Computer Networks

Topic 9:

Firewalls

Computer Networks

Topic 9 – Lecture 1:

Functions of a Firewall

Scope and Coverage

This topic will cover:

- Functions of a firewall
- Types of firewall
- Installing and configuring a firewall

Learning Outcomes

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

- Describe the functions of a firewall
- Describe different types of firewall
- Install and configure a firewall on an Internet-connected system

What is a Firewall?

- In the industrial world, it is a solid wall that has been built to contain a fire
  - For example, an area of a chemical plant will have a firewall to contain any fire that may break out.
- In computing, a firewall is built to ***protect*** a network.
- The aim is to protect the network from malicious traffic.

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.

What Are The Rules?

- Each organisation has to decide on the level of security they require
  - There is no “one size fits all” solution
- Firewalls can be configured to allow or block traffic based upon rules.
- Software firewalls often come with a set of preconfigured options based upon the security level required.
- Can usually be configured rule by rule

What to Block

- 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.

Words, Phrases & Domain Names

- Lists of words and phrases that are not allowed can be used to block traffic
  - There can be problems when a legitimate word contains a blocked word within it.
- Similarly, lists of domain names can be used to block traffic
  - Could be a blocked list where access is prevented
  - Could be an allowed list and access is only allowed to domains on the list and nothing else

IP Addresses & Ports

- A firewall typically filters information by examining I.P. addresses and port information.
- The firewall can determine which ports and I.P. addresses are normal.
- It keeps a list of situations that are suspicious.
- If something looks suspicious, it will stop the flow of data.

Source & Destination IP Address - 1

- Some firewalls can filter traffic based on source or destination IP address.
- Enables you to allow or deny traffic based on the computers or networks that are sending or receiving the traffic
  - Can configure firewalls to block specific websites
  - Can allow/deny traffic based on the sending computer
  - Can disable a protocol on one set of computers and allow the same protocol on a different set of computers

Source & Destination IP Address - 2

- Allows you to give greater access to users on internal networks than those on external networks
  - Common to use a firewall to block all requests sent to an internal email server except those requests from users on the internal network
- Can also use ***source filtering*** to block all requests from a specific address
  - e.g. to block traffic from an IP address identified as having attacked the network

Protocols

- Firewalls can also filter traffic based on protocol
  - this option is not usually enabled by default.
- This allows an organisation to block all traffic of a particular type
  - A business might have a firewall block HTTP traffic to prevent employees from accessing the Internet while at work.
  - A business may block all FTP traffic to prevent files being uploaded or downloaded.

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 should have both.

Software Firewall

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

Router Firewall

- Protects your entire network or part of a network
- Located on your router
- Protects 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

Do You Need a Firewall?

- The answer is always YES
  - Unless you never connect to an outside network
- Firewalls are a critical part of Internet security.
- It is recommended that all computers have a software firewall.
- Firewalls can be found in all commercial Internet security suites.

Computer Networks

Topic 9 – Lecture 2:

Types of Firewall

Types of Firewall

- Can be divided into three main types:
  - ***Packet filters***
  - ***Application gateways***
  - ***Packet inspection***
- Individual vendors of firewalls may provide additional features
  - You should look at their products for details

What do Packet Filters Examine?

- Packet-filtering firewalls validate individual packets based on:
  - Protocol
  - Source and/or destination IP address
  - Source and/or destination port numbers
  - Time range
  - Type of service (ToS)
  - Various other parameters within the IP header

Access Control Lists

- Packet filtering is generally accomplished using Access Control Lists (ACL) on routers or switches.

- Normally very fast
  - Traffic enters or exits an interface
  - ACLs are used to match selected criteria
  - Either permit or deny individual packets

Advantages of Packet Filters

- Big advantage is that they are present in many networked devices
- Packet-filtering firewalls are located in:
  - Routers
  - Switches
  - Wireless access points
- Routers have the capability to control the flow of packets through the use of ACLs

Does My Network Use Packet Filters?

- Almost certainly (or it should!)
- These devices do not have lots of features.
- But when you need to quickly implement a security policy, this may be the quickest solution to deploy:
  - to mitigate an attack
  - protect against infected devices
  - etc.

Problems With Packet Filters

- Packet filtering can be circumvented in a number of ways including:
  - Misrepresenting traffic using well-known port numbers
  - Tunnelling traffic unsuspectingly within traffic allowed by the ACL rules
- It was quickly discovered that peer-to-peer sharing applications could use port 80 (HTTP) to gain access through the firewall.

Using Packet Filters

- Packet filters alone are insufficient
- Multiple devices can provide defence in depth
- Packet filtering is best used on the outer edge of your network
- Can prevent spoofed traffic and private IP addresses from entering or exiting your network

The OSI Application Layer

- Application Gateways, or Application Layer Firewalls, work at the application layer of the OSI model.
- Layer 7, the application layer
  - It is the user interface to your computer (the programs), for example, word processor, email application, telnet, and so on.
- We include “proxies” in this category of firewalls.

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.

Proxies

- A proxy device may be dedicated hardware (e.g. a server) or software.
- Acts as a firewall by responding to input packets (connection requests, for example) in the manner of an application, whilst blocking other packets
- Make tampering with an internal system from the external network more difficult
- Act on behalf of a client so they provide an additional buffer to the network

Advantages

- 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 proxy 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 determines 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.

Network Address Translation (NAT)

- Firewalls often have NAT functionality
- Hosts behind a firewall commonly have addresses in a private address range.
- Hides the true address of protected hosts
- Hiding the addresses of protected devices is a defence against network reconnaissance.

Computer Networks

Topic 9 – Lecture 3:

Installing and Configuring a Firewall

Planning the Firewall

- A number of factors must be considered before purchasing and installing a firewall or firewalls:
  - Firewall policy
  - Risk analysis
  - Identifying requirements
  - Creating rules
  - Managing the firewall

Firewall Policy

- Defines how an organisation's firewalls should handle inbound and outbound network traffic, based on the organisation's information security policies, for:
  - Specific IP addresses
  - IP address ranges
  - Protocols
  - Applications
  - Content types

Risk Analysis

- Organisations should conduct risk analysis to develop a list of:
  - The types of traffic needed by the organisation
  - How they must be secured
  - Which types of traffic and under what circumstances
- All inbound and outbound traffic not expressly permitted should be blocked.
- This reduces the risk of attack and can decrease the volume of traffic on the network.

Identifying Requirements

- Which network areas need to be protected?
- Which firewall technologies will be most effective for the types of traffic that require protection?
- Integrating the firewall into existing network and security infrastructures
- Requirements relating to physical environment and personnel
- Consideration of possible future needs

Creating Rules

- Implement the firewall policy and support firewall performance
- Rulesets should be as specific as possible with regards to the network traffic they control:
  - Types of traffic
  - Protocols
- The details of creating rulesets vary widely by type of firewall and specific products.

Managing the Firewall

- Policy rules need to be updated as the organisation's requirements change.
- Firewall performance needs to be monitored.
- Logs and alerts should also be continuously monitored to identify threats.
- Rulesets and policies should be managed by a formal change management control process.
- Firewall software should be patched as vendors provide updates to address vulnerabilities.

Small Networks

- Firewalls at a network's perimeter provide some measure of protection for internal hosts.
- Network firewalls are not able to recognise all forms of attack, some reach internal hosts.
- Attacks sent from one internal host to another may not even pass through a network firewall.
- Network designers include firewall functionality at places other than the network perimeter to provide an additional layer of security.

Host Based Firewalls - 1

- Firewalls for servers and personal firewalls for desktop and laptop computers
- Provide an additional layer of security
- Software-based, residing on the hosts they are protecting
- Monitor and control the incoming and outgoing network traffic for a single host

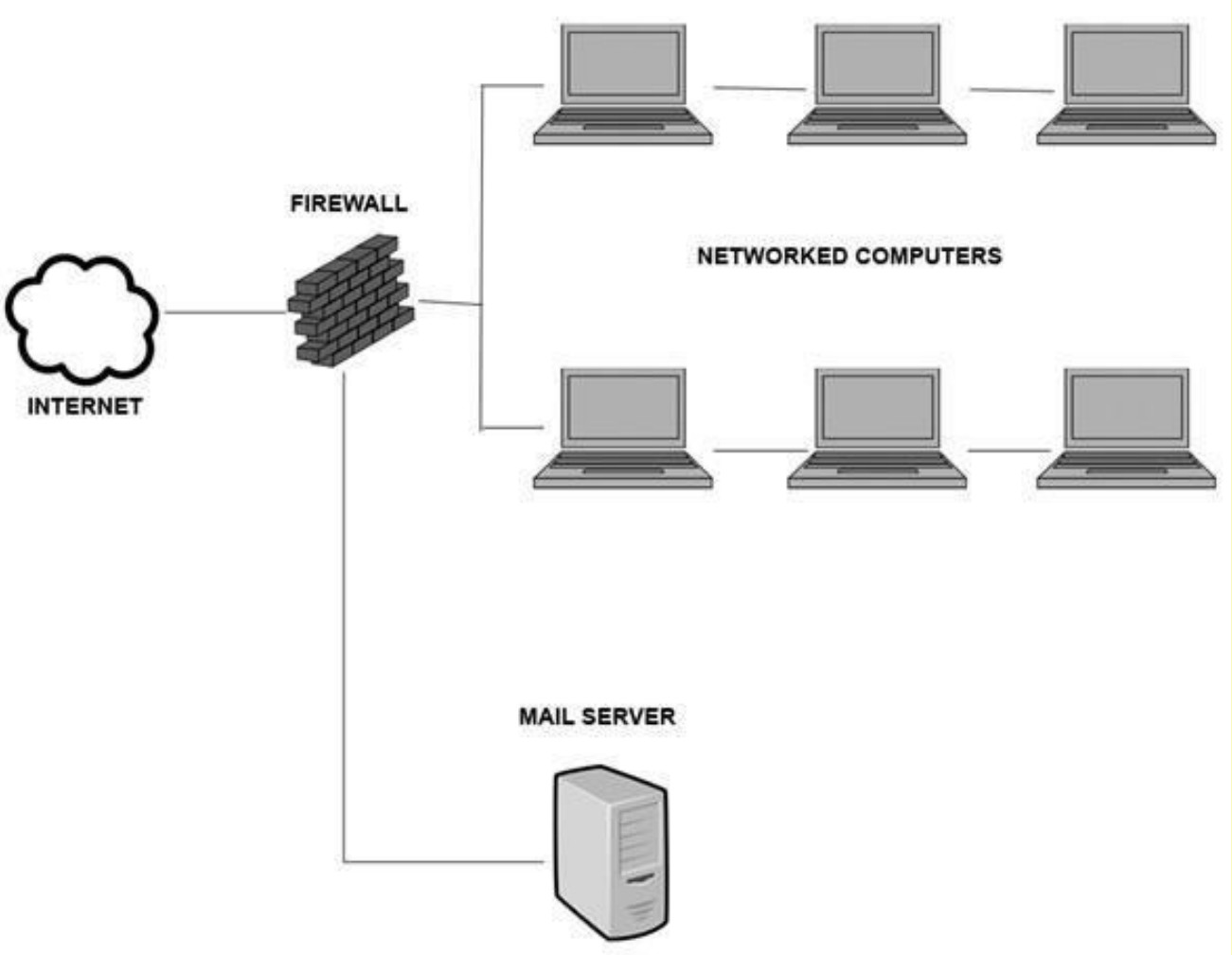
Host Based Firewalls - 2

- May come with OS
- Can be installed as third-party add-on
- Perform logging
- Can be configured to perform address-based and application-based access controls
- Can also act as intrusion prevention systems that detect an attack in progress and take action to prevent damage to the targeted host

Demilitarised Zones (DMZ) - 1

- 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) - 2



Multiple Firewall Layers

- Firewalls should be at the edge of a logical network boundary.
- A network administrator may wish to have additional boundaries within the network.
- Can deploy additional firewalls to establish such boundaries
- The use of multiple layers of firewalls is quite common to provide defence-in-depth.

Many Layers of Trust

- Internal users may have varying levels of trust
  - Accounting databases may only allow access by members of the accounting department
  - Many organisations deploy specific wireless access points within their networks for visitor use

- Have one firewall at the edge of the network and another at the edge of the internal network that has extra protection

Problems with Multiple Layers

- Increased difficulty in tracing firewall problems

- Multiple layers of application/proxy gateways is problematic as each can change a message, which makes debugging even more difficult.

Planning and Implementation

The lifecycle is:

1. Plan
2. Configure
3. Test
4. Deploy
5. Manage

Plan

- Should consider:
  - Security Capabilities
  - Management
  - Performance
  - Integration
  - Physical Environment
  - Personnel
  - Future Needs

Configure

- This includes:
  - Installing hardware
  - Installing software
  - Configuring policies
  - Configuring logging and alerting
  - Integrating the firewall into the network architecture
- The details of creating a ruleset vary by type of firewall and specific products.

Test

- A number of features should be tested:
  - Connectivity
  - Ruleset
  - Application compatibility
  - Management
  - Logging
  - Performance
  - Interoperability
  - Any additional features

Deploy

- Administrators should notify users of the planned deployment
- Involves integrating the firewall with other network elements
- Has to be integrated into the routing structure
- Can mean changing the routing tables for other routers in the network
- If elements in the network use dynamic routing, they may need to have their configuration modified

Manage

- The longest lasting phase
- Managing the solution involves maintaining:
  - Firewall architecture
  - Policies
  - Software
  - Other components of the solution
- Review the firewall policy at regular intervals

References

- Price B. (ed) (2003). *Networking Complete,* 3rd edition, Sybex.
- Tanenbaum, A.S. & Weatherall, D.J. (2010). *Computer .Networks,* 5th edition, Pearson Education.

Topic 9 – Firewalls

Any Questions?