)



Next generation firewall (NGFW)

Firewall need to evolve to deal with sophisticated threats

- Botnet delivery methods invisible to first-generation firewall.
- Increased use of service-orientated architectures via (HTTP/HTTPS) render port/protocol-based rules less relevant.
- Cannot identify/block misuse of application-specific features in first-generation firewall

Nanyang Polytechnic

Next generation firewall (NGFW)

- In traditional firewalls, ports were opened and closed to allow or disallow traffic without consideration beyond basic characteristics.

- NGFW provides deeper insight into the traffic attempting to access the network.

Next generation firewall (NGFW)

1. Application Awareness
   Does not assume a specific application is running on a specific port. Firewall can monitor traffic from layers 2 to 7 with greater granularity Eg: HTTP Port 80 assumed to be HTTP Traffic. Useful for bandwidth control (P2P)

2. Identity Awareness

   Track the identity of the local traffic device and user,

   Typically using existing enterprise authentication systems

   (i.e. Active Directory, LDAP). Control the what a specific

   User or groups is allowed to send and receive.

Next generation firewall (NGFW)

3. Extra firewall Intelligence
   Optimized rule set and intelligence gathered from outside sources continually (Whitelist, blacklist, directory integration to block by identity)

4. Integrated IPS

   Automatic correlation to IPS(To cover in PM) to suggest blocking of certain malicious websites. Eg: Block and address that is continually loading the IPS with bad traffic

Nanyang Polytechnic

Next generation firewall (NGFW)

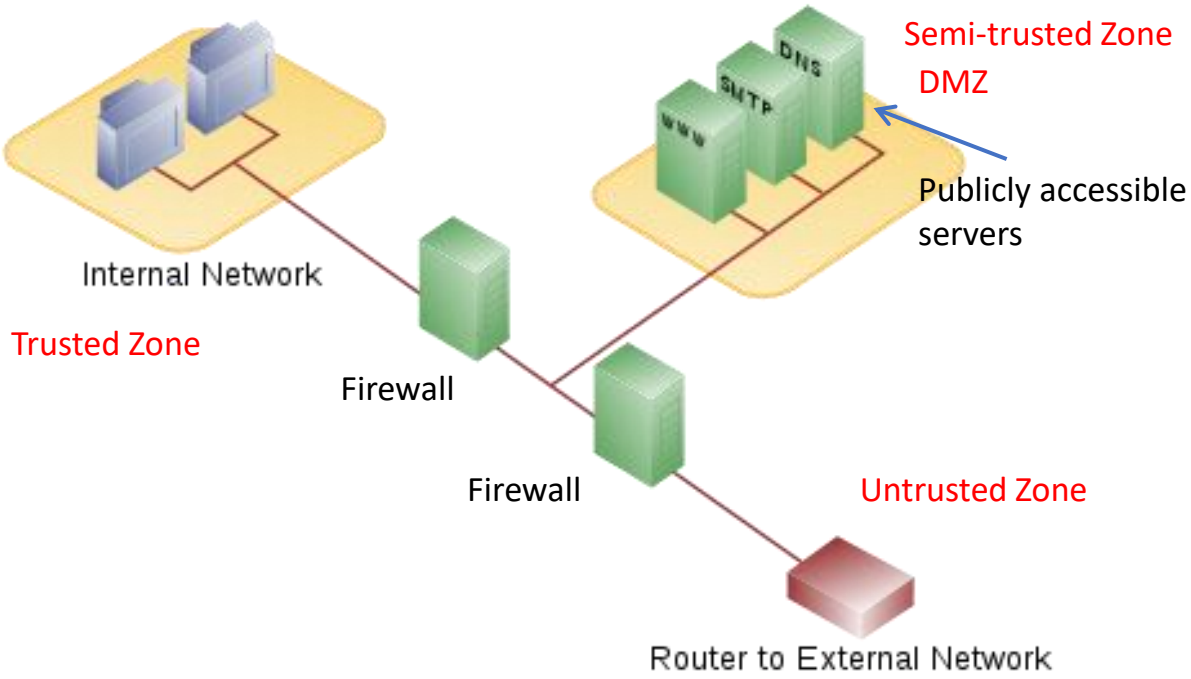
Traditional Firewall	NGFW
ISO/OSI L4 Port Protocol	Application-Centric (Content Flow) Protocol
Basic Security + Add-ons	Integrated Security Solutions
Complex Architecture	Integrated Architecture
Complex Control	Simplified Control
Simple – Moderate Security	Integrated Complex Security

Next generation firewall (NGFW)

- NGFW configuration

Application	Category	Risk	Login IDs	Sessions (Blocked/Allowed)	Files (up/Down)	Videos Played	Bytes (Sent/Received)
YouTube	Video/Audio		1	15		7	34.69 MB
Box	Storage/Backup		3	7	1 / 1		243.16 MB
Google.docs	Collaboration		1	1	0 / 1		466.04 KB
Vimeo	Video/Audio		1	1			9.78 KB
Facebook	Social Media		1	1			265.56 KB

Firewall Policy Design and Enforcement



Nanyang Polytechnic

Firewall Policy Design and Enforcement

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
1	Out	Internal	Any	TCP	>1023	23	Permit
2	In	Any	Internal	TCP	23	>1023	Permit
3	Any	Any	Any	Any	Any	Any	Deny

- Filtering rules are applied to the packet in order. The first matching condition is the rule applied the packet.
- For safety, filtering rules should have a deny all condition at the end of the rules.

Nanyang Polytechnic

Firewall Policy Design and Enforcement

Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	Action
1	Out	Internal	Any	TCP	>1023	23	Permit
2	In	Any	Internal	TCP	23	>1023	Permit
3	Any	Any	Any	Any	Any	Any	Deny

- Eg: Filtering telnet
- Rule 1 - allows outgoing Telnet (port 23)
- Rule 2 - allows response from Telnet server
- Rule 3 - is the default deny rule

Nanyang Polytechnic

Firewall Policy Design and Enforcement

Packet Filtering Rules (Two common strategies)

1) Build rules from most specific to most general. This is to ensure that a general rule does not “override” a more specific but conflicting rule.

2) Rules should be ordered such that the ones most often used are at top of list. Done for performance reasons.

Nanyang Polytechnic

Firewall Best Practices

Best Practices

1) Deny all traffic by default, and only enable those services that are needed.
2) Disable or uninstall any unnecessary services and software on the firewall that are not specifically required.
3) Limit the number of applications that run on the firewall in order to let the firewall do what it's best at doing.
4) Run the firewall service as a unique user ID instead of administrator or root.

Nanyang Polytechnic

Firewall Best Practices

5) Change the default firewall administrator or root password

6) Do not rely on packet filtering alone. Use stateful inspection and application proxies if possible.

7 Ensure that physical access to the firewall is controlled.

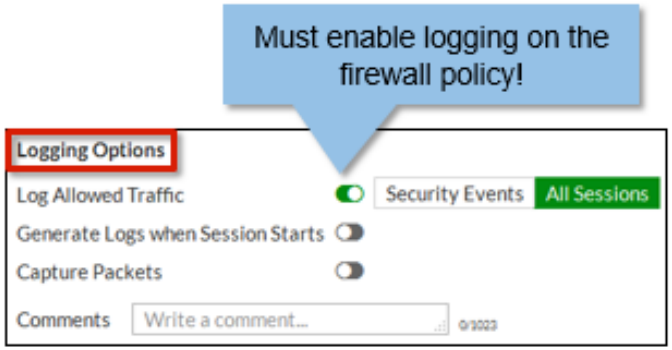
8) Regularly monitor firewall logs.

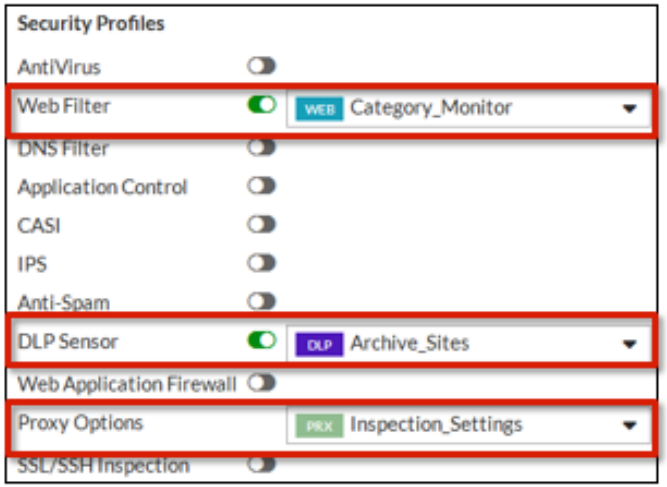
9) Document all firewall rule changes.

Firewall and Cyber Intelligence

- Enable logging on Firewall policy

- Firewall policy setting decides if a log message is generated or not
  - **Log Settings** only decides if and where log is stored





Nanyang Polytechnic

Summary

- Firewall and its purpose
- Types and various architectures of Firewall
- Next Generation Firewall (NGFW)
- Firewall ACL rules
- Best practices

Nanyang Polytechnic

THE END