IT Fundamentals for Cyber Security

Chapter 05: Security Technologies and Tools

Co-funded by
the European Union

Table of Contents

List of figures

5. Security Technologies and tools

5.1. Introduction to Firewall Technolgies

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

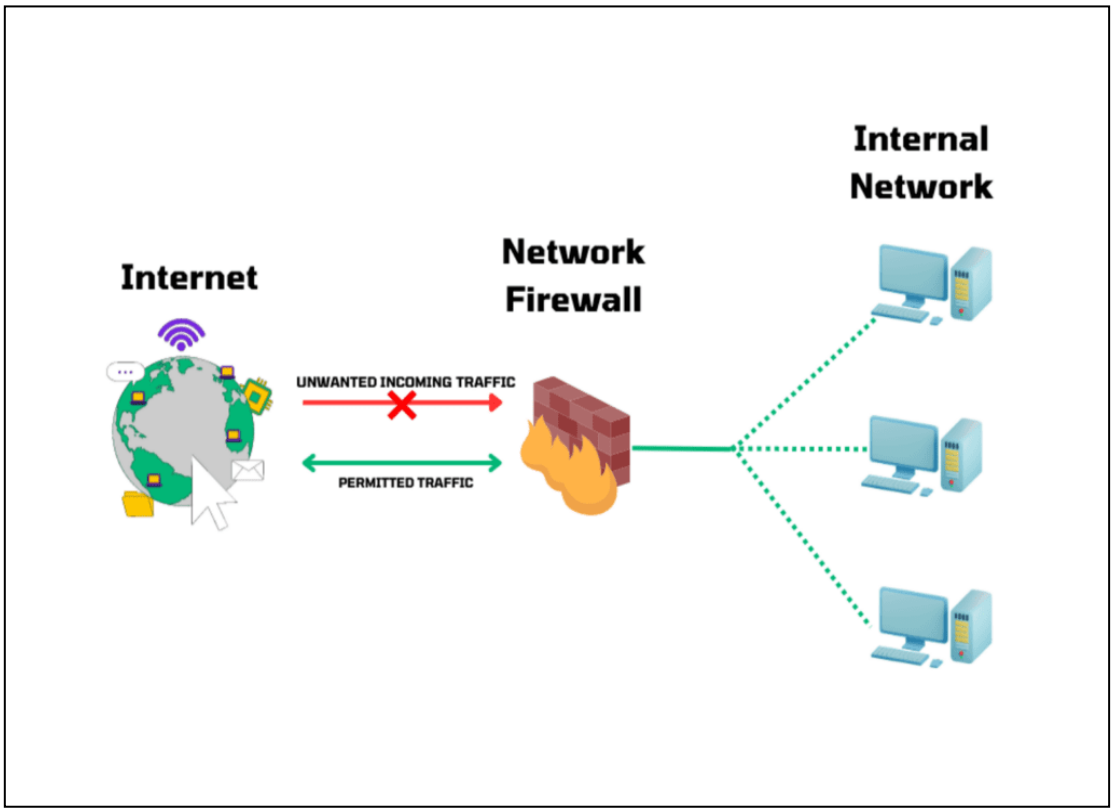

Figure 1. Firewall Technologies

5.1.1. Types and Importance of Firewalls

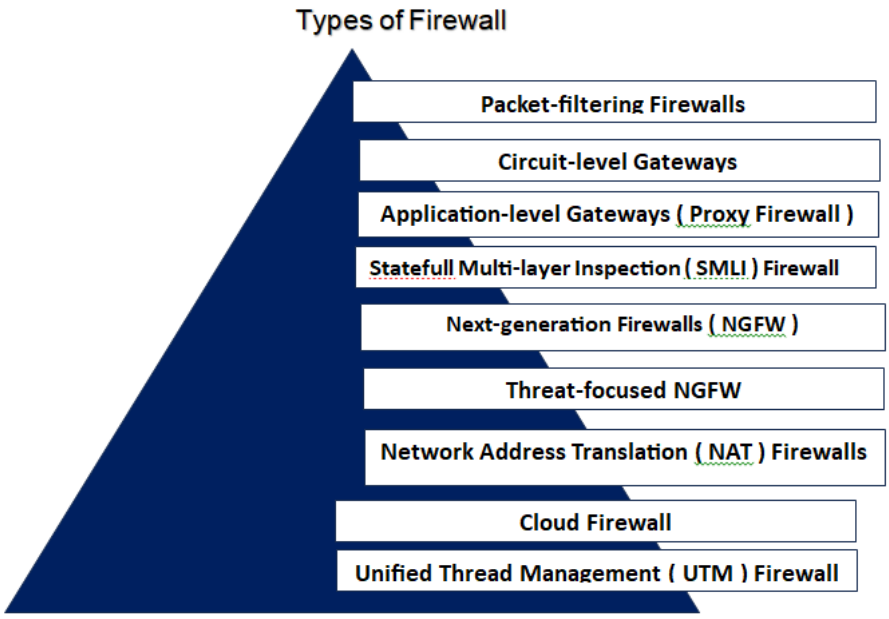

Figure 2. Types of Firewall

Depending on their structure and functionality, there are different types of firewalls. The following is a list of some common types of firewalls:

1. **Packet-filtering firewalls:-**A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.
2. **Circuit-level gateways** :- Simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying TCP (Transmission Control Protocol) connections and sessions. Circuit-level gateways are designed to ensure that the established sessions are protected.
3. **Application-level Gateways (Proxy Firewalls)**:- Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.
4. **Stateful Multi-layer Inspection (SMLI) Firewalls:-** Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.
5. **Next-generation Firewalls (NGFW):-** Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-

generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

6. **Threat-focused NGFW:-** Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly. With intelligent security automation, threat-focused NGFW set security rules and policies, further increasing the security of the overall defense system.
7. **Network Address Translation (NAT) Firewalls:-** Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These types of firewalls usually hide the IP addresses of our devices, making it safe from attackers.
8. **Cloud Firewalls:-** Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or FaaS (firewall-as-service). Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers. However, they are configured based on requirements.
9. **Unified Threat Management (UTM) Firewalls:-** UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management, etc.

Importance of Firewall

The following points listed below are the most relevant in explaining the importance of firewalls is as follows.

Feature 1: Monitoring Network Traffic

Firewall security starts with effective monitoring of network traffic based on pre-established rules and filters to keep the systems protected. Monitoring of network traffic involves the following security measures.

1. Source or destination-based blocking of incoming network traffic

This is the most common feature of most firewalls, whereby the firewalls block the incoming traffic by looking into the source of the traffic.

2. Outgoing network traffic can be blocked based on the source or destination

Many firewalls can also filter data between your internal network and the Internet. You might, for example, want to keep employees from visiting inappropriate websites.

3. Block network traffic based on content

More modern firewalls can screen network traffic for inappropriate content and block traffic depending on that. A firewall that is integrated with a virus scanner, for example, can prevent virus-infected files from entering your network. Other firewalls work in tandem with e-mail services to filter out unwanted messages.

4. Report on network traffic and firewall activities

When filtering network traffic to and from the Internet, it's also crucial to know what your firewall is doing, who tried to break into your network, and who tried to view prohibited information on the Internet. A reporting mechanism of some sort is included in almost all firewalls.

Feature 2 Stops Virus Attacks and spyware

With cyber thieves creating hundreds of thousands of new threats every day, including spyware, viruses, and other attacks like email bombs, denial of service, and malicious macros, it's critical that you put protections in place to keep your systems safe. The number of entry points criminals can exploit to get access to your systems grows as your systems become more complicated and strong. Spyware and malware programs designed to penetrate your networks, manage your devices, and steal your data are one of the most common ways unwelcome persons obtain access. Firewalls are a crucial line of defense against malicious software.

Feature 3: Preventing Hacks

Cyber threats are evolving at a fast pace and are widespread. Firewalls keep hackers out of your data, emails, systems, and other sensitive information. A firewall can either entirely block a hacker or push them to choose a more vulnerable target.

Feature 4: Promotes Privacy

Having a firewall keeps the data safe and builds an environment of privacy that is trustworthy and a system without a firewall is accepting every connection into the network from anyone. Without a firewall, there would be no way to detect incoming threats. As a result, malicious users may be able to gain access to your devices and thereby compromising privacy. It's critical to take advantage of existing defenses to safeguard your network and the personal information stored on your computer against cybercrime.

5.1.2. Best Practices for Firewall configuration

Key firewall best practices includes:

1. Harden and configure firewalls properly.
2. Adopt a customized, phased deployment strategy.
3. Enhance and regularly update firewall protocols.
4. Regularly review and update access controls.
5. Implement a comprehensive logging and alert mechanism.

6. Establish backup and restoration protocols.
7. Align policies with compliance standards.
8. Subject firewalls to regular testing.
9. Conduct routine firewall audits.

5.2. Overview of Antivirus and Anti-malware Software

Antivirus is a program that is created to search, detect, prevent, and remove software viruses from your system that can harm your system.

Benefits of Antivirus

1. Spam and advertisements are blocked.
2. Virus protection and transmission prevention.
3. Hackers and data thieves are a threat.
4. Protected against devices that can be detached.
5. To improve security.
6. Password Protection.

Drawbacks of Antivirus

1. Slows down system's speed.
2. Popping up of Advertisements.
3. Security Holes.
4. No customer care service.

Anti Malware is software designed for scanning, detecting, blocking, and preventing malicious programs from accessing our system

Benefits of Antimalware

1. Protection Against Malware.
2. Improved System Performance.
3. Data Protection.
4. System Maintenance and Updates.

Drawbacks of Antimalware

1. Resource Consumption.
2. Subscription Fees.
3. Complexity and Maintenance.
4. Security Vulnerabilities.

5.2.1. Definition and Purpose of Antivirus and Anti Malware

Antivirus is a program that is created to search, detect, prevent, and remove software viruses from your system that can harm your system.

Anti Malware is software designed for scanning, detecting, blocking, and preventing malicious programs from accessing our system

Purpose of Antivirus and Anti Malware

Antivirus protection is essential for any business wanting to protect their data and computer systems from becoming corrupted. Antivirus software is the security person at the gate preventing unwanted persons from entering. Prevention is much more effective than cure, so it's better to have a system in place designed to detect and prevent virus attacks than having to spend time and money repairing infected machines.

Additionally, from a business perspective, your reputation could be on the line if a virus exposes personal client data or sends unsolicited emails to your contacts in an attempt to spread the virus further.

Anti-malware is a proactive software program that is designed to protect your IT systems and provide real-time protection by scanning networks and data for malware (or malicious software). When it identifies malware, it removes it.

Anti-malware program is important due to following reasons;-

1) Real-time Malware Prevention:

Anti-malware blocks malicious software from infiltrating your system and does so by scanning downloaded files, websites you visit and applications you use.

2) Advanced Malware Detection:

Anti-malware also helps identify any existing malicious software on your system.

3) Automatic Malware Removal:

If it detects any malware, anti-malware programs work in the background and quarantine or remove malicious software to minimize downtime and potential damage to your systems and networks.

5.2.2. Best Practices for using Antivirus and Anti Malware Software

Figure 3. Best Practices for using Antivirus and Anti Malware Software

1. Keep your antivirus software up to date: Regularly update your antivirus software to ensure it has the latest virus definitions and security patches. This will help it detect and protect against new threats.

2. Enable real-time scanning: Enable real-time scanning or active protection feature in your antivirus software. This will continuously monitor your system for any suspicious activity or malware and take immediate action if necessary.

3. Regularly scan your system: Perform regular system scans using your antivirus software to check for any hidden or dormant threats. Schedule automatic scans at a convenient time when your computer is idle.

4. Enable automatic updates for your operating system and other software: Keeping your operating system and other software up to date is crucial for security. Enable automatic updates whenever possible, as they often include important security patches.

5. Be cautious of email attachments and downloads: Exercise caution when opening email attachments or downloading files from the internet. Your antivirus software can help detect and block malicious files, but it's important to be mindful of potential threats.

6. Use strong, unique passwords: Protect your antivirus software and other sensitive accounts with strong, unique passwords. Avoid using common or easily guessable passwords and consider using a password manager to securely store and manage your passwords.

7. Be wary of phishing attempts: Antivirus software can help detect some phishing emails, but it's essential to remain vigilant. Avoid clicking on suspicious links or providing personal information in response to unexpected emails or messages.

8. Keep backups of your important data: Regularly back up your important files and data to an external storage device or cloud storage service. In the event of a malware infection or other security incident, having backups will allow you to recover your data.

9. Practice safe browsing habits: Be cautious while visiting websites, especially those of unknown or suspicious nature. Stick to reputable websites and avoid clicking on pop-up ads or downloading files from untrusted sources.

10. Educate yourself about security best practices: Stay informed about the latest security threats, scams, and best practices. Keep up with security news, follow reputable sources, and educate yourself on how to stay safe online.

5.3. Intrusion Detection and Prevention System(IDPS)

An intrusion detection and prevention system (IDPS) is a solution that monitors a network for threats and then takes action to stop any threats that are detected.

An IDPS is closely related to an intrusion detection system (IDS). While both systems detect threats and send alerts about them, an IDPS also attempts to remediate those threats.

An IDPS is sometimes called an intrusion prevention system (IPS). The terms IDPS and IPS are mostly used interchangeably, but when someone mentions an IPS they are often referring to the threat hunting function of an IDPS.

5.3.1. Types and Components of IDPS

There are many types of IDPS technologies. For the purposes of this document, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed:

A. Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

B. Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network tomonitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring.

C. Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks).

D. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes.

The Typical components in an IDPS solution are as follows:

1. **Sensor or Agent.** Sensors and agents monitor and analyse activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behaviour analysis technologies. The term agent is typically used for host-based IDPS technologies.

2. **Management Server**. A management server is a centralized device that receives information from the sensors or agents and manages them.

Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.

3. **Database Server.** A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.

4. **Console.** A console is a program that provides an interface for the IDPS's users and administrators.

Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

5.3.2. Implementing and Managing IDPS

Step 1: Define Your Network Segmentation

- **Identifying Critical Assets:** Begin by identifying the critical assets within your network. These could include servers containing sensitive data, customer information databases, or proprietary software systems. Understanding what needs protection is the first step in effective security.
- **Creating Segmentation Zones:** Once you've identified your critical assets, create network segmentation zones. These zones group assets with similar security requirements. For example, you might have a zone for customer data servers and another for public-facing web servers. This segmentation is crucial for controlling and monitoring network traffic effectively.

Step 2: Selecting the Right Hardware and Software

- **Hardware Requirements:** Carefully choose the hardware that will host your IDS/IPS solution. Factors to consider include processing power, memory, network interfaces, and storage. Ensure that your hardware can handle the expected traffic load and scale as needed.
- **Software Requirements:** Select IDS/IPS software that aligns with your organization's requirements. Consider open-source solutions like Snort or commercial products like Cisco Firepower. Evaluate features, scalability, and support options when making your decision.
- **Compatibility Checks:** Before installation, verify that your chosen IDS/IPS solution is compatible with your existing network infrastructure and security tools. Incompatibilities can lead to functionality issues and may compromise security.

Step 3: Installation and Configuration

- **Deploying IDS/IPS Sensors:** Install sensors at key points in your network, such as between network segments or at entry/exit points. Sensors capture and analyze network traffic for suspicious activity. Proper sensor placement is essential for effective threat detection.
- **Configuring Network Taps or SPAN Ports:** Ensure that your sensors can access the network traffic they need to monitor. Use network taps or SPAN (Switched Port Analyzer) ports to mirror traffic to the sensors without disrupting network operations.
- **Initial Setup and Configuration**: Follow the installation and configuration guidelines provided by your IDS/IPS vendor or open-source project. Configure network interfaces, set up alerting mechanisms, and establish initial rules or signatures.

Step 4: Rule and Signature Management

- **Fine-tuning Detection Rules:** Customize detection rules to align with your network's specific characteristics and threat landscape. Regularly review and adjust rules to reduce false positives and increase detection accuracy.

- **Updating Signatures and Rules:** Stay up-to-date with the latest threat intelligence by regularly updating signatures and rules. This ensures your IDS/IPS can detect emerging threats effectively.
- **Customization for Your Environment:** Tailor your IDS/IPS to your organization's needs. Customize alerting thresholds, response actions, and reporting to align with your security policies.

Step 5: Monitoring and Alerts

- **Real-time Monitoring:** Monitor network traffic and IDS/IPS alerts in real-time. Invest in a centralized dashboard or SIEM (Security Information and Event Management) system to aggregate and analyse data from multiple sensors.
- **Alert Management:** Develop an alert escalation process to prioritize and respond to alerts efficiently. High-priority alerts require immediate attention, while lower-priority alerts can be investigated later. Incident Response Planning: Develop a well-defined incident response plan that outlines actions to take in the event of a security incident. Ensure all team members are trained on this plan and conduct regular drills.

Step 6: Regular Updates and Maintenance

- **Patch Management:** Keep your IDS/IPS software and hardware up-to-date by applying patches and updates. Vulnerabilities in your security tools can be exploited by attackers, so timely updates are essential.
- **Performance Optimization:** Monitor the performance of your IDS/IPS system and fine-tune it for optimal efficiency. Over time, adjust configurations based on traffic patterns and the evolving threat landscape.
- **Periodic Auditing and Testing:** Conduct regular security audits and penetration testing to identify vulnerabilities and weaknesses in your network. Use the results to refine your security strategy.

5.3.3. Challenges and Best Practices of IDPS

Challenges of IDPS

1. Ensuring an effective deployment

To attain a high level of threat visibility, organisations must ensure that intrusion detection technology is correctly installed and optimised. Due to budgetary and monitoring constraints it may not be practical to place NIDS and HIDS sensors throughout an IT environment. With many organisations lacking a complete overview of their IT network however, deploying IDS effectively can be tricky and if not done well may leave critical assets exposed.

2. Managing the high volume of alerts

HIDS and NIDS typically utilise a combination of signature and anomaly-based detection techniques. This means alerts are generated when a sensor either detects activity that matches

a known attack pattern, or flags traffic that falls outside a list of normal behaviours. Anomalous activity could include high-bandwidth consumption and irregular web or DNS traffic.

The vast quantity of alerts generated by intrusion detection can be a significant burden for internal teams. Many system alerts are false positives but rarely do organisations have the time and resources to screen every alert, meaning that suspicious activity can often slip under the radar.

Most intrusion detection systems come loaded with a set of pre-defined alert signatures but for most organisations these are insufficient, with additional work needed to baseline behaviours specific to each environment.

3. Understanding and investigating alerts

IDS alerts consist of base-level security information which, when viewed in isolation, may mean very little. Upon being presented with an alert, it is often not immediately obvious what caused it, or what actions are required to establish whether or not it poses a genuine threat.

Investigating IDS alerts can be very time and resource-intensive, requiring supplementary information from other systems to help determine whether an alarm is serious. Specialist skills are essential to interpret system outputs and many organisations lack the dedicated security experts capable of performing this crucial function.

4. Knowing how to respond to threats

A common problem for organisations that implement IDS is that they lack an appropriate incident response capability. Identifying a problem is half the battle, knowing how to respond appropriately and having the resources in place to do so is equally important.

Effective incident response requires skilled security personnel with the knowledge of how to swiftly remediate threats, as well as robust procedures to address issues without impacting day-to-day operations. In many organisations there is a big disconnect between the people charged with monitoring alerts and those managing infrastructure, meaning that swift remediation can be difficult to achieve.

To highlight the importance of having an appropriate incident response plan in place, the General Data Protection Regulation (GDPR) requires organisations that process any type of personal data to have appropriate controls in place to report breaches to a relevant authority within 72 hours, or risk a large fine.

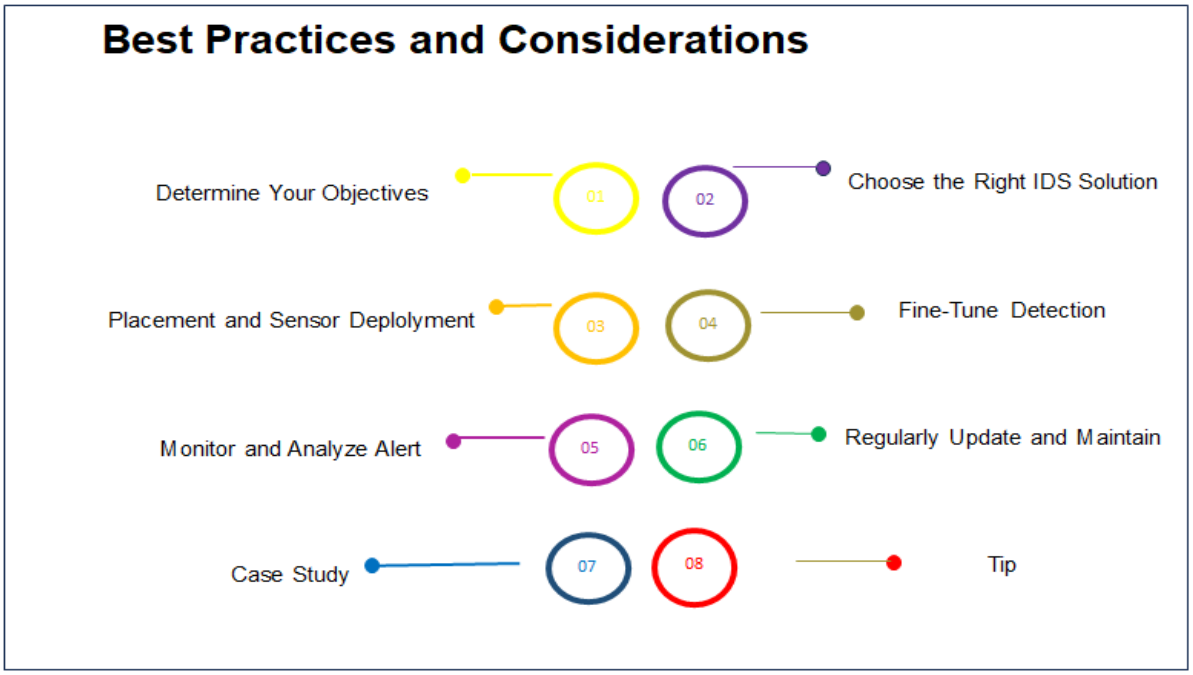

Figure 4. Best Practices of Intrusion Detection Prevention System

1. **Determine Your Objectives:** Before deploying an intrusion detection system (IDS), it is crucial to clearly define your objectives. Consider what you want to achieve with the IDS and how it aligns with your overall security strategy. Are you primarily looking to detect and prevent network-based attacks, or are you also interested in monitoring host-based activity? Understanding your objectives will help you choose the right type of IDS and configure it effectively.
2. **Choose the Right IDPS Solution:** There are various types of IDS solutions available, each with its own strengths and weaknesses. Network-based IDS (NIDS) monitors network traffic for suspicious activity, while host-based IDS (HIDS) focuses on individual systems. Additionally, there are hybrid IDPS solutions that combine both approaches. Consider your network architecture, the level of control you require, and the resources available to manage the IDPS when selecting the appropriate solution.
3. **Placement and Sensor Deployment:** Proper placement of IDPS sensors is crucial for effective threat detection. Place NIDS sensors strategically at critical network junctures, such as the border between internal and external networks, to monitor incoming and outgoing traffic. For HIDS, install agents on individual systems to monitor local activities. Consider deploying sensors in areas where attackers are more likely to target, such as servers containing sensitive data or high-value assets.
4. **Fine-Tune Detection Rules:** Out-of-the-box IDPS configurations may not provide optimal results for your specific environment. Take the time to fine-tune detection rules to reduce false positives and increase the accuracy of threat detection. Analyze your network traffic patterns, understand the normal behavior of your systems, and

customize the IDS rules accordingly. Regularly review and update the rules to adapt to emerging threats and changes in your network infrastructure.

5. **Monitor and Analyze Alerts:** IDPS generates alerts when suspicious or malicious activity is detected. Establish a process to efficiently monitor and analyze these alerts to respond promptly to potential threats. Implement a centralized logging and alerting system that consolidates alerts from multiple IDPS sensors for easier analysis. Define escalation procedures and assign responsibilities to ensure that alerts are promptly addressed and investigated.
6. **Regularly Update and Maintain:** Just like any security solution, an IDPS requires regular updates and maintenance to remain effective against evolving threats. stay up to date with the latest IDPS software updates, including new detection rules and patches for vulnerabilities. Regularly review and fine-tune your IDPS configurations to adapt to changes in your network environment. Conduct periodic assessments to ensure the IDPS remains aligned with your security objectives and is effectively protecting your network.
7. **Case Study:** XYZ Corp's IDS Success Story: XYZ Corp, a mid-sized financial institution, deployed an IDPS to enhance their overall security posture. By strategically placing NIDS sensors at critical network junctions and HIDS agents on their servers, they achieved comprehensive network and host-based threat detection. Through careful customization of detection rules and continuous monitoring, they significantly reduced false positives and improved their incident response capabilities. The IDPS played a crucial role in detecting and mitigating a sophisticated malware attack, preventing a potential data breach.
8. **Tip: Integrate IDPS with SIEM:** Integrating your IDPS with a Security Information and Event Management (SIEM) system can enhance threat detection and incident response capabilities. SIEM aggregates and correlates data from multiple sources, including IDPS alerts, logs, and other security solutions, providing a holistic view of your network's security posture. This integration enables more efficient analysis, correlation, and response to security incidents.

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security , Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

1. https://www.researchgate.net/publication/281148436_Security_Technologies
2. https://www.researchgate.net/publication/376600966_CYBER_SECURITY_TOOLS_AND_THEIR_USES
3. https://www.tandfonline.com/journals/tsec20

Question Answers

Q. No. 01 **Marks**

Question: What is a firewall? **05**

Answer: A firewall can be defined as a special type of network security device or software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

Q. No.02 **05**

Question: Elaborate the most important feature of a firewall?

Answer: The most important feature of a firewall:

- **Monitoring Network Traffic:**

Firewall security starts with effective monitoring of network traffic based pre-established rules and filters to keep the systems protected. Monitoring Network traffic involves the following security measures. 1. Source or destination-based blocking of incoming network trafficThis is the most common feature of most firewalls, whereby the firewall block the incoming traffic by looking into the source of the traffic. 2. Outgoing network traffic can be blocked based on the source or destination. Many firewalls can also filter data between your internal network and Internet. You might, for example, want to keep employees from visiting inappropriate websites.

- **Stops Virus Attacks and spyware:**

With cyber thieves creating hundreds of thousands of new threats everyday, including spyware, viruses, and other attacks like email bombs, denial of service, and malicious macros, it's critical that you put protections place to keep your systems safe.

- **Preventing Hacks:**

Cyber threats are evolving at a fast pace and are widespread. Firewalls Keep Hackers out of your data, emails, systems, and other sensitive information. A firewall can either entirely block a hacker or push them to choose more vulnerable target.

- **Promotes Privacy:**

Having a firewall keeps the data safe and builds an environment of privacy whois trustworthy and a system without a firewall is accepting every connection the

network from anyone. Without a firewall, there would be no way to detect incoming threats.

Q. No.03 **05**

Question: Discuss the benefits and drawbacks of Antivirus.

Answer: Antivirus is a program that is created to search, detect, prevent, and remove software viruses from your system that can harm your system.

Benefits of Antivirus

1. Spam and advertisements are blocked.
2. Virus protection and transmission prevention.
3. Hackers and data thieves are a threat.
4. Protected against devices that can be detached.
5. To improve security.
6. Password Protection.

Drawbacks of Antivirus

1. Slows down system's speed.
2. Popping up of Advertisements.
3. Security Holes.
4. No customer care service.

Q. No.04 **05**

Explain the Purpose of Antivirus and Anti Malware.

Answer: Antivirus protection is essential for any business wanting to protect their data and computer systems from becoming corrupted. Antivirus software is the security person at the gate preventing unwanted persons from entering. Prevention is much more effective than cure, so it's better to have a system in place designed to detect and prevent virus attacks than having to spend time and money repairing infected machines.

Anti-malware is a proactive software program that is designed to protect your IT systems and provide real-time protection by scanning networks and data for malware (or malicious software). When it identifies malware, it removes it.

Q. No.05 **05**

Elaborate Intrusion Detection and Prevention System (IDPS)

Answer: An intrusion detection and prevention system (IDPS) is a solution that monitors a Network for threats and then takes action to stop any threats that are detected. An IDPS is closely related to an intrusion detection system (IDS). While both systems detect threats and send alerts about them, an IDPS also attempts to remediate those threats. An IDPS is sometimes called an intrusion prevention system (IPS). The terms IDPS and IPS are mostly used interchangeably, but when someone mentions an IPS they are often referring to the threat hunting function of an IDPS.

Q. No.06 **05**

Describe the Types of IDPS.

Answer: For the purposes of this document, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are

deployed:

A. Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. and wireless networks.

B. Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring.

C. Network Behavior Analysis (NBA): NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks. business partners' networks).

D. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic

Q. No.07 **05**

Illustrate the benefits and drawbacks of Antimalware.

Answer: Anti Malware is software designed for scanning, detecting, blocking,and preventing malicious programs from accessing our system.

Benefits of Antimalware

1. Protection Against Malware.
2. Improved System Performance.
3. Data Protection.
4. System Maintenance and Updates.

Drawbacks of Antimalware

1. Resource Consumption.
2. Subscription Fees.
3. Complexity and Maintenance.
4. Security Vulnerabilities.

Q. No.08 **05**

Enlist the typical components of the IDPS solution.

Answer:

1. Sensor or Agent. Sensors and agents monitor and analyse activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behaviour analysis technologies. The term agent is typically used for host-based IDPS technologies.

2. Management Server. A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot.

3. Database Server. A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.

4. Console. A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

Q. No.09 **05**

Emphasize the Challenges and Best Practices of IDPS

Answer:

Challenges of IDPS

1 – Ensuring an effective deployment To attain a high level of threat visibility, organizations must ensure that intrusion detection technology is correctly installed and optimized. Due to budgetary and monitoring constraints it may not be practical toplaceNIDS and HIDS sensors throughout an IT environment. With many Organizations lacking a complete overview of their IT network however, deploying IDS effectively can be tricky and if not done well may leave critical assets exposed.

2 – Managing the high volume of alerts HIDS and NIDS typically utilize a combination of signature and anomaly-based detection techniques. This means alerts are generated when a sensor either detects activity that matches a known attack pattern, or flags traffic that falls outside a list of normal behaviours. Anomalous activity could include high-bandwidth consumption and irregular web or DNS traffic

3 – Understanding and investigating alerts IDS alerts consist of base-level security information which, when viewed in isolation, may mean very little. Upon being presented with an alert,itis often not immediately obvious what caused it, or what actions are required to establish whether or not it poses a genuine threat..

4 – Knowing how to respond to threats

A common problem for organizations that implement IDS is that they lack an appropriate incident response capability. Identifying A Problem Is half the battle, knowing how to respond appropriately and having the resources in place to do so is equally important.

Q. No.10 **05**

Give the Comparison between IDS and IPS?

Answer: The difference between IDS and IPS is that IPS actively blocks threats while IDS simply provides alerts. Both systems serve a purpose in an organization's strategy and come with their own benefits and challenges.

- **Intrusion Detection System (IDS):** Intrusion detection system software continuously analyses network traffic or system activity for suspicious patterns that might indicate an ongoing attack. These patterns can be identified through signature-based detection, which matches traffic

against known attack signatures, or anomaly-based detection, which looks for deviations from regular behaviour. Upon detecting suspicious activity, an IDS can raise alerts, log events, and provide valuable insights for security personnel to investigate and respond to potential threats.

- **Intrusion Prevention System (IPS):** An IPS extends the functionality of IDS by actively taking steps to prevent intrusions. Based on predefined security policies and identified threats, an IPS can block malicious traffic, terminate suspicious connections, or otherwise disrupt the attacker's progress. This can involve techniques like packet filtering, which blocks unwanted traffic based on predefined rules, or deep packet inspection, which examines the content of packets for malicious payloads. It is important to note that one of the challenges with IPS is the possibility of non-malicious traffic being blocked based on a “false positive”