Computer Network Security

Lesson 12

Intrusion Prevention Systems

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 11

- The two IDS types are host-based (HIDS) and network-based (NIDS)
- IDS are categorized according to the method of detection used. There are four categories – anomaly based, signature based, rules based and heuristic.
- An IDS policy needs to be setup by an organization that will capture the parameters associated with the use of the IDS.

Content

- Introduction to Intrusion Prevention Systems
- Firewall Characteristics
- Firewall Types
- Firewall Configurations
- Intrusion Prevention Systems (IPS)
- Comparison of IDS, IPS and Firewalls

Part 1

Introduction to Intrusion Prevention Systems

Introduction

- In lesson 11 we learnt about intrusion detection systems and their functionalities.
- One of the key weaknesses of all IDS is that whereas they are able to detect attacks they are not equipped to prevent them. What happens once the alarm is triggered?
- Well the administrator must take a series of steps in order to contain the attack right?
- This essentially takes up quite some time which the admin could utilize doing a lot of other things to optimize network performance for example.

Introduction

- This is where intrusion prevention systems, or better still, intrusion prevention comes in.
- Intrusion prevention systems are those systems designed to prevent attacks from taking place in the first instance.
- These systems do so by following rules that determine what should be allowed into the system (network or independent one) and what should not.
- It is not possible to discuss intrusion prevention without describing the role of firewalls in the network and how they protect an organization's internal network.
- Whereas they are not strictly IPS (a table of differences will be shared at the end of the lesson) they do play a big role in intrusion prevention; they are discussed first, followed by a discussion of intrusion prevention systems (IPS)

Part 2

Firewall Characteristics

Introduction

- Firewalls are normally used to protect an internal (secure) network from an external (insecure) network.
- As such they are placed between the internal and the external network; consequently all traffic coming in or going out must pass via the firewall.
- Further it is expected that the firewall is hardened; that is to say it has been made as invulnerable as possible.
- The most common network of communication nowadays is the Internet, and therefore firewalls are configured to monitor and prevent harmful packets from accessing the internal network based on some rules.
- There are a variety of reasons why the Internet is considered so insecure.

Introduction

- Some of these are:
- Lack of security features such as authentication by some of the applications found on the networks.
- Applications such as freeware which many users download to their devices do not contain sufficient security; even downloading them alone can pose a threat to an internal network.
- The challenges presented by hackers such as spoofing, DoS attacks, and so on.

Firewall Policy

- Just like the IDS policy a firewall should have a policy that clearly defines the type of traffic that the firewall will permit and what it will block.
- Just like the IPSec policy we developed this policy will be broad in terms of what data the organization will support, then go into the finer details.
- An example of what a firewall policy can adapt in filtering traffic is provided by Scar (2009) and adopted by Stallings and Brown (2015).
- These are IP address and protocol values, application protocols, user identity, and network activity.

Firewall Capabilities

- Since the firewall is the single point of entry (and departure) to the network it presents an opportunity for easier management since it is focused on a single system.
- The firewall's purpose is to observe activities and therefore it can be audited and alarms set up on it (like the IDS).
- It provides a platform for other functions that may be of interest to the organization (not necessarily security related) for example logging of Internet activity by staff (users).
- Can be used to implement VPNs through IPSec.

Firewall Limitations

- Firewalls are not without their limitations, which are centered around their functionality or lack thereof.
- They can only prevent against attacks that pass through them; if an organization has other ways for internal network to communicate with external network then the firewall is useless.
- It does not protect against insider threats (unhappy employees or employees working in cahoots with outsiders)
- The challenge of bring your own device (BYOD) where an employee can access the internal network after their device has been infected by an external network.
- To add on to this the same can be said of insecure WLANs; they can be accessed from the outside rendering the firewall useless.

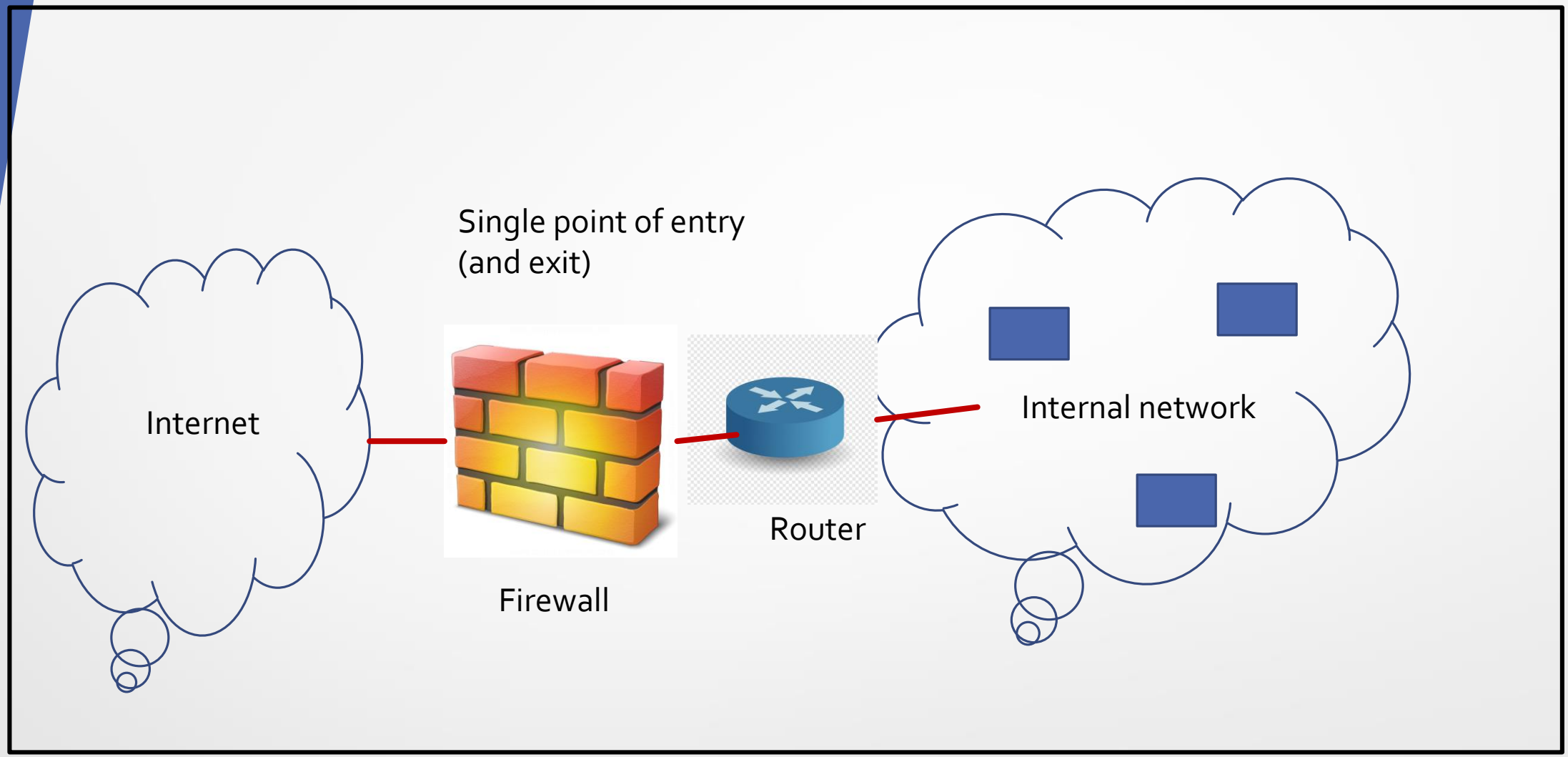


Fig 1. Simple firewall setup

Simple Firewall Setup

- Fig 1 illustrates the concept of a simple firewall setup
- In the figure the firewall is configured to be the single point of entry to the internal network.
- The router is configured to be behind the firewall.
- All data being received from the internet or any external network for that matter, is vetoed by the firewall and then allowed to proceed (or rejected).

Part 3

Firewall Types

Introduction

- Firewalls come in different types based on the functionality they specifically provide.
- The functionality, however, at the end of the day is the same; only allow desired traffic to pass. It is like taking a journey to a given destination; you can choose to go by air, bus, or train depending on your specific needs or circumstances (some people can't stand air travel while others can't stand sea travel)
- There are two broad classifications of firewalls: application gateways (also known as proxy gateways) and packet filters.

Application Gateways

- These are also known as proxy gateways. From the 2 terms it might be easy to guess that they work at the application layer of the OSI model and they present themselves as proxies for the actual user in the internal network.
- A user will contact the gateway via a TCP/IP application requesting to access an application beyond it (such as ftp or http). The gateway will then ask the user to authenticate himself; if the credentials are okay the gateway will then contact the application and pass the data from the user to it.
- If the application is not supported then communication will not be allowed; further the proxy can be configured to only allow certain features of the application while not allowing others.
- Fig 2 demonstrates the position of the proxy gateway and how the communication is vetoed at layer 7 (application layer) of the OSI model.

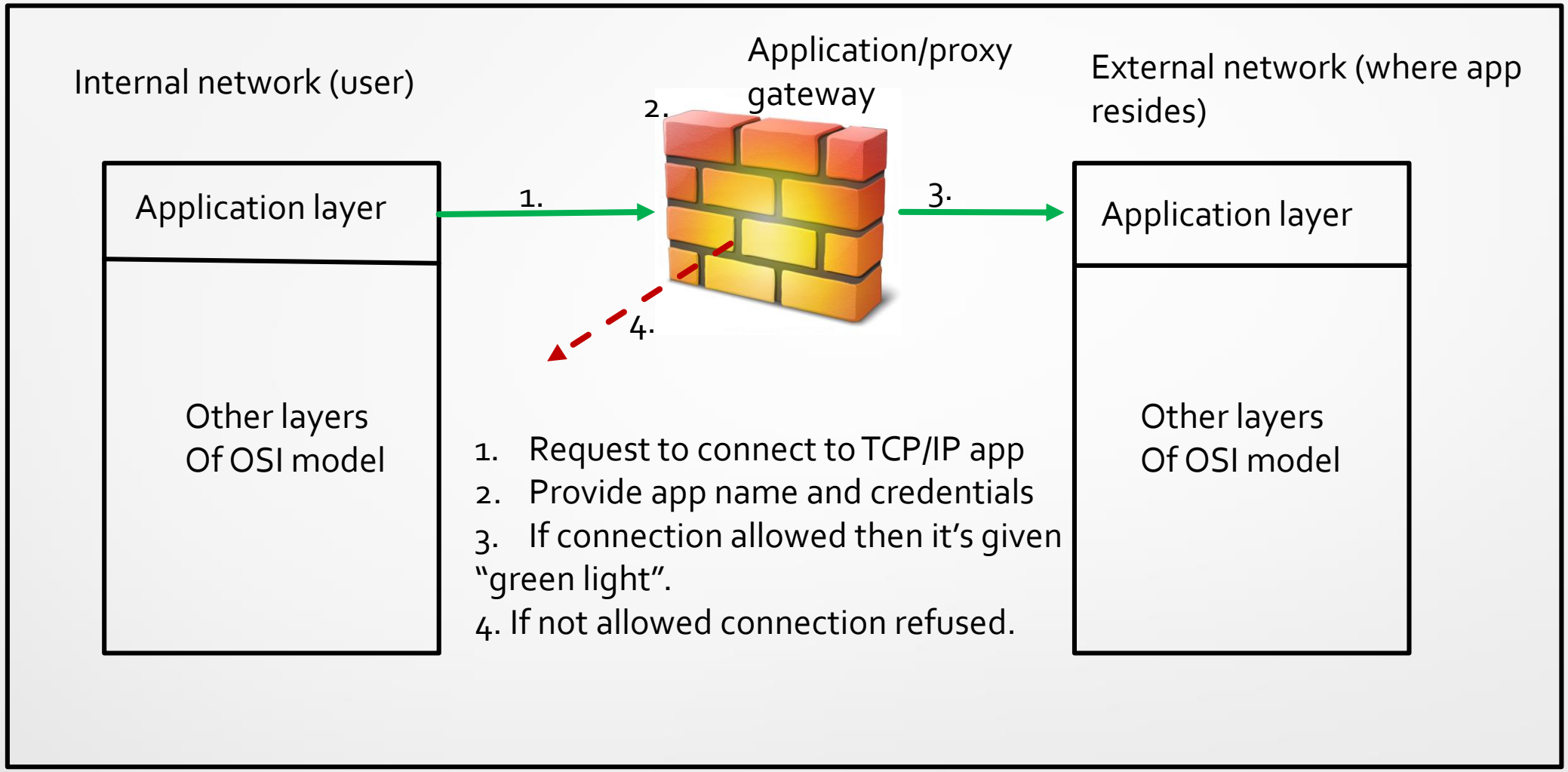


Fig 2. Application (proxy) gateway

Application (Proxy) Gateway

- Application proxies are usually transparent to the network; this means that they do not have any IP address of their own. Most times they masquerade as a server.
- This type of gateway has the advantage of protecting internal client from external clients.
- They do this by terminating connections from clients and taking them over. When a client is communicating with an external network the proxy will take the packet and give it a new address (it's own) before sending it on to the application.
- When a response is received it is sent to the proxy, which will then tear down the connection, place the right address on the packet and send it to the client.
- This protects the client since external applications will not be aware of the internal network and its clients.
- This is demonstrated in Fig 3.

Application (Proxy) Gateway

- It is worthy to note that a proxy is written for each supported application.
- This means that one has to get a proxy from a vendor that supports that particular application.
- The downside to this happens when the application is upgraded; this means that you are at the mercy of the vendor to get the upgrade to you so that the firewall can continue functioning as it should!
- As earlier described they are usually transparent in the network.

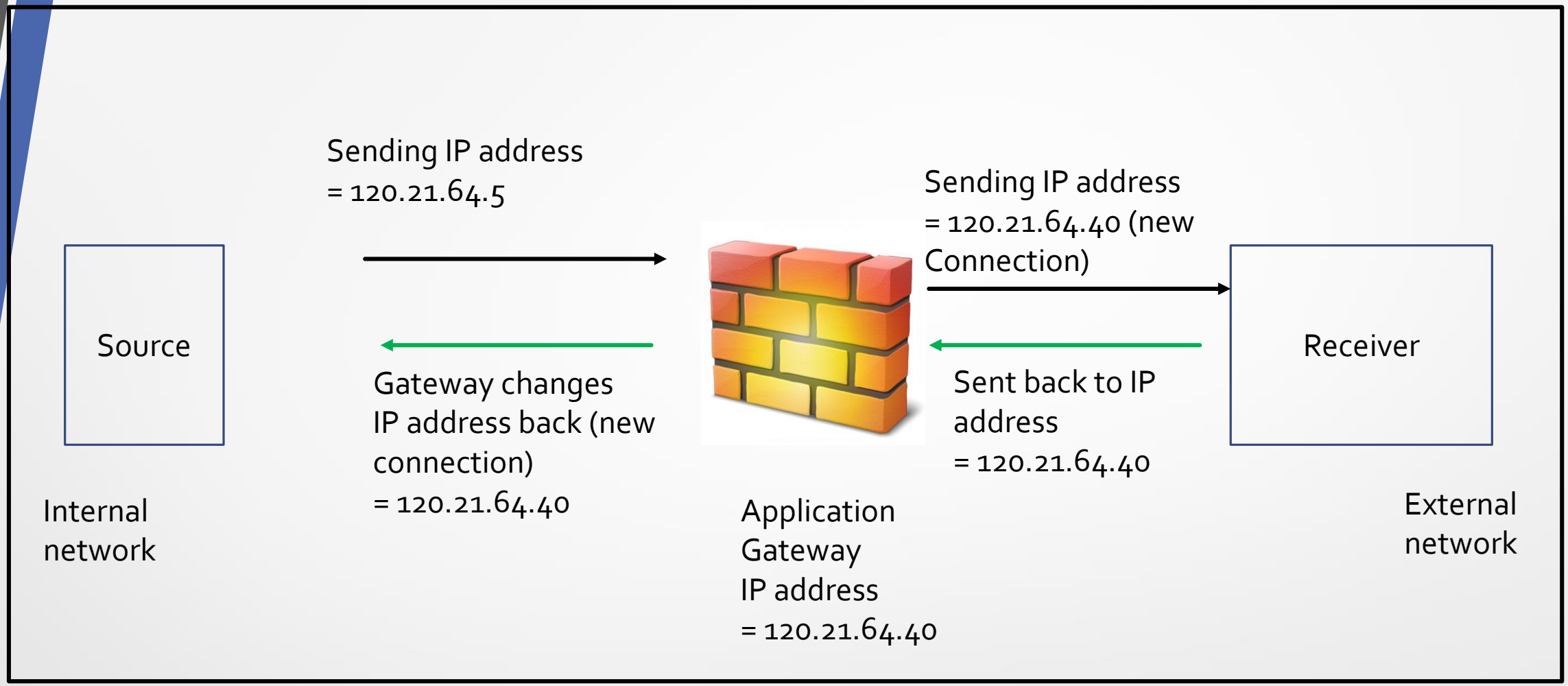


Fig 3. IP address takeover by application (proxy) gateway

Circuit-level Gateway

- This type of gateway operates using the same principle as an application level gateway.
- It will take packets from the sender then tear down the connection; it will then establish the connection with recipient and communicate directly with them as if they were the original sender.
- Once the packets are received they perform the reverse process in sending the packet back to the original sender.
- The difference occurs in where the OSI model the filtering occurs. Circuit level gateways operate at the circuit level (transport layer).
- Connectivity rules are checked at this layer. The issue is that the gateway trusts the internal network and thus there is no need to filter contents.
- Circuit level gateways do not perform any content filtering and thus require less processing compared to application level gateways.
- They can be incorporated within an application level gateway or as standalones.

Application (Proxy) Gateway

- Application gateways offer certain distinct advantages over other types of firewalls:
- They are more secure due to the fact that they only deal with certain applications; this in fact hardens them.
- Logging and auditing of traffic at layer 7 is much easier.
- They offer more control in determining which applications to allow in or out (and vice versa).
- Reverse proxies (which check outgoing packets) can help in checking the contents of outgoing packets for security reasons (they are able to do content filtering unlike the circuit level gateways).

Application (Proxy) Gateway

- Disadvantages of application gateways include:
- Since they have to break down connections and create new ones they tend to slow down network performance.
- Updating issues. As the proxy is written for specific application then you have to wait for updates from the vendor when they occur; it is not possible to do any updates on your own since they are written in the OS of the gateway.
- Customizing the gateway to suit you is a challenge (depending on the vendor)

Packet Filter

- A packet filter is a router that will apply some specific rules to determine whether to allow a packet through or not.
- Most routers are configured with default rules, meaning that there is a course of action for it to take if the admin has not configured any.
- The default is to either accept the packet or discard the packet.
- The rules are defined for both incoming and outgoing packets.
- The rules are based on source and destination addresses or ports, or type of protocol.
- The rules are applied to each incoming and outgoing packet.

Packet Filter

- The sequence of events in a packet filter can be easily demonstrated in a series of steps:
- Step 1: Packet arrives at the filter
- Step 2: Examine packet source and destination address, as well as source and destination port.
- Step 3: Apply the rules to the packet.
- Step 4: If a match is found, apply the rules as described (accept or reject the packet).
- Step 5: If no match or if no rules have been set apply the default (which again can be either to accept or reject the packet).
- It is good practice to have the default as to reject the packet…this will protect the network better.

Packet Filter

- When the rules are written down properly packet filtering is a very effective way of vetoing packets at the filter.
- As a way of demonstration supposing I do not wish my internal clients to use the ftp port; all I would need to do is to block packets destined for port number 20 (this is the port that establishes ftp connections). And to make it even more pronounced I would also block port 21 (used for ftp data exchange).
- Similarly I can also block packets destined to a particular IP address, say **128.116.114.3** which is the IP address of roblox the popular gaming site ..ha ha ha, now my users can't play games during office hours.
- One can similarly block packets from reaching internal IP addresses in a similar manner.

Packet Filter

- Advantages:
- They should be deployed at the organization's perimeter where they are found to be very effective.
- They are very fast and won't slow the network down in any way.
- They allow for quick setup and implementation; once the rules are known they can be quickly configured on the router and implementation is immediate.
- Disadvantages:
- Since they only perform packet inspection they are less secure compared to other firewall designs.
- They have limitations on the use of ports.

Stateful Inspection

- These types of filters are also called dynamic filters.
- They determine whether to accept a packet or not based on the current state of the network; that is to say they are adaptable.
- This means that they could for example allow certain packets into the network based on responses from other packets (like from a particular IP address).
- These types of filters are very popular and for obvious reasons too; recall that packet filters have a fixed set of rules which have been written right?

Stateful Inspection

- Let us examine some of these popular features:
- An OS built specifically for firewall purposes and nothing else makes it robust.
- Stateful packet filtering is provided via a connection table that ensures only the right vetoed traffic passes through.
- Websites can be blocked using this firewall (also known as URL filtering)
- It can block both java applets and active X.
- Better security through network address translation (NAT) and port address translation (PAT).
- VPN capabilities
- Stateful inspection firewalls also have intrusion detection functionality.

Stateful Inspection

- They can act as either DHCP clients or servers.
- They support several routing protocols and algorithms.
- They have failover in place.

Stateful Inspection

- Advantages:
- They offer the best of packet filters and application gateways in terms of performance.
- They are accepted as the benchmark for protection in networking.

- Disadvantages:
- They are slower than packet filters
- Less overall control as their software is generic as opposed to packet filters which are written for specific applications.

Part 4

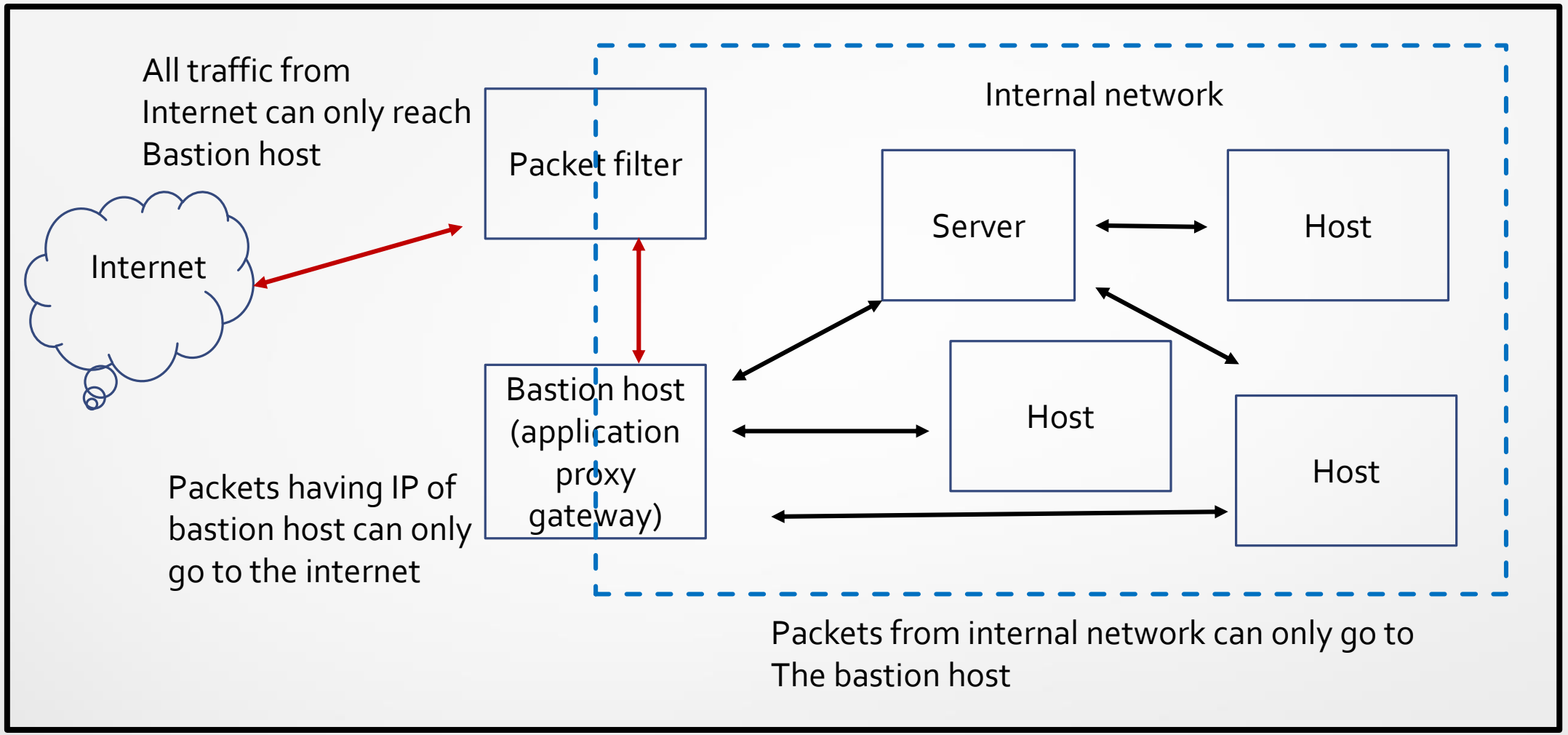
Firewall Configurations

Introduction

- Normally firewalls are configured as a combination of packet filters and application gateways. Three configurations are normally used:
- Screened host firewall – single homed bastion host
- Screened host firewall – dual homed bastion host
- Screened subnet firewall

Screened host firewall – single homed bastion host

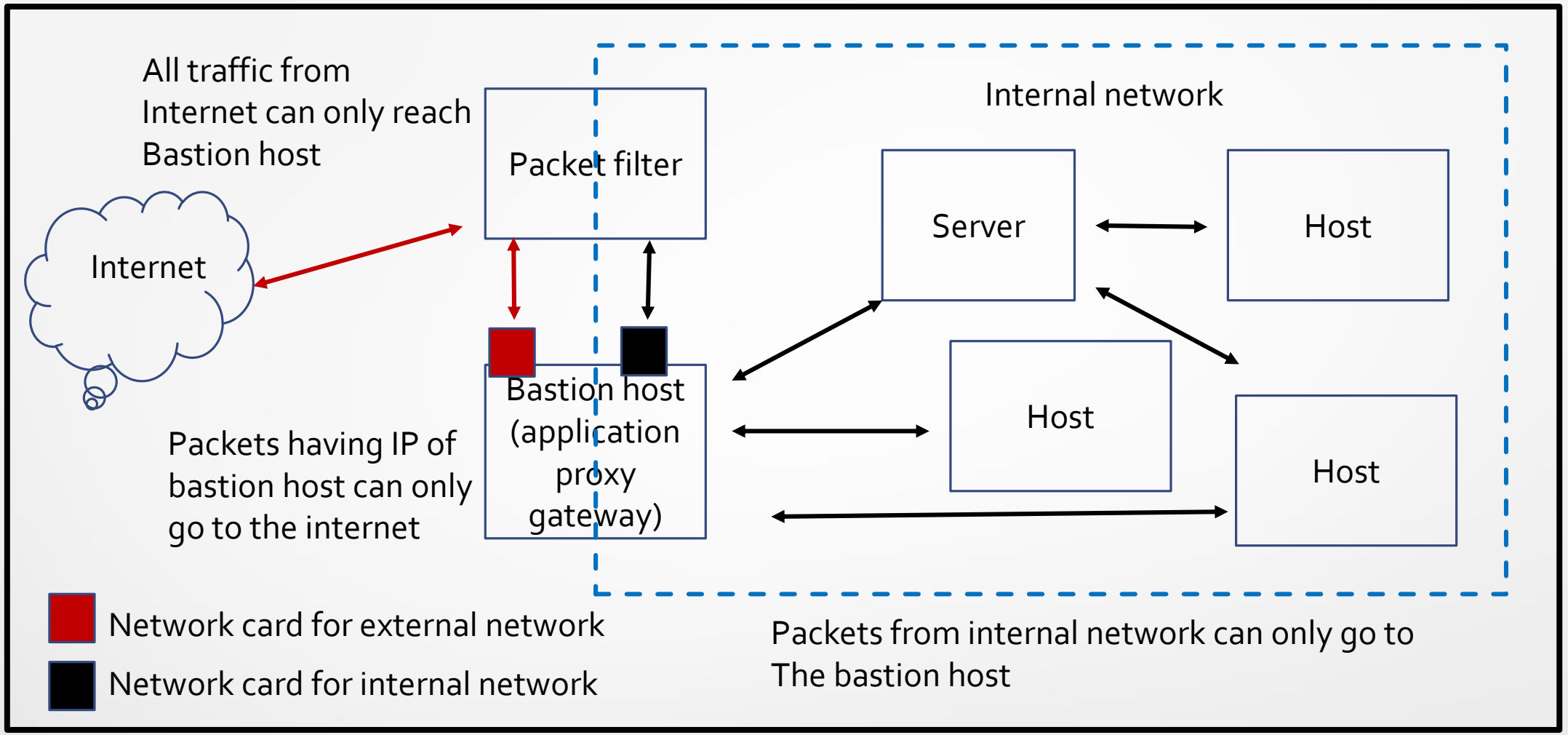
- This configuration makes use of a packet filter and a bastion host.
- A bastion host is normally a special purpose computer designed to repel attacks; it can be an application proxy (gateway) for example.
- In this configuration all traffic is configured to go through the bastion host; that is to say, all traffic from the internet can only reach the bastion host. Further no traffic from the internal network can go directly to the internet, it must originate from the bastion host. Consequently, packets having the IP of the bastion host can only go to the internet.
- Fig 4 easily demonstrates this configuration. As can be seen from the configuration if the packet filter gets compromised then the whole network is compromised. A way around this is to use a configuration that will not compromise the internal network.



- Fig 4. Screened host firewall – single homed bastion host configuration

Screened host firewall – dual homed bastion host

- This configuration overcomes the weakness of screened host firewall – single homed bastion host by alienating the internal network from the packet filter.
- This is done by configuring the bastion host with 2 network cards; one card connects to the packet filter while the other one connects to the internal network.
- By using such a configuration the internal network is protected from an attack should the packet filter fail; this is so since the internal network is invisible to an attacker since it is configured on another network card in the bastion host.
- Fig 5 shows the configuration of a screened host firewall – dual homed bastion host; it has been modified from fig 4.



- Fig 5. Screened host firewall – dual homed bastion host configuration

Screened subnet firewall

- This is the most secure configuration architecture.
- In this architecture a second packet filter is added between the bastion host and the internal network.
- This creates a network in-between the external network and the internal network (another subnet so to speak).
- The extra subnet makes it even harder for an attacker to penetrate the internal network since there is an extra network to pass through.
- Fig 6 demonstrates a screened subnet firewall configuration.

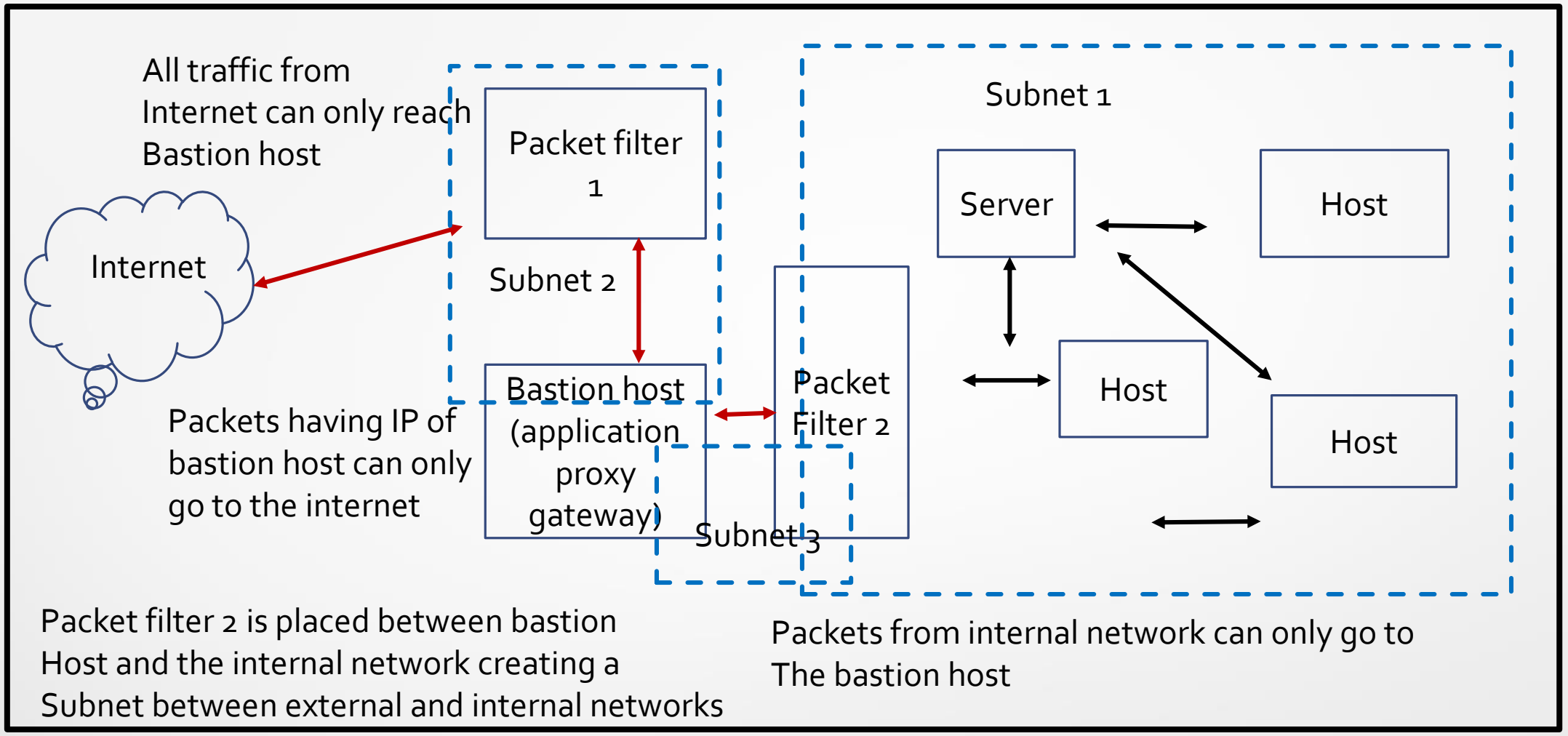


Fig 6 demonstrates a screened subnet firewall configuration

Part 4

Intrusion Prevention Systems

Introduction

- These systems are also known as intrusion detection and prevention systems (IDPS). There are four main types which build on the strengths of their respective IDS types.
- They are:
  - Host – based IPS
  - Network – based IPS
  - Distributed/Hybrid IPS

Host – based IPS (HIPS)

- They use either signature, anomaly or heuristic mode of detection as described in lesson 11.
- The functionality can be customized to specific platforms
- Further HIPS can also be designed to protect from application attacks.
- Due to the mode of detection of anomaly and signature, the HIPS uses its inbuilt rules or signatures for matching purposes. If it finds a match then it halts the attack and prevents it from executing.
- It is recommended to use HIPS as part of a larger strategy in a network environment that will include more protective devices such as firewalls.

Network – based IPS (NIPS)

- It uses the same detection modes like HIPS.
- They additionally use protocol analysis and traffic analysis to detect potential intrusions.
- Protocol analysis studies any deviations from normal standards defined for a given protocol.
- Traffic analysis studies any unusual traffic observed or any new services on the network.

Distributed/Hybrid IPS

- This uses the distributed approach defined earlier in lesson 11.
- The central console halts an prevents attacks based on detection received from the distributed NIDS
- Based on this it can halt or prevent an attack from taking place.
- This concept has been implemented in SNORT Inline (an IPS of snort IDS) and digital immune system.

Table of comparison

- Table 1 compares IDS, IPS and Firewalls
- Source: https://ipwithease.com/firewall-vs-ips-vs-ids/

PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	> Stateful packet filtering > permits and blocks traffic by port/protocol rules	> Anomaly based detection > Signature detection > Zero day attacks > Blocking the attack	> Anomaly based detection > Signature detection > Zero day attacks > Monitoring > Alarm

Table 1

Summary

- Just like the IDS policy a firewall should have a policy that clearly defines the type of traffic that the firewall will permit and what it will block.
- There are two broad classifications of firewalls: application gateways (also known as proxy gateways) and packet filters.
- Three standard firewall configurations that are used: screened host firewall – single homed bastion host, screened host firewall – dual homed bastion host and screened subnet firewall
- There are three types of intrusion prevention systems (IPS): Host – based IPS (HIPS), network – based IPS (NIPS) and distributed/Hybrid IPS

References

- Cantrell, C., Henmi, A., Lucas, M., & Singh, A. (2006). *Firewall policies and VPN configurations*. Syngress.
- Cole, E., Krutz, R. L., & Conley, J. W. (2005). *Network security bible*. Wiley Pub.
- Kahate, A. (2013). *Cryptography and network security*. McGraw Hill Education.
- Stallings, W., & Brown, L. (2015). *Computer security: Principles and practice*. Pearson.