FIT5037: Network Security
Security at Network Layer (firewalls and wireless security)

Faculty of Information Technology
Monash University

April 10, 2019

Copyright Notice

Lecture 6: Security at Network Layer (firewalls and wireless security)

Lecture Topics:

- Symmetric key cryptography
- Asymmetric key cryptography
- Pseudorandom Number Generators and hash functions
- Authentication Methods and AAA protocols
- Security at Network Layer (IPsec)
- **Security at Network Layer (firewalls and wireless security)**
- Security at Transport Layer
- Security at Application Layer
- Computer system security and malicious code
- Computer system vulnerabilities and penetration testing
- Intrusion detection
- Denial of Service Attacks and Countermeasures / Revision

Outline

- Firewall Concepts
- Firewall Types
- Wireless Network Security

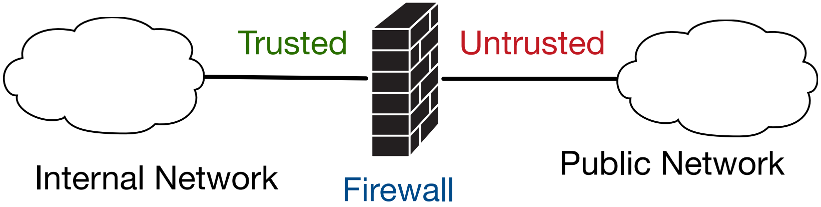
Firewalls: Introduction

- Information systems have evolved
  - from centralized data processing system to Inter-networked distributed data access and Internet connection
- This growth has introduced persistent security concerns, because
  - it is not practical to equip each workstation and server with intrusion protection
  - flawless OS and software cannot be guaranteed
  - networks usually consists of hundreds and thousands of systems running mixed version of software
- A firewall can add to the security scheme
  - creates an outer security wall
  - provides a single point where security and audit can be imposed
  - acts as the first line of defence

Firewall: Design Goals

Firewalls are based on the following design goals:

- all traffic in both directions must pass through the firewall
  - implemented by physically blocking all accesses to the local network except via the firewall
- only authorised traffic, defined by local security policies, will be allowed to pass
- firewall itself must be immune to penetration
  - underpins the use of trusted system with a secure operating system



Firewall: Services

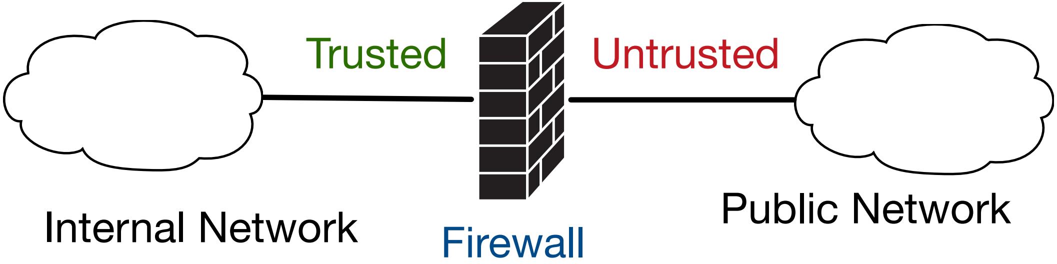
Techniques used by firewalls to control access and enforce site's security policy:

- Service control:
  - determines the types of Internet services that can be accessed, inbound and outbound
  - e.g., may filter traffic on the basis of IP address and TCP port number
- Direction control:
  - determines the direction in which particular service requests may be initiated and allowed to flow through the firewall
- User control:
  - controls access to a service by authorised users
  - applied to internal and external users
- Behaviour control:
  - controls how particular services are used
  - e.g., filters e-mail to eliminate spam, allows access to only a portion of information on web server

What Firewalls can do?

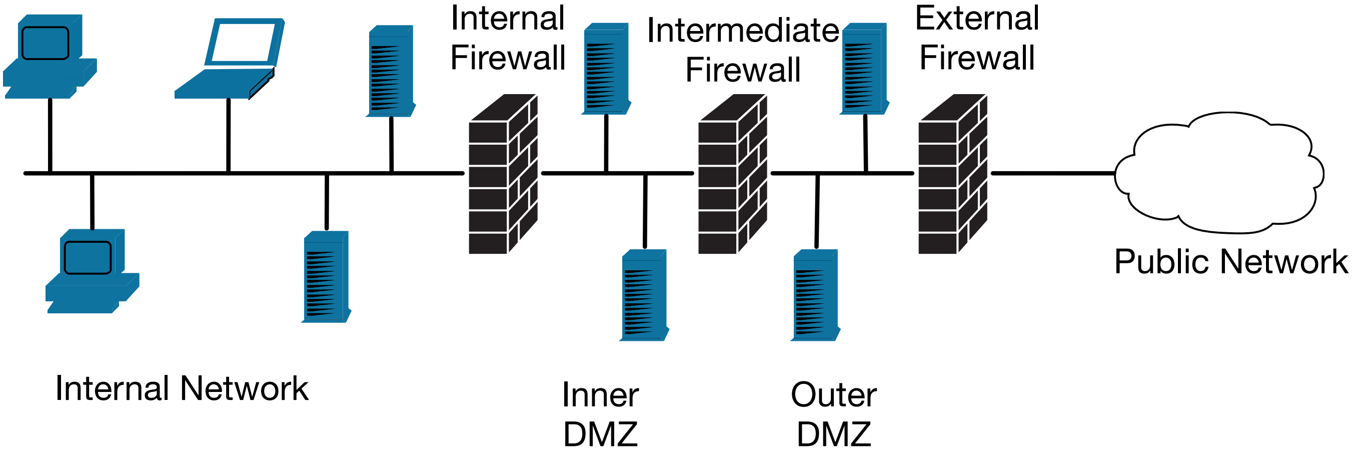
- Manage access between the organization's network (trusted) and Internet (untrusted)
  - without a firewall, security depends on the "hardness" of each host's security features
  - overall security is only as good as the weakest link
- Allow the network administrator to define a centralised "choke point"
  - offer access control, protection from vulnerable services and routing attacks
  - simplify security management
- Offer a convenient network point where security-related events can be monitored and alarms can be generated
- Network Address Translation (NAT) can be deployed at the firewall
- Firewall is a convenient point to audit or log Internet usage
- implement VPNs using IPsec
- There are arguments that the deployment of firewalls creates a single point of failure
  - failover: design products to operate in Active-Active or Active-Standby configurations

Simple Firewall Setup



Protects the internal (trusted) network from external (untrusted) network

Architecture with Multiple Layers of Firewall



Firewall Limitations

- cannot protect from attacks bypassing it
    - e.g. sneakernet, utility modems, trusted organisations, trusted services (e.g. SSL/SSH), VPN terminating behind firewall
- cannot protect against internal threats
    - e.g. disgruntled or colluding employees
- cannot protect against access via WLAN
    - if improperly secured against external use
- cannot protect against malware imported via laptops, tablets, storage devices infected outside

Firewall Types

- NIST SP 800-41r1: Guidelines on Firewalls and Firewall Policy, defines 10 firewall technologies
  - Packet Filtering
  - Stateful Inspection
  - Application Firewalls
  - Application-Proxy Gateways
  - Dedicated Proxy Servers
  - Virtual Private Networking
  - Network Access Control
  - Unified Threat Management (UTM)
  - Web Application Firewalls
  - Firewalls for Virtual Infrastructures
- Not listed in NIST
  - Circuit-level Proxy/Gateway

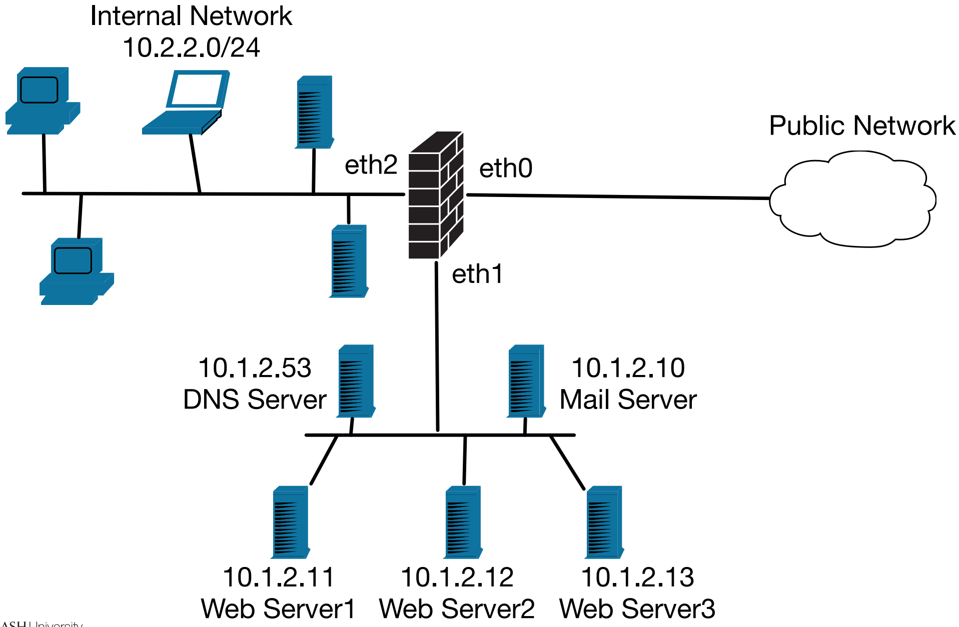
Packet Filtering

- Apply a *set of rules* to each incoming IP packet and then either forwards or discards the packet
- Use Transport and Network layer information based on matches to fields in the IP or TCP header on individual packets
  - source IP address
  - destination IP address
  - source and destination TCP or UDP port number
  - type of the protocol (IP, TCP, UDP or ICMP)
  - interface and direction *ingress* or *egress*
- Allow end-to-end connections (traffic passes through firewall)

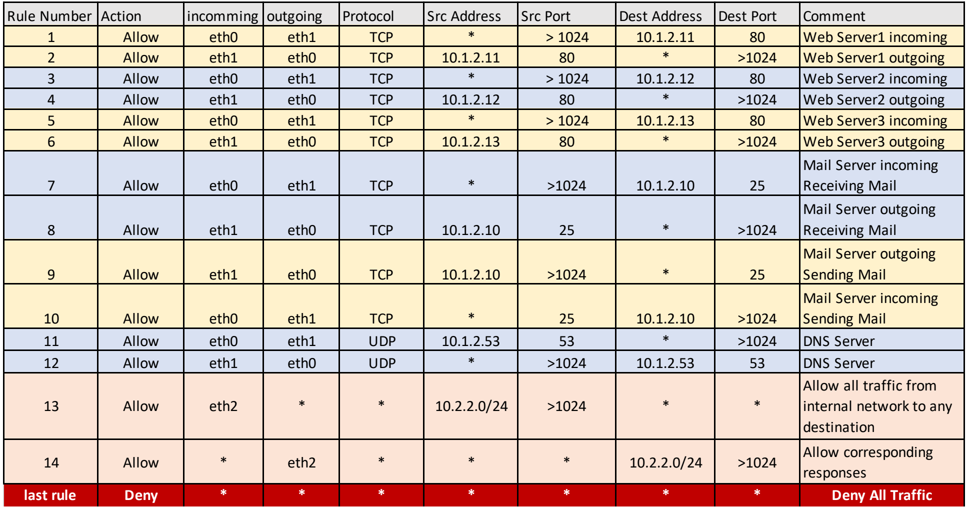
Packet Filtering: Firewalls Policy

- Default policy (discard or forward)
  - Discard: Discard all traffic unless explicitly permitted (more secure approach)
  - Forward: Allow all traffic unless explicitly prohibited (hence reduced security)
- Only allow necessary IP protocols
  - some protocols can be blocked on both (internal and external) sides of firewall
    - e.g. IGMP (control multicast networks)
  - Allow only packets going to specific protocol and ports while rest of the packets are dropped
    - e.g., Web (TCP, port 80), DNS (UDP, port 53), and SMTP (TCP, port 25) be allowed
- Only permit appropriate source and destination addresses
  - block invalid addresses e.g. 127.0.0.0-127.255.255.255
  - block incoming traffic from external with internal source addresses
    - provides anti-spoofing protection
- Write matching rules for ingress and egress traffic
- IPv6 policies
  - capable of filtering IPv6 packets
  - capable of inspection and filtering of tunnelled 6-to-4 and 4-to-6 traffic
- ICMP
  - can be used for reconnaissance or manipulation of network traffic flow
  - block all ICMP incoming and outgoing except the flows necessary for diagnostics

Packet Filtering: Example Network Diagram



Packet Filtering: Example Firewall Rules



Rule Number	Action	incomming	outgoing	Protocol	Src Address	Src Port	Dest Address	Dest Port	Comment
1	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.11	80	Web Server1 incoming
2	Allow	eth1	eth0	TCP	10.1.2.11	80	*	>1024	Web Server1 outgoing
3	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.12	80	Web Server2 incoming
4	Allow	eth1	eth0	TCP	10.1.2.12	80	*	>1024	Web Server2 outgoing
5	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.13	80	Web Server3 incoming
6	Allow	eth1	eth0	TCP	10.1.2.13	80	*	>1024	Web Server3 outgoing
7	Allow	eth0	eth1	TCP	*	>1024	10.1.2.10	25	Mail Server incoming Receiving Mail
8	Allow	eth1	eth0	TCP	10.1.2.10	25	*	>1024	Mail Server outgoing Receiving Mail
9	Allow	eth1	eth0	TCP	10.1.2.10	>1024	*	25	Mail Server outgoing Sending Mail
10	Allow	eth0	eth1	TCP	*	25	10.1.2.10	>1024	Mail Server incoming Sending Mail
11	Allow	eth0	eth1	UDP	10.1.2.53	53	*	>1024	DNS Server
12	Allow	eth1	eth0	UDP	*	>1024	10.1.2.53	53	DNS Server
13	Allow	eth2	*	*	10.2.2.0/24	>1024	*	*	Allow all traffic from internal network to any destination
14	Allow	*	eth2	*	*	*	10.2.2.0/24	>1024	Allow corresponding responses
last rule	**Deny**	*	*	*	*	*	*	*	**Deny All Traffic**

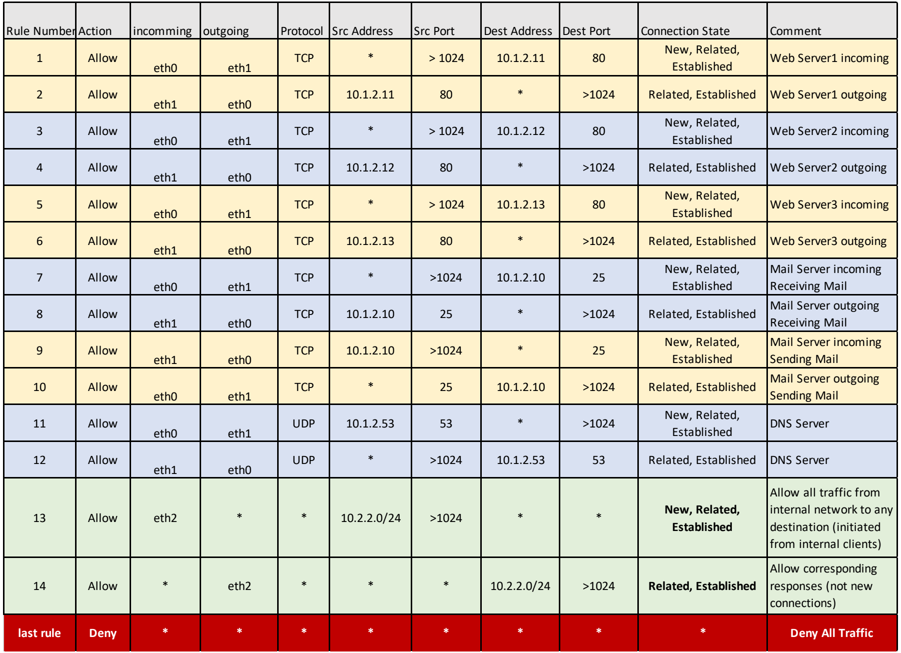
- rules 13 and 14 are quite permissive (allow connections to be initiated from outside to internal clients)

Stateful Packet Inspection

- Use Transport and Network layer information based on matches to fields in the IP or TCP header and tracks the *state* of the communication
  - TCP message flags (SYN, ACK, FIN, RST)
  - communication initiated from which interface (trusted or untrusted)
  - following sequence numbers and check if they match
  - source IP address
  - destination IP address
  - source and destination TCP or UDP port number
  - type of the protocol (IP, TCP, UDP or ICMP)
  - interface and direction *ingress* or *egress*
- Firewalls Policy: in addition to packet filtering policy
  - prevent connection initiation from external network to internal clients (not providing services to public)
  - prevent servers in DMZ to initiate connection to internal or external (only responding to requests) why?

Stateful Packet Inspection: Example Rules

where should the rules to drop packets with invalid source addresses be?

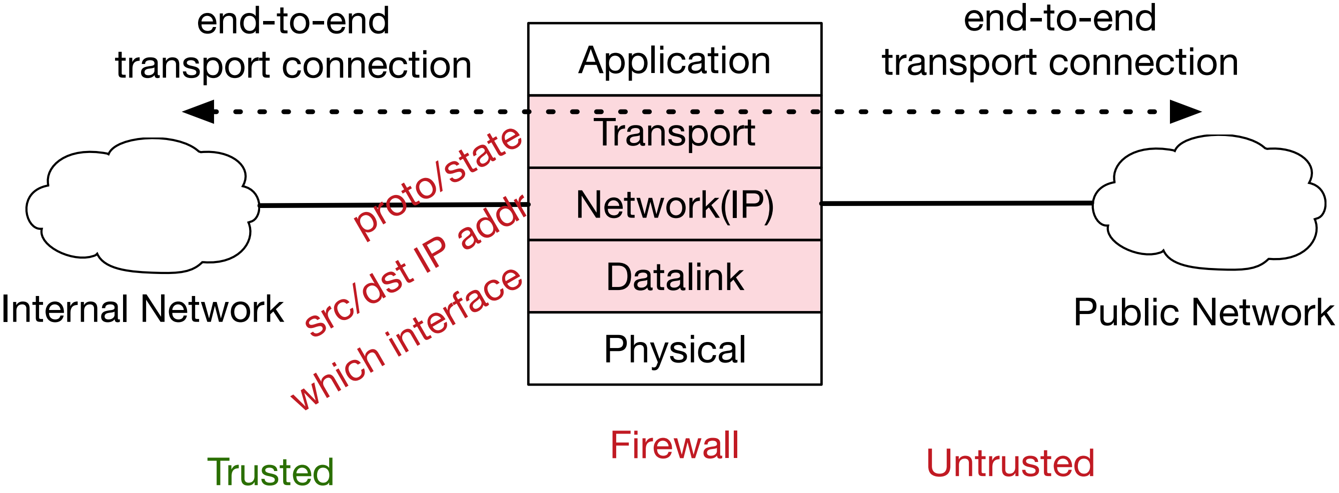


Rule Number	Action	incomming	outgoing	Protocol	Src Address	Src Port	Dest Address	Dest Port	Connection State	Comment
1	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.11	80	New, Related, Established	Web Server1 incoming
2	Allow	eth1	eth0	TCP	10.1.2.11	80	*	>1024	Related, Established	Web Server1 outgoing
3	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.12	80	New, Related, Established	Web Server2 incoming
4	Allow	eth1	eth0	TCP	10.1.2.12	80	*	>1024	Related, Established	Web Server2 outgoing
5	Allow	eth0	eth1	TCP	*	> 1024	10.1.2.13	80	New, Related, Established	Web Server3 incoming
6	Allow	eth1	eth0	TCP	10.1.2.13	80	*	>1024	Related, Established	Web Server3 outgoing
7	Allow	eth0	eth1	TCP	*	>1024	10.1.2.10	25	New, Related, Established	Mail Server incoming Receiving Mail
8	Allow	eth1	eth0	TCP	10.1.2.10	25	*	>1024	Related, Established	Mail Server outgoing Receiving Mail
9	Allow	eth1	eth0	TCP	10.1.2.10	>1024	*	25	New, Related, Established	Mail Server incoming Sending Mail
10	Allow	eth0	eth1	TCP	*	25	10.1.2.10	>1024	Related, Established	Mail Server outgoing Sending Mail
11	Allow	eth0	eth1	UDP	10.1.2.53	53	*	>1024	New, Related, Established	DNS Server
12	Allow	eth1	eth0	UDP	*	>1024	10.1.2.53	53	Related, Established	DNS Server
13	Allow	eth2	*	*	10.2.2.0/24	>1024	*	*	**New, Related, Established**	Allow all traffic from internal network to any destination (initiated from internal clients)
14	Allow	*	eth2	*	*	*	10.2.2.0/24	>1024	**Related, Established**	Allow corresponding responses (not new connections)
last rule	**Deny**	*	*	*	*	*	*	*	*	**Deny All Traffic**

MONASH University

Packet Filtering and Stateful Packet Inspection

- utilises information from the transport, network, and data link layers to make decisions on allowable traffic flows.



Packet Filtering and Stateful Packet Inspection

- In practice: unlikely to find packet filtering firewalls without stateful inspection capability
- **Advantages:**
  - Typically faster than other types of firewalls
    - because packet filtering is done at the lower levels of the OSI model, takes less time to process a packet
  - Can be implemented transparently, typically require no additional configuration for clients
  - Quite inexpensive to build routers with packet-filtering abilities
    - routers are already in the network providing routing functionality, with packet-filtering capabilities
    - thus avoids additional cost of deploying a packet-filter firewall
  - Packet filtering firewalls typically scale better than other types of firewalls
  - Packet filtering firewalls are application independent
- **Disadvantages:**
  - cannot prevent attacks that exploit application-specific vulnerabilities
  - lack advanced user authentication
  - defining rules and filters on a packet filtering firewall can be a complex task
  - accuracy of rules or filters on packet filtering firewalls can be very difficult to test
  - packet filtering firewalls are prone to certain types of attacks, e.g. DoS attack
  - packet filtering firewalls do not work well in an environment that needs dynamic rules

Attacks on Packet Filter Firewall

- IP address spoofing
  - fakes source address so that it appears to be coming from a trusted source
  - countermeasure: discard packets with an inside source address if the packets arrive on an external interface
- Source routing attacks
  - attacker specifies a route other than default
  - countermeasure: block source routed packets
- IP fragment attacks
  - intruder uses the IP fragmentation option
  - overlapping offset
    - reassembled packet overwrites the IP header and changes the values e.g. destination address
  - split header over several small packets
    - cannot enforce the policy since all information is not in a single packet
  - countermeasure: either discard or check before reassemble

Application Firewall

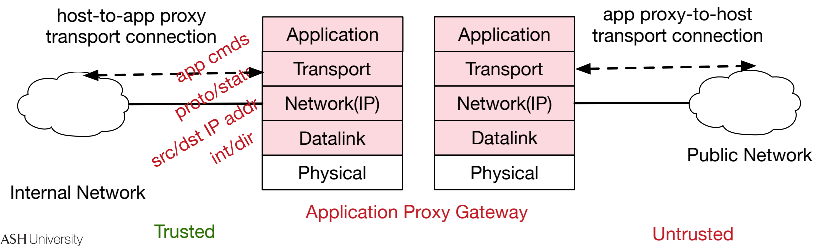
- Provides a *stateful protocol analysis* in addition to stateful inspection
  - also referred to as *deep inspection*
- Analyses the protocol at application layer
  - adds basic intrusion detection techniques
    - however are not as capable as intrusion detection and prevention systems
  - tries to detect deviation from benign protocol activities
- For instance detect:
  - the type of attachment of an email message (rules to deny certain types)
  - usage of Instant Messaging over port 80
  - specific actions of a protocol, e.g. FTP “put” command
  - web pages active content such as Java or ActiveX
  - unexpected sequence of commands

Application-Proxy Gateway

- combine lower-layer access control with upper-layer functionality
- contain a *proxy* agent that acts as intermediary between two hosts (internal and external)
  - never allows direct connection between the two hosts
  - a successful connection results in two separate connections
    - internal host to proxy
    - proxy to external host
  - meant to be transparent to the two hosts
  - differs from application firewalls in operating as a proxy
- can hide internal IP addresses
- can have capability to authenticate each individual network user
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- operates at application layer
- may have the capability to decrypt the traffic e.g. TLS-protected traffic
  - another difference with application firewalls

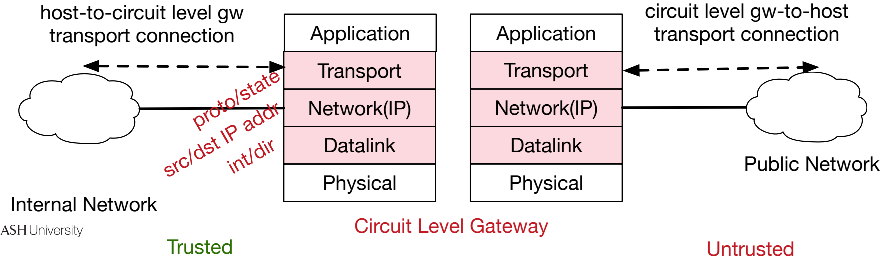
Application-Proxy Gateway: Advantages and Disadvantages

- **Advantages**
  - more secure compared to packet filtering and stateful inspection
  - allows more control
  - can authenticate users
- **Disadvantages**
  - slower than packet filtering and stateful inspection firewalls
    - require more time to inspect application layer content
  - limited support for new network applications and protocols
    - packet filter and stateful inspection only need the transport protocol and port number
  - application-specific proxy gateway is needed for each application
  - may have higher implementation costs



Circuit Level Gateway/Proxy

- Not listed in NIST document
- A packet filter/stateful inspection firewall that provides proxy service
  - Sets up two TCP connections
    - one between itself and the internal host and another between itself and the outside host
- The gateway typically relays TCP segments from one connection to the other without examining the contents of higher layer
- The security function consists of determining which connections will be allowed
- An example of circuit level gateway implementation is the SOCKS package specified in RFC1928.
- relaying UDP packets is more problematic, because of the lack of connection context
  - relaying UDP require a parallel TCP connection to provide these details.



Other Types

- Dedicated Proxy Servers
  - provide proxy service but have much more limited firewall capabilities
  - used in application-specific proxy scenarios e.g. HTTP or email
- Virtual Private Networking
  - used to terminate VPN connections
  - require additional resources to perform cryptographic operations
- Network Access Control
  - allow remote access by verifying whether the client complies with organisational policy
    - e.g. latest updates and proper configuration of anti-virus software
- Unified Threat Management (UTM)
  - combination of multiple features in a single system
    - firewall, malware detection, network intrusion detection etc.
- Web Application firewalls
  - HTTP protocol has been exploited in many ways
  - specialised application firewall for web service
- Firewalls for Virtual Infrastructures
  - In cloud-based services the infrastructure such as routers and switches may be virtual nodes
  - provide firewall services as a virtual node (built-in or third party)

Host-Based Firewalls

- software module used to secure individual host
  - available in many Operating Systems
  - or can be installed as an add-on package
- often used on servers
- advantages:
  - can tailor filtering rules to host environment
  - protection is provided independent of topology
  - enforce the concept of *defence in depth*
    - provides an additional layer of protection

Personal Firewalls

- controls traffic between
  - PC and Internet or PC and enterprise network
- a software module on personal computer
- or in home/office DSL/cable/ISP router
- typically much less complex than other firewall types
- primary role is to deny unauthorised remote access to the computer
- and monitor outgoing activity for malware

Firewall Planning and Implementation

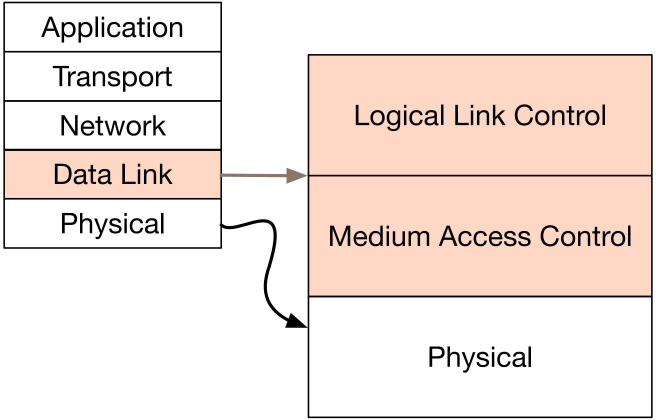
1. **Plan**: identifying all requirements and determine which firewall to implement to enforce organisation's security policy
   - use devices as intended and document firewall's capabilities
   - consider internal threats
2. **Configure**: installing hardware and software and setup rules
   - content filtering should be performed as close to content provider as possible
   - logging and alert configuration: modifications to firewall rules, system reboots, disk shortage etc.
3. **Test**: implement and test a prototype in a lab environment and evaluate the functionality, performance, scalability and security
   - identify any issues and interoperability with other components
4. **Deploy**: after testing is completed and issues resolved deploy the firewall
5. **Manage**: maintain and support the firewall

Wireless Network Security

- Wireless communication is inherently exposed due to the use of unguided medium
- IEEE 802.11 committee formed in 1990's
  - charter to develop a protocol and transmission specifications for wireless LANs (WLANs)
  - has developed many standards: 802.11a/b/g/n/ac (up to 3.4Gb/s)/ax (up to 10.5 Gb/s)
- Wi-Fi Alliance
  - Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999
  - to assist interoperability of products
  - renamed Wi-Fi (Wireless Fidelity) Alliance
  - created a test suite to certify interoperability
  - initially for 802.11b, later extended to 802.11g
  - concerned with a range of WLANs markets, including enterprise, home, and hot spots

IEEE 802.11 Protocol Stack

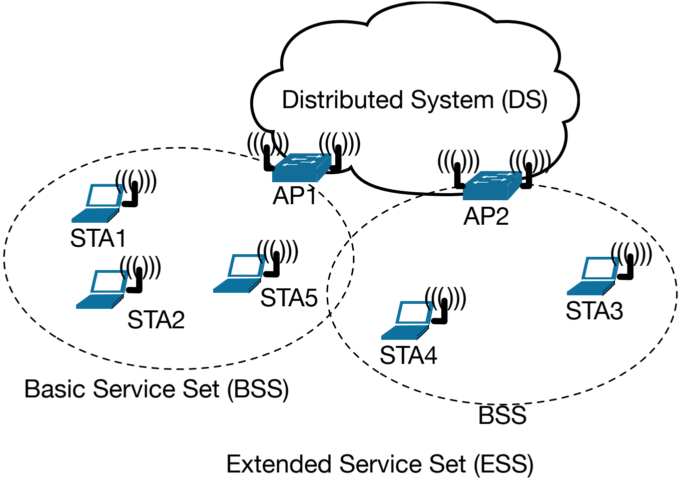
- 802.11 is a datalink layer (layer 2) protocol



	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow Control Error Control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocol
Physical	Encoding/decoding of signals Bit transmission/reception Transmission medium	Frequency band definition Wireless signal encoding

Network Components and Architecture

- Basic Service Set (BSS)
  - Smallest WLAN block
- Distribution System (DS)
  - Connects BSS blocks
- Access Points (AP)
  - Functions as a bridge or relay point
- Extended Service Set (ESS)
  - Two or more BSS interconnected by a DS



802.11 Wireless LAN Security

- Wireless traffic can be monitored by any radio wave receiver in range (unguided medium)
- Original 802.11 specifications had security features
  - Wired Equivalent Privacy (WEP) algorithm
  - but found this contained major weaknesses
- 802.11i task group developed capabilities to address WLAN security issues
  - Wi-Fi Alliance Wi-Fi Protected Access (WPA)
  - final 802.11i Robust Security Network (RSN)

WEP Problems

- WEP Security:
  - $c = (m||CRC(m)) \oplus RC4(IV||k)$
  - send $IV||c$
  - IV: 24 bits
- Manual key distribution: Difficult to change keys
- Single set of Keys shared by all: Frequent changes necessary
- No mutual authentication
- **IV Collisions**: IV value is too short and is not protected from reuse
  - only requires $\approx \sqrt{2^{24}} = 2^{12} = 4096$ frames, each at most 1156 bytes, about 4MB to get a collision
  - IV is sent in clear so attacker can observe which message had the same IV
- **Malleability**: Weak integrity check (CRC)
  - $\exists L()$ such that $CRC(m \oplus \Delta) = CRC(m) \oplus L(\Delta)$
- **RC4 Related Keys**:
  - Instead of random keys, related keys were used: $1||k$, $2||k$, ...
  - shown after 1 million frames long term secret key can be recovered[1]
- Directly uses master key
- No protection against replay

[1] A key recover attack on WEP

802.11i RSN Services and Protocols

- Authentication
  - define an exchange between a user and an Authentication Server (AS)
  - provides mutual authentication
    - pre-shared key (Authenticator)
    - EAP (a backend AS)
- Key Management
  - generates temporary keys to be used to protect the wireless communication between the client and the AP
- Access Control using 802.1X access control mechanism[2]
  - enforces the use of the authentication function
    - provides a framework to encode, decode, address, and validate EAP Over LANs (EAPOL) PDUs
  - only allows authentication frames to be carried until authentication procedure completes successfully
- Privacy with message integrity
  - encryption at Medium Access Control (MAC sub-layer) level
  - message integrity code

[2] IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control," in IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004) , vol., no., pp.1-205, 5 Feb. 2010 doi: 10.1109/IEEESTD.2010.5409813

802.11i Authentication and Key Management (AKM)[3]

- STA discovers AP's security policy through
  - passive monitoring Beacon frames
  - active probing
- if 802.1X authentication is used the EAP authentication will start

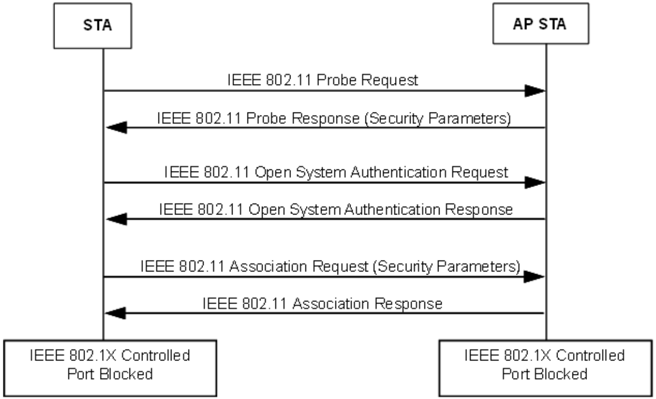
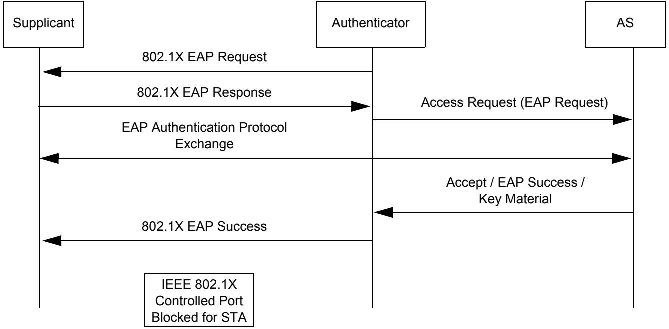

STA
AP STA
IEEE 802.11 Probe Request
IEEE 802.11 Probe Response (Security Parameters)
IEEE 802.11 Open System Authentication Request
IEEE 802.11 Open System Authentication Response
IEEE 802.11 Association Request (Security Parameters)
IEEE 802.11 Association Response
IEEE 802.1X Controlled Port Blocked
IEEE 802.1X Controlled Port Blocked

Figure 11a—Establishing the IEEE 802.11 association

[3] IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, doi:10.1109/IEEESTD.2004.94585

802.11i Authentication and Key Management (AKM)

- Entities:
  - *Authenticator*: an entity that facilitates authentication
  - *Supplicant*: an entity on one end of a point-to-point LAN segment that seeks to be authenticated
- The EAP authentication starts with either
  - `EAP-Request` from Authenticator
  - `EAPOL-Start` from STA's Supplicant
- The EAP messages can be protected depending on the authentication method
- EAP Key Management Framework is defined in RFC 5247
  - derive keys to protect EAP messages
  - derive Master Session Key (MSK)
- The EAP messages are transferred using 802.1X PDUs (encapsulated)



Supplicant
Authenticator
AS
802.1X EAP Request
802.1X EAP Response
Access Request (EAP Request)
EAP Authentication Protocol Exchange
Accept / EAP Success / Key Material
802.1X EAP Success
IEEE 802.1X Controlled Port Blocked for STA

Figure 11b—IEEE 802.1X EAP authentication

802.11i Authentication and Key Management (AKM)

- After successful EAP authentication STA and AP will have a Master Session Key (MSK)
  - also referred to as AAA Key
  - 802.1X unblocks the port (allows other frames to be transmitted)
- Authenticator initiates a 4-way handshake to:
  - confirm a live peer holds the PMK
    - Pairwise Master Key (from MSK)
  - confirm the PMK is current
  - derive a fresh Pairwise Transient Key (PTK)
  - transport the GTK
  - confirm the cipher suite selection
- The `EAPOL-Key` message structures are defined in 802.1X protocol

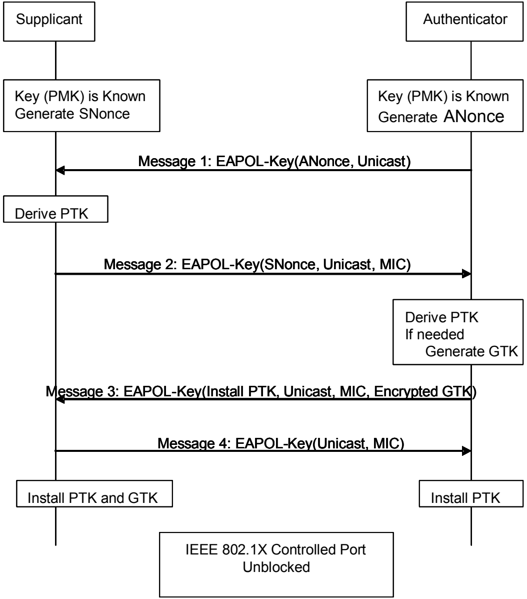

Supplicant
Authenticator
Key (PMK) is Known
Generate SNonce
Key (PMK) is Known
Generate ANonce
Message 1: EAPOL-Key(ANonce, Unicast)
Derive PTK
Message 2: EAPOL-Key(SNonce, Unicast, MIC)
Derive PTK
If needed
Generate GTK
Message 3: EAPOL-Key(Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key(Unicast, MIC)
Install PTK and GTK
Install PTK
IEEE 802.1X Controlled Port
Unblocked

Figure 11c—Establishing pairwise and group keys

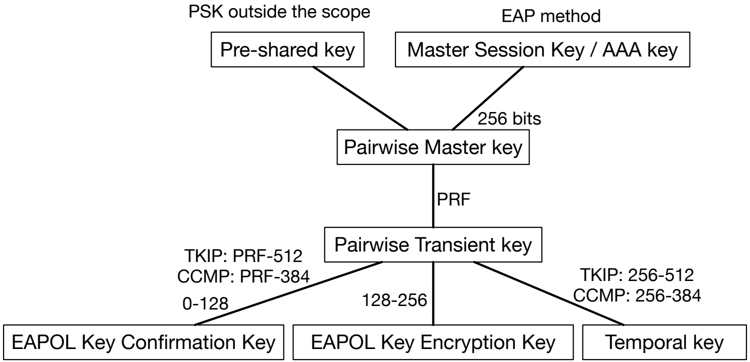
802.11i Security Services

- Support cipher suites: WEP, TKIP, and CCMP
  - Confidentiality
  - Authentication
  - Access control
- WEP
  - RC4 with 40-bit and 104-bit keys
  - only support group keys (all users share the same GTK)
- TKIP
  - RC4, different Key and IV generation than WEP
  - software support for pre-RSNA hardware
  - use Michael Message Integrity Code (MIC)
- CCMP
  - CCM with AES-128
    - Counter mode for encryption
    - CBC-MAC for message authentication
    - a unique 48-bit nonce is needed under the same temporal key
    - Frame header is included in Authenticated Associated Data (AAD)
- HMAC-SHA-1 is used as PRF to derive keys

802.11i Key Management: Pairwise Keys

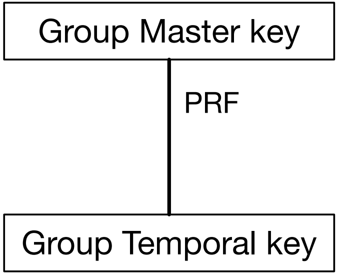
- start with a master key and derive other keys using PRF
  - Pre-shared key (PSK): a secret key shared by AP and STA installed in some fashion outside the scope of IEEE 802.11i
  - derived from AAAK or Master Session Key (MSK) generated using authentication phase of EAP enforced by IEEE 802.1X protocol
  - derived by truncation if necessary

- used for communication between an STA and an AP
- KCK used by 802.1X to provide data origin authenticity
- KEK used by EAPOL to provide confidentiality in 4-way Handshake and Group key Handshake messages



802.11i Key Management: Group Keys

- WEP: for communication with all STAs
  - has no pairwise key
- TKIP and CCMP: for multicast/broadcast communication



WEP: 40 or 104 bits
TKIP: 256 bits
CCMP: 128 bits

References

Materials in this document, at times without modification, are reproduced from the following references:

- NIST SP 800-41r1: Guidelines on Firewalls and Firewall Policy
- IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements, doi:10.1109/IEEESTD.2004.94585
- IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control," in IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004) , vol., no., pp.1-205, 5 Feb. 2010 doi: 10.1109/IEEESTD.2010.5409813
- A key recover attack on WEP
- RFC 5247: EAP Key Management Framework