6 System Security

Syllabus

At the end of this unit, you should be able to understand and comprehend the following syllabus topics ::

- IDS
- Firewall Design Principles
- Characteristics of Firewalls
- Types of Firewalls

6.1 Computer Intrusions and Intrusion Detection and Prevention Systems (IDS/IPS)

Note: Intrusion detection and Intrusion prevention system works in similar way. So, this topic is combined under one section. I would generally be referring to IDS, but it does mean that the modern and smarter systems could have possibly prevented the intrusion in the first place from occurring. Hence, when you read about IDS or IPS, think of them as similar but IPS to be slightly more powerful and effective against preventing intrusions!

Intrusion means to encroach (or to capture) a place. For example, suppose there is a vacant site and you manage to build a small hut there without seeking permission of the site owner that is precisely what intrusion is. You, as an individual, are trying to intrude on someone's property.

6.1.1 Introduction

- In digital terms, intrusion refers to the similar situation where the malicious code or attackers try to encroach (forcibly enter and capture) information systems without requiring permission of the system owner. An Intrusion Detection System (IDS) is defined as,

✍ ***Definition :*** *A software that helps to find out if a system is breached.*

Note : Breach is a word used in information security domain to describe any form of attack or unauthorized actions. You can use this word to mean anything that refers to the undesired actions and outcomes with respect to information security.

- So, in a nutshell, IDS can help you to find out if there were undesired actions or attacks carried out on your information systems. IDS works using various techniques as we will see later in this section. Note here that IDS does not help to prevent the attacks unlike anti-virus. It is only a system that can gather system information and find out if everything looks alright or not.

6.1.2 Need for IDS

IDS is one of the software-based security mechanisms that help to protect information system. At a high level, it is needed for the following reasons :

1. Defense in Depth

As you saw in the security architecture section, security is about minimizing the damage that can be possibly done. Defense in depth (or the layered approach) of security designing ensures that even if one of the controls is to fail, the overall security of the system would still be possibly healthy. IDS fulfill this need to bring an added layer of protection where any breaches or their possibilities can be identified quickly.

2. Automate intrusion detection

Imagine that you have a large set of machines, say 1,000 and more. How would you inspect each and every machine and find out if there were attacks or attempts to attack it? IDS helps you to automate this need and alert you when it detects any threat or likely a breach.

3. Corrective actions

Learning from threats or breaches that the IDS identifies, you can take corrective actions on your infrastructure design and could possibly strengthen its security. You might have some unprotected areas in your infrastructure that can be highlighted with the use of IDS.

6.1.3 Types of IDS

- Broadly speaking, IDS can be classified based on **what** it monitors and **how** it monitors.

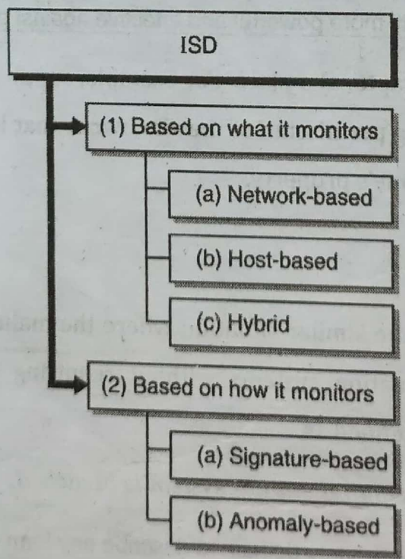


Fig. 6.1.1 : "Hybrid" to this diagram under "Host-based

1. Based on what it monitors

IDS can be classified into Network-based IDS (NIDS) and Host-based IDS (HIDS).

a. **Network-based IDS (NIDS) :** Network-based IDS evaluate intrusions from the networking side. They watch all network traffic as it reaches the various information systems.

If there are any alerting situations based on the network traffic analysis, it notifies the administrator to take the corrective actions. NIDS do not have visibility into what's actually going on within the information system. It can only watch and detect threats and breaches from the networking viewpoint.

b. **Host-based IDS (HIDS) :** Host-based IDS are typically installed on the individual information systems and then they watch for suspicious activities occurring on the system. A system entity such as system services and processes, system files, privileged user actions, downloads etc. are closely monitored to detect any undesired activities. HIDS do not have visibility into what's going on at the networking side of the system. It can only watch and detect activities with respect to individual machines only.

c. **Hybrid :** Hybrid IDS can monitor both host as well as network at the same time to give you best of both worlds. Hybrid models can typically correlate network activities with host activities and give you more meaningful insights into what's going on in your environment and protect you from intrusions.

2. Based on how it monitors

IDS can be classified into Signature-based and Anomaly-based.

a. **Signature-based :** Like banks and other organizations use human signature to validate requests and transactions, similarly Signature-based IDS has a pre-loaded database of various attack signatures (patterns of a possible attack). When it watches the activities, it constantly compares the activities' patterns with that in the database. If a match is found, it raises an alert. If you notice, there are 3 things to understand here:

- Signature based IDS can only detect attacks if it already and historically knows about an attack pattern.
- For new types of attack, signature-based IDS would not raise alerts.
- It is important for you to update the signature definitions time to time (like how you do in anti-virus system).

b. **Anomaly-based :** Anomaly typically means "deviation from routine". For example, if you wake up at 7 AM every day and one day you wake up at 4 AM that is an anomaly situation.

If I were to plot your wake-up time graph, 4 AM would show up away from your regular wake-up time. That 4 AM point on the graph is called outlier (or away from other samples). Similarly, the Anomaly-based IDS first establishes the baseline (common routine) of activities. It might take up to 2-3 weeks to "learn" what's right for a system. Once the learning phase is over, it would watch out for any activities that are not part of that baseline and raise alerts. If you notice, there are 3 things to understand here as well:

- It does not require signature and hence can possibly detect new attacks.
- It requires a learning period during which the system should have undergone all possible activities.
- If you plan to use the system for other purposes, you need to retrain the IDS.

6.1.4 Limitations and Challenges of IDS

1. Does not prevent attacks

As you understand, IDS can only detect and raise alerts when it finds a likelihood of a breach. It cannot prevent or block the breach from happening.

2. **High rate of false alerts (noise)**

IDS might generate a lot of false alerts. It could happen so for example, when there is a new traffic from a source that IDS has not seen before. You need to spend your resources to take a note of each alert and appropriately deal with it – either fix it or ignore it.

3. **Complex systems**

IDS systems are typically complex in nature and require regular administrative actions and tuning for adequate operations.

4. **Bypassing IDS**

Advanced attackers know what actions and activities a version and brand of IDS can detect and what not. They tune their activities to bypass such detection mechanisms and go undetected.

6.2 Firewalls

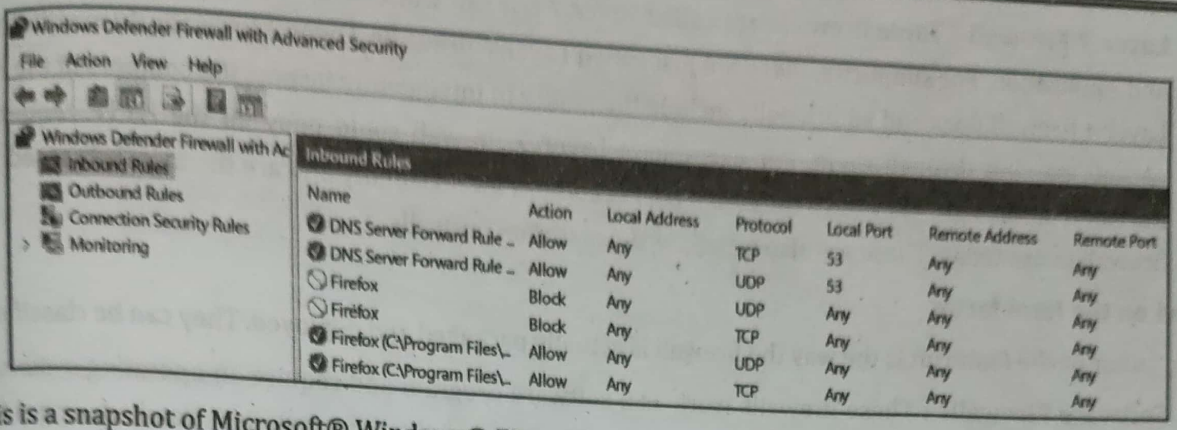
- Your computer is connected to the internet. How do you protect it from someone trying to access it over the internet? How do you prevent some rogue programs on your computer to send information to the attacker? Firewalls could be a mechanism.

✍ ***Definition :*** *Firewalls are network security systems that protect the computing resources on a trusted network from unauthorized access.*

- For example, you can access google.com website but not it's webserver's operating system. If you try connecting to the webserver except over the HTTP or HTTPS, the connection would be denied. That's what a firewall does at a high level.
- You need to define various rules, as per your security requirements, in the firewall and the firewall evaluates those rules before granting or denying access to the requested resource.

Components of a firewall rule

- Typically, a firewall rule consists of the following parameters :
  1. Source IP address or hostname
  2. Destination IP address or hostname
  3. Source Port number
  4. Destination Port number
  5. Direction of communication [inbound or outbound]
  6. Protocol name [TCP, UDP, ICMP or various others]
  7. Action [allow, deny, log, etc.]
  8. Various optional parameters such as Rule Name, Evaluation Order, etc.



- This is a snapshot of Microsoft® Windows® Firewall.

6.2.1 Classification of Firewalls

Firewalls can be classified based on various attributes. Fig. 6.2.1 shows types of firewalls.

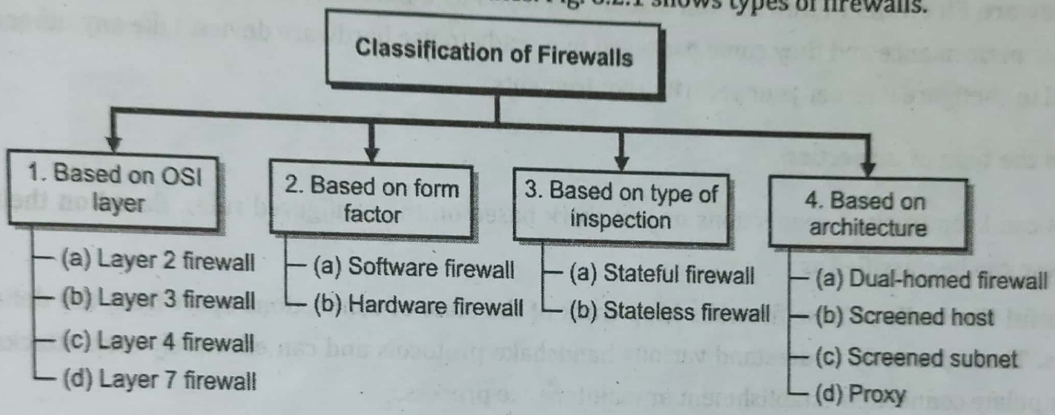


Fig. 6.2.1

1. Based on the OSI Layer

As you understand, OSI is a conceptual networking model. Based on the various layers, firewalls can be classified as following:

a. **Layer 2 Firewall :** These firewalls work at the "Data Link" layer of the OSI model. These firewalls require MAC, VLAN or device hardware level information to operate. One of the greatest advantage of these types of firewalls is that they are not IP dependent.

b. **Layer 3 Firewall :** These firewalls work at the "Network" layer of the OSI model. These filter traffic based on source/destination IP, port, and protocol. These are one of the most prevalent types of firewalls in use today. These are also called as Stateless firewalls. These are also called *first-generation* firewalls.

c. **Layer 4 Firewall :** These firewalls work at the "Transport" layer of the OSI model. These firewalls do everything that a Layer 3 firewall does and additionally track the active network connections and allow/deny traffic based on the state of those connections.

These can effectively stop DoS attacks such as the ones based on TCP SYN/ACK as these are aware of the state of connection. These are also called as Stateful firewalls. These are also called *second-generation* firewalls.

d. **Layer 7 Firewall :** These firewalls are called Layer 7 but can work at three layers – Session, Presentation and Application. For simplicity, these are just called Layer 7 firewalls. Layer 7 firewalls do everything that a Layer 4 firewall does and additionally include the ability to intelligently inspect the contents of the network packets passing through them. For example, a Layer 7 firewall could deny all the HTTP requests from Korean IP addresses. They have the actual packet content level visibility and are the most advanced types of firewall in use today. These are also called *third-generation* firewalls.

2. Based on the form factor

Form factor or the footprint is the way the firewall is actually packaged and deployed. They can be classified as,

a. **Software Firewalls :** These firewalls work as a software program and require an operating system to run them. All the implementation logic is coded in software and they are installed, patched, upgraded and maintained like a regular computer software. These firewalls could work at any of the OSI layers as discussed before.

b. **Hardware Firewalls :** Firewalls can also be deployed as a hardware device. Hardware firewall may have better performance and they come packaged in a ready to use hardware device. Like any other firewall, you need to configure it as per your security requirements.

3. Based on the type of inspection

Firewalls can keep track of connections or just work based on the configured rules. Based on their inspection types, these can be classified as

a. **Stateful Firewalls :** These firewalls keep track of the state of connections apart from the defined firewall rules. These precisely understand various handshake protocols and can effectively stop attacks that try to manipulate connection establishment or maintenance process.

b. **Stateless Firewalls :** Stateless firewalls typically work at the Layer 3 and take decisions based on the defined rule parameters such as IP, Port and Protocol. These do no track connection states and cannot effectively protect against attacks that manipulate connection processes.

4. Based on architecture

Firewalls can be deployed in many ways. They have special properties that make them suitable for one deployment type over the another. Based on the deployment possibilities, firewalls can be classified as

a. **Dual-homed Firewalls :** A Dual-Homed Firewall has two interfaces – one facing the external network and the other facing the internal network. It receives the external packets on one of its interfaces, evaluates firewall rules, and passes on the traffic to the designated internal resources via the second interface. The two interfaces are kept separate to isolate the external traffic with the internal traffic physically.

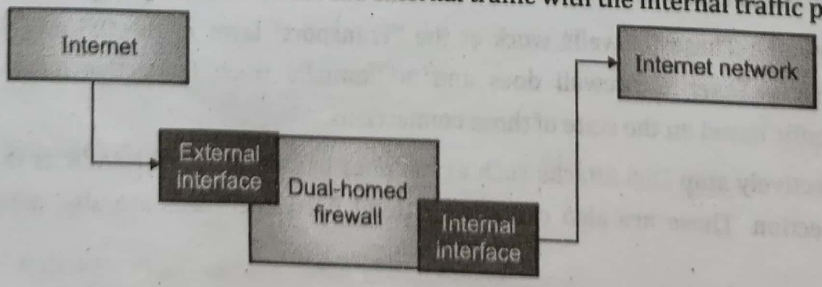


Fig. 6.2.2

b. **Screened Host :** In a screened host firewall, all internet (and other regulated) traffic goes through the firewall, no matter what. The internet router device first screens (filters) all the packets that are relevant to the network and then passes it to the Screened Host firewall for further inspection and applying rules.

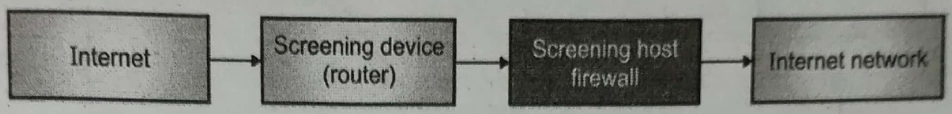


Fig. 6.2.3

c. **Screened Subnet :** In screened subnet architecture, two firewalls are used. One just after the external network and the one just before the internal network. Any network that lies between the two firewalls is called a Demilitarized Zone (DMZ).

You place your public facing servers such as webservers, email servers etc. in DMZ. An attacker would have to bypass both the firewalls before she can hit the internal network. This kind of architecture is commonly used in the industry today.

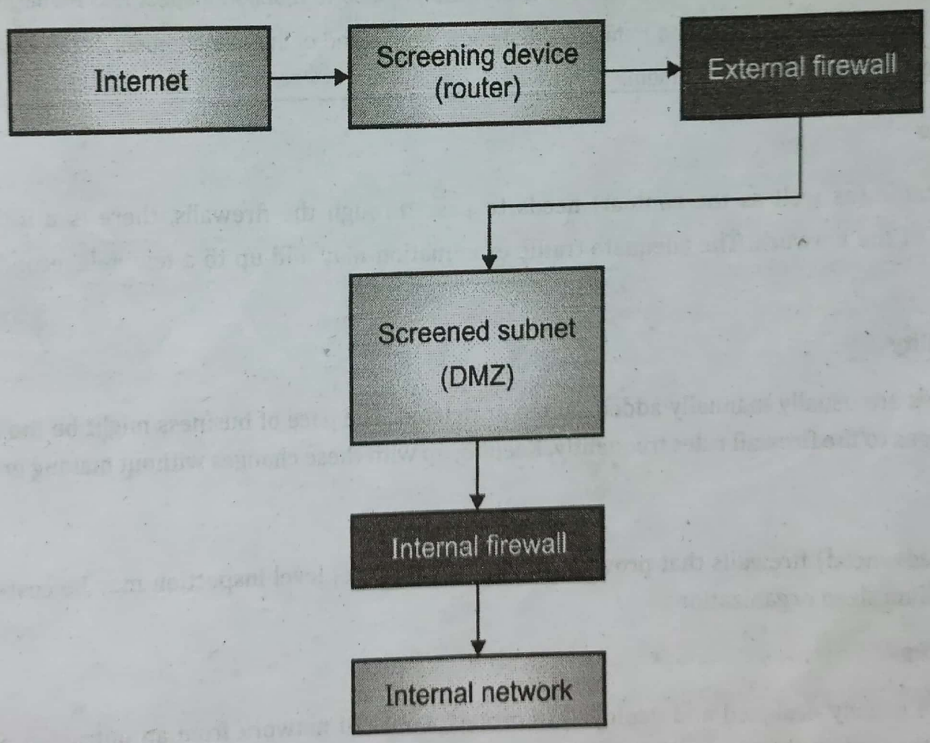


Fig. 6.2.4

d. **Proxy :** A proxy firewall stands between the trusted and the untrusted network and takes allow or deny decisions after careful inspection of what is being passed along.

Like a regular proxy, the proxy firewall breaks the connection between the source and the destination. After examining the traffic, it self-establishes a connection with the destination and passes the intended traffic to the destination as if the packets were originating from it.

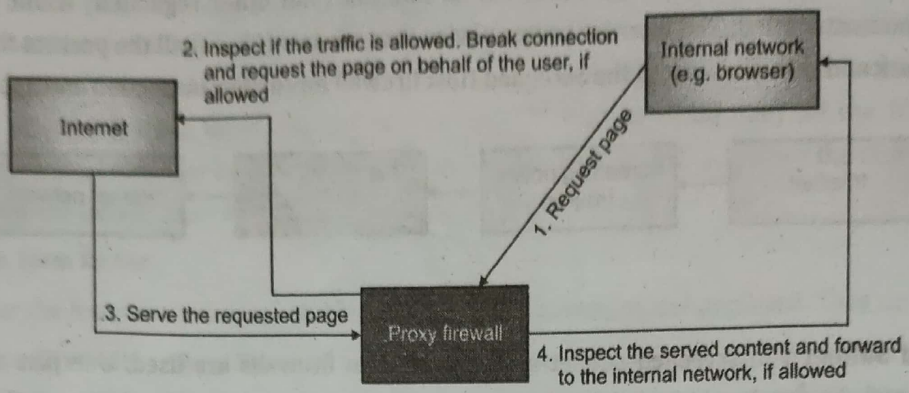


Fig. 6.2.5

6.2.2 Challenges in Managing and Deploying Firewalls

Note : Irrespective of what challenges or limitations firewalls may have, they are heavily used throughout the industry. You cannot just imagine any network without several firewalls in place to monitor, inspect and manage legitimate traffic and separate it from the illegitimate traffic. So, just know what some of the management or technical challenges are and do not worry too much about them.

1. **Performance**

   Since the traffic (as well as the content) needs to pass through the firewalls, there is a little performance degradation of the network. The adequate traffic examination may add up to a few milliseconds of latency on each packet.

2. **Business agility**

   Firewall rules are usually manually added, edited or deleted. The pace of business might be too high to require several changes to the firewall rules frequently. Keeping up with these changes without making errors is difficult.

3. **Costs**

   Modern (or advanced) firewalls that provide content and protocol level inspection may be cost-prohibitive for small or medium sized organizations.

4. **Insider attacks**

   Firewalls are usually designed and deployed to protect a trusted network from an untrusted network. But, if there were other vulnerabilities (such as a missing OS security patch) that were exploited such that an attacker is already on the trusted network, firewalls might not be able to protect or limit damages to the other resources on the trusted network.

5. **Managing firewalls themselves**

   Like your OS, printers or other software or hardware devices, firewalls need to be installed, patched, updated, etc. to remain operational. This adds a management overhead. Additionally, firewalls could have known vulnerabilities that need to be patched else a firewall that itself is lacking protection may not be very useful in providing you the required level of protection.

6.3 DMZ Networks (Firewall Design Principles)

- DMZ is an acronym for Demilitarized Zone.

Definition : *A DMZ is a network segment located between the protected and unprotected networks.*

- Typically, an organisation configures and establishes a DMZ network to protect and isolate internal networks and assets from public facing components and assets.
- Following is a high-level deployment diagram for creating a DMZ network.

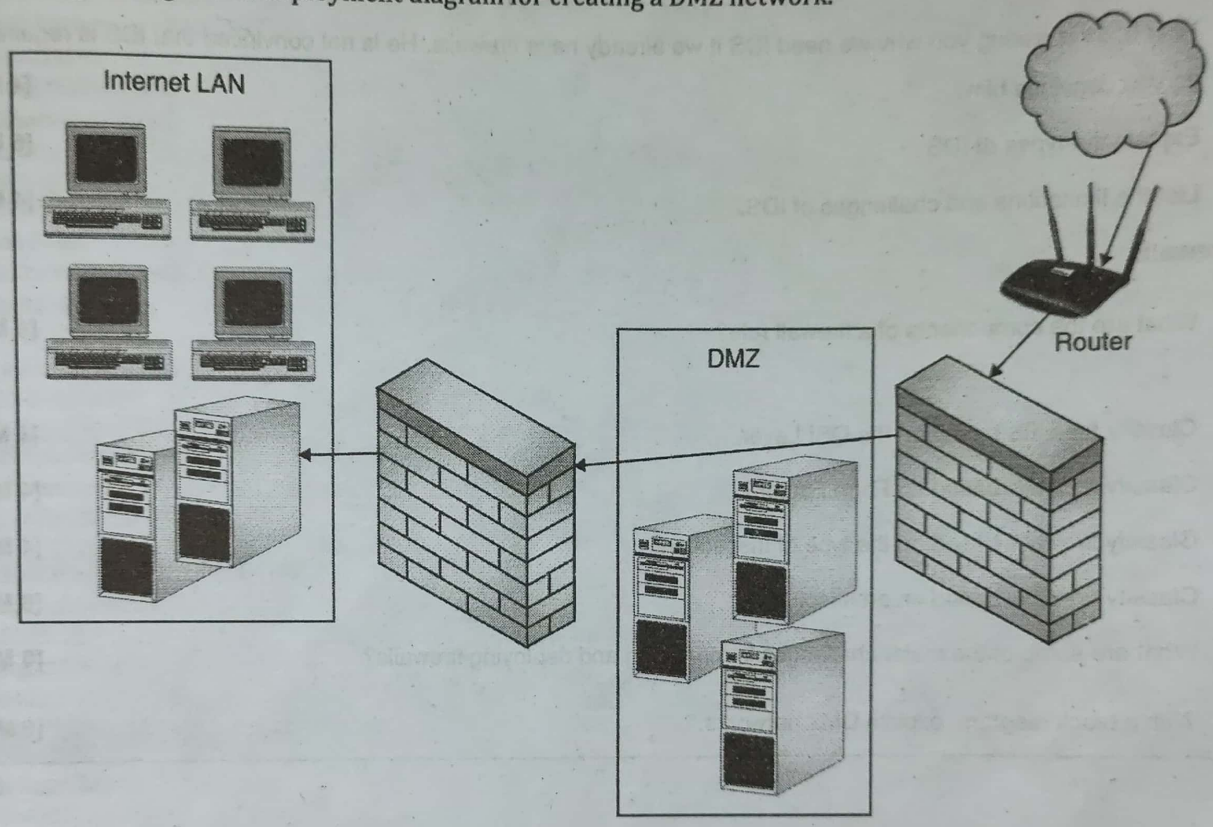


Fig. 6.3.1

- At least two firewalls, or firewall interfaces, are generally used to construct a DMZ. A DMZ provides a buffer zone between the dangerous Internet and the internal network that the organisation is trying to protect.
- The DMZ usually contains web, mail, and DNS servers, which must be strongly secured systems because they would be the first in line for attacks.
- Many DMZs also have an IDS sensor that listens for malicious and suspicious behaviour.

Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

[A] Computer Intrusions and Intrusion Detection and Prevention Systems (IDS / IPS)

Q. 1 What is a computer intrusion? What can you do to detect or prevent it? [4 Marks]

Q. 2 Your boss is asking you why we need IDS if we already have firewalls. He is not convinced that IDS is required. How do you convince him? [4 Marks]

Q. 3 Explain the types of IDS. [6 Marks]

Q. 4 List the limitations and challenges of IDS. [4 Marks]

[B] Firewalls

Q. 5 What are the components of a firewall rule? [4 Marks]

Q. 6 Classify firewalls based on the OSI Layer. [4 Marks]

Q. 7 Classify firewalls based on Form Factor. [4 Marks]

Q. 8 Classify firewalls based on the type of Inspection. [4 Marks]

Q. 9 Classify firewalls based on architecture. [8 Marks]

Q. 10 What are some of the major challenges in managing and deploying firewalls? [6 Marks]

Q. 11 With a block diagram, explain DMZ networks. [6 Marks]

❑❑❑