NCC education

Bringing British
Education to You
www.nccedu.com

Network Security and Cryptography

Topic 9:

Firewalls

V1.0

Bringing British Education to You

www.nccedu.com

Network Security and Cryptography

Topic 9 – Lecture 1:

Firewall Operation

Scope and Coverage

This topic will cover:

- Firewall architectures and their limitations
- The DMZ firewall and its limitations

Learning Outcomes

By the end of this topic students will be able to:

- Describe the components of a firewall
- Configure a DMZ firewall
- Evaluate the limitations of firewalls

Network Firewall

- A firewall is the first line of defence for your network
- The purpose of a firewall is to keep intruders from gaining access to your network
- Usually placed at the perimeter of network to act as a gatekeeper for incoming and outgoing traffic
- It protects your computer from Internet threats by erecting a virtual barrier between your network or computer and the Internet

How Does a Firewall Work?

- Examines the traffic sent between two networks
  - e.g. examines the traffic being sent between your network and the Internet
- Data is examined to see if it appears legitimate:
  - if so the data is allowed to pass through
  - If not, the data is blocked
- A firewall allows you to establish certain rules to determine what traffic should be allowed in or out of your private network

Creating Rules

- Traffic blocking rules can be based upon:
  - Words or phrases
  - Domain names
  - IP addresses
  - Ports
  - Protocols (e.g. FTP)

- While firewalls are essential, they can block legitimate transmission of data and programs

Common Firewall Types

- In general there are software firewalls and hardware firewalls
  - Even in home networks
- Hardware firewalls are typically found in routers, which distribute incoming traffic from an Internet connection to computers
- Software firewalls reside in individual computers
- Ideally a network has both

Software Firewall

- Protect only the computer on which they are installed
- Provide excellent protection against threats (viruses, worms, etc.)
- Have a user-friendly interface
- Have flexible configuration

Router Firewall

- Protect your entire network or part of a network
- Located on your router
- Protect network hardware which cannot have a software firewall installed on it
- Allows the creation of network-wide rules that govern all computers on the network

Firewall Operation

- Can be divided into three main methods:
  - Packet filters (see last topic)
  - Application gateways
  - Packet inspection

- Individual vendors of firewalls may provide additional features
  - You should look at their products for details

Application Gateways

- Application-layer firewalls can understand the traffic flowing through them and allow or deny traffic based on the content
- Host-based firewalls designed to block objectionable Web content based on keywords are a form of application-layer firewall
- Application-layer firewalls can inspect packets bound for an internal Web server to ensure the request isn’t really an attack in disguise

Advantages of Application Gateways

- Provide a buffer from port scans and application attacks
  - if an attacker finds a vulnerability in an application, the attacker would have to compromise the application/proxy firewall before attacking devices behind the firewall

- Can be patched quickly in the event of a vulnerability being discovered
  - This may not be true for patching all the internal devices

Disadvantages

- Needs to know how to handle traffic to and from your specific application
  - If you have an application that's unique, your application layer firewall may not be able to support it without making some significant modifications
- Application firewalls are generally much slower than packet-filtering or packet-inspection firewalls
  - They run applications, maintain state for both the client and server, and also perform inspection of traffic

Packet Inspection Firewalls

- Examine the session information between devices:
  - Protocol
  - New or existing connection
  - Source IP address
  - Destination IP address
  - Port numbers
  - IP checksum
  - Sequence numbers
  - Application-specific information

Outbound Internet Traffic

- Client initiates connection to IP address of the web server destined for port 80 (HTTP)
- Firewall determines whether that packet is allowed through the firewall based on the current rule-set
- Firewall looks into the data portion of the IP packet and determine whether it is legitimate HTTP traffic
- If all the requirements are met, a flow entry is created in the firewall based on the session information, and that packet is allowed to pass

Inbound Internet Traffic

- Web server receives the packet and responds
- Return traffic is received by the firewall
- Firewall determines if return traffic is allowed by comparing the session information with the information contained in the local translation table
- If return traffic matches the previous requirements, payload is inspected to validate appropriate HTTP
- Then it is forwarded to the client

Advantages

- Generally much faster than application firewalls
  - They are not required to host client applications
- Most of the packet-inspection firewalls today also offer ***deep-packet inspection***
  - The firewall can dig into the data portion of the packet and also:
  - Match on protocol compliance
  - Scan for viruses
  - Still operate very quickly

Disadvantages

- Open to certain denial-of-service attacks

- These can be used to fill the connection tables with illegitimate connections

Bringing British Education to You

www.nccedu.com

Network Security and Cryptography

Topic 9 – Lecture 2:

Firewall Architecture

Firewall Architecture

- Firewalls are used to protect the perimeter of a network and the perimeter of sections of networks
- A key question for a network administrator is where firewalls should be located
- The positioning of firewalls in relation to other network elements is the firewall architecture
- We will only look at the position of firewalls and the consequences of this
  - Other security devices should also be used

Firewall Architecture

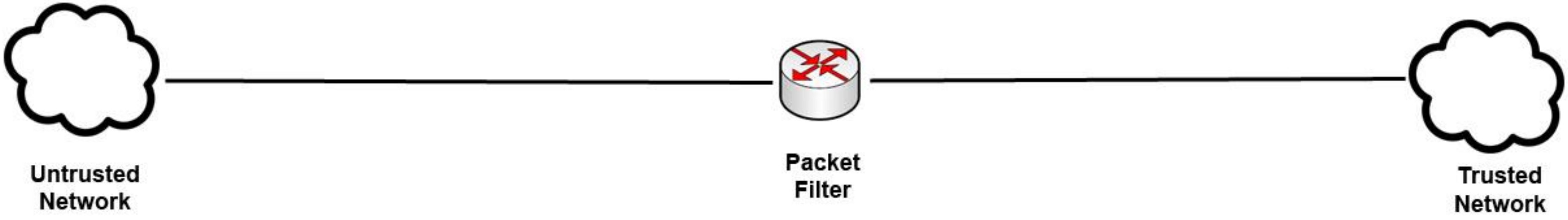
- The following are common firewall architectures:
  - Screening router
  - Screened host
  - Dual homed host
  - Screened subnet
  - Screened subnet with multiple DMZs
  - Dual firewall

Screening Router

- Simplest of firewall architectures
- Traffic is screened by a router
  - Packet filtering
  - Using ACLs
- Traffic is screened according to:
  - Source or destination IP address
  - Transport layer protocol
  - Services requested

Screening Router

- Usually deployed at the perimeter of the network
- May be used to control access to a Demilitarized Zone (DMZ) – see later
- More often used in conjunction with other firewall technologies



Advantages & Disadvantages

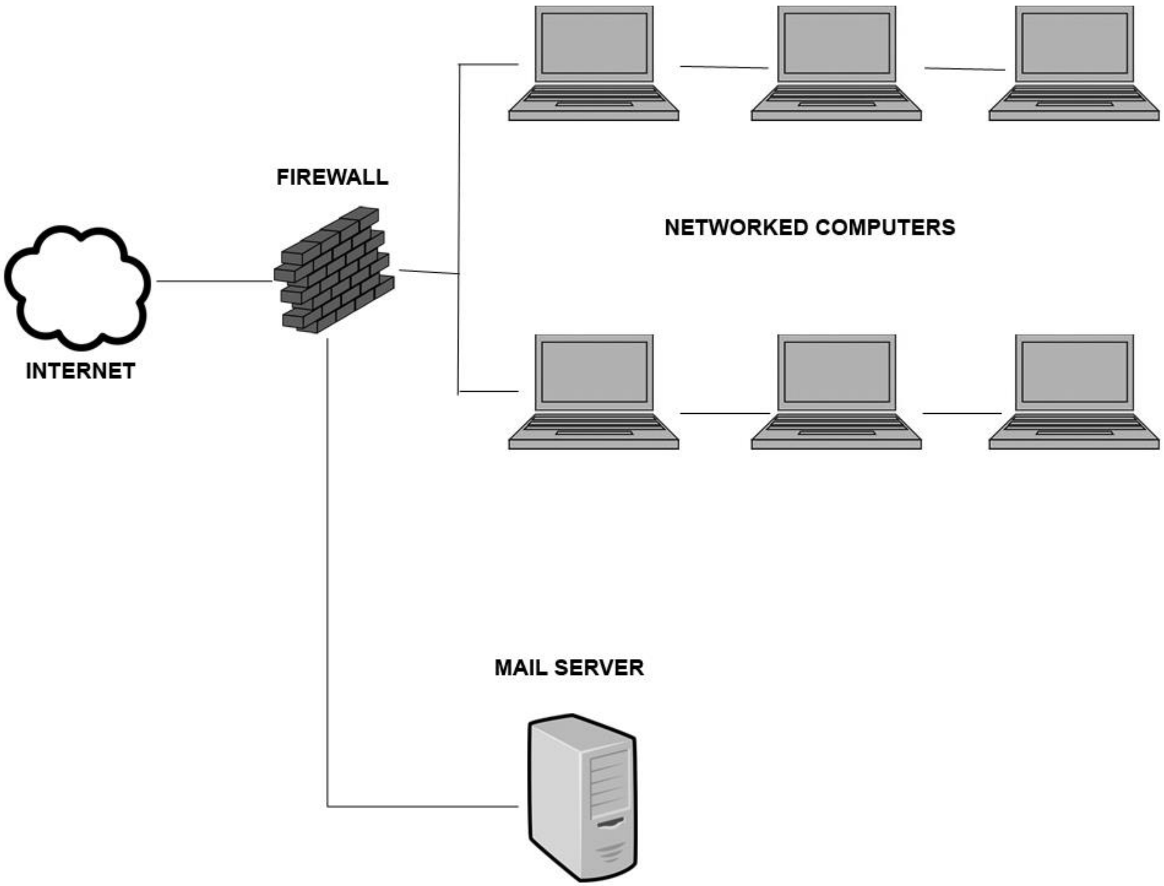
- Advantages
  - Simple
  - Cheap

- Disadvantages
  - No logging
  - No user authentication
  - Difficult to hide internal network structure

Demilitarised Zones (DMZ)

- A DMZ is part of the internal network but separated from the rest of the internal network
- Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall
- This traffic has firewall protection policies applied
- Common to put public-facing servers on the DMZ:
    - Web servers
    - Email servers

Demilitarised Zones (DMZ)

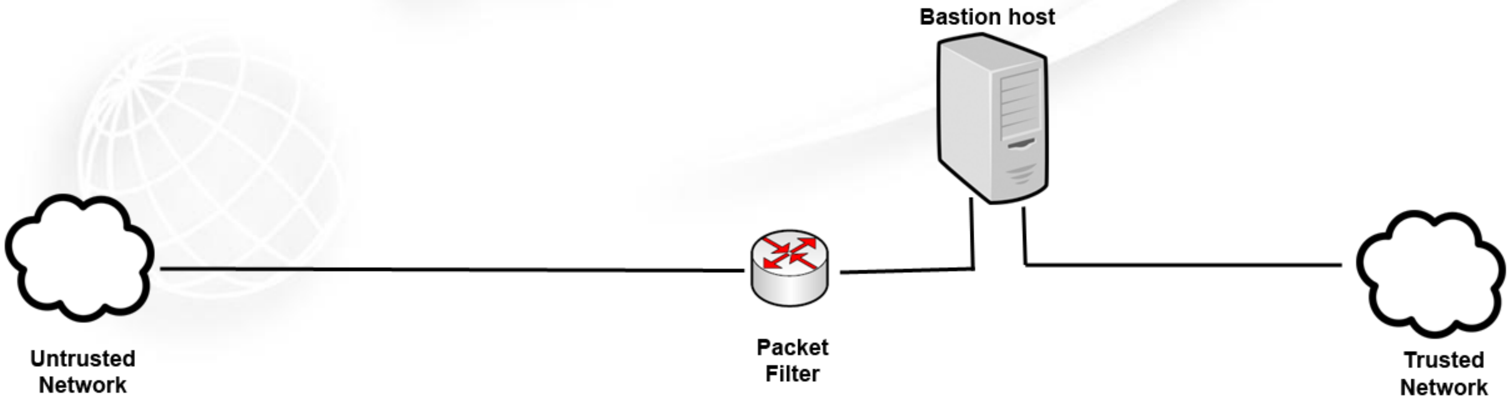


Screened Host Firewall

- Adds an extra layer of protection in comparison to a screening router
- Has a Bastion Host/Firewall between networks
- Bastion Host/Firewall has two NICs
- Bastion Host/Firewall connects the trusted network to the untrusted network
    - Stateful and proxy technologies are used to filter traffic up to the application layer

Bastion Host

- A special purpose computer specifically designed and configured to withstand attacks



- The router is the first line of defence
  - packet filtering/access control is carried out at the router
- The bastion host is the server that connects to the unsecure network through the router

Advantages & Disadvantages

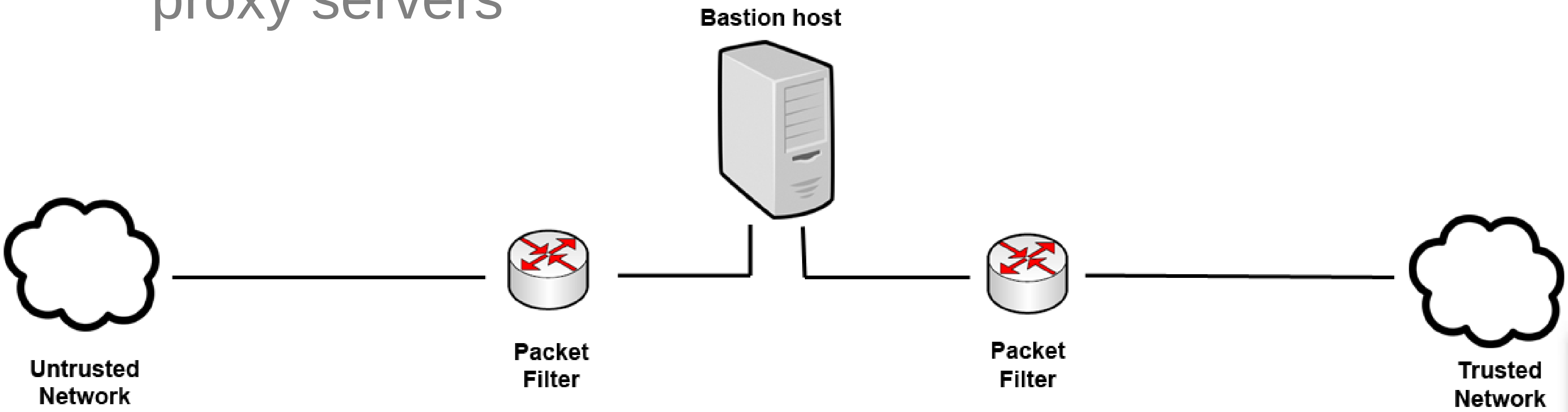
- Advantages
  - Security is distributed between two points
  - Greater security than screening router
  - Transparent outbound access/restricted inbound access
- Disadvantages
  - Difficult to hide internal structure
  - There is a single point of failure in the network

Dual-Homed Host

- A Bastion Host/Firewall is surrounded with packet filtering routers
  - Dual-homed - outside world and protected network
  - Multi-homed - outside world and multiple protected networks
- Routers filter traffic to the Bastion Host
- Bastion Host adds additional filtering capabilities
- Bastion Host has no routing capabilities

Advantages & Disadvantages

- Advantages
  - Hides internal network structure
- Disadvantages
  - Requires users to log onto bastion host or the use of proxy servers

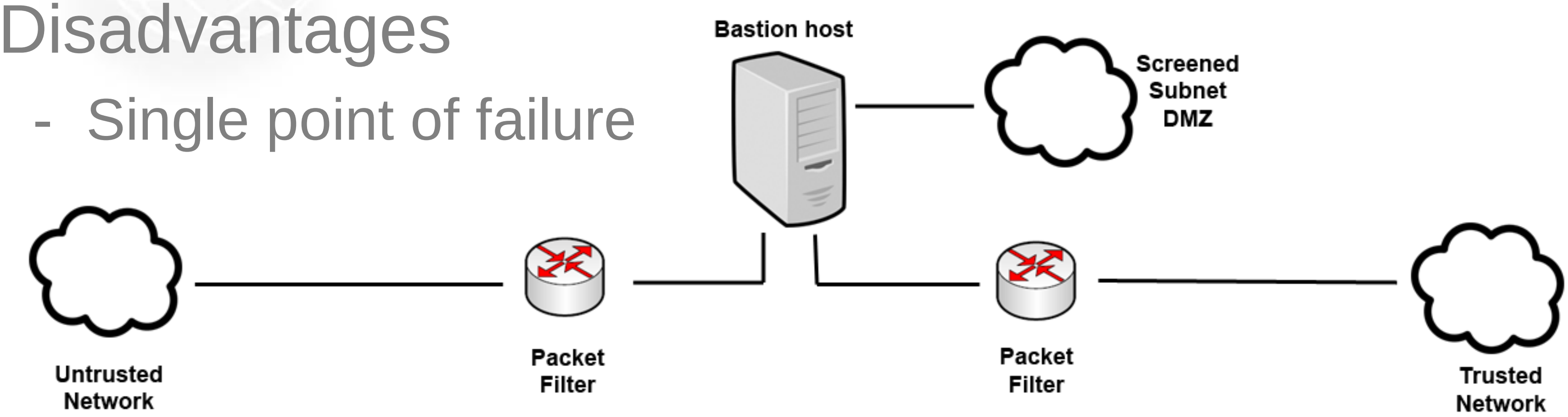


Screened Subnet DMZ

- Bastion Host is surrounded with packet filtering routers
- These control traffic into and out of the trusted and untrusted network sections
- Has an extra layer of functionality with a DMZ
- Traffic from DMZ to trusted network must go through Bastion Host and packet filtering router

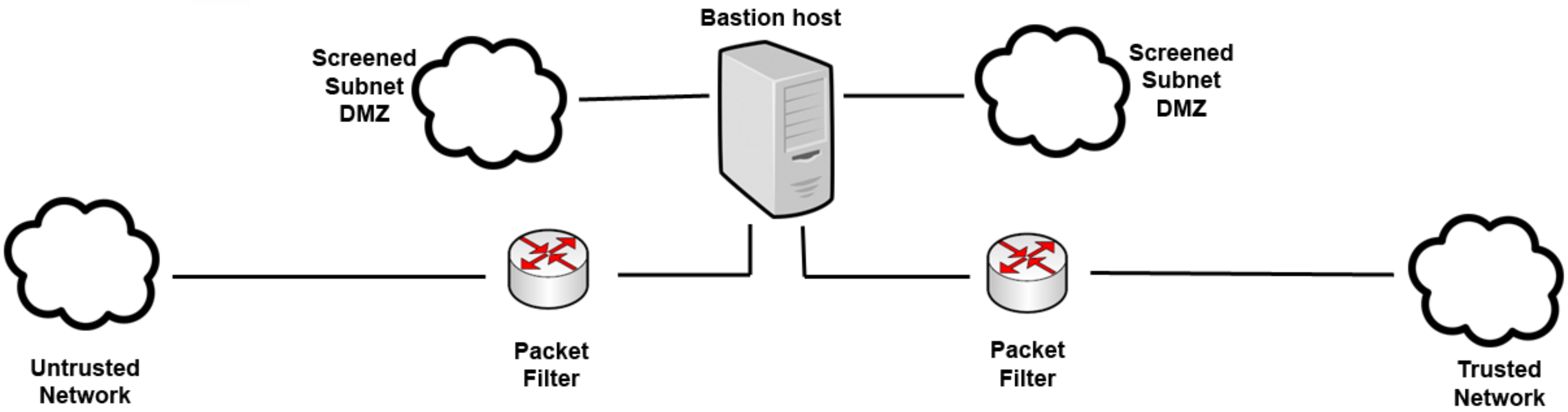
Advantages & Disadvantages

- Advantages
  - Provides services to outside without compromising inside
  - Internal network hidden
- Disadvantages
  - Single point of failure



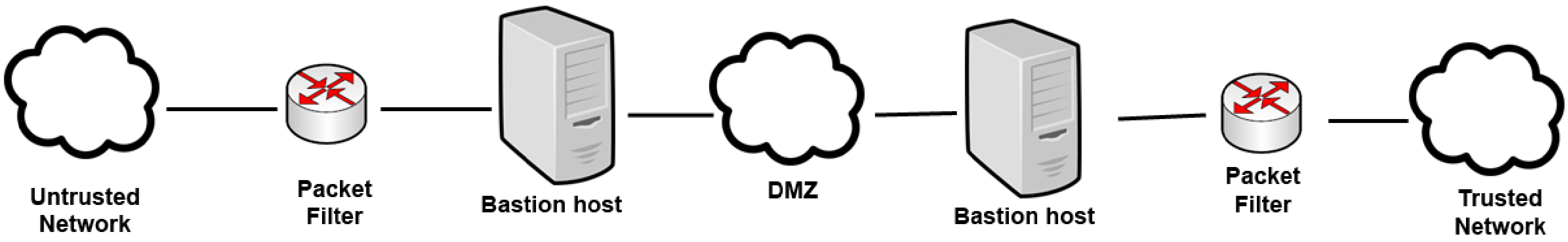
Screened Subnet Multiple DMZs

- Allows configuration of varying levels of security between:
  - DMZs and the untrusted network
  - Different DMZs
  - DMZs and the trusted network



Dual Firewall Architecture

- Using two or more firewalls enhances security
- Can be used to create DMZs
- Using technology from multiple vendors can enhance security



References

- Scambrey, J., McClure, S. and Kurtz, J. (2001). *Hacking Exposed: Network Security Secrets & Solutions, 2nd Edition*. McGraw Hill.
- Zwicky, E.D. (2000). *Building Internet Firewalls, 2nd Edition*. O'Reilly Media.

Topic 9 – Firewalls

Any Questions?

Bringing British
Education to You
www.nccedu.com