Lesson

1.1. Identifying Unauthorized Devices

Most organizations today use some form of asset management. These systems work great for managing assets that are known and permitted within the environment, but offer little visibility or control over rogue machines that may be connecting to the network.

The challenge with rogue devices is that they are not part of the management framework. This means that they are not part of any standards, policies, security controls, or patch updates. They pose a unique threat to an environment.

Consider a server that a developer built to test something and never decommissioned. This server remains online, running company code on an unpatched database. Without actively monitoring the network, there is no way that an administrator can have any real idea of the volume of unmanaged systems on the network.

The greater the number of unmanaged systems, the greater the risk to the network. Where administrators have audited the network, typically between 1 percent and 10 percent of assets were previously unknown to the administrator. Once detected, local system administrators can manage modest numbers of assets. However, if the volume or location of rogue assets is excessive or dangerous, these results provide justification and motivation for automated and proactive enforcement performed by Network Access Control.

Identify Assets

There are two general approaches to identifying assets on the network, techniques that are very similar in nature to finding viruses:

- on-access or real-time detection,
- on-demand or scheduled detection.

Note that the optimal solution is likely to be able to cater for both approaches to device identification.

Real-time detection - Relies on detection of traffic generated by the endpoint. The benefit is its timely nature—detection is immediate. Consequently, you can take action very quickly. The downside of this approach is that since detection is based on traffic generated by the endpoint, there must be a sensor located near this traffic. This technique may not be practical for all network topologies.

Scheduled detection - The system queries network addresses for a response according to a schedule. This model can overcome the proximity limitations of the first approach. Sensors can execute scans from a limited number of locations or a single location on the network. The downside of this approach is that detection is not immediate. It is limited to the detection interval determined by the schedule. As in the example of off-hours scanning, rogue systems may operate on the network between detection scans and escape identification.

Further steps to identifying unauthorised devices include asset inventory tool.

Asset Inventory Tool

Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both, active tools that scan through network address ranges and passive tools that identify hosts based on analysing their traffic should be employed.

Deploy DHCP Server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.

All equipment acquisitions should automatically update the inventory system as new, approved devices are connected to the network.

Maintain an asset inventory of all systems connected to the network and the network devices themselves recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device.

The inventory should include every system that has an Internet Protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc.

The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether or not they are attached to the organization's network. Make sure that asset inventory database is properly protected and a copy stored in a secure location.

In addition to an inventory of hardware, organizations should develop an inventory of information assets that identifies their critical information.

Information asset inventory should map critical information to the hardware assets (including servers, workstations, and laptops) on which it is located. A department and individual responsible for each information asset should be identified, recorded, and tracked.

Further to the asset inventory tool the organisation needs to:

- Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network.
- Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.
- Create separate VLANs for BYOD (bring your own device) systems or other untrusted devices.
- Utilize client certificates to validate and authenticate systems prior to connecting to the private network.

Organizations must first establish information/asset owners, deciding and documenting which organizations and individuals are responsible for each component of a business process that includes information, software, and hardware. In particular, when organizations acquire new systems, they record the owner and features of each new asset, including its network interface media access control (MAC) address and location. This mapping of asset attributes and owner-to-MAC address can be stored in a free or commercial database management system.

Use tools to pull information from network assets such as switches and routers regarding the machines connected to the network.

Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

Effective organizations configure free or commercial network scanning tools to perform network sweeps on a regular basis, sending a variety of different packet types to identify devices connected to the network. In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces looking for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

The system must be capable of identifying any new unauthorized devices that are connected to the network within 24 hours. Alerting or sending e-mail notification to a list of enterprise administrative personnel. The system must automatically isolate the unauthorized system from the network within one hour of the initial alert.

Send a follow-up alert or e-mail notification when isolation is achieved. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until the unauthorized system has been removed from the network. The asset inventory database and alerting system must be able to identify the location, department, and other details of where authorized and unauthorized devices are plugged into the network.

To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network, including a selection of subnets associated with demilitarized zones (DMZs), workstations, and servers. Two of the systems must be included in the asset inventory database, while the other systems are not. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team must verify that the system provides details of the location of all the test machines connected to the network. For those test machines included in the asset inventory, the team must also verify that the system provides information about the asset owner. The evaluation team must then verify that the test systems are automatically isolated from the production network within one hour of initial notification and that an e-mail or alert indicating the isolation has occurred. The team must then verify that the connected test systems are isolated from production systems.

1.2. Testing the Traffic Filtering Devices

There are four basic recommendations for Traffic Filtering in order to reduce security threats, organisations use various devices, technologies and techniques for traffic filtering. Each institution/organisation that wishes to improve the efficiency of filtering and increase the level of security in its network should apply the following recommendations:

1. **Define traffic-filtering rules** that will determine the manner in which the incoming and outgoing traffic flows in the network will be regulated. A set of traffic-filtering rules can be adopted as an independent packet filtering policy or as a part of the information security policy;
2. **Select a traffic-filtering technology** that will be implemented depending on the requirements and needs;
3. **Implement defined rules** on the selected technology and optimise the performance of devices accordingly;
4. **Maintain all the components of the solution**, including not only devices, but also the policy.

Traffic-filtering technologies are commonly divided into

- **packet filtering/stateless firewall**
- **stateful firewall technologies.**

The **packet-filtering functionality (stateless firewall**) is built into the majority of operating systems and devices with a traffic routing feature. In most cases, it is a router on which access control lists (ACLs) are applied. A packet filter implemented on a router is the simplest, but only one of the available traffic-filtering methods.

Packet filtering is the basic feature of all firewall devices. The first firewall devices, with only a packet filter, were also called stateless inspection firewalls. Unlike them, modern firewall devices provide far more possibilities for packet filtering. A packet filter enables the implementation of control of access to resources by deciding whether a packet should be allowed to pass, based on the information contained in the IP packet header. The packet filter does not analyse the content of the packet (unlike a content filter), nor does it attempt to determine the sessions to which individual packets belong, based on the information contained in the TCP or UPD header, and therefore it does not make any further decisions in that regard. For this reason, the process is also known as stateless packet inspection. Due to its manner of operation, which does not track the information on the state of connections, it is necessary to explicitly allow two-way traffic on the connection when configuring a stateless firewall device. Stateless firewall devices analyse each packet individually and filter them based on the information contained in Layers 3 and 4 of the OSI reference model. A filtering decision is made based on the following information:

- source IP address;
- destination IP address;
- protocol;

- source port number;
- destination port number.

They are commonly implemented as a part of the functionality on routers (ACL, firewall filters, etc.), but can also be implemented on servers.

The advantages of applying packet filters:

- simple implementation;
- supported by most routers, so there is no need to invest in new equipment and software;
- rarely cause bottlenecks in the area of their application, even at high speeds in Gigabit networks.

The disadvantages of applying packet filters:

- vulnerability to IP spoofing attacks;
- vulnerability to attacks that exploit problems within the TCP/IP specification and the protocol stack;
- problems with filtering packets that are fragmented (causing interoperability and non-functioning of VPN connections);
- no support for the dynamic filtering of some services (the services that require
- dynamic negotiation about the ports that will be used in communication – passive FTP).

Stateful packet inspection improves the packet filtering process by monitoring the state of each connection established through a firewall device. It is known that the TCP protocol, allows two-way communication and that TCP traffic is characterised by three phases: establishing the connection, data transfer, and terminating the connection. In the connection establishment phase, stateful packet inspection records each connection in the state-table. In the data transfer phase, the device monitors certain parameters in the header of the L3 packet and L4 segment and makes a filtering decision depending on their values and the content of the state-table. The state-table contains all currently active connections. As a result, a potential attacker trying to spoof a packet with a header indicating that the packet is a part of an established connection can only be detected by the stateful inspection firewall device, which verifies whether the connection is recorded in the state-table. The state-table contains the following information:

- source IP address;
- destination IP address;
- source port number;
- destination port number;
- TCP sequence numbers;
- TCP flag values.

The state of the synchronize (SYN), reset (RST), acknowledgment (ACK) and finish (FIN) flags are monitored within the TCP header and a conclusion is reached about the state of a specific connection. The UDP protocol does not have a formal procedure for establishing and terminating a connection. However, devices with stateful inspection can monitor the state of individual flows1 and match different flows when they logically correspond to each other (e.g., a DNS response from an external server will only be allowed to pass if the corresponding DNS query from the internal source to that server has previously been recorded).

The advantages of applying stateful firewall devices:

- a higher level of protection compared to stateless firewall devices (greater efficiency and more detailed traffic analysis);
- detection of IP spoofing and DoS attacks;
- more log information compared to packet filters.

The disadvantages of applying stateful firewall devices:

- no protection against application layer attacks;
- performance degradation of the router on which they are deployed (this depends on the size of the network and other services run on the router);
- not all of them provide support for UDP, GRE and IPSEC protocols, treating them in the same way as stateless firewall devices;
- no support for user authentication.

Lately, attempts have been made to improve the standard stateful packet inspection technology by adding basic solutions from intrusion detection technology. The improved version is called stateful protocol analysis, also known as DPI (Deep Packet Inspection) analysis of data on the application layer. The devices resulting from this development trend include Application Firewall, Application Proxy Gateways and Proxy servers. Unlike stateful firewall devices that filter traffic based on the data on layers 3, 4 and 5 of the OSI reference model, these devices also enable traffic filtering based on the information on the application layer of the OSI reference model (Layer 7).

Application Firewall

Application Firewall (AF) devices perform a stateful protocol analysis of the application layer. They support numerous common protocols, such as HTTP, SQL, e-mail service (SMTP, POP3 and IMAP), VoIP and XML. Stateful protocol analysis relies on predefined profiles of acceptable operating modes for the selected protocol, enabling the identification of potential deviations and irregularities in the message flow of the protocol through the device. Problems may arise if there is a conflict between the operating mode of a specific protocol, which is defined on the AF device, and the way in which the protocol is implemented in the specific version of the application or of the operating systems used in the network.

The stateful protocol analysis can:

- determine whether an e-mail message contains a type of attachment that is not allowed (e.g., exec files);
- determine whether instant messaging is used via an HTTP port;
- block the connection through which an unwanted command is executed (e.g., an FTP put command on the FTP server);
- block access to a page with unwanted active content (e.g., Java);
- identify an irregular sequence of commands exchanged in the communication between two hosts (e.g., an unusually large number of repetitions of the same command or the use of a command before using the command it depends on);
- enable the verification of individual commands and the minimum and maximum length of appropriate command-line arguments (e.g., the number of characters used in a username). An AF device cannot detect attacks that meet the generally acceptable procedures of operation of a specific protocol, such as DoS (Denial of Service) attacks caused by the repetition of a large number of acceptable message sequences in a short time interval. Due to the complexity of the analysis they perform, and the large number of concurrent sessions they monitor, the main disadvantage of the method of stateful protocol analysis is the intensive use of AF devices.

Application Proxy Gateway

Application Proxy Gateway (APG) devices also perform an analysis of the traffic flow on the application layer. Compared to AF devices, APG devices provide a higher level of security for individual applications since they never allow a direct connection between two hosts, and they can perform an inspection of the content of application-layer messages.

APG devices contain so-called proxy agents or “intermediaries” in the communication between two end hosts. In this way, they prevent direct communication between them. Each successful connection between the end hosts consists of two connections – one between the client and the proxy server and the other between the proxy server and the destination device. Based on the filtering rules defined on the APG device, proxy agents decide whether network traffic will be allowed or not. Traffic-filtering decisions can also be made based on the information contained in the header of an application-layer message or even based on the content conveyed by that message. In addition, proxy agents can require user authentication. There are also APG devices with the capability of packet decryption, analysis and re-encryption, before a packet is forwarded to the destination host. Packets that cannot be decrypted are simply forwarded through the device.

Compared to packet filters and stateful devices, APG devices have numerous deficiencies. The manner of operation of APG devices requires a significantly greater utilisation of resources, i.e., they require more memory and greater utilisation of processor time for analysing and interpreting each packet passing through the device. As a result, APG devices are not suitable for filtering applications that are more demanding in terms of bandwidth or applications that are sensitive to time delays

(real-time applications). Another deficiency of these devices is the limitation in the number of services that can be filtered through them. Each type of traffic passing through the device requires a specific proxy agent that acts as an intermediary in the communication. Consequently, APG devices do not always support the filtering of new applications or protocols. Due to their price, APG devices are commonly used for protecting data centres or other networks containing publicly available servers that are of high importance to an organisation. In order to reduce the load on APG devices and achieve greater efficiency, modern networks more frequently use proxy servers (dedicated proxy servers) that are dedicated to specific services that are not so sensitive to time delays (e.g., e-mail or web proxy servers).

Dedicated Proxy Server

Like APG devices, Dedicated Proxy (DP) servers also have a role as "intermediaries" in the communication between two hosts, although their traffic-filtering capabilities are significantly lower. This type of device is intended for the analysis of the operation of specific services and protocols (e.g., HTTP or SMTP). Due to their limited traffic-filtering capabilities, DP devices are deployed behind firewall devices in the network architecture. Their main function is to perform specialised filtering of a specific type of traffic (based on a limited set of parameters) and carry out the logging operation. The execution of these specific activities significantly reduces the load on the firewall device itself, which is located in front of the DP server. The most widely used devices of this type are Web Proxy servers. A common example of their use is an HTTP proxy server (placed behind the firewall device or router), to which users need to connect when they wish to access external web servers. If an institution has an outgoing connection (uplink) of lower bandwidth, the use of the caching function is recommended in order to reduce the level of traffic and improve the response time. As a result of an increase in the number of available web applications and the number of threats transferred through the HTTP protocol, Web Proxy servers are growing in significance. Consequently, many equipment manufacturers today add the functionality of various firewall technologies to the standard Web Proxy servers, thus increasing their traffic-filtering capabilities.

1.3. Solutions Combining Traffic Filtering with Other Technologies

In addition to their basic purpose of blocking unwanted traffic, firewall devices often combine their filtering functionality with other technologies, primarily routing. It is the other way around with routers. As a result, NAT (Network Address Translation) is sometimes considered to be a firewall technology, although essentially it is a routing technology.

Other related functionalities, such as VPN and IDP, are often available on firewall devices. In order to have a complete overview and due to their frequent use, these technologies are also addressed briefly in this chapter.

NAT (Network Address Translation)

NAT is a technology that enables devices that use private IP addresses to communicate with devices on the Internet. This technology translates private IP addresses, which can be used by devices within a Local Area Network (LAN), into publicly available Internet addresses.

The application of NAT technology may limit (intentionally or unintentionally) the number of available services, i.e., it may disable the functioning of the services that require direct, end-to-end connectivity (e.g., VoIP).

There are three types of NAT translations: dynamic, static and PAT.

Dynamic NAT uses a set of publicly available IP addresses, successively assigning them to hosts with private IP addresses. When a host with a private IP address needs to communicate with a device on the Internet, dynamic NAT translates its private IP address into a publicly available IP address, by taking the first available IP address from a defined pool of publicly available IP addresses. Dynamic NAT is suitable for client computers.

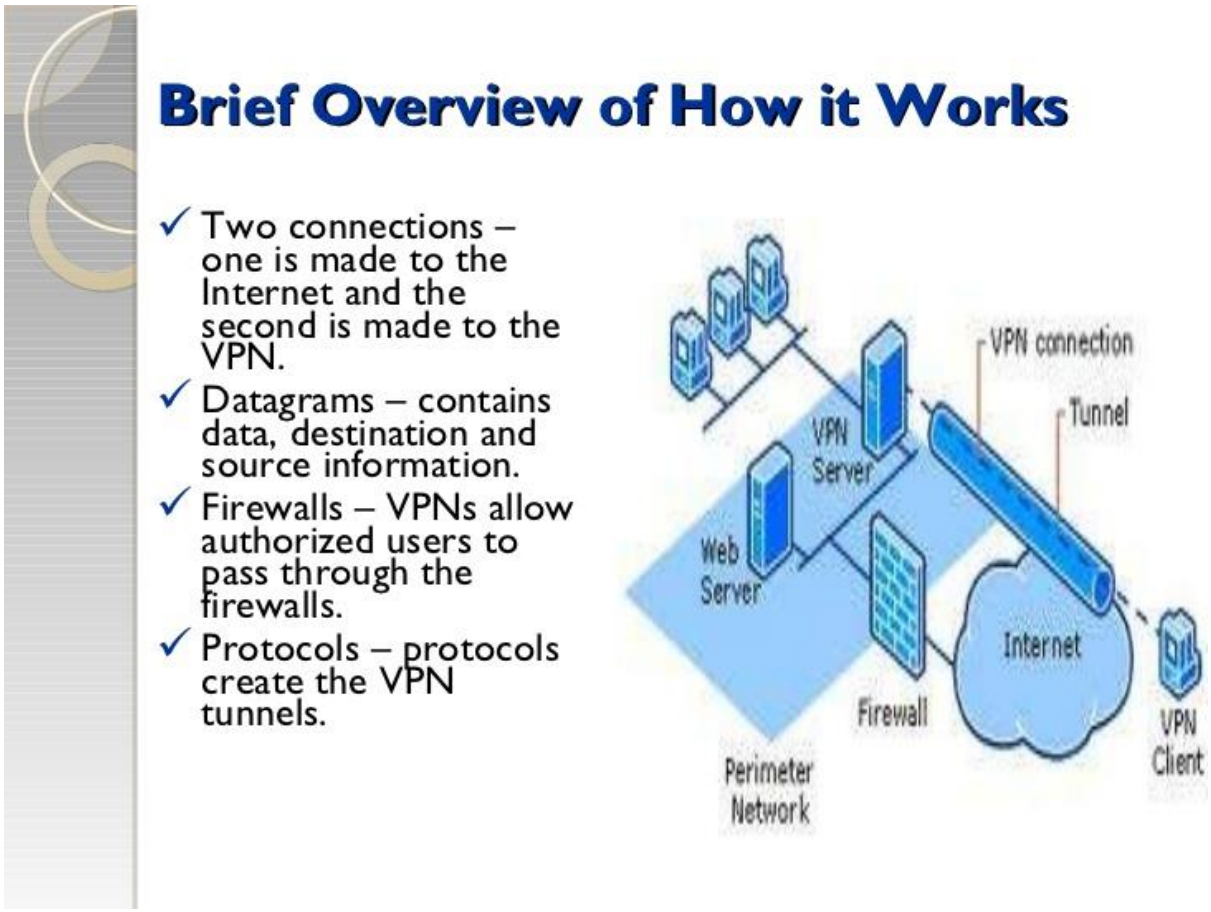
Static NAT provides one-to-one mapping between the private IP address of a host and the public IP address assigned to it. In this manner, the host with a private IP address always appears on the Internet with the same public IP address. This is the main difference between static and dynamic translation. Static NAT is suitable for servers. In both types of translation mentioned above, each private IP address is translated into a separate, public IP address. In order to support a sufficient number of simultaneous user sessions, an organisation using dynamic and/or static NAT needs to have a sufficient number of public IP addresses.

PAT (Port Address Translation or so-called NAT overload) performs mapping between several private IP addresses and one or more public IP addresses. The mapping of each private IP address is performed by way of the port number of the public IP address. PAT translation ensures that each client on a LAN that establishes a connection with a device on the Internet is assigned a different port number of the public IP address. The response from the Internet, which comes as a result of the request, is sent to the port from which the request was forwarded. In this manner, a device that performs the translation (a router, firewall or server) knows to which host from the LAN it should forward the packet. This feature of PAT increases the level of security of the LAN to a certain degree, since it prevents a connection from the Internet being established directly with the hosts on the LAN. Due to this manner of operation, PAT is sometimes, incorrectly, regarded as a security technology, although it is primarily a routing technology.

VPN (Virtual Private Network)

VPN (Virtual Private Network) technology is used to increase the security of data transfer through a network infrastructure that does not provide a sufficient degree of data security. It enables the encryption and decryption of network traffic between external networks and an internal, protected network.

VPN functionality can be available on firewall devices or implemented on VPN servers that are placed behind firewall devices in the network architecture. In many cases, the implementation of VPN services on a firewall device itself is the most optimal solution. Placing a VPN server behind the firewall device requires the VPN traffic to pass through the firewall device in an encrypted form. As a result, the firewall device cannot perform an inspection, access control or logging of the network traffic, and therefore cannot scan it for certain security threats. However, regardless of the place of the implementation, the VPN service requires the application of certain filtering rules of the firewall device in order to enable its uninterrupted operation. Accordingly, special attention should always be paid to making sure that the appropriate protocols and the TCP/UDP services that are necessary for the functioning of the chosen VPN solution are supported.



IDP (Intrusion Detection and Prevention)

Network Intrusion Detection (ID) is based on monitoring the operation of computer systems or networks and analysing the processes they perform, which can point to certain incidents. Incidents are events posing a threat to or violating defined security policies, violating AUP (Acceptable Use Policy) rules, or generally accepted security norms. They appear as a result of the operation of

various malware programmes (e.g., worms, spyware, viruses, and Trojans), as a result of attempts at unauthorised access to a system through public infrastructure (Internet), or as a result of the operation of authorised system users who abuse their privileges.

Network Intrusion Prevention (IP) includes the process of detecting network intrusion events, but also includes the process of preventing and blocking detected or potential network incidents.

Network Intrusion Detection and Prevention systems (IDP) are based on identifying potential incidents, logging information about them, attempting to prevent them and alerting the administrators responsible for security. In addition to this basic function, IDP systems can also be used to identify problems concerning the adopted security policies, to document existing security threats and to discourage individuals from violating security rules. IDP systems use various incident-detection methods.

There are three primary classes of detection methodology:

1. Signature-based detection

Certain security threats can be detected based on the characteristic manner in which they appear. The behaviour of an already detected security threat, described in a form that can be used for the detection of any subsequent appearance of the same threat, is called an attack signature. This detection method, based on the characteristic signature of an attack, is a process of comparing the known forms in which the threat has appeared with the specific network traffic in order to identify certain incidents. Although it can be very efficient in detecting the subsequent appearance of known threats, this detection method is extremely inefficient in the detection of completely unknown threats, of threats hidden by using various techniques, and of already known threats that have somehow been modified in the meantime. It is considered the simplest detection method and it cannot be used for monitoring and analysing the state of certain, more complex forms of communication.

2. Anomaly-based detection

This method of IDP is based on detecting anomalies in a specific traffic flow in the network. Anomaly detection is performed, based on the defined profile of acceptable traffic and its comparison with the specific traffic in the network. Acceptable traffic profiles are formed by tracking the typical characteristics of the traffic in the network during a certain period of time (e.g., the number of e-mail messages sent by a user, and the number of attempts to log in to a host, or the level of utilisation of the processor in a given time interval). These characteristics of the behaviour of users, hosts, connections or applications in the same time interval are then considered to be completely acceptable. However, acceptable-behaviour profiles can unintentionally contain certain security threats, which lead to problems in their application. Likewise, imprecisely defined profiles of acceptable behaviour can cause numerous alarms, generated by the system itself as a reaction to certain (acceptable) activities on the network. The greatest advantage of this detection method is its exceptional efficiency in detecting previously unknown security threats.

3. Detection based on stateful protocol analysis

Stateful protocol analysis is a process of comparing predefined operation profiles with the specific data flow of that protocol on the network. Predefined profiles of operation of a protocol are defined by the manufacturers of IDP devices and they identify everything that is acceptable or not acceptable in the exchange of messages in a protocol. Unlike anomaly-based detection, where profiles are created based on the hosts or specific activities on the network, stateful protocol

analysis uses general profiles generated by the equipment manufacturers. Most IDP systems use several detection methods simultaneously, thus enabling a more comprehensive and precise method of detection.

Testing tools are used for testing the detection, recognition and response capabilities of devices that perform packet filtering (including those that use network address translation), such as firewalls, IDSes/IPSes, routers and switches. These test the Traffic Filtering devices' ability to detect and/or block DoS attacks, spyware, backdoors, and attacks against applications such as IIS, SQL Server and WINS. Standard traffic sessions can be used to test how packet filtering devices handle a variety of protocols including HTTP, FTP, SNMP and SMTP.

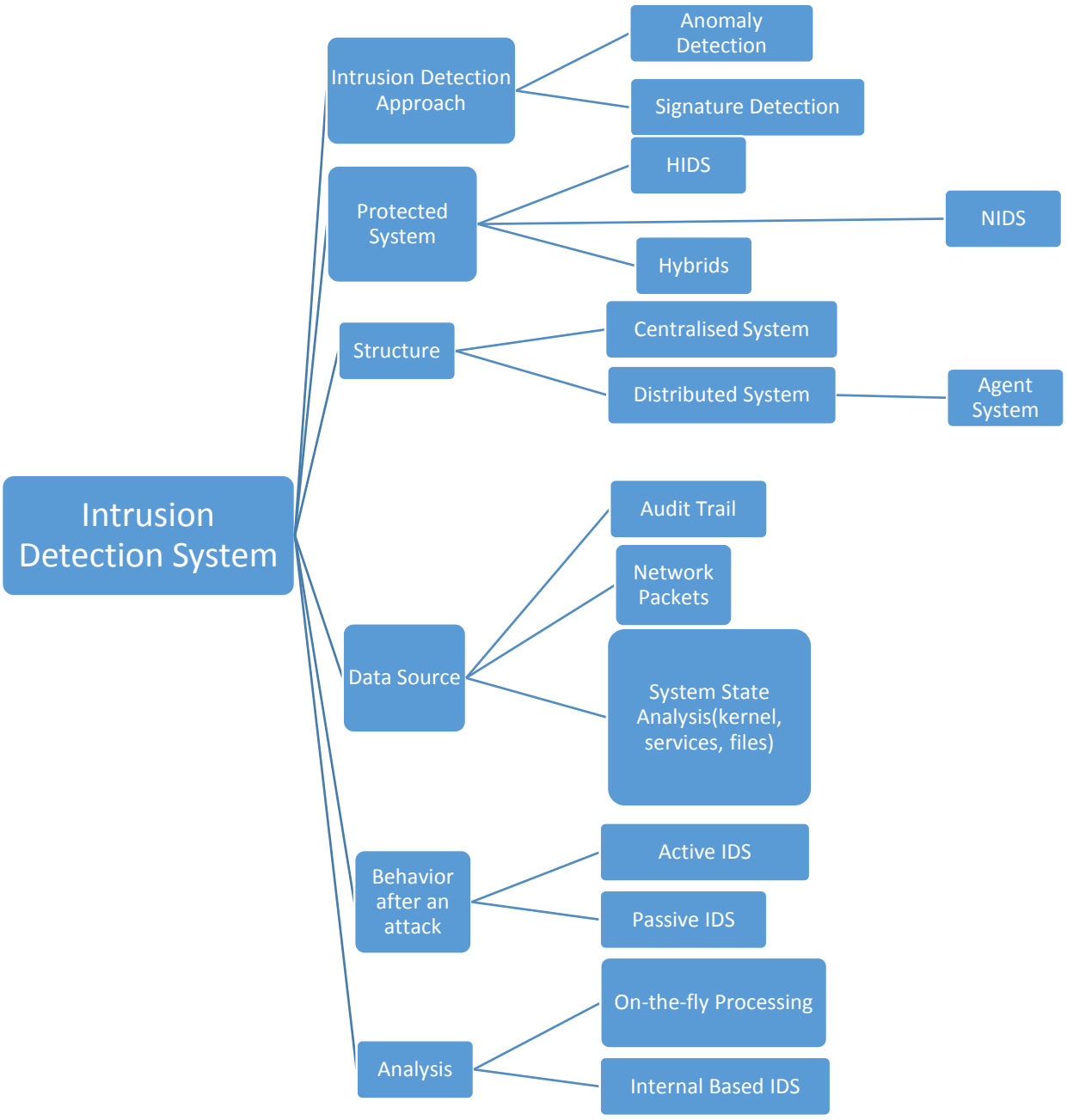


Figure: Intrusion Detection System

Summary

- ✓ The greater the number of unmanaged systems, the greater the risk to the network. Where administrators have audited the network, typically between 1 percent and 10 percent of assets were previously unknown to the administrator.
- ✓ Further to the asset inventory tool the organisation needs to:
  - Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network.
  - Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.
  - Create separate VLANs for BYOD (bring your own device) systems or other untrusted devices.
  - Utilize client certificates to validate and authenticate systems prior to connecting to the private network.
- ✓ There are four basic recommendations for Traffic Filtering in order to reduce security threats, organisations use various devices, technologies and techniques for traffic filtering. Each institution/organisation that wishes to improve the efficiency of filtering and increase the level of security in its network should apply the following recommendations:
  - Define traffic-filtering rules that will determine the manner in which the incoming and outgoing traffic flow in the network will be regulated. A set of traffic-filtering rules can be adopted as an independent packet filtering policy or as a part of the information security policy;
  - Select a traffic-filtering technology that will be implemented depending on the requirements and needs;
  - Implement defined rules on the selected technology and optimise the performance of devices accordingly;
  - Maintain all the components of the solution, including not only devices, but also the policy.
- ✓ Traffic-filtering technologies are commonly divided into
  - packet filtering/stateless firewall
  - stateful firewall technologies
- ✓ NAT is a technology that enables devices that use private IP addresses to communicate with devices on the Internet. This technology translates private IP addresses, which can be used by devices within a Local Area Network (LAN), into publicly available Internet addresses.
- ✓ There are three types of NAT translations: dynamic, static and PAT.