SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience

Firewalls

Lecture nine

Outline of Lecture

- In this lecture we will look at a key piece of security infrastructure, the Firewall
  - Introduction to firewalls
  - Firewall types
  - Firewall architectures
- We will then demonstrate the process of how policy is formulated and then implemented
  - We will use firewalls to demonstrate the process

Learning outcomes

- You should be able to
  - Explain the difference between
    - Packet filters
    - Stateful packet filters
    - Proxy firewalls
    - Dynamic firewalls
  - Describe the following firewall architectures
    - Dual homed gateway
    - Screened host gateway
    - Screened subnets

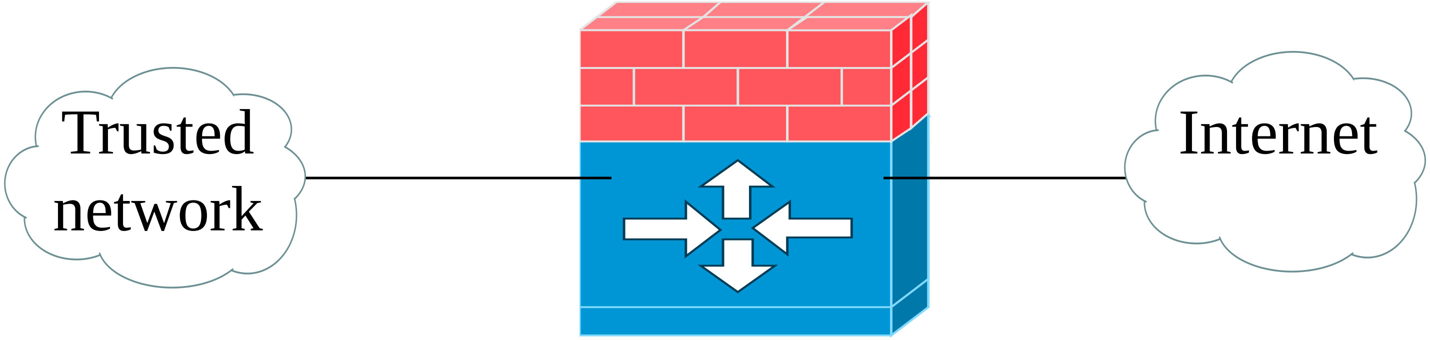
Introduction to firewalls

- Firewalls are used to restrict access to one network from another network
- A key mechanism in implementing security policy
- Mostly used by companies to protect internal network from the Internet
- Can also be used internally
  - Eg prevent employees from accessing confidential financial data
- This lecture we have a look at types of firewalls and their architectures

Firewall

- A firewall is a type of gateway that might be a router, server, specialised hardware device, or a combination of all three
  - Earliest firewalls were implemented with routers and packet filtering hosts
- Firewalls monitor packets coming in and out of the firewall
- Firewalls filter out packets that do not meet the requirements of the security policy
- Modern firewalls not just packet filters
  - Can do deep inspection of higher layer protocols embedded in the packets and filter based on contents
  - Can keep track of past events to assist in packet filtering decisions

Firewall



Types of firewalls

- Firewall types can be classified as
    - Packet filters
    - Stateful packet filters
    - Proxy firewalls
    - Dynamic firewalls
- Some firewalls may implement more than one of the above
    - Eg Stateful packet filtering with proxy support for http

Packet layer firewalls

- Built around one or two routers that carry out packet filtering
- Can be used in the following ways
  - Block all incoming connections from systems other than services such as email
  - Block all connections to or from certain distrusted systems
  - Allow some services (eg email) but block services based on port number that can be dangerous
    - TFTP, X-Window system, RPC, rlogin

Packet layer filtering

- Packet filtering is based on information in packet header only
  - IP source address
  - IP destination address
  - Protocol
    - TCP, UDP, ICMP
  - TCP/UDP source port
  - TCP/UDP destination port
  - ICMP message type
- Additional information known to the filter is
  - Interface packet arrived on
  - Interface packet will go out on

Packet layer filtering

- Filtering based on Access Control Lists
  - Cisco calls them ACLs
- Usually includes some mechanism to block on a range of IP addresses and ports
  - Cisco refer to Wild card masks
- Filtering also includes specific applications
  - Based on port numbers
    - Eg 23 Telnet

Ports typically policed by a Packet Filter

- You would expect a firewall to police these ports
- Inbound requests of the following would almost certainly be blocked
  - TFTP (port 59)
  - rlogin, rsh, rexec (ports 513, 514 and 512)
  - telnet (port 23)
  - RPC (port 111)
- Inbound requests for the following would probably be blocked
  - FTP (ports 20 and 21)
  - SMTP (port 25)
  - DNS (port 53)
- The following would be tightly controlled
  - HTTP (port 80)
  - SMTP (port 25)

Example of packet firewall rules

- Permit SMTP connections into the network

Direction	Source address	Dest. Address	Protocol	Source port	Dest port	ACK set	Action
In	Internal	Any	TCP	>1023	25	Either	Permit
Out	Any	Internal	TCP	25	>1023	Yes	Permit
Either	Any	Any	Any	Any	Any	Either	Deny

Advantages and disadvantages of packet filtering

- Advantages
  - Scaleable
  - Very fast processing
  - Independent of the application
- Disadvantages
  - Does not examine packet past header information
    - Can be subverted through ‘tunnelling’
  - Does not keep track of state of connection
    - Won’t protect against SYN flooding, TCP hijacking and TCP SYN attacks
  - Comparatively low security

Question

- What do the following set of rules do?

Direction	Source address	Dest. Address	Protocol	Source port	Dest port	Action
In	External	Internal	TCP	>1024	25	Deny
Out	Internal	External	TCP	25	>1024	Deny
Out	Internal	External	TCP	>1024	25	Permit
In	External	Internal	TCP	25	>1024	Permit
Either	Any	Any	Any	any	Any	Deny

Deep Packet Inspection

- Can extend packet beyond header information to contents
- For example if destination is a port 80 then the contents should be http or SOAP or one of the other protocols that legitimately use port 80
- In the first lab we saw how one protocol can be carried inside another (tunnelling)
- Deep Packet Inspection polices such connections
  - If (for example) we see packet contents that resembles telnet then we may decide to drop the packet

Stateful packet filters

- Packet filtering in context
- Examines packet stream based on state tables
  - State information stored in state tables
- Usually operate at the transport and network layers
  - Allows or denies packet based upon rules appropriate to the TCP service

Stateful packet filters

- Retains in memory connection information
- As well as IP addresses and ports may include packet sequence numbers and flags
- Most intense scrutiny is during connection set up, particularly of the SYN bit
  - All packets with SYN set should be a new connection or a response to a new connection
  - All packets with an ACK set should be an existing connection
  - We should not see a SYN flag on an established connection once the 3-way handshake is completed
  - We should not see an ACK flag on a new connection
- Requires the state of the connection to be maintained
  - Connection is new or established

Advantages and disadvantages of stateful packet filters

- Advantages
  - Provides an extra level of protection to that of packet filters
  - More flexible than ordinary packet filters
    - Can permit some services that a stateless filter would probably have to prohibit
- Disadvantages
  - Slower and more expensive than packet filters
    - Much more complicated processing
  - Can be subject to denial of service attacks
    - Need to maintain a table of connection state than can be flooded with bogus information

Proxy services

- Proxy service intermediates between client and server
- Proxy services sit transparently between a user on the internal network and a service on the Internet
  - Instead of direct communication between the user and the service each talks to the proxy
  - Need to be located at sole point where communication between internal host and external service occurs

Advantages and disadvantages of proxy firewalls

- Advantages
  - Information hiding
    - Internal systems not revealed to hosts on the untrusted network
  - Authentication and logging much stronger
  - Simple filtering rules
  - The only host visible to the untrusted network
- Disadvantages
  - Much poorer performance
  - Restricted to well known applications
  - Doesn’t scale well
  - Breaks end to end principle
    - Can be a problem with some applications such as VoIP
    - Problems with running IPSec through a proxy firewall

Application and Circuit level proxies

- Two kinds of proxy firewalls
  - Application level
  - Circuit level
- Application level proxies
  - Inspect entire contents of packet and make decisions based on the content of the packet
  - Have an in-built understanding of the application
- Circuit level
  - Operate at the session or transport layer of the protocol
  - Makes decisions based on address, port and protocol type
  - ‘SOCKS’ an example
    - TCP only commonly used example

Dynamic firewalls

- Where rules are statically defined we often need to allow all ports above 1024
  - Most client-server interactions will talk to the server on a well known port (eg 80) with an arbitrary port number (>1024) for the client
- A dynamic firewall opens the client port number for the duration of the transaction and closes it afterwards
- Enables policing of higher port numbers not possible with a static firewall

Firewall appliances

- Firewalls may be either software that is installed on a regular computer or router or a dedicated hardware appliance
- Dedicated hardware appliance is usually more secure
  - Typically uses a stripped down version of an operating system
    - Usually Linux or BSD
    - Most operating systems contain a great deal of code and functionality that is not needed for firewall functionality
    - Additional code introduces potential vulnerabilities
    - If a firewall can be compromised then the organisation is very vulnerable
  - Can also be made more physically secure
    - Redundant power supplies, disk striping etc

Firewall architectures

- We have looked at types of firewalls
  - Essentially make the decision of whether or not to drop a packet
- Now look at architecture of firewalls
  - How the components of a firewall are arranged
- Firewall architectures
  - Bastion host
  - Dual homed gateway
  - Screened host
  - Screened subnet

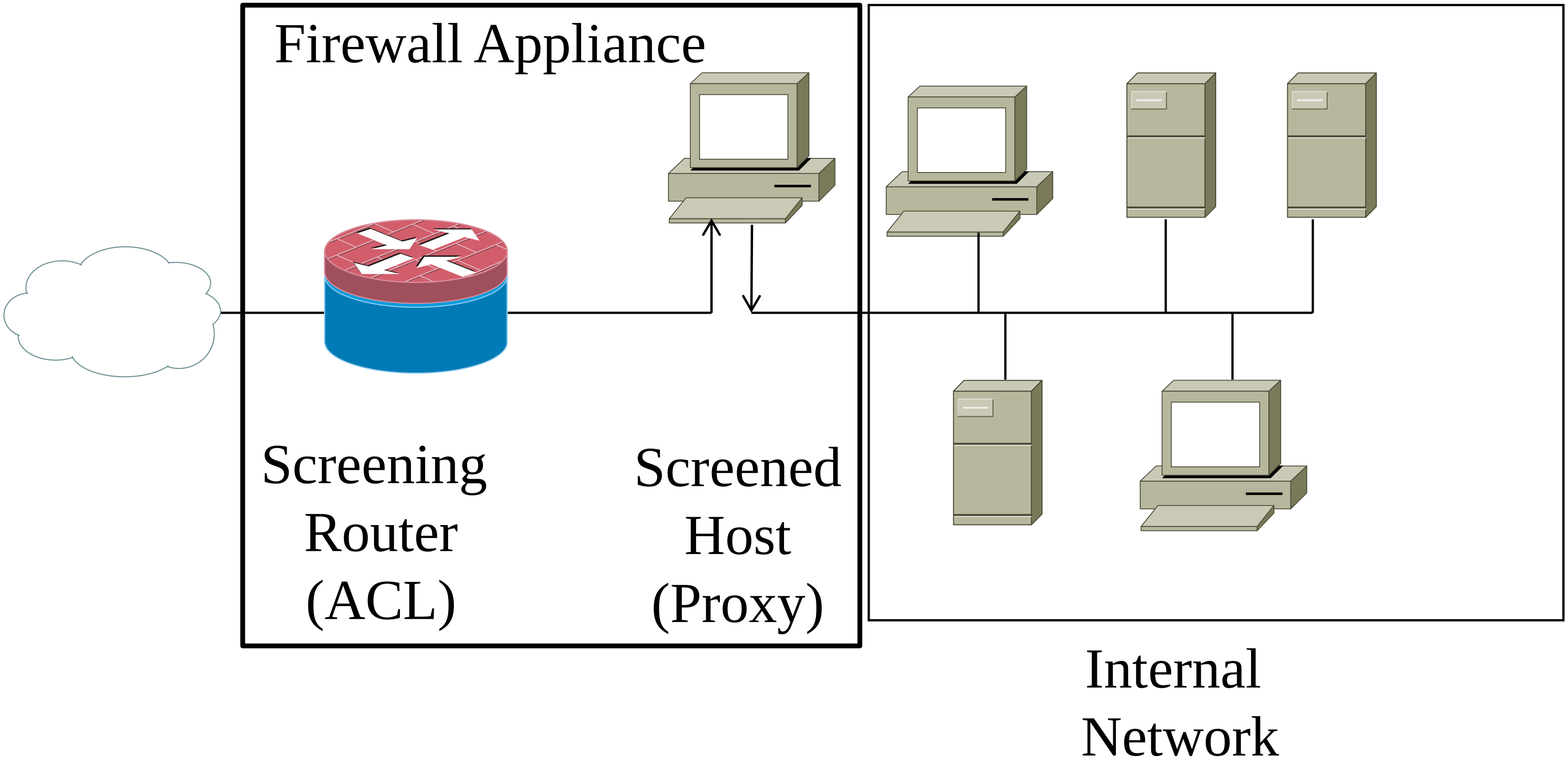
Bastian host

- A host that is exposed to the Internet or runs in the DMZ
- Must be an extremely secure system
  - No unnecessary services
  - No unused subsystems (printing for example)

Screened host

- A firewall that communicates directly with a perimeter router and the internal network
- The perimeter router applies packet filtering via ACLs
- The screened host then then applies its own filtering
  - Usually a proxy (application) layer firewall

Screened host



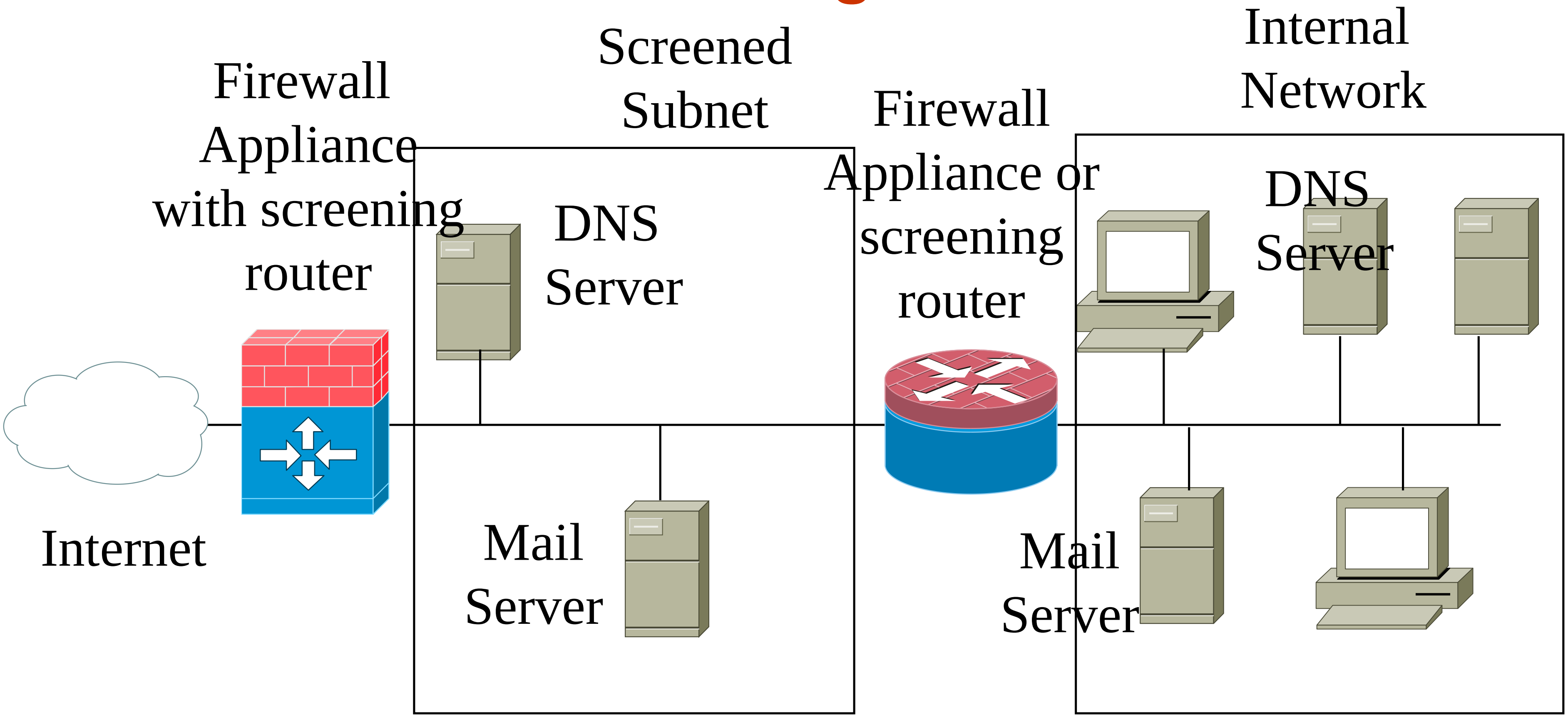
Screened host

- Benefits
  - Provides control on available services
  - Reduction of router program complexity
  - All traffic passes through single point
  - Router configuration rules need only consider firewall’s IP address
  - Other packets arriving at filter discarded
- Risks
  - If packet filter compromised entire internal network is at risk
  - More secure implementation is to use a screened subnet

Screened subnet

- Screened subnet considered to be the most secure firewall architecture
- Involves three devices (or three lines of defence) that must be compromised before internal network compromised
- Isolated networks positioned between the external and internal networks
- Allows non-critical hosts to be placed outside the internal network but still in a protected environment
  - In the DMZ

Screened subnet using firewall devices



Screened subnets (complex)

- Complex screened subnets built around multiple networks and multiple firewalls can be built
- May have a number of perimeter networks and DMZs protecting the interior network
- May have different functions (email, DNS, Web) in separate DMZs
- Will usually be constructed with multiple physical firewalls devices and routers

Firewall disadvantages

- Usually many access points into a network
  - Can't just use one firewall
- Firewall can be a traffic bottleneck
- Firewalls may restrict access to desirable services
- Most firewalls do not protect against viruses
  - Performance constraints
- Border firewalls provide no protection against internal attacks
- Firewalls do not protect against internally connected modems and wireless access points

Summary

- Purpose of a firewall
- Firewall architectures
- Firewall configurations