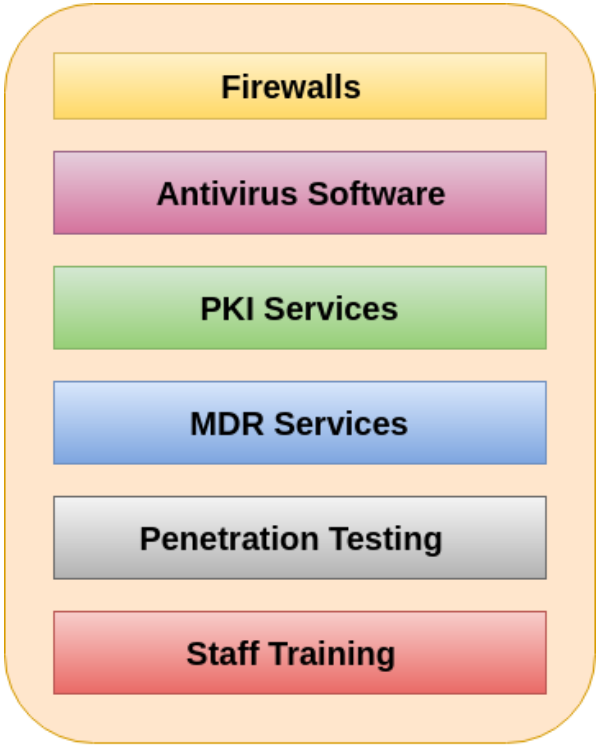
UNIT-4
CYBER SECURITY TOOLS

1. Discuss about various Cyber Security Tools

Protecting our IT environment is very critical. Every organization needs to take cyber security very seriously. There are numbers of hacking attacks which affecting businesses of all sizes. Hackers, malware, viruses are some of the real security threats in the virtual world. It is essential that every company is aware of the dangerous security attacks and it is necessary to keep themselves secure. There are many different aspects of the cyber defence may need to be considered. Here are six essential tools and services that every organization needs to consider to ensure their cyber security is as strong as possible. They are described below:



Cyber Security Tools

1. Firewall

As hacking and cyber-criminals become more sophisticated and defenses become stronger, firewall is arguably the most core of security tools, it remains one of the most important. Its job is to block any unauthorized access to your system. A firewall monitors network traffic as well as connection attempts, deciding on whether or not these should be able to pass freely onto your network or computer.

All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those messages that do not meet the specified security criteria. The Firewall is very useful, but it has limitations also. A skilled hacker knew how to create data and programs that are believing like trusted firewalls. It means that we can pass the program through the firewall without any problems. Despite these limitations, firewalls are still very useful in the protection of less sophisticated malicious attacks on our system.

Antivirus Software

Antivirus software is a program which is designed to prevent, detect, and remove viruses and other malware attacks on the individual computer, networks, and IT systems.

It also protects our computers and networks from the variety of threats and viruses such as Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware.

Most antivirus program comes with an auto-update feature and enabling the system to check for new viruses and threats regularly. It provides some additional services such as scanning emails to ensure that they are free from malicious attachments and web links.

PKI Services

PKI stands for Public Key Infrastructure. This tool supports the distribution and identification of public encryption keys. It enables users and computer systems to securely exchange data over the internet and verify the identity of the other party. We can also exchange sensitive information without PKI, but in that case, there would be no assurance of the authentication of the other party.

People associate PKI with SSL or TLS. It is the technology which encrypts the server communication and is responsible for HTTPS and padlock that we can see in our browser address bar. PKI solve many numbers of cybersecurity problems and deserves a place in the organization security suite.

PKI can also be used to:

- Enable Multi-Factor Authentication and access control
- Create compliant, Trusted Digital Signatures.
- Encrypt email communications and authenticate the sender's identity.
- Digitally sign and protect the code.
- Build identity and trust into IoT ecosystems.

Managed Detection and Response Service (MDR)

MDR is an advanced security service that provides threat hunting, threat intelligence, security monitoring, incident analysis, and incident response. It is a service that arises from the need for organizations (who has a lack of resources) to be more aware of risks and improve their ability to detect and respond to threats. MDR also uses Artificial Intelligence and machine learning to investigate, auto detect threats, and orchestrate response for faster result.

- Managed detection and response is focused on threat detection, rather than compliance.
- MDR relies heavily on security event management and advanced analytics.
- While some automation is used, MDR also involves humans to monitor our network.
- MDR service providers also perform incident validation and remote response.

Penetration Testing

Penetration testing, or pen-test, is an important way to evaluate our business's security systems and security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities exist in operating systems, services and application, improper configurations or risky end-user behavior.

In Penetration testing, cybersecurity professionals will use the same techniques and processes utilized by criminal hackers to check for potential threats and areas of weakness.

Staff Training

Staff training is not a 'cybersecurity tool' but ultimately, having knowledgeable employees who understand the cybersecurity which is one of the strongest forms of defence against cyber-attacks.

Today's many training tools available that can educate company's staff about the best cybersecurity practices. Every business can organize these training tools to educate their employee who can understand their role in cybersecurity.

2.Discuss about FireWalls.

Cryptographic mechanisms protect the confidentiality and integrity of data in transit.
Authentication protocols verify the source of data.

To control what traffic is allowed to enter your network (ingress filtering) or leave your network (egress filtering) you may
deploy a *firewall*.

A firewall is a network security device controlling traffic flow between two parts of a network.

Firewalls are often installed between the network of an entire organization and the Internet, but could also be installed in an intranet to protect individual departments.

For example, a university could put firewalls between the subnets of academic departments and the main campus network.

Firewalls defend a protected network against parties who try to access services from outside the network that are intended to be available only internally.

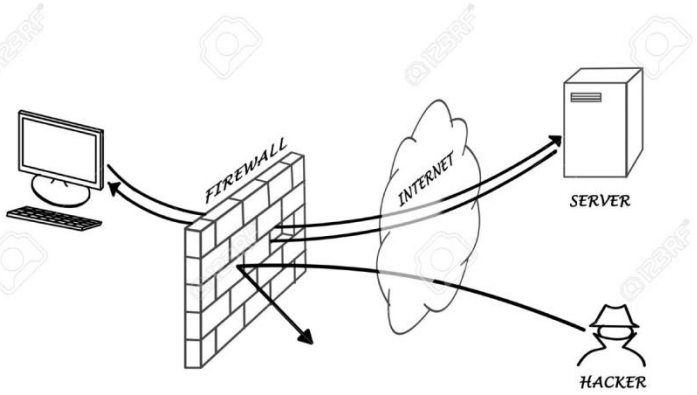
Firewalls can also restrict access from inside to external services that are deemed dangerous or unnecessary for the work of an organization.

All traffic has to go through the firewall for protection to be effective. Dial-in lines (in the distant past), wireless LANs, laptops, and USB sticks are notorious examples of unprotected entry points into the network behind a firewall.

A firewall can decide to route sensitive traffic via a *virtual private network* (VPN). A VPN establishes a secure connection between the gateways of subnets of an organization that are not directly connected.

All traffic between the subnets has to go through these gateways where cryptographic protection is added to extend the security perimeter.

firewall can also perform network address translation, hiding internal machines with private addresses behind public IP addresses, and translating public addresses to private addresses for internal servers. Hiding the internal structure of a network reduces the attack surface. Fewer targets are known to the attacker.



3. Explain about various types fire walls.

Firewalls implement access control. Parameters that could be used for access control can be found at each network layer.

- ✓ **At OSI layer 3** you have source and destination IP addresses.
- ✓ **At OSI layer 4** you have TCP and UDP port numbers. Note that the port number does not necessarily define the service running at that port.
- ✓ **At OSI layer 7** there is information related to various applications: email addresses, email contents, web requests, executable files, viruses and worms, images, usernames, and passwords, to name just a few.

Types of Firewalls:

- Packet filtering firewalls. Packet filtering firewalls are the oldest, most basic type of firewalls.
- Circuit-level gateways.
- Stateful inspection firewalls.
- Application-level gateways (proxy firewalls)
- next-generation firewall (NGFW)

Packet Filtering Firewalls

Packet filters work at OSI layers 3 and 4. Rules specifying which packets are allowed through the firewall and which are dropped are applied to packets individually.

Typical rules specify source and destination IP addresses, and source/destination TCP and UDP port numbers. Rules for traffic in both directions can be defined.

Such a firewall can be implemented by a TCP/IP packet filtering router which examines the TCP/IP headers of every packet going through and can drop packets.

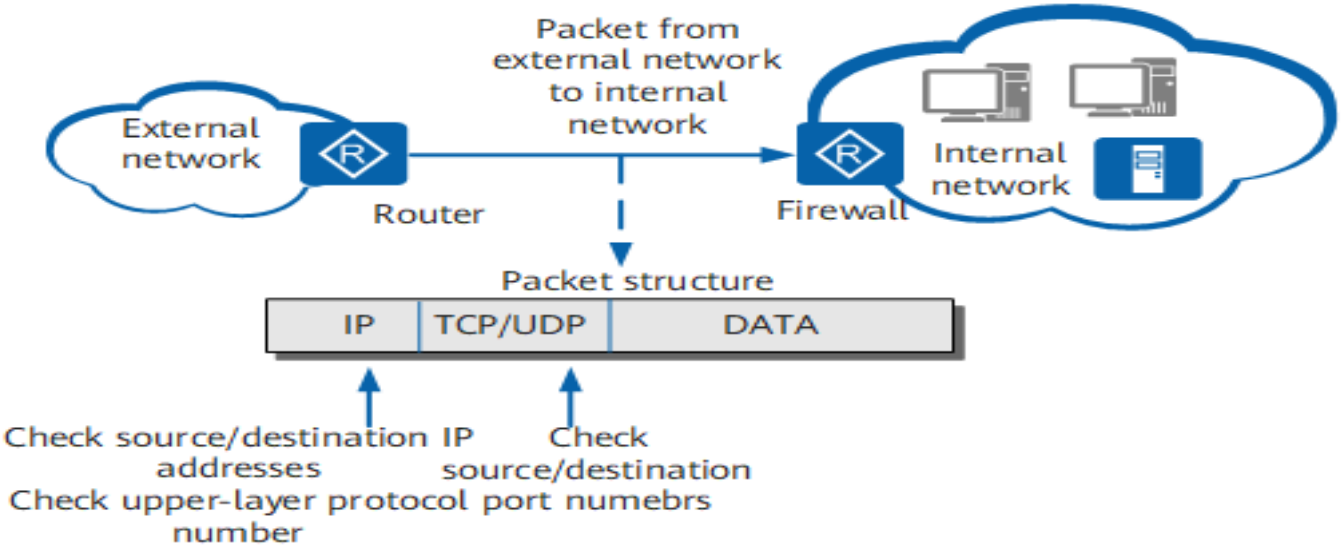
Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on other resources, network performance and end-user experience

Packet filtering firewall disadvantages

- Because traffic filtering is based entirely on IP address or port information, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be easily spoofed
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

Packet filtering may not provide the level of security necessary for every use case, but there are situations in which this low-cost firewall is a solid option. For small or budget-constrained organizations, packet filtering provides a basic level of security that can provide protection against known threats. Larger enterprises can also use packet filtering as part of a layered defense to screen potentially harmful traffic between internal departments.



Packet filtering can be done by routers, giving high performance at lower cost. Moreover, it is easier to configure securely platforms that offer only limited functionality.

Stateful (dynamic) packet filters understand requests and replies. For example, they would know about the (SYN, SYN-ACK, ACK) pattern of a TCP open sequence. Rules are usually only specified for the first packet in one direction, and a new rule is created dynamically after the first outbound packet. Further packets in the communication are then processed automatically. Stateful firewalls can support policies for a wider range of protocols than simple packet filter, e.g. FTP, IRC, or H323.

A stateful firewall is **a firewall that monitors the full state of active network connections**. This means that stateful firewalls are constantly analyzing the complete context of traffic and data packets, seeking entry to a network rather than discrete traffic and data packets in isolation.

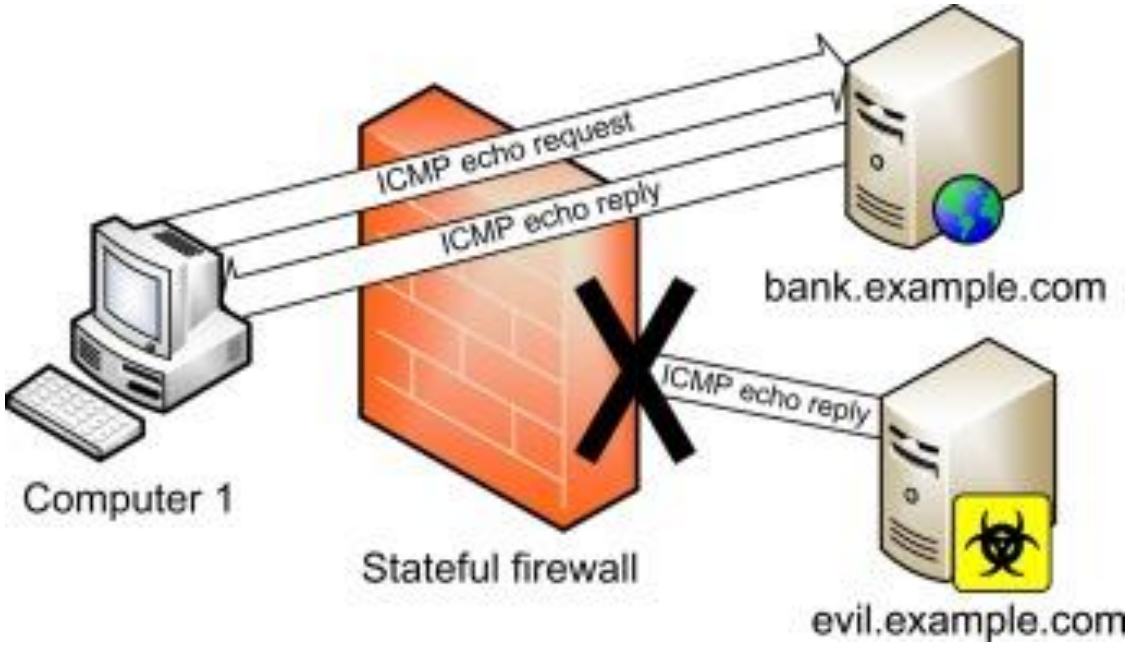
Stateful inspection firewall advantages

- Monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security
- Offers a high degree of control over what content is let in or out of the network
- Does not need to open numerous ports to allow traffic in or out
- Delivers substantive logging capabilities

Stateful inspection firewall disadvantages

- Resource-intensive and interferes with the speed of network communications
- More expensive than other firewall options
- Doesn't provide authentication capabilities to validate traffic sources aren't spoofed

Most organizations benefit from the use of a stateful inspection firewall. These devices serve as a more thorough gateway between computers and other assets within the firewall and resources beyond the enterprise. They also can be highly effective in defending network devices against particular attacks, such as DoS.



Circuit-Level Proxies

Circuit-level proxies have rules similar to packet filters but do not route packets. Rules determine which connections are allowed and which will be blocked. Allowed connections generate a new connection from firewall to destination. This type of firewall is mentioned for the sake of completeness. It is rarely used in practice as the functionality is similar to that of stateful packet filters but the performance is lower.

Circuit-level gateway advantages

- Only processes requested transactions; all other traffic is rejected
- Easy to set up and manage
- Low cost and minimal impact on end-user experience

Circuit-level gateway disadvantages

- If they aren't used in conjunction with other security technology, circuit-level gateways offer no protection against data leakage from devices within the firewall
- No application layer monitoring
- Requires ongoing updates to keep rules current

While circuit-level gateways provide a higher level of security than packet filtering firewalls, they should be used in conjunction with other systems. For example, circuit-level gateways are typically used alongside application-level gateways. This strategy combines attributes of packet- and circuit-level gateway firewalls with content filtering.

Application-level gateways (proxy firewalls)

For each application protocol the firewall should police, a proxy implements the server and client part of the protocol on the firewall. When a client connects to the firewall, the proxy at the firewall acts as the server and validates the request.

A mail proxy, for example, could filter out viruses, worms and spam. If the client request is allowed, the proxy acts as a client and connects to the destination server. Responses come back through the firewall and are again processed and checked by the proxy.

The proxy server is the only entity seen by the outside world and it appears transparent to the internal users except for filtering, e.g. removing email attachments. Proxies can be seen as another instance of *controlled invocation*.

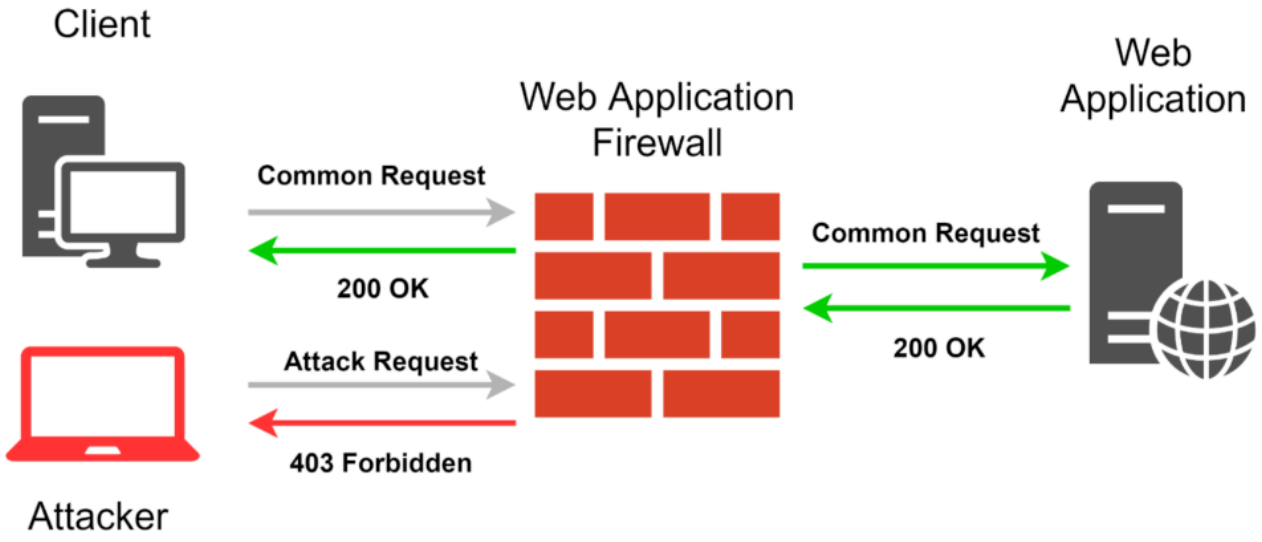
Application-level gateway advantages

- Examines all communications between outside sources and devices behind the firewall, checking not just address, port and TCP header information, but the content itself before it lets any traffic pass through the proxy
- Provides fine-grained security controls that can, for example, allow access to a website but restrict which pages on that site the user can open
- Protects user anonymity

Application-level gateway disadvantages

- Can inhibit network performance
- Costlier than some other firewall options
- Requires a high degree of effort to derive the maximum benefit from the gateway
- Doesn't work with all network protocols

Application-layer firewalls are best used to protect enterprise resources from web application threats. They can both block access to harmful sites and prevent sensitive information from being leaked from within the firewall. They can, however, introduce a delay in communications.



Next-generation firewall

A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

NGFW advantages

- Combines DPI with malware filtering and other controls to provide an optimal level of filtering
- Tracks all traffic from Layer 2 to the application layer for more accurate insights than other methods
- Can be automatically updated to provide current context

NGFW disadvantages

- In order to derive the biggest benefit, organizations need to integrate NGFWs with other security systems, which can be a complex process
- Costlier than other firewall types

4. Write about deployment of FireWalls:

Hardware-based firewalls

A hardware-based firewall is an appliance that acts as a secure gateway between devices inside the network perimeter and those outside it. Because they are self-contained appliances, hardware-based firewalls don't consume processing power or other resources of the host devices.

Sometimes called *network-based firewalls*, these appliances are ideal for medium and large organizations looking to protect many devices. Hardware-based firewalls require more knowledge to configure and manage than their host-based counterparts.

Software-based firewalls

A software-based firewall, or *host firewall*, runs on a server or other device. Host firewall software needs to be installed on each device requiring protection. As such, software-based firewalls consume some of the host device's CPU and RAM resources.

Software-based firewalls provide individual devices significant protection against viruses and other malicious content. They can discern different programs running on the host, while filtering inbound and outbound traffic. This provides a fine-grained level of control, making it possible to enable communications to/from one program but prevent it to/from another.

5. What Is a Stateless Firewall?

Stateless firewalls are **designed to protect networks based on static information such as source and destination**. Whereas stateful firewalls filter packets based on the full context of a given network connection, stateless firewalls filter packets based on the individual packets themselves.

Stateless firewalls use clues from the destination address, source and other key values to assess whether threats are present, then block or restrict those deemed untrusted. Preset rules enforce whether traffic is permitted or denied, but the system is typically unable to determine the difference between truly desired communications and sophisticated attempts to disguise unauthorized communications as trusted ones.

As one of the earlier iterations of firewalls, stateless firewalls don't look beyond the header of packet contents to determine if traffic is authorized.

The stateless firewall also does not examine an entire packet, but instead decides whether the packet satisfies existing security rules.

These firewalls require some configuration to arrive at a suitable level of protection.

6.XML Gateway-Firewalls

The XML Firewall processes XML requests and responses over HTTP or HTTPS.

An XML firewall is an application layer firewall that specifically defends XML-based applications against a wide variety of XML message and parser level attacks. XML firewalls are generally implemented as proxies due to the requirement that incoming and outgoing messages must be inspected for vulnerabilities before being passed to the application or client.

XML firewalls are designed to address familiar Web-based attacks that can be transported via XML, such as SQL injection and cross-site scripting (XSS). They are primarily geared toward detecting and preventing XML specific attacks such as extremely large messages, highly nested elements, coercive parsing, recursive parsing, schema and WSDL poisoning, and routing based attacks.

XML firewalls improve the security of XML-based applications by preventing attacks that are likely to cause a service outage were they to be consumed by a Web application server. They remove the need for highly duplicated security-focused code within applications that can degrade performance.

7.Explain about Firewall Administration

Firewall Administration is **ensuring the proper management, configuration, and change management of the firewall**. It is comprised of controlling access to the platform, platform operating system builds, log reviews, time synchronization and backups.

An organization may have many different firewalls protecting its devices and network as standard.

Management of these firewalls means setting rules and policies, tracking changes, and monitoring compliance logs.

It also includes the monitoring of user access to firewall settings.

The configuration ensures the firewall functions securely and efficiently.

Analysis of firewall logs and records helps to identify and react to any network threats or unauthorized changes to settings.

A well-managed firewall will perform efficiently and safely, lowering the chance of cyber attacks within the organization.

Firewall Management

1. Block all access by default

When configuring a firewall, it's important to start by blocking access to the network from all traffic. Rules and policies can then be introduced to highlight the traffic that is permitted to connect to the network.

2. Regularly audit firewall rules and policies

Regularly audit rules and settings to remove any unused, old rules, as well as any that conflict. Old or unused rules can be exploited to gain access to the network, heightening the chance of cyberattacks. A firewall could have hundreds of unused rules which have become outdated. By highlighting and updating old rules, firewalls can become more efficient as well as more secure.

3. Keep the firewall up-to-date

Firewall software should be kept up-to-date so any vulnerabilities highlighted by the vendor can be fixed. The latest version will ensure the firewall will be as efficient and secure as possible. Where possible, any software updates or patches should be automated.

4. Keep track of authorized users

Firewall management is an important responsibility, and there's a severe risk in allowing too many users access to firewall settings. Those with access should be senior network administrators, and all changes to configuration should be monitored.

5. Document all firewall changes

Changes to firewall rules should be well documented within the organization so any damaging changes can be reversed. If rules are documented, it lessens the risk of conflicting rules causing unforeseen access issues in the network.

A clear process for recording and approving changes to firewall rules should be set as part of the management system. Documentation should record the business requirements for any change, and the context for the decision. New rules can be assessed for their business needs and risk levels.

Firewall policies

Firewall Policies

Permissive policies allow all traffic but block certain dangerous services, such as Telnet or *snmp*, or port numbers known to be used by an attack. If you forget to block something

Restrictive policies block all traffic and allow only traffic known to meet a useful purpose, such as HTTP, POP3, SMTP, or SSH. This is the more secure option. If you block something that is needed, someone will complain and you can then allow the protocol.

A policy is usually represented as an ACL with positive and negative entries.
A typical firewall ruleset could look like this:

- Allow from internal network to Internet: HTTP, FTP, SSH, DNS
- Allow from anywhere to mail server: SMTP only
- Allow from mail server to Internet: SMTP, DNS
- Allow from inside to mail server: SMTP, POP3
- Allow reply packets
- **Block everything else**.

Firewall Configuration

A firewall plays a vital role in network security and needs to be properly configured to keep organizations protected from data leakage and cyber attacks.

This is possible by configuring domain names and Internet Protocol (IP) addresses to keep the firewall secure.

Firewall policy configuration is based on network type, such as public or private, and can be set up with security rules that block or allow access to prevent potential attacks from hackers or malware.

Improper firewall configuration can result in attackers gaining unauthorized access to protected internal networks and resources.

As a result, cyber criminals are constantly on the lookout for networks that have outdated software or servers and are not protected. Gartner highlighted the size and magnitude of this issue, predicting that 99% of firewall breaches would be caused by misconfigurations in 2020.

Firewalls shall be configured in accordance with Firewall Security Procedures, and at a minimum shall address the following:

- All inbound traffic shall be denied unless explicitly allowed.
- All outbound traffic shall be denied unless explicitly allowed.
- Firewall devices shall be configured to prevent all known network attacks (e.g., Internet Protocol (IP) spoofing, TCP SYN, directed broadcast, Internet Control Message Protocol (ICMP) mapping, Simple Network Management Protocol (SNMP) mapping, Denial of Service (DoS), etc.).
- Firewall devices shall be secured behind locked doors within rooms that have air conditioning and air filtration.
- Firewall devices shall be connected to a dedicated battery-backup power supply.
- All firewall management functions must use encryption along with user id and password.
- Firewall operating system builds shall be based upon minimal feature sets. All unnecessary operating system features shall be removed from the build prior to firewall implementation. All appropriate operating system patches shall be applied before any installation of firewall components.
- All firewalls shall have a failover configuration.
- All firewalls shall be configured to use various logging facilities. The level and matter of logging shall include the following at a minimum: 1) Critical warnings and error messages 2) All login attempts 3) All logon access 4) All configuration attempts 5) All configuration changes

Firewall monitoring

Firewall monitoring is the **tracking of important firewall metrics** that play a critical role in the efficient firewall performance.

Firewall monitoring should typically include

- Firewall log monitoring
- Firewall rule monitoring
- Firewall configuration monitoring
- Firewall alert monitoring

An important aspect of the firewall monitoring services is that it should be proactive. Identifying internal and external security threats proactively helps in identifying issues at an early stage. To prevent network attacks, it is critical to manage firewall monitoring service efficiently.

Firewall monitoring important?

A firewall is a piece of hardware or software that controls what enters and exits a network. The efficiency of a firewall depends on a couple of things:

- The firewall's processing speed
- The rules governing the firewall

Firewall log monitoring plays an important role in business risk assessment. Analyzing firewall traffic logs is vital to understand network and bandwidth usage

Firewall logs analysis reveals a lot of information about the security threat attempts at the periphery of the network and on the nature of traffic coming in and going out of the firewall.

The analyzed firewall logs information, provides real-time information to the Administrators on the security threat attempts and so that they can swiftly initiate remediation action. It allows you to plan your bandwidth requirement based on the bandwidth usage across the firewall.

Firewalls rule monitoring ensures rules are sufficient, and makes firewall as the backbone of robust network security infrastructure. However, firewall rules can be difficult to manage. Security administrators are often busy with multiple change requests that they neither have the time nor resources to investigate all the implications of a change and implement changes manually. In an enterprise network, there are often multiple firewalls, and most organizations have moved or are moving to the cloud, adding more complexity and increasing challenges for admins.

Automating firewall rules plays a key role in managing firewalls effectively. Enterprise networks need a firewall policy management tool that not only provides visibility into the entire firewall rule set, but also helps understand the repercussions of changes and can push these changes to the respective firewall device.

User activity monitoring can be performed using log analysis. Firewall logs help reveal information about infiltration attempts at the perimeter of a network, and on the nature of traffic coming in and going out of the firewall; this means security administrators can monitor user level security threats and traffic usage by optimally analysing the firewall logs. Security administrators need to also set user specific alarms by setting traffic and bandwidth triggers, this is helpful in identifying anomalous activities in the network

Alert Administration

- Firewall Analyzer lets you to administer the triggered alerts, so that the network administrators take care of the triggered alerts and carry out remediation if required.
- The triggered Alerts can be administered by the users. You can assign owner to a particular Alert, add or view Note for a particular Alert, view the history of the Alert from the time of trigger.

In a Firewall device, there could be numerous rules/access-list defined to secure the network from external attacks. Out of the rules/access-list configured, there could be certain rules which would be most used and certain which are least used or never used. Firewall Analyzer captures the most used rules in the **Top Used Rules** as they would be available in the logs generated by Firewall.

But, to get the **Unused Rules**, one needs to configure the Firewall Analyzer to fetch the complete rules from the device. Once, Firewall Analyzer fetches the complete rules configured in the Firewall, it can provide the **Unused Rules** view.

7. Discuss about Firewall Selection

There are seven key points to consider before you buy.

Visibility & Control Of Your Applications

- Traditional port-based firewalls only provide you with limited control and visibility of the applications and end-users accessing your network.

- With the right firewall in place, you can apply policies to certain end-users, allowing access to those with jobs pertinent to the applications being used.

- Different end-users can have different polices applied that prohibit them from accessing certain applications.

Furthermore, next-gen firewalls can limit access to certain parts of applications. For instance a user might be able to use Facebook calling and messaging but not be able to post to their timeline or on a friends “wall.”

Protection and Prevention From Threats

if the firewall can't see the devices or applications being used- how will it protect your network and your end-users?
A next-gen firewall can see and control all of the applications and sensitive information on your wireless network. They can limit traffic and risks to your network by only allowing approved applications to be used.
You can even scan these approved applications to ensure there are no potential threats. As an added bonus, because applications have to be approved by the firewall, it can also reduce bandwidth consumption helping to improve your overall wifi performance.

Legitimate 1 Gigabit Throughput

Port-based firewalls often claim with each port you get 1 gigabit, however once all of the services are turned on like malware, you can cut that throughput by a third.
With next- generation firewalls 1 gigabit is as claimed, you get 1 gigabit of throughput with ALL of the services turned on.

It's About Your Devices Not IP Addresses

Instead of searching to find a user using an IP address, your next-gen firewall is capable of finding a device by user name.
This way you know exactly how many devices each of your employees are using to access the network, and if they cause a breach you can find the device and wipe it clean.

Remote Users

With the influx in employers allowing remote workers in every industry, employees need to be able to access your internal network and applications from any location.

Whether it's from home, the library, a co-working space or even a Starbucks, they should be able to connect and complete their work.

The same rules and policies should be enforced by the firewall outside of the hospital, school grounds, warehouse, or university. This keeps traffic coming in and out of your internal server safe and threat free.

Streamlined Security Infrastructure

Buying more security components (appliances) hoping they fix your security needs isn't always the answer, and often times ends up being costly and ineffective.
Adding more and more components means there's more to manage and update, which can decrease your efficiency by creating a unnecessarily more complex system.
Next-gen firewalls already have the necessary security infrastructure components built-in, including:

- Anti-virus protection
- Spam filtering
- Deep packet inspection
- Application filtering

It's a comprehensive security component that enables you to not have to worry about what other pieces you'll need to add in order to make your network more secure.

Cost

Last but not least, cost is always a factor when it comes to choosing the right firewall. It's important that you think about not only how much something costs but how it will fit into your budget.

Often times we fail to see the harm in not purchasing something, and waiting until something goes wrong. Well if something goes wrong, and data is leaked, it can end up costing you a lot more than just money.

Modern firewalls are more affordable than you might think, especially when compared to the cost of a major network security breach, or the decreased efficiency you'll experience from having poor wifi performance due to an old or insufficient firewall.

USES OF A FIREWALL

The uses of a Firewall are numerous.

- The useful thing about a Firewall is that it prevents unauthorized remote access and remote control of your computer by a hacker for evil purposes.
- Data security is ensured based on IP address and protocol.
- It ensures continuity of operations and availability of information.
- It blocks destructive or unsuitable or pornographic content.
- It prevents ransomware, malware, and phishing attacks.
- It shields older PCs with earlier versions of OS.
- It is safer for online gamers.

8. Write about IDPS Administration

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

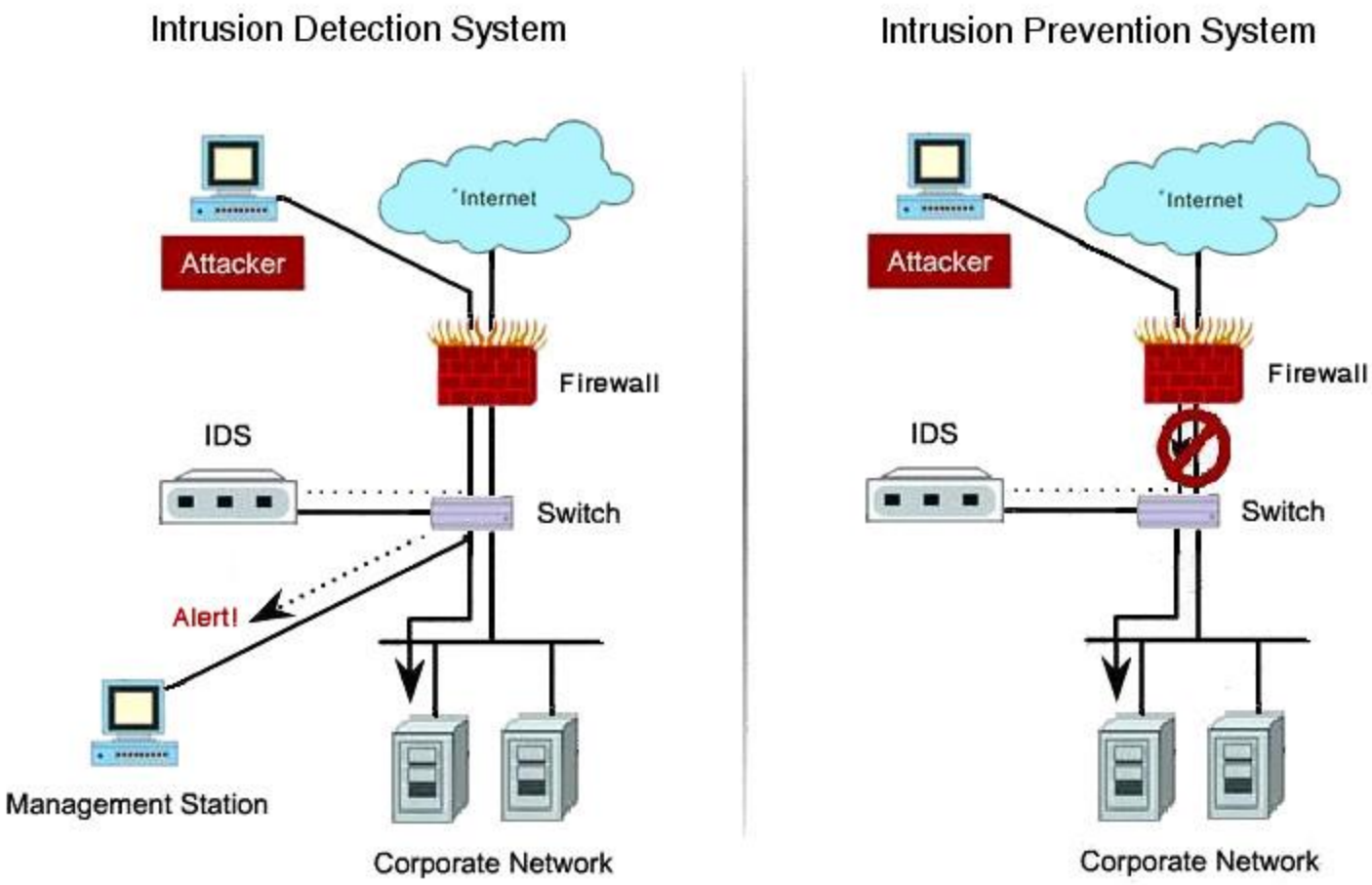
Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

The IDP currently provides different mechanisms to detect attacks.

Stateful signatures Detect known attack patterns. This mechanism allows you to detect a greater number of attacks, and reduce the incidence of false positive alerts

Protocol anomaly detection Reviews the different types of connections that go through the IDP and acknowledges any connections that deviate from the proper protocol standards

Backdoor detection Looks through interactive traffic for possible malicious communications. A backdoor is an application that resides on a host system unknown to the end user. When using the backdoor detection mechanism on your IDP, you can identify these intrusive connections and then block these connections to eliminate this harmful traffic.


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network
Intrusion Prevention System
Internet
Attacker
Firewall
IDS
Switch
Corporate Network

Traffic anomaly detection Allows you to look further than a single packet or a single session. It allows you to look across multiple sessions and identify anomalous traffic

Layer-2 detection Monitors network traffic on the second layer of the Open Systems Interconnect (OSI) model. This allows you to detect address resolution protocol (ARP) attacks on your network.

-

DoS detection Allows you to detect certain types of Denial of Service (DoS) attacks. Denial of Service attacks can bring your network to its knees and early detection is critical to mitigate these attacks.

-

Spoofing detection Provides the capability to detect spoofed IP packets. A spoofed IP packet is a packet that seems to be coming from a host, but really is coming from a malicious attacker.

Key Functions of IDPS Technologies

Recording information related to observed events.

Notifying security administrators of important observed events. This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

Producing reports. Reports summarize the monitored events or provide details on particular events of interest.

Four types of IDPS technologies:

- Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.

- Wireless, which monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves.

- Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as DDoS attacks, scanning, and certain forms of malware.

- Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

Once an IDPS product has been selected, the administrators need to design an architecture, perform IDPS component testing, and deploy and secure the IDPS components. There are many architectural considerations, including component placement, solution reliability, interoperability with other systems, management network architecture, and necessary changes to other security controls

Ongoing Solution Maintenance Administrators should maintain IDPSs on an ongoing basis. This should include the following:

- Monitoring the IDPS components themselves for operational and security issues
- Periodically verifying that the IDPS is functioning properly (e.g., processing events, alerting appropriately on suspicious activity)
- Performing regular vulnerability assessments
- Receiving notifications from vendors of security problems with IDPS components including OSs and non-IDPS applications) and responding appropriately to those notifications

- the administrators need to design an architecture, perform IDPS component testing, and deploy and secure the IDPS components. There are many architectural considerations, including component placement, solution reliability, interoperability with other systems, management network architecture, and necessary changes to other security controls.

- Before performing a production implementation, organizations should consider implementing the components in a test environment first to reduce the likelihood of implementation problems disrupting production. activating many sensors or agents at once might overwhelm the management servers and consoles, making it difficult for administrators to perform tuning and customization.
- Acquiring and Applying Updates

9.What is VPN and administration of VPN

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

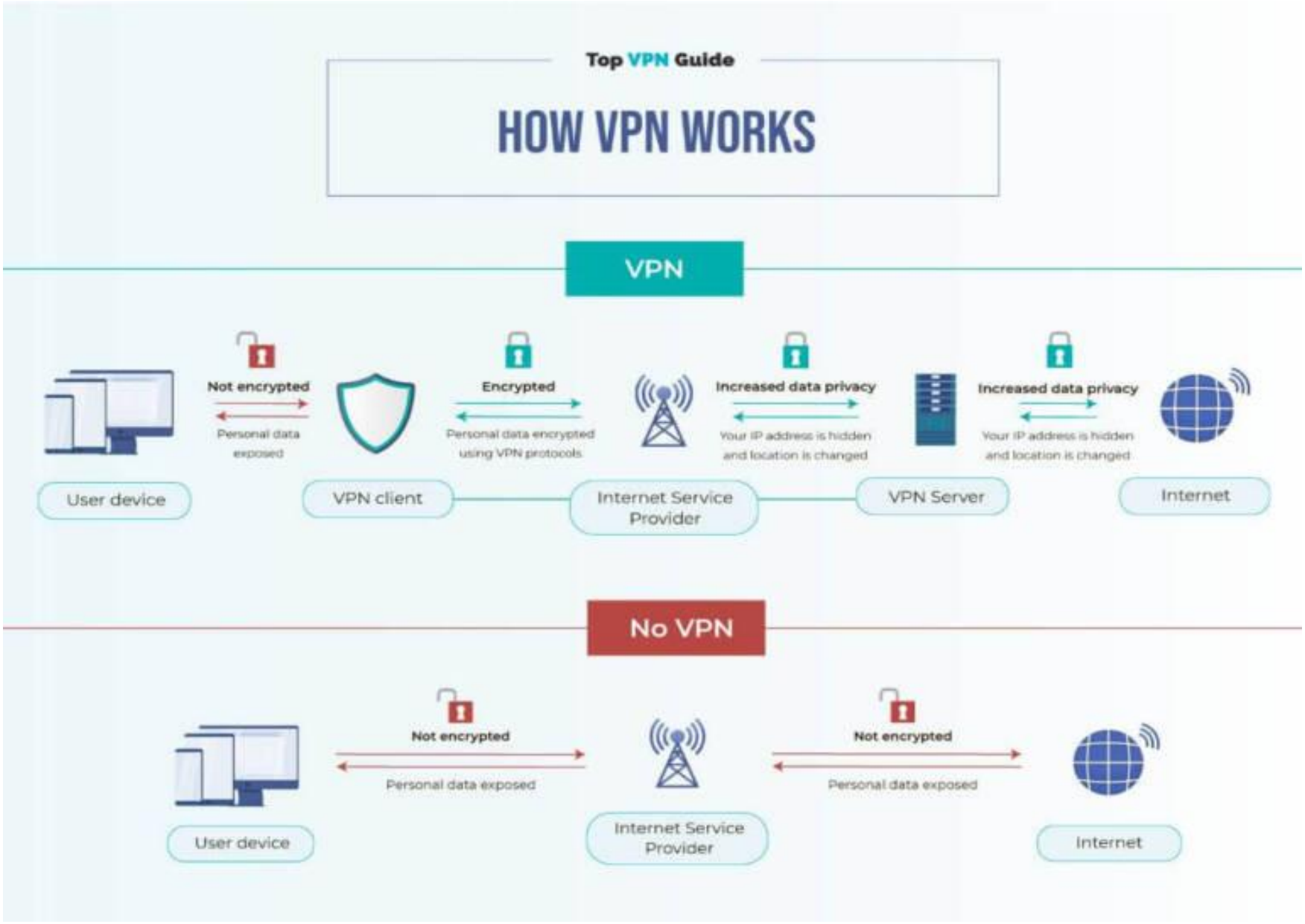
Today, **VPN provides employees to access information from company servers remotely** without necessarily having to be in their offices.

How does VPN Work?

The idea behind VPN revolves majorly on the **encryption and decryption of data**. Usually, a Virtual Private Network (VPN) works as a distinct tunnel that provides for a flow of information to your destination through the internet.

What simply happens is that the VPN works by **routing/ directing your computer's internet connection through the VPN private servers rather than your internet service provider**.

It provides you with a **new IP address**, different from the one on your device, and therefore masking your identity. The **VPN server then encrypts your data** making it difficult to read in the off chance that it is intercepted by cybercriminals.


Top VPN Guide
HOW VPN WORKS
VPN
Not encrypted
Personal data exposed
Encrypted
Personal data encrypted using VPN protocols
Increased data privacy
Your IP address is hidden and location is changed
Increased data privacy
Your IP address is hidden and location is changed
User device
VPN client
Internet Service Provider
VPN Server
Internet
No VPN
Not encrypted
Personal data exposed
Not encrypted
Personal data exposed
User device
Internet Service Provider
Internet

VPN Models

Virtual private networks may be classified by several categories:

Remote access: A *host-to-network* configuration is analogous to connecting a computer to a local area network. This type provides access to an enterprise network, such as an intranet. This may be employed for telecommuting workers who need access to private resources, or to enable a mobile worker to access important tools without exposing them to the public

Internet.Site-to-site : A *site-to-site* configuration connects two networks. This configuration expands a network across geographically disparate offices, or a group of offices to a data center installation. The interconnecting link may run over a dissimilar intermediate network, such as two IPv6 networks connected over an IPv4 network.[4]

Extranet-based site-to-site : In the context of site-to-site configurations, the terms **intranet** and **extranet** are used to describe two different use cases.[5] An *intranet* site-to-site VPN describes a configuration where the sites connected by the VPN belong to the same organization, whereas an *extranet* site-to-site VPN joins sites belonging to multiple organizations.

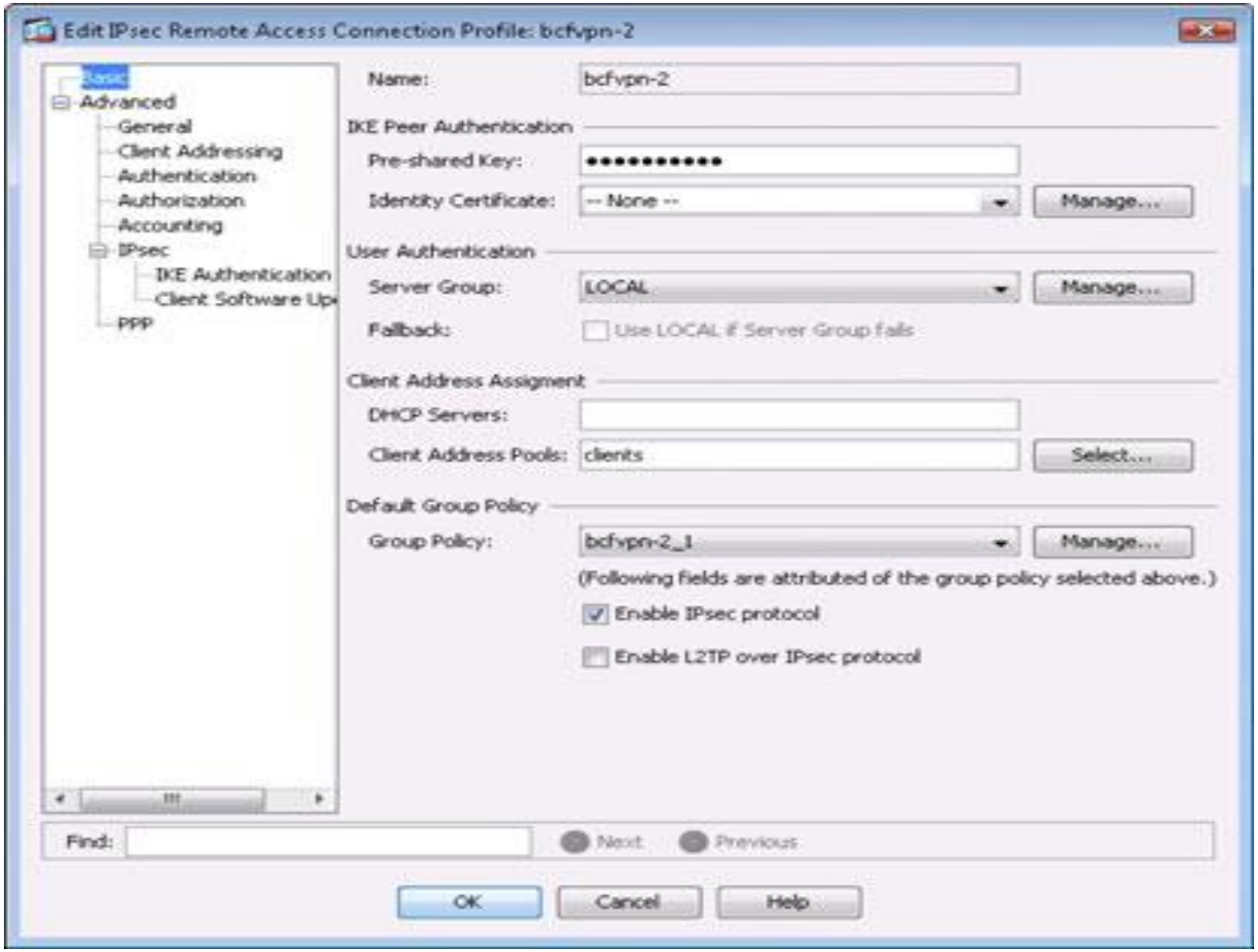
An Administrator is **a special type of User that has been granted rights to administer and configure all aspects of the VPN**.

A VPN connection requires a **VPN Server and a VPN Clie**nt — the server is the gatekeeper at one end of the tunnel, the client at the other. The main difference between the server and the client is that it's the client that initiates the connection with the server. A VPN client can establish a connection with just one server at a time. However, a server can accept connections from many clients.

the VPN server is a separate hardware device, most often a security appliance such as a Cisco ASA security appliance. VPN servers can also be implemented in software.

The following illustration shows one of the many VPN configuration screens for a Cisco ASA appliance. This screen provides the configuration details for an IPSec VPN connection.

The most important item of information on this screen is the Pre-Shared Key, which is used to encrypt the data sent over the VPN. The client will need to provide the identical key in order to participate in the VPN.


Edit IPsec Remote Access Connection Profile: bcfvpn-2
Basic
Advanced
General
Client Addressing
Authentication
Authorization
Accounting
IPsec
IKE Authentication
Client Software Up
PPP
Name:
bcfvpn-2
IKE Peer Authentication
Pre-shared Key:
Identity Certificate:
-- None --
Manage...
User Authentication
Server Group:
LOCAL
Manage...
Fallback:
Use LOCAL if Server Group fails
Client Address Assignment
DHCP Servers:
Client Address Pools:
clients
Select...
Default Group Policy
Group Policy:
bcfvpn-2_1
Manage...
(Following fields are attributed of the group policy selected above.)
Enable IPsec protocol
Enable L2TP over IPsec protocol
Find:
Next
Previous
OK
Cancel
Help

A VPN client is usually software that runs on a client computer that wants to connect to the remote network. The VPN client software must be configured with the IP address of the VPN server as well as authentication information such as a username and the Pre-Shared Key that will be used to encrypt the data.

If the key used by the client doesn't match the key used by the server, the VPN server will reject the connection request from the client.

The following illustration shows a typical VPN software client. When the client is configured with the correct connection information (which you can do by clicking the New button), you just click Connect. After a few moments, the VPN client will announce that the connection has been established and the VPN is connected.

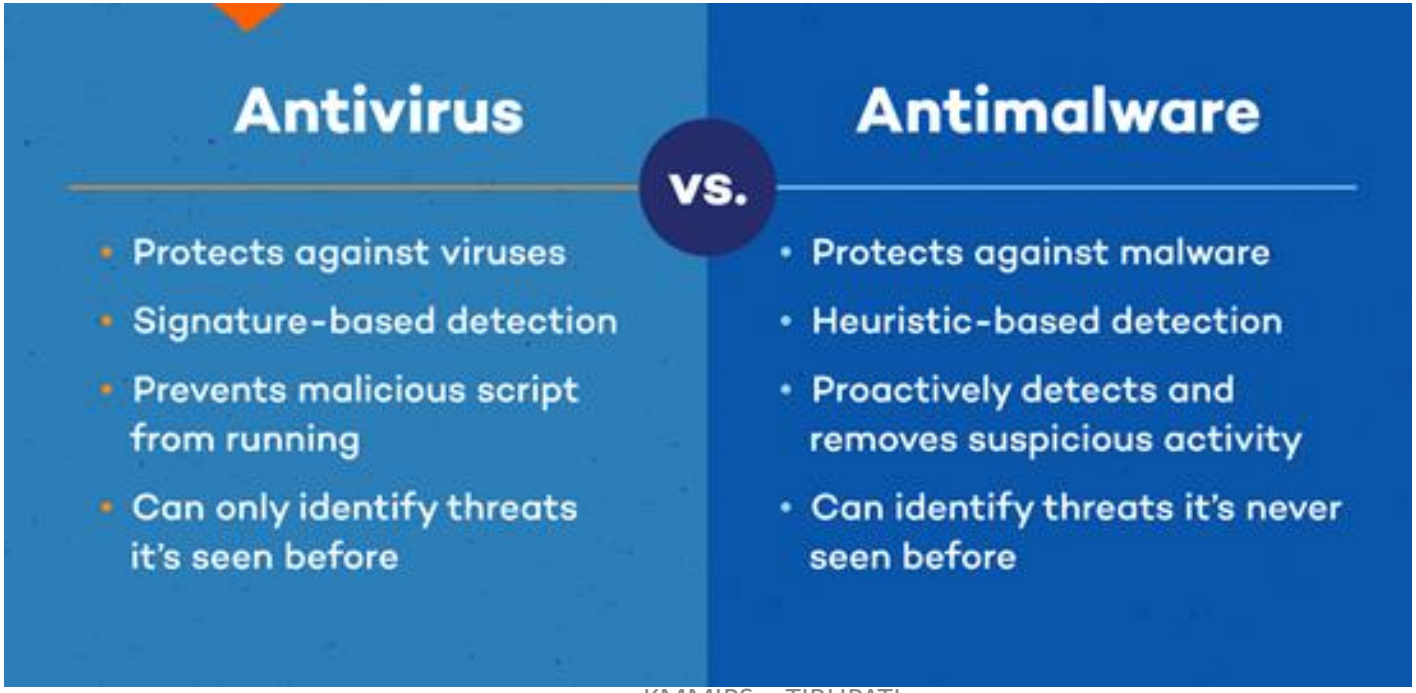
The ability to automatically scale up and down depending on organizational needs is crucial, and central management allows IT administrators to do exactly that by enabling them to:

- Simultaneously manage 100 to 50,000+ connections
- Automate roll-out of company-wide VPN software updates, monitor policy compliance and easily provision or de-provision user access
- Easily scale up or down based on the latest organizational needs
- Integrate with an existing user database (such as Active Directory)
- Deciding in type of VPN to be created
- Purchase of VPN server/client software
- Type of authentication mechanism to identify VPN client.

10. write about AntiVirus/ AntiMalware

A computer virus spreads from user to user by replicating itself through programming a file. Antivirus works to identify known threats using signature-based detection. This type of detection matches file signatures to a database of known malware. In contrast, antimalware utilizes heuristic-based detection to proactively find source codes that indicate a threat.

Antivirus and antimalware were both created to detect and protect against malicious software. While the term antivirus denotes that it only protects against computer viruses, its features often protect against the many common forms of malware today.



What Should Your Antivirus Software Include?

Key indicators of well-rounded antivirus software include:

- ✓ **Real-time scanning:** background scanning means the program will detect threats as you encounter them.
- ✓ **Automatic updates:** updates target any new forms of malware since installation.
- ✓ **Remove threats:** your software should remove malware, not just detect and block it.

What to Look For In Antimalware Software

Whether you find a separate antimalware software or purchase antivirus with added capabilities, look for a program with the following:

- ✓ **Sandboxing:** this controlled environment allows the software to test suspected threats and determine whether or not they're safe to use.
- ✓ **Traffic filtering:** this type of filtering protects your device by blocking access to suspicious servers and sites involved with malware distribution.
- ✓ **Proactive security:** your software should scan, detect, and remove known malware threats like trojans, adware, and spyware.

11.Explain about various Penetration test Methodologies

Penetration testing (or pen testing) is a simulation of a cyber attack that tests a computer system, network, or application for security weaknesses. These tests rely on a mix of tools and techniques real hackers would use to breach a business.

Other common names for penetration testing are **white hat attacks** and **ethical hacking**.

Standardized Penetration Testing Methodologies
Companies typically rely on one of the five standardized penetration testing methods: **OWASP**, **OSSTMM**, **ISSAF**, **PTES**, and **NIST**.

OWASP
The OWASP (Open Web Application Security Project) is a framework for identifying application vulnerabilities. This method allows a team to:

- Recognize vulnerabilities within web and mobile applications.
- Discover flaws within development practices.

The OWASP also enables testers to rate risks, which saves time and helps prioritize issues. This framework has a huge user community, so there is no shortage of OWASP articles, techniques, tools, and technologies.

OSSTMM

The OSSTMM (Open-Source Security Testing Methodology Manual) relies on a scientific methodology for network penetration testing. This peer-reviewed framework provides an accurate characterization of operation security ideal for ethical hacking.

The OSSTMM enables pen testers to run customized tests that fit the organization's technological and specific needs.

ISSAF

The ISSAF (Information System Security Assessment Framework) provides a specialized and structured approach to testing.

This framework is ideal for testers looking to plan and document every step of the pen test in detail. The ISSAF is also useful for testers using different tools as the method allows you to tie each step to a specific tool.

PTES

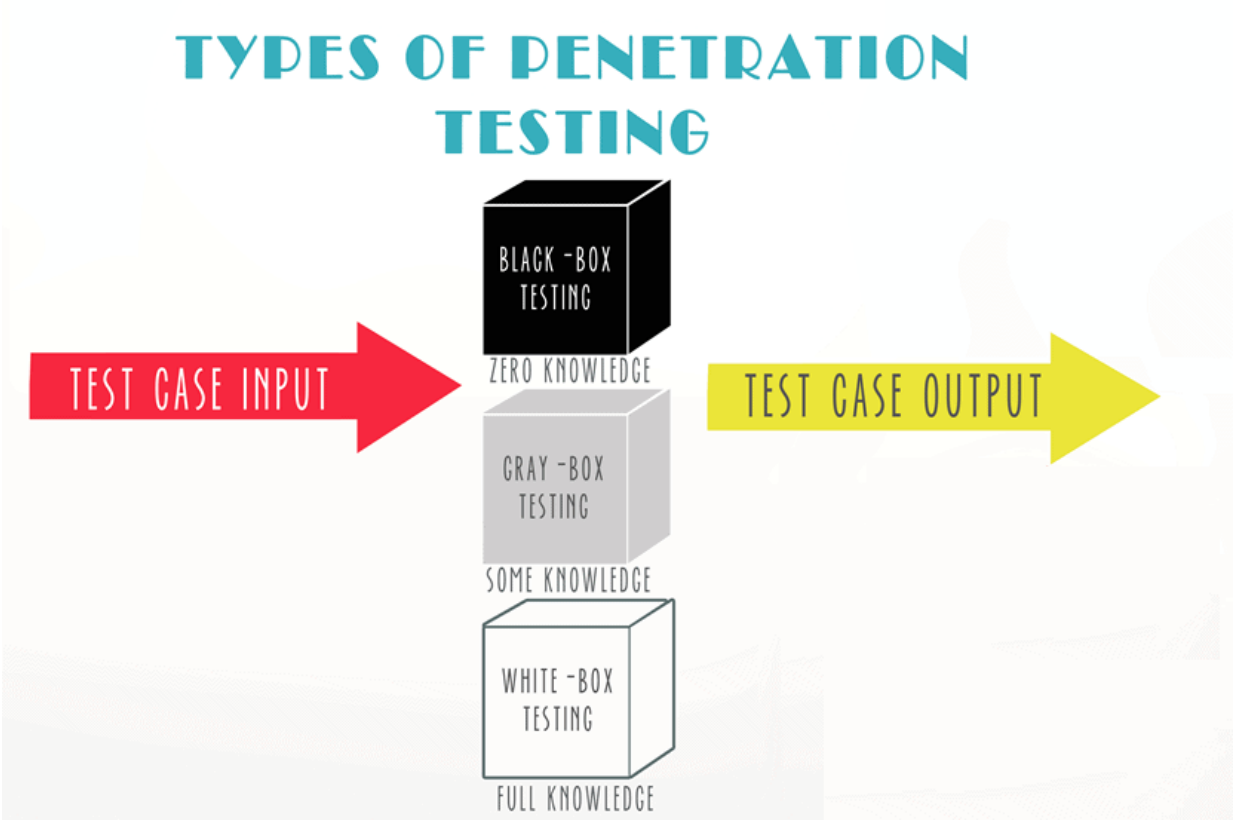
The PTES (Penetration Testing Methodologies and Standards) offers a highly structured seven-step approach to testing. This methodology guides testers through all penetration testing steps, from reconnaissance and data gathering to post-exploitation and reporting.
The PTES requires testers to know the organization's processes to run successful tests.

NIST

The NIST (National Institute of Standards and Technology) offers precise penetration testing guidelines to improve overall cybersecurity. This framework is popular within high-danger industries like banking, communications, and energy.

Types of Penetration Testing

Penetration tests differ in terms of goals, conditions, and targets. Depending on the test setup, the company provides the testers varying degrees of information about the system. In some cases, the security team is the one with limited knowledge about the test.



Black Box Penetration Testing

The penetration team has no information about the target system in a black box test. The hackers must find their own way into the system and plan on how to orchestrate a breach. Typically, the testers only have the name of the company at the start of a black box test. The penetration team must start with detailed reconnaissance, so this form of testing requires considerable time.

Grey Box Penetration Testing

The testing team has the knowledge of a user with elevated privileges. The hacker knows about:

The design and architecture of documentation.

Internal structures.

A grey box pen test allows the team to focus on the targets with the greatest risk and value from the start. This type of testing is ideal for mimicking an attacker who has long-term access to the network.

White Box Penetration Testing

Pen testers have information about the target system before they start to work. This information can include:

IP addresses.

Network infrastructure schematics.

User protocols.

System artifacts (source code, binaries, containers).

Penetration Testing Approaches

- Network penetration testing
- Web application tests
- Website & wireless testing
- Social engineering attacks
- Physical testing
- Cloud pen testing