TNE20003 - Internet and Cybersecurity for Engineering Applications

Introduction to Cybersecurity

Outline of Lecture Content

- What is security?
- Frameworks, policy and implementation
- Important technologies in network security

What is security

- Security in Information Systems is anything that comes under the "Security Triad" CIA
- Confidentiality
  - Ensuring only those who are entitled to view information do sc

- Integrity
  - Ensuring data is accurate and preventing or detecting unauthorised modifications
- Availability
  - Ensuring systems are available for the organisation to carry out its normal operations

Security involves trade-offs

- Never enough resources to do everything you want to do
- Need to identify priorities and address them
  - Securing an organisation involves risk assessment
  - All too easy to do what is obvious, easy rather than what is important

- Risk Assessment
  - Needs to be continuously done
    - Risk environment changes with new threats but also with new technologies
    - How does the introduction of a new system affect the security of our organisation?
  - Techniques for Risk Assessment include Qualitative (Delphi), Quantitative

Security frameworks

- Many issues come under the topic “Security”
- Need a structured and coherent way of addressing them
  - Need to make sure you’ve covered everything
  - Role of framework
- Frameworks provide a ‘checklist’ of what to consider when securing an organisation or system
  - Most comprehensive and useful is ISO270002
  - Broad categories
    - Organisational controls
    - People controls
    - Physical controls
    - Technological controls

Security policy

- Level of security needs to be assessed
  - Has to be appropriate to the purpose of the network, the risk associated with the enterprise
  - It is too expensive and too restrictive to make any modern network totally secure
- Need to have a methodical way of assessing risk and deciding on appropriate level of security
  - Need to develop a security policy
  - The security policy is concerned with confidentiality, integrity and availability
  - Depending on the size and nature of an organisation it will have different requirements for each of these

CIA

Confidentiality

- What information needs to be kept secret and how secret does it need to be?
- What is the appropriate level of confidentiality needed for particular information
  - Passwords, encryption keys need to be absolutely secure
  - Credit card numbers, customer lists, customer transactions probably very high
  - Stock lists probably very low
- Different ways of providing confidentiality
  - passwords on files and servers
  - physical access restrictions
  - encryption

Integrity

- Usually concerned with timeliness and accuracy
- What information must be accurate in realtime and what information is less important?
- What is an appropriate level of integrity for the particular information
  - Financial transactions probably very high
  - Personal Emails on corporate server probably quite low
- Usually some broad kind of classification
  - High, Moderate, Low
- Can be provided through passwords, physical isolation or digital signing

Availability

- Part of Business Continuity Planning
- A global online business such as Amazon.com or eBay.com will have much greater requirements for availability than a home user’s blog
- Some systems within an organisation will have more stringent availability requirements than others
  - Eg. After an outage a bank will want its customer transaction processing systems to be back up and running immediately
  - Other systems such as payroll (while important) can probably tolerate more delay
- Can be provided through backup machines, alternate sites, backup power supplies, alternate ISPs etc
  - Again, key issue is how much money will it cost the organization for these systems not to be operational

Technological controls

- Main ones of interest to us in this unit & the most significant technologies for implementing technological controls are
  - Firewalls
  - Access Control
  - Intrusion Detection
  - Virtual Private Networks

Firewalls

Firewalls

- A key technology for implementing security policy
- Firewalls are used to restrict access to one network from another network
- Can be used to protect internal network from the Internet
- Can also be used internally
  - Eg prevent employees from accessing confidential financial data
- Firewall architectures
  - Screened host and screened subnet
- Firewall types
  - Packet filters, Deep Packet Inspection, Stateful Packet Filters, Proxy Servers, Dynamic Firewalls

Firewall systems and appliances

- 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

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

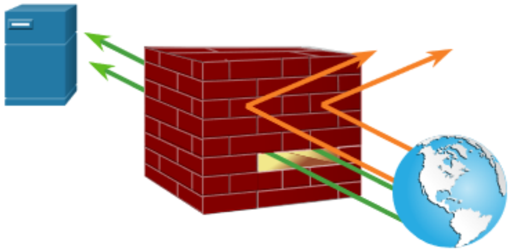
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



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

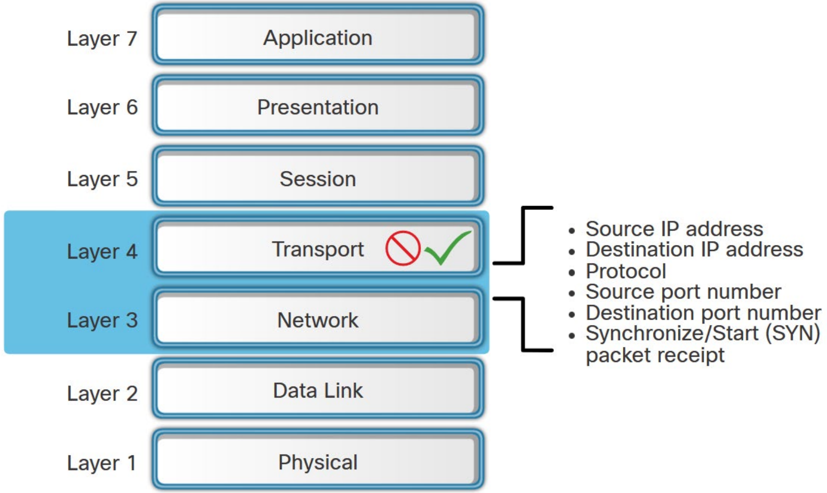
Eg Stateful packet filtering with proxy support for http

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



- Source IP address
- Destination IP address
- Protocol
- Source port number
- Destination port number
- Synchronize/Start (SYN) packet receipt

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

- Scalable
- Very fast processing
- Independent of the application
- Are easy to implement on most routers

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

Deep Packet Inspection

- **This occurs when one extends the checking or comparison packet beyond header information to contents**

  - **For example if destination is port 80 then the contents should be http or SOAP (Simple Object Access Protocol) or one of the other protocols that legitimately use port 80**
  - **Protocols can be tunnelled inside each other**
    - **Sometimes good (eg VPNs)**
    - **Sometimes bad (eg Covert Channels)**
  - **Deep Packet Inspection polices can be applied to such connections**
    - **If (for example) the firewalls sees packet contents to or from port 80 that resembles telnet rather than http then the firewall may decide to drop the packet**

Stateful packet filters

Stateful packet filters

- Packet filtering in context & Retains in memory the connection information
- 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
  - IP add, Port nos., Sequence nos. 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

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 servers (or services)

Proxy servers 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

- 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

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 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

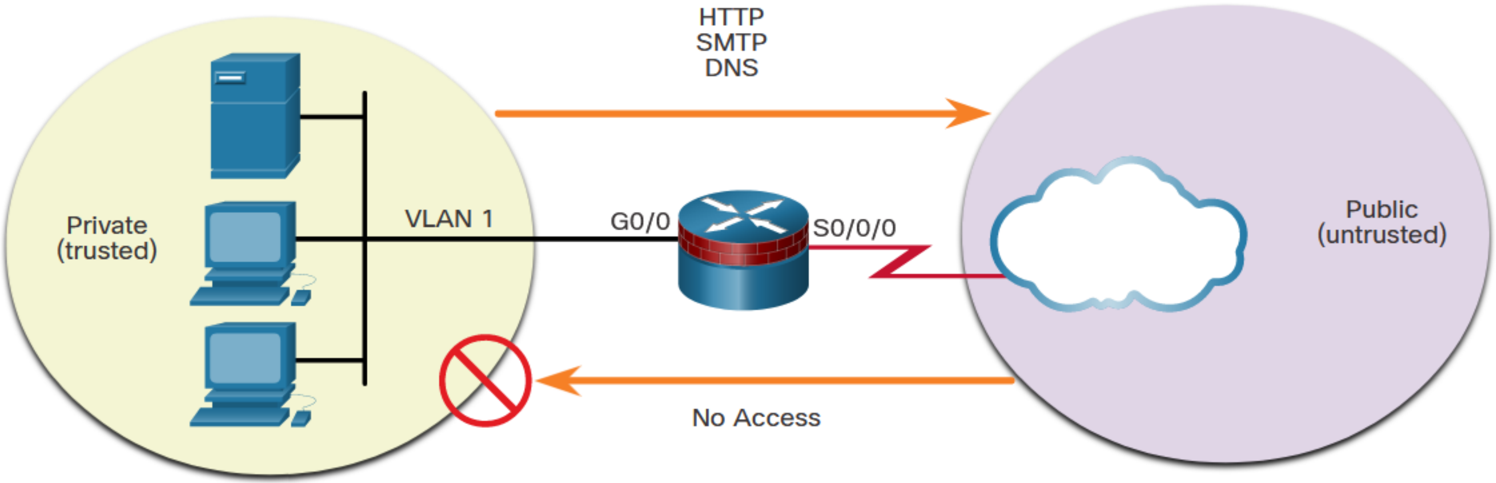
Common Security Architectures

Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic. Here are three common firewall designs:

- **Private and Public**
- **Demilitarized Zone (DMZ)**
- **Zone-Based Policy**

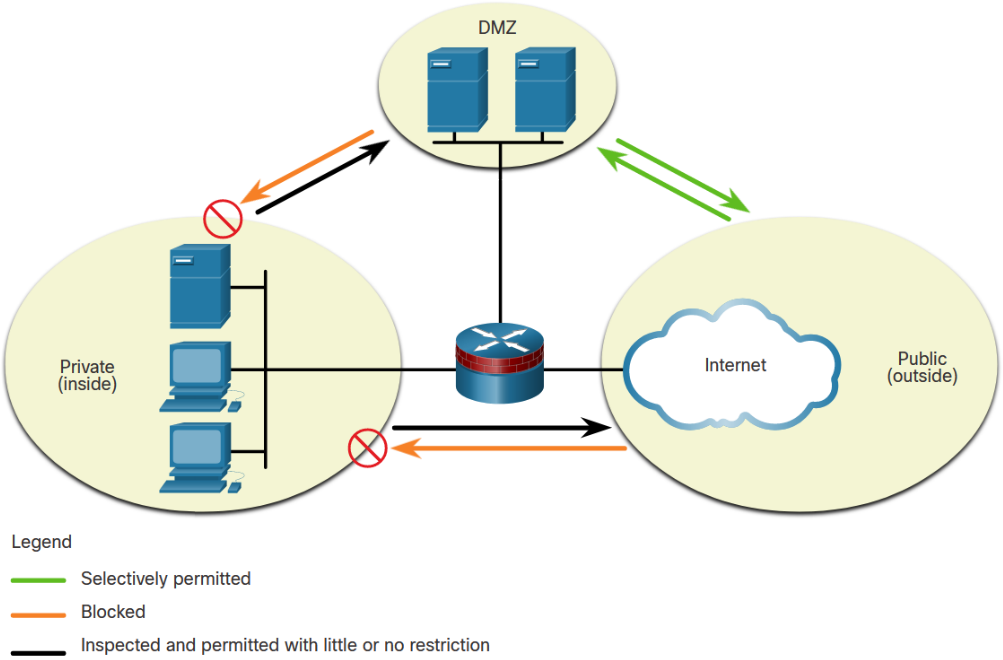
Common Security Architectures

- **Private and Public** - The public network (or outside network) is untrusted, and the private network (or inside network) is trusted.



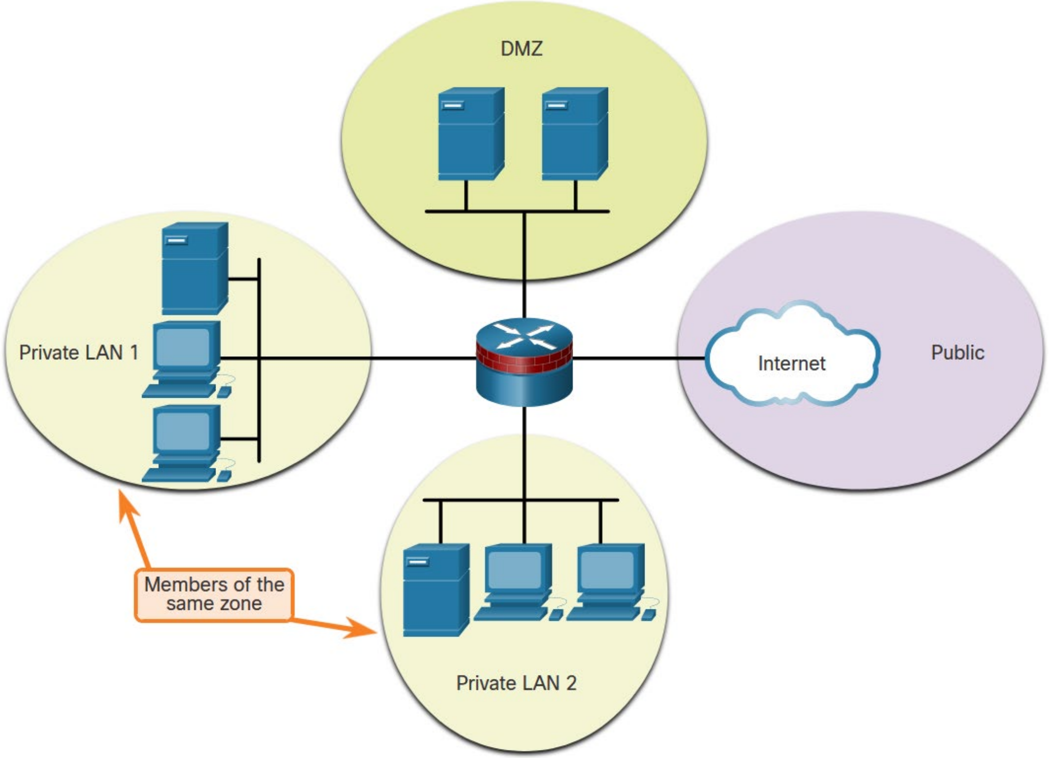
Common Security Architectures

- **Demilitarized Zone (DMZ)** - This is a firewall design where there is typically one inside interface connected to the private network, one outside interface connected to the public network, and one DMZ interface.



Common Security Architectures

- **Zone-Based Policy** - Zone-based policy firewalls (ZPFs) use the concept of zones to provide additional flexibility. A zone is a group of one or more interfaces that have similar functions or features. Zones help you specify where a firewall rule or policy should be applied.



Other Firewall architectures

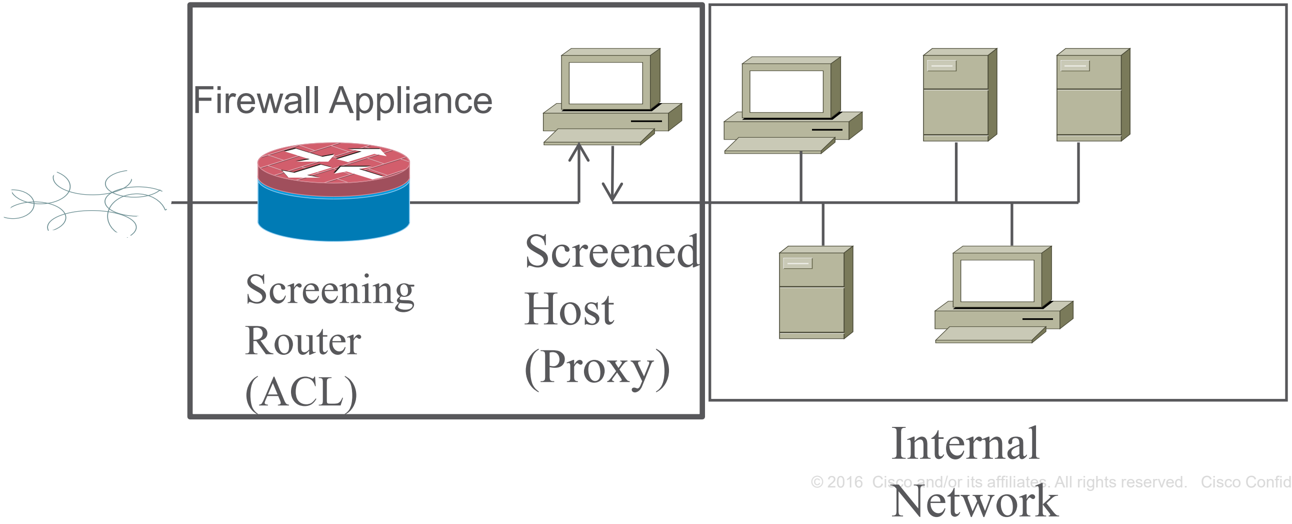
- Firewall architectures
  - Bastion host
  - Sreened host
  - Screened subnet

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



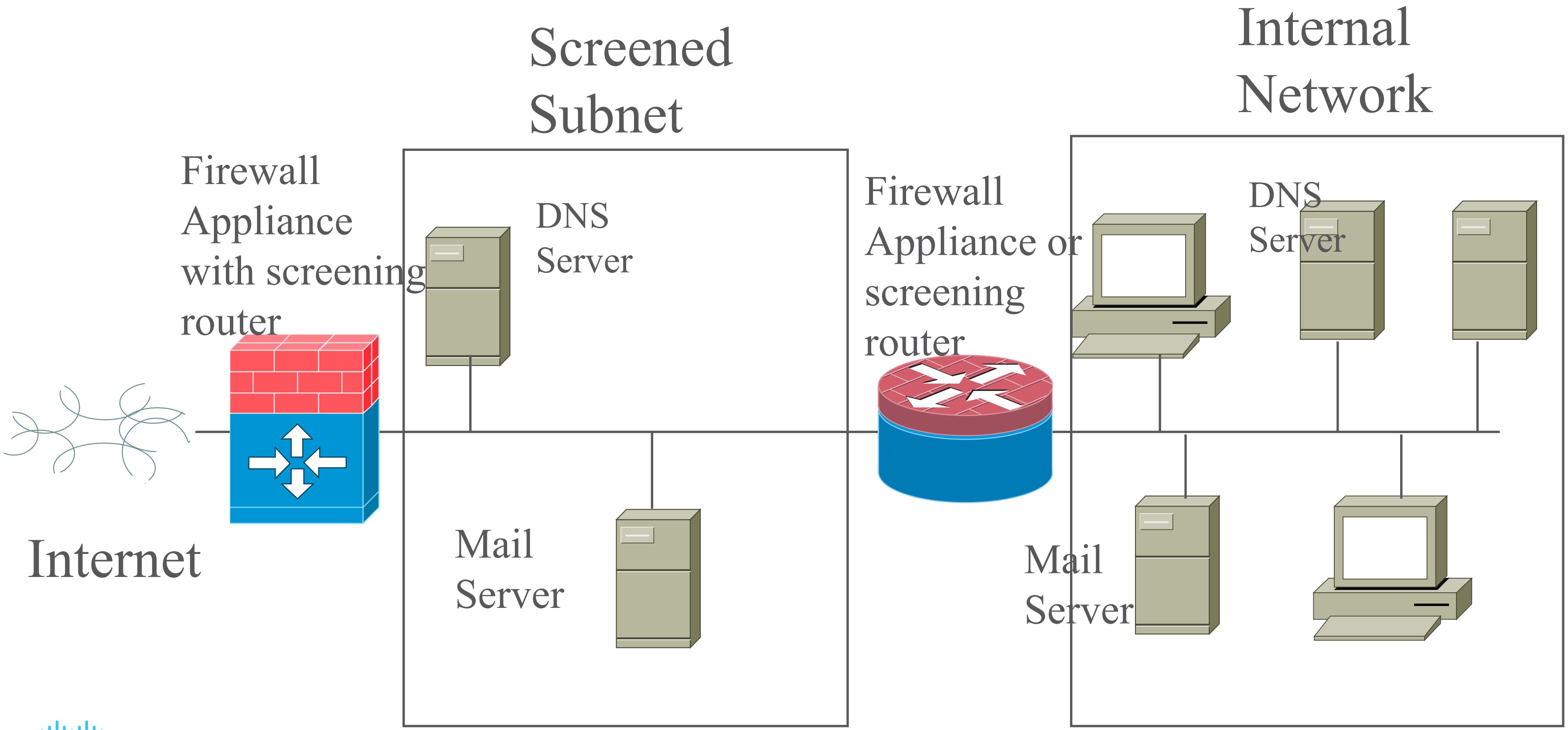
Screened host

- 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



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 of Intro to Cybersecurity

- Security involves any activity that affects Confidentiality, Integrity or Availability
- Must carry out ongoing Risk Assessments
- Security needs to be implemented in a coherent manner via a security policy using a framework such as ISO20007
- A key technology for implementing policy is a firewall
- Firewall architectures include public/private, demilitarized (DMZ), zone based, screened host and screened subnet
- Firewall types include packet filter, deep packet inspection, stateful packet filtering, proxy servers and dynamic firewalls