



**QUEEN'S  
UNIVERSITY  
BELFAST**



# AAA/Firewalls – Part 2



**Dr. Sandra Scott-Hayward**

CSC3064 Lecture 12

School of Electronics, Electrical Engineering and Computer Science

# Session Overview

## □ Firewalls

### References:

Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.

Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.

Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007



# Introduction to Network Firewalls

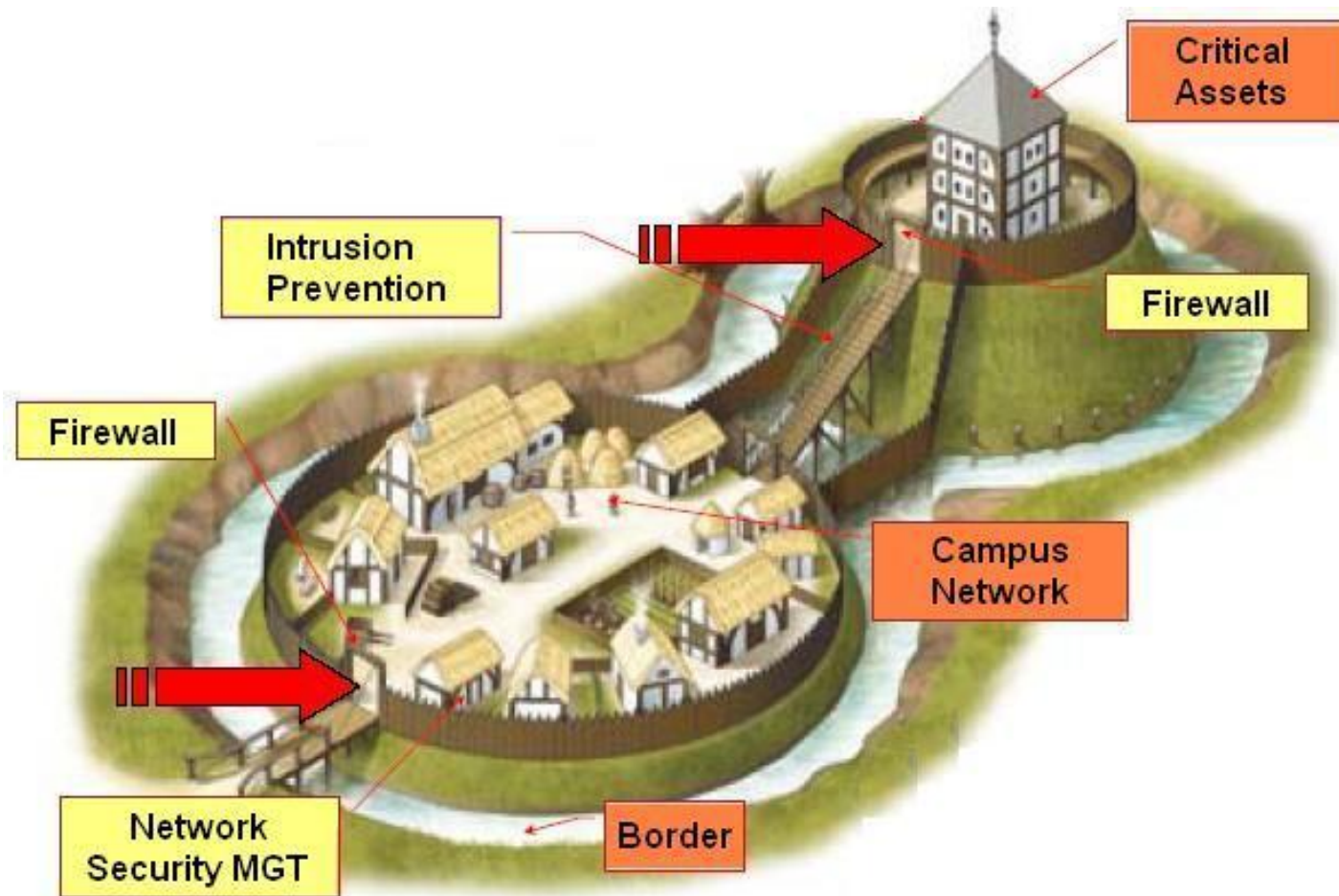
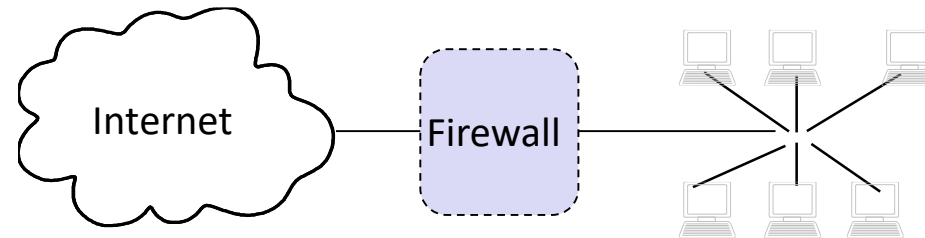


Image source: <https://nigesecurityguy.wordpress.com/2013/06/28/architecture-case-study-part-1/>

# Introduction to Network Firewalls

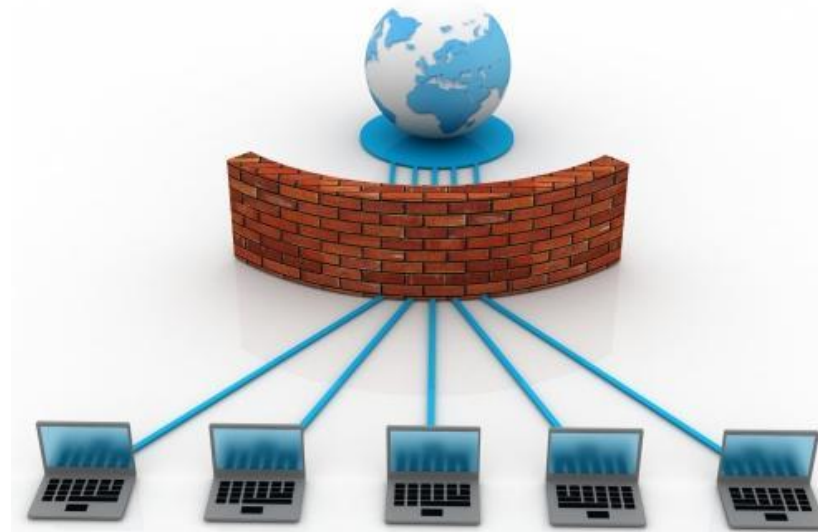
- A network firewall can be compared to a moat of a medieval castle:
  - It restricts people to entering at one carefully controlled point
  - It prevents attackers from getting close to other defenses
  - It restricts people to leaving at one carefully controlled point
- Usually, a network firewall is installed at a point where the protected subnetwork is connected to a less trusted network:
  - Example: Connection of a corporate local area network to the Internet



- Basically, firewalls realize access control on the subnetwork level

# What can firewalls do?

- A firewall is a focus for security decisions
- A firewall can enforce a security policy, i.e. access control
- A firewall can log Internet activity efficiently
- A firewall can limit exposure to security problems to one part of a network



# What can firewalls not do?

- A firewall cannot protect against malicious insiders
- A firewall cannot protect against connections that do not go through it
  - If, for example, there is an access point behind a firewall that provides unauthenticated access to the subnetwork, the firewall can not provide any protection against malicious WLAN users
- A firewall cannot protect against completely new threats
- A firewall cannot fully protect against viruses
- A firewall cannot set itself up correctly (→ cost of operation)

# Fundamental Approaches to Firewall Policies

## Default deny strategy:

- *“Everything that is not explicitly permitted is denied”*
- Examine the services the users of the protected network need
- Consider the security implications of these services and how the services can be safely provided
- Allow only those services that can be safely provided and for which there is a legitimate need
- Deny any other service

## Default permit strategy:

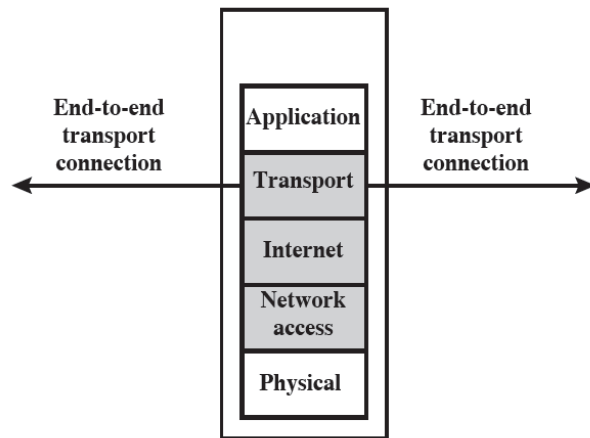
- *“Everything that is not explicitly forbidden is allowed”*
- Permit every service that is not considered dangerous
- Example:
  - *Server Message Block (SMB)* and X-Windows is not permitted across the firewall
  - Incoming SSH connections are only allowed to one specific host



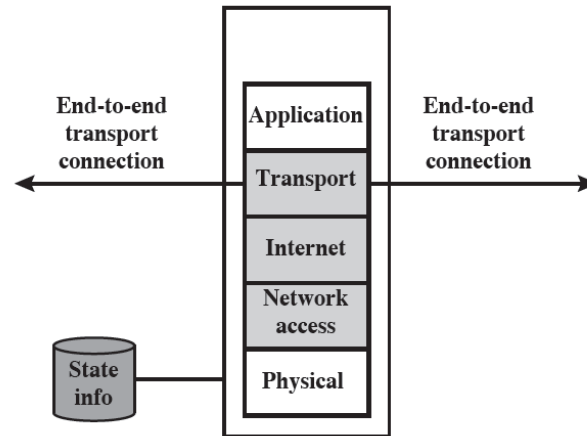
# Firewall Types

According to NIST 800-41:

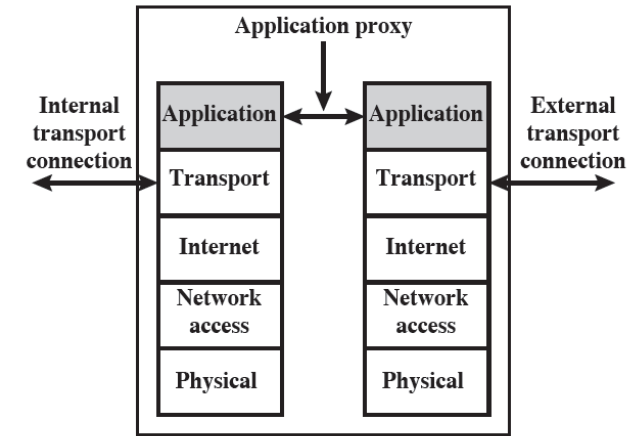
## Packet Filtering



## Stateful Inspection

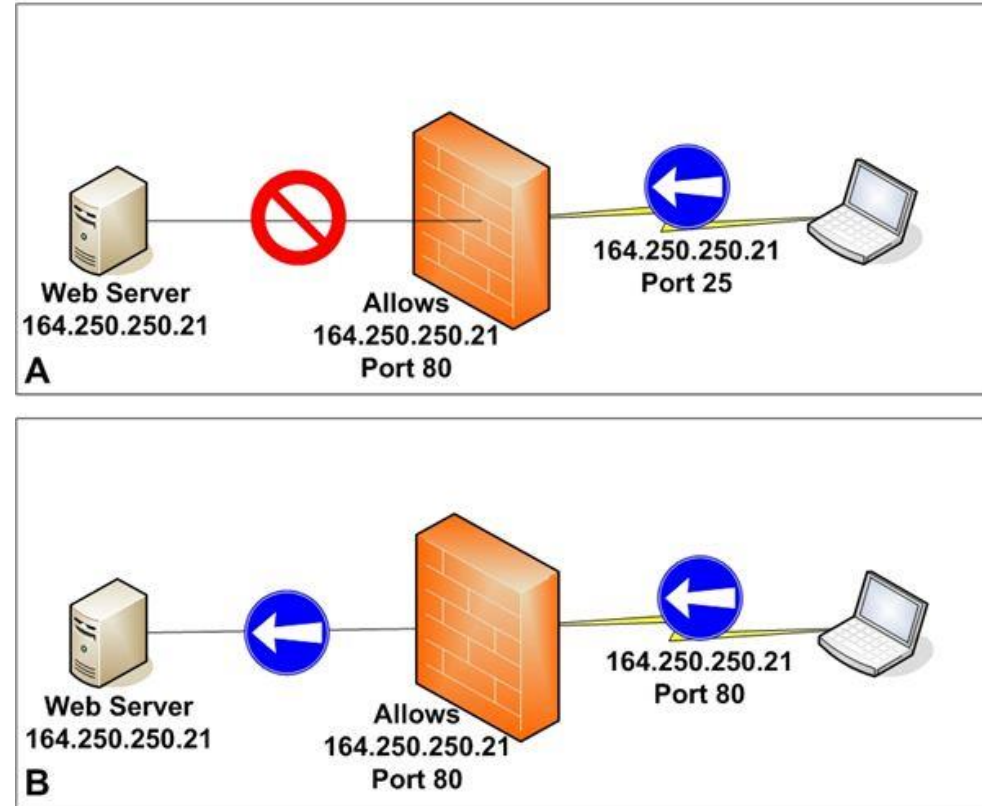


## Application Proxy



# Packet Filtering Firewall

- Network layer firewall
- Acts like a normal router
- Often some stateless firewall functionality included in most routers



# Firewall Rules - Stateless

## Stateless

- Each packet is independent
- Very fast and simple to implement
- Only simple rules
- Example: “*Block incoming port 53 packets except known trusted servers*”

# Stateful Inspection Firewall

- Tracking the state of connections
- State Table => state machine describing protocol communication
- E.g. TCP – connection establishment, usage, termination

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

# Firewall Rules - Stateful

## Stateful

- Deals with packet streams
- Slower and requires more resources
- Can implement complex rules
- Example 1: *“Let incoming UDP packets through only if they are responses to outgoing UDP packets that have been observed”*
- Example 2: *“Accept TCP packets with the SYN bit set only as part of TCP connection initiation”*

# What Internet Services/Protocols to consider?

- Electronic mail: Simple Mail Transfer Protocol (SMTP), IMAP, POP3
- File exchange: Web-based Distributed Authoring and Versioning (WebDAV), File Transfer Protocol (FTP), Network File System (NFS)
- Remote terminal access and command execution: Secure SHell (SSH)
- World wide web: HyperText Transfer Protocol (HTTP, HTTPS)
- Real-time conferencing services: ICQ, Jabber, Skype, Adobe Connect, ...
- Name services: Domain Name Service (DNS)
- Network management: Simple Network Management Protocol (SNMP)
- Time service: Network Time Protocol (NTP)
- Window systems: Remote Desktop Protocol (RDP), X-Windows
- Printing systems: Internet Printing Protocol (IPP)

# Important protocol fields (1)

## Access Protocol:

- Network Layer Protocol: IPv4, IPv6
- Access Protocol Addresses: Ethernet MAC address, etc.

## IP:

- Source address
- Destination address
- Flags, in particular, the indication of an IP fragment (in IPv6 an option)
- Protocol type: TCP, UDP, ICMP, ...
- Options:
  - Source routing:
    - the sender explicitly specifies the route an IP packet will take - as this is often used for attacks most firewalls discard these packets

# Important protocol fields (2)

## TCP:

- Source port, Destination port:
  - Evaluation of source and destination ports allow to determine (with a limited degree of confidence) the sending / receiving application, as many Internet services use well-known port numbers
- Control:
  - ACK: this bit is set in every segment but the very first one transmitted in a TCP connection, it therefore helps to identify connection requests
  - SYN: this bit is only set in the first two segments of a connection, so it can be used to identify connection confirmations
  - RST: if set, this bit indicates an ungraceful close of a connection, it can be used to close peers off without returning helpful error messages


## Application protocol:

- In some cases, a firewall might look at application protocol header fields
- Not covered in this class ...



# Packet Filtering Firewalls – Pros and Cons

## Weaknesses

- 
- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions
  - Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited
  - Most packet filter firewalls do not support advanced user authentication schemes
  - Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack
  - Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations

## Strengths

- 
- Its simplicity
  - Transparent to users and are very fast



**QUEEN'S  
UNIVERSITY  
BELFAST**

# Attacks and Countermeasures

## IP address spoofing

The intruder transmits packets from the outside with a source IP address field containing an address of an internal host

Countermeasure is to discard packets with an inside source address if the packet arrives on an external interface

## Source routing attacks

The source station specifies the route that a packet should take as it crosses the internet, in the hopes that this will bypass security measures that do not analyze the source routing information

Countermeasure is to discard all packets that use this option

## Tiny fragment attacks

The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment

Countermeasure is to enforce a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header

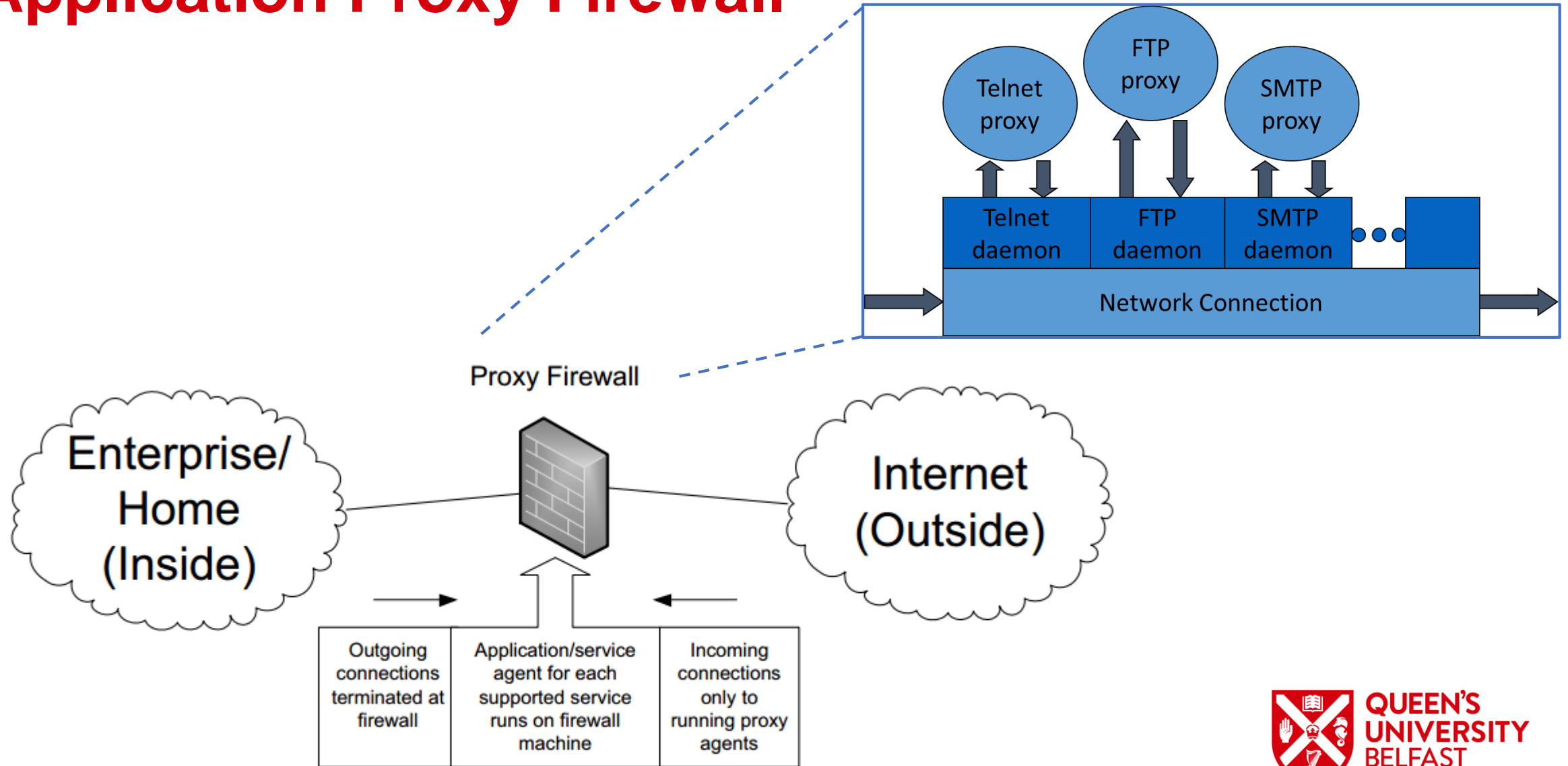


**QUEEN'S  
UNIVERSITY  
BELFAST**

# What is a proxy?

- A program that deals with external servers on behalf of internal clients
- Proxies relay approved client requests to real servers and also relay the servers answers back to the clients
- If a proxy interprets and understands the commands of an application protocol it is called an *application level proxy*, if it just passes the PDUs between the client and the server it is called a *circuit level proxy*

# Application Proxy Firewall



# Application Proxy Firewall

- Acts as a relay of application-level traffic
- Proxying provides access to a specific Internet service for a single host while appearing to provide it for all hosts of a protected network
- Candidate services for proxying:
  - FTP, Telnet, DNS, SMTP, HTTP
- Proxy servers usually run on bastion hosts
- The use of a proxy service usually leads to the following situation:
  - The user of a proxy service has the illusion of exchanging data with the actual server host
  - The actual server has the illusion of exchanging data with the proxy host

# Application Proxy Firewall

- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall
- The gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features
- Tend to be more secure than packet filters
- Disadvantage:
  - The additional processing overhead on each connection

# Next-Generation Firewalls (NGFWs)

Platform for network security policy enforcement and network traffic inspection.

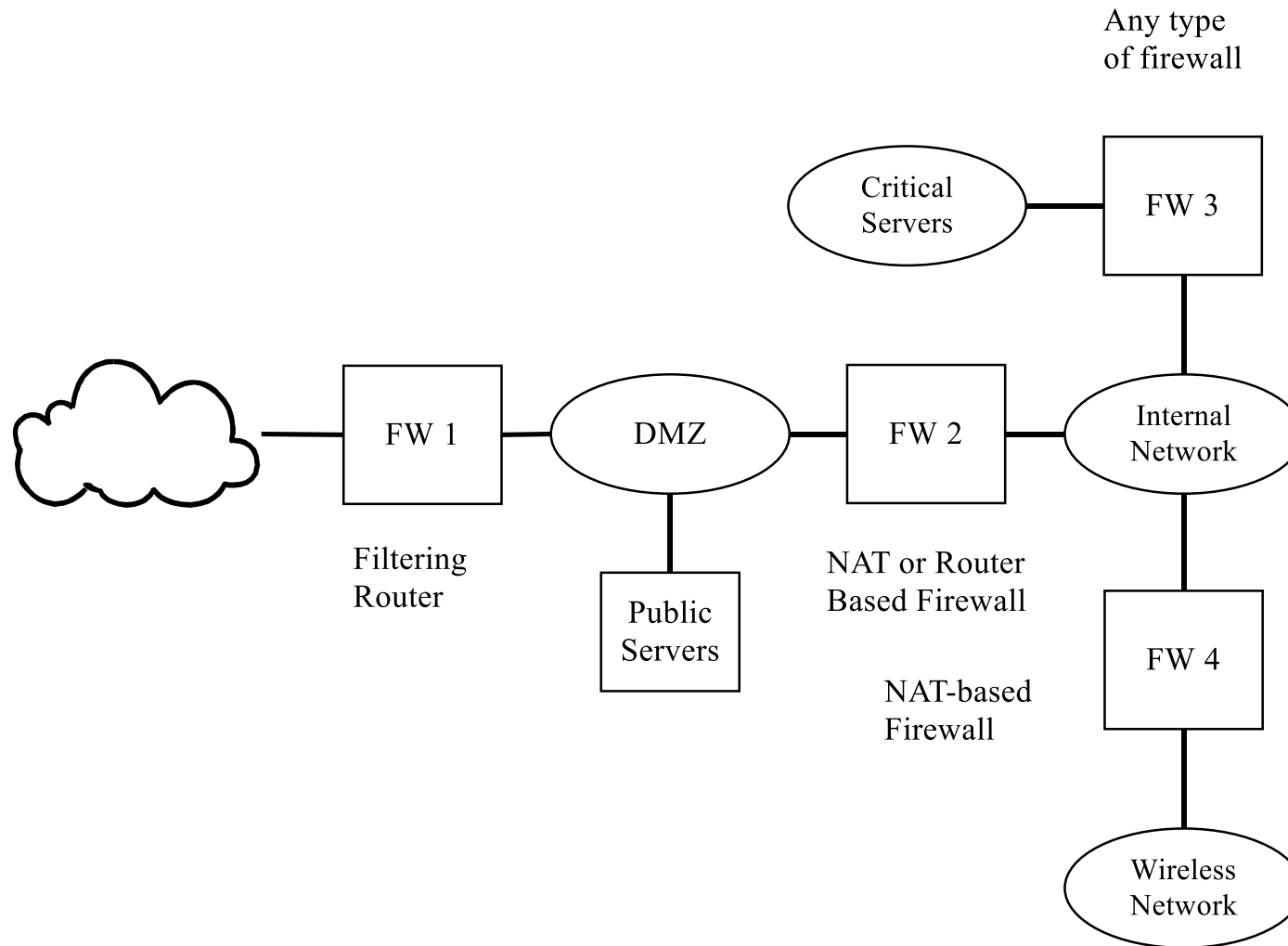
- **Standard capabilities of the first-generation firewall:** This includes packet filtering, stateful protocol inspection, network-address translation (NAT), VPN connectivity, etc.
- **Integrated intrusion prevention:** This includes support for both vulnerability-facing and threat-facing signatures, and suggesting rules (or taking action) based on IPS activity.
- **Full stack visibility and application identification:** ability to enforce policy at the application layer independently from port and protocol.
- **Extra intelligence:** ability to take information from external sources and make improved decisions. Examples include creating blacklists or whitelists and being able to map traffic to users and groups using active directory.
- **Adaptability to the modern threat landscape:** support upgrade paths for integration of new information feeds and new techniques to address future threats.
- **In-line support** with minimum performance degradation or disruption to network operations.

# Next-Generation Firewalls (NGFWs)





# Firewall Deployment

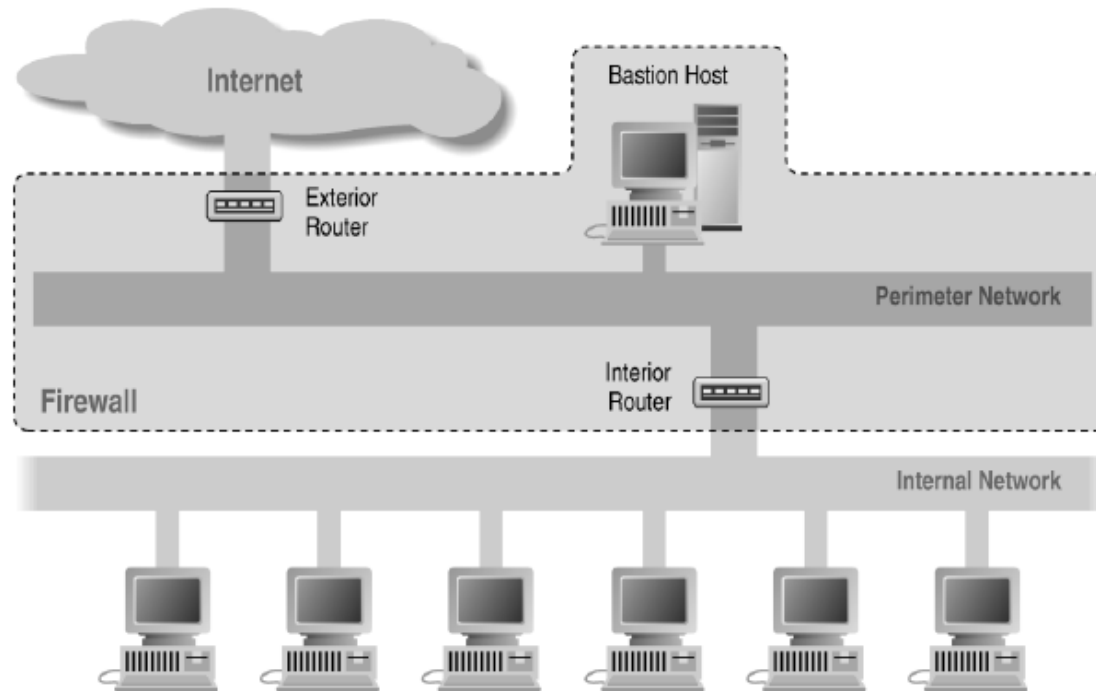


# What is a bastion host?

- A computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
- A bastion host in a firewall is usually the main point of contact for user processes of hosts of internal networks with processes of external hosts

# What is a DMZ?

- A de-militarized zone (also called a perimeter network)
- A subnetwork added between an external and an internal network, in order to provide an additional layer of security
- Remember NAT: DMZ is a good place to host a publicly accessible information server e.g. a web server



# Example Ruleset (1)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP		25		Permit
B	Outbound	Internal	External	TCP		>1023		Permit
C	Outbound	Internal	External	TCP		25		Permit
D	Inbound	External	Internal	TCP		>1023		Permit
E	Either	Any	Any	Any		Any		Deny

- This first ruleset aims to specify that incoming and outgoing email should be the only allowed traffic into and out of a protected network
- Email is relayed between two servers by transferring it to an SMTP-daemon on the target server (server port 25, client port > 1023)
- Rule A allows incoming email to enter the network and rule B allows the acknowledgements to exit the network
- Rules C and D provide the same filtering for outgoing email
- Rule E denies all other traffic

# Example Ruleset (2)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP		25		Permit
B	Outbound	Internal	External	TCP		>1023		Permit
C	Outbound	Internal	External	TCP		25		Permit
D	Inbound	External	Internal	TCP		>1023		Permit
E	Either	Any	Any	Any		Any		Deny

- Consider, for example, a packet which “wants” to enter the protected subnet and has a forged IP source address from the internal network:
  - As all allowed inbound packets must have external source and internal destination addresses (A, D) this packet is successfully blocked
  - The same holds for outbound packets with external source addresses (B, C)
- Consider now SSH traffic:
  - As an SSH server resides usually at port 22, and all allowed inbound traffic must be either to port 25 or to a port number > 1023, incoming packets to initiate an incoming SSH connection are successfully blocked
  - The same holds for outgoing SSH connections
- However, the ruleset is flawed as, for example, it does not block the RDP-protocol for terminal server applications:
  - An RDP server usually listens at port 3389, clients use port numbers > 1023
  - Thus, an incoming RDP request is not blocked (D), neither is any answer (B)
  - This is highly undesirable, as the RDP protocol may allow attackers to log into clients with weak passwords

# Example Ruleset (3)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25		Permit
B	Outbound	Internal	External	TCP	25	>1023		Permit
C	Outbound	Internal	External	TCP	>1023	25		Permit
D	Inbound	External	Internal	TCP	25	>1023		Permit
E	Either	Any	Any	Any	Any	Any		Deny

- The RDP-related flaw can be fixed by including the source ports in the ruleset specification:
  - Now outbound traffic to ports >1023 is allowed only if the source port is 25 (B), traffic from internal RDP clients or servers (port >1023) will be blocked
  - The same holds for inbound traffic to ports >1023 (D)
- However, it is not certain that an attacker will not use port 25 for her attacking RDP client:
  - In this case the above filter will let the traffic pass

# Example Ruleset (4)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25	Any	Permit
B	Outbound	Internal	External	TCP	25	>1023	Yes	Permit
C	Outbound	Internal	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Internal	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- This problem can be addressed by also specifying TCP's ACK-bit in rules B and D:
  - As the ACK-bit is required to be set in rule B, it is not possible to open a new TCP connection in the outbound direction to ports >1023, as TCP's connect-request is signaled with the ACK-bit not set
  - The same holds for the inbound direction, as rule D requires the ACK bit to be set
- As a basic rule, any filtering rule that permits incoming TCP packets for outgoing connections should require the ACK-bit be set

# Example Ruleset (5)

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

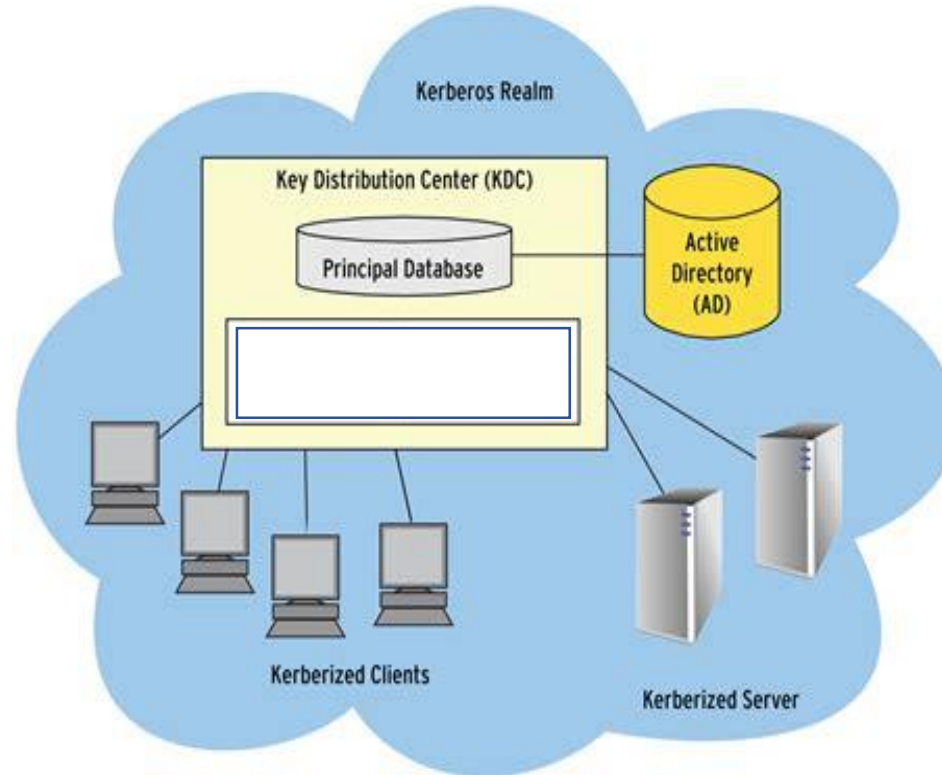
- If the firewall comprises a bastion host, the packet filtering rules should further restrict traffic flow (→ screened host architecture):
  - As in the modified rules above only traffic between the Internet and the bastion host is allowed, external attackers can not attack SMTP on arbitrary internal hosts any longer
- In a screened subnet firewall, two packet filtering routers are set up:
  - one for traffic allowed between the Internet and the bastion host, and
  - one for traffic allowed between the bastion host and the internal network



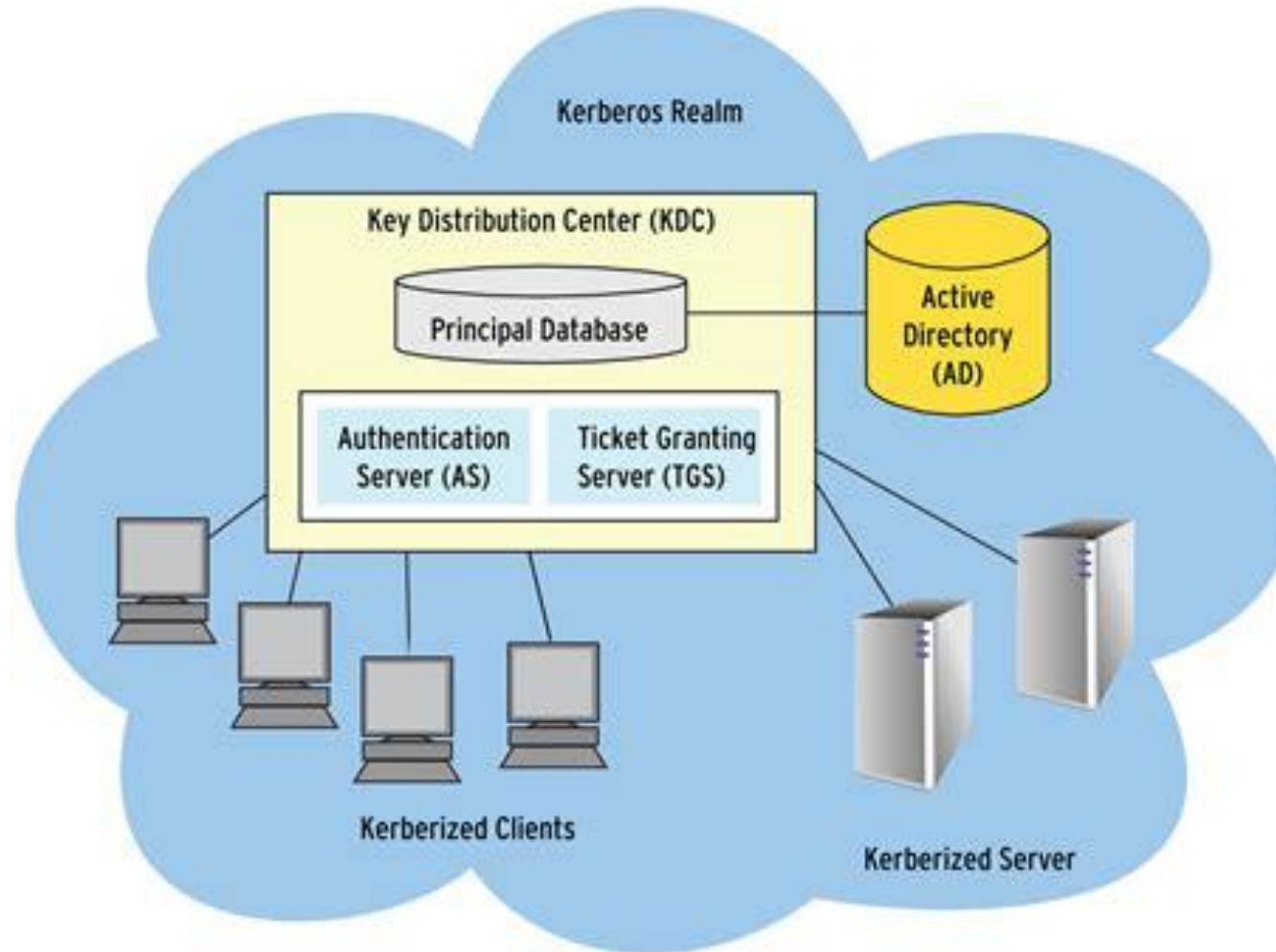
# Summary

- Firewalls
  - What they can and can't do
  - Default permit/default deny strategies
  - Types:
    - Packet Filtering
    - Stateful Inspection
    - Application Proxy
    - Next Generation Firewalls
  - Deployment:
    - Bastion Host/DMZ
  - Example Ruleset

# What elements are missing in the figure?

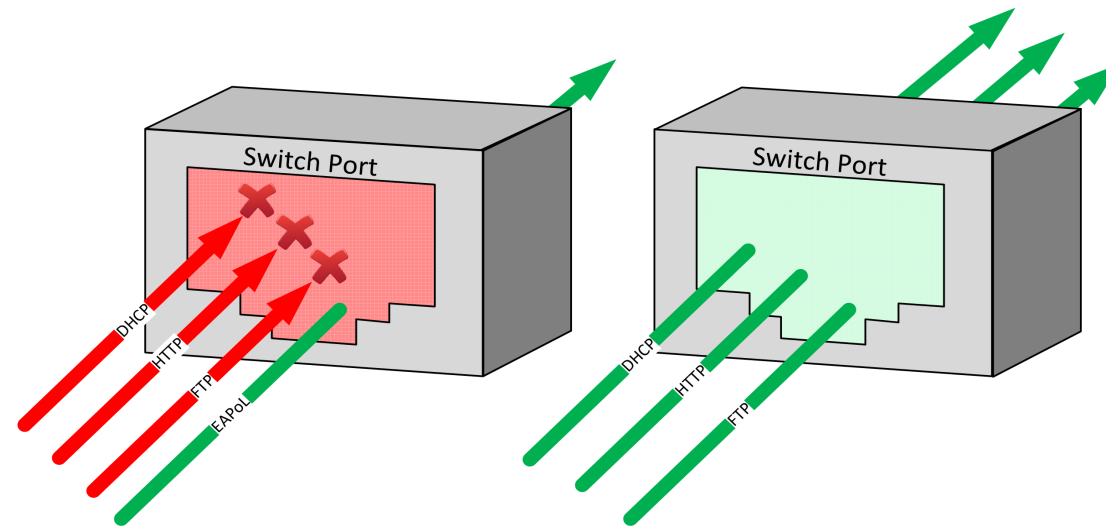


# Kerberos



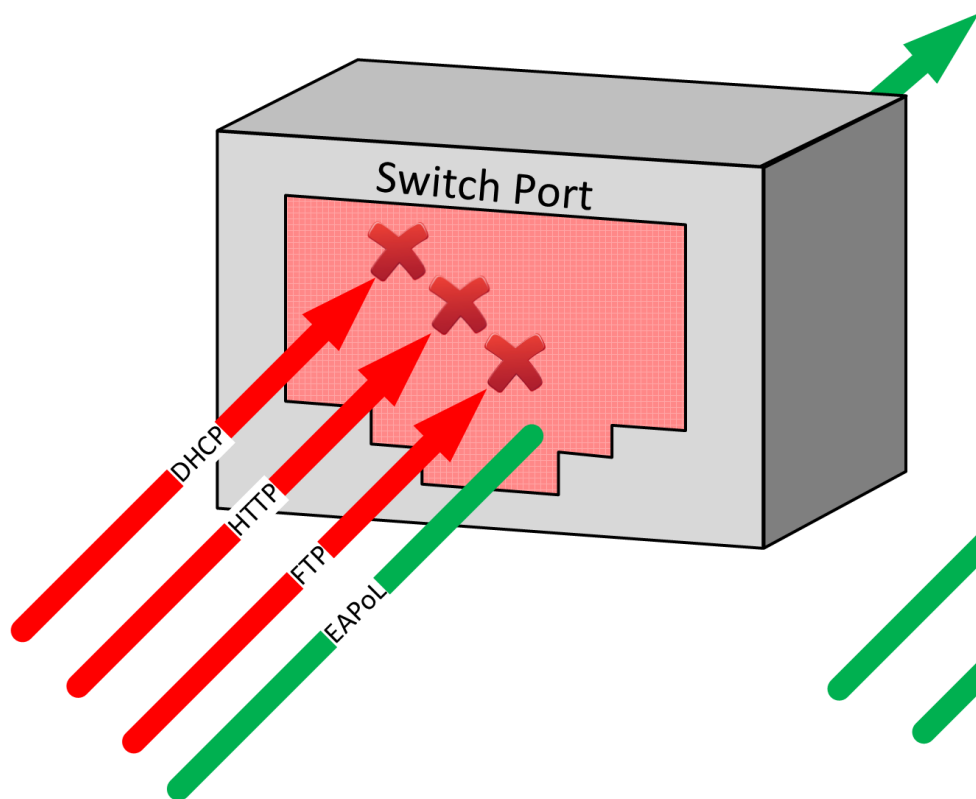
# What is shown in the figure?

- A. IEEE 802.1Q
- B. RADIUS
- ✓ C. IEEE 802.1X
- D. IEEE 802.11

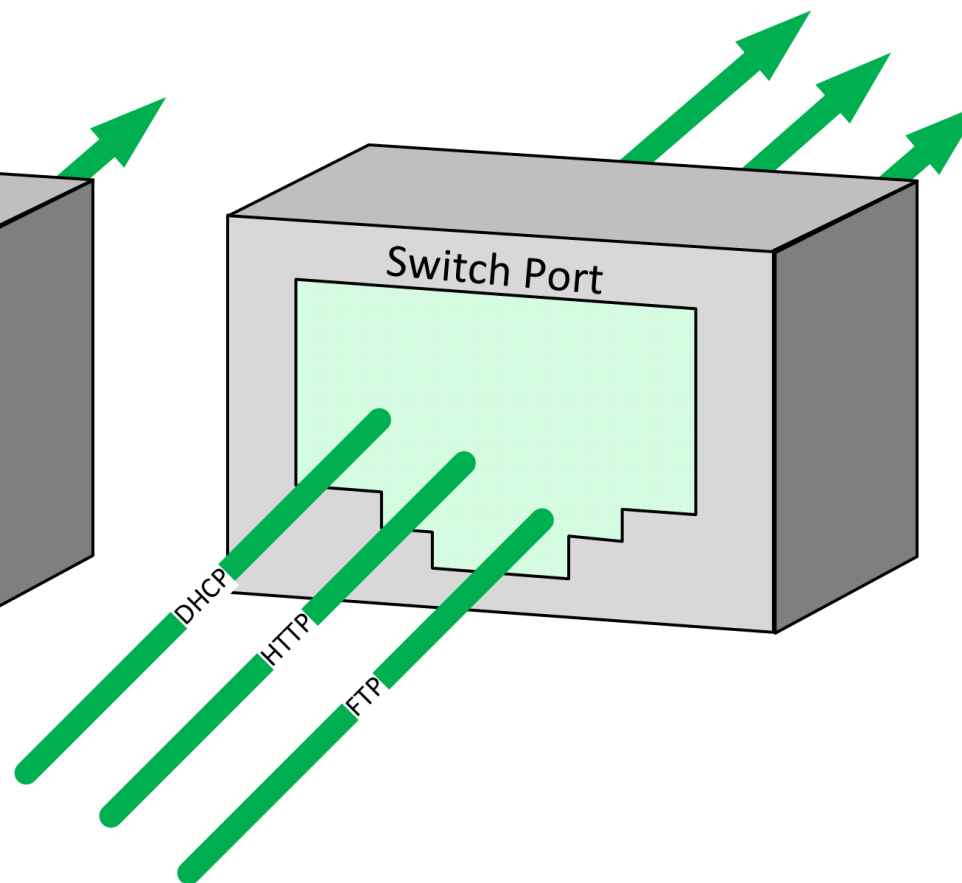


# Port-based Network Access Control (IEEE 802.1X)

Before 802.1X Authentication

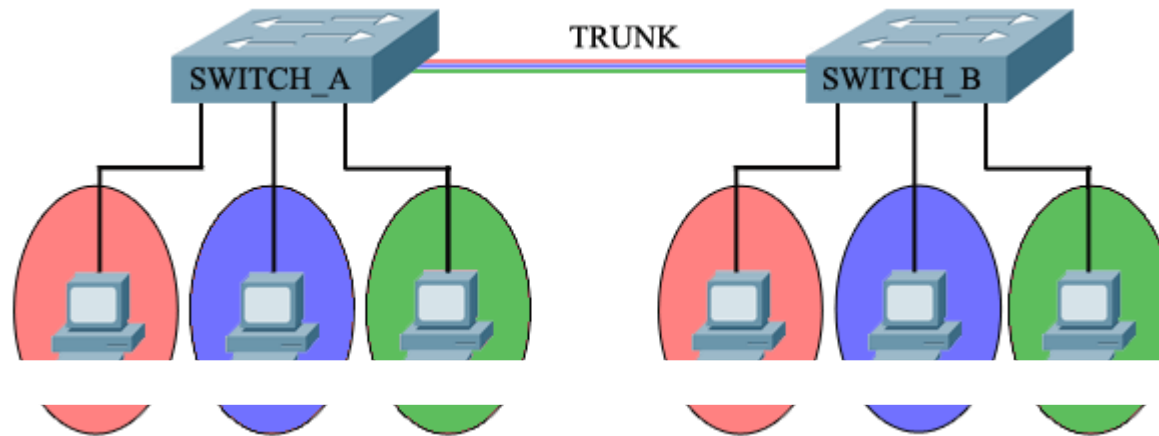


After 802.1X Authentication

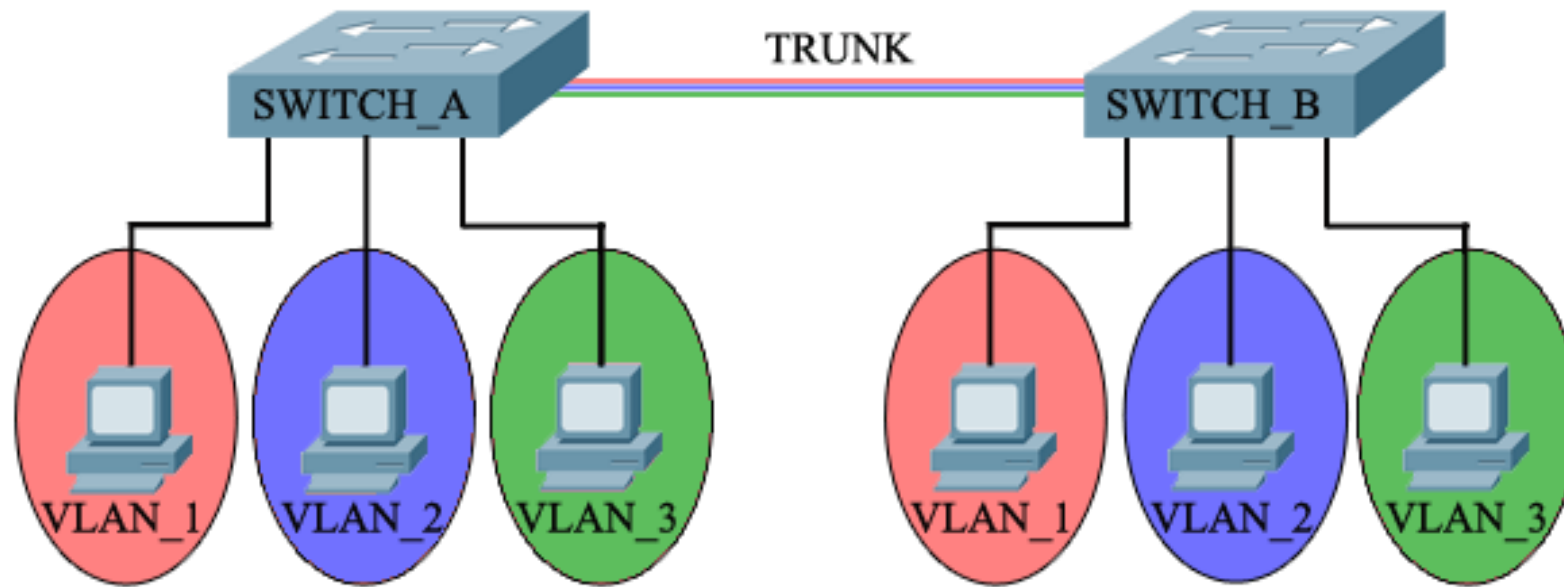


# What is shown in the figure?

- A. IEEE 802.1X
- B. Port-based NAC
- C. NAT
- ✓ D. VLAN



# Virtual Local Area Networks (IEEE 802.1Q)



# Questions?

Next Session: IDPS – Part 1

Thursday, 28 February 2019