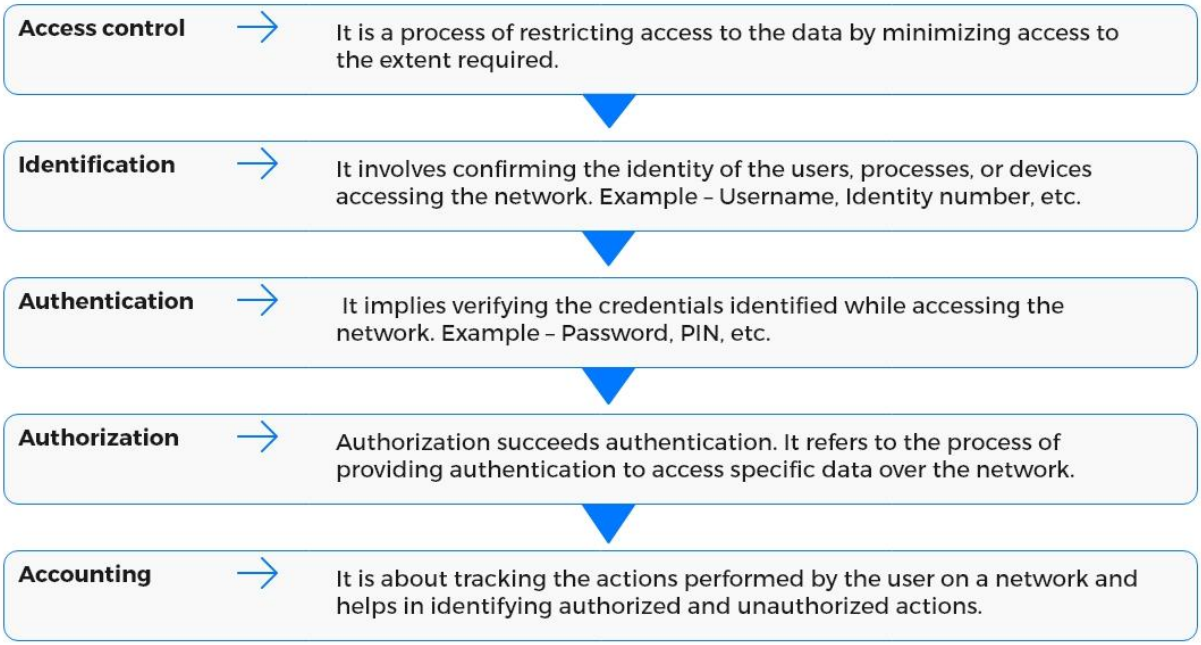
Network Security Controls, Protocols in Network Security Devices

Fundamental Elements of Network Security

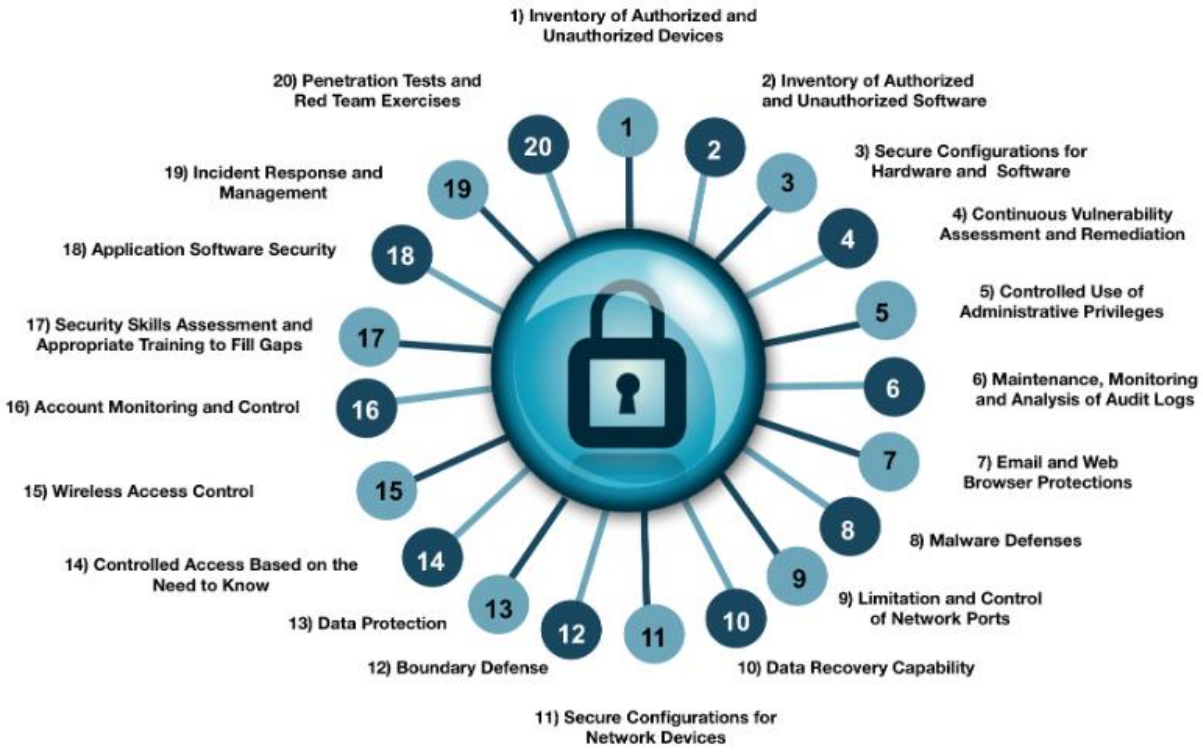
Network security relies on three main security elements:

1. Network Security Controls
2. Network Security Protocols
3. Network Security Devices

Network Security Controls



Network security controls are the security features that should be appropriately configured and implemented to ensure network security. These are the cornerstones of any systematic discipline of security. These security controls work together to allow or restrict the access to organization's resources based on identity management.

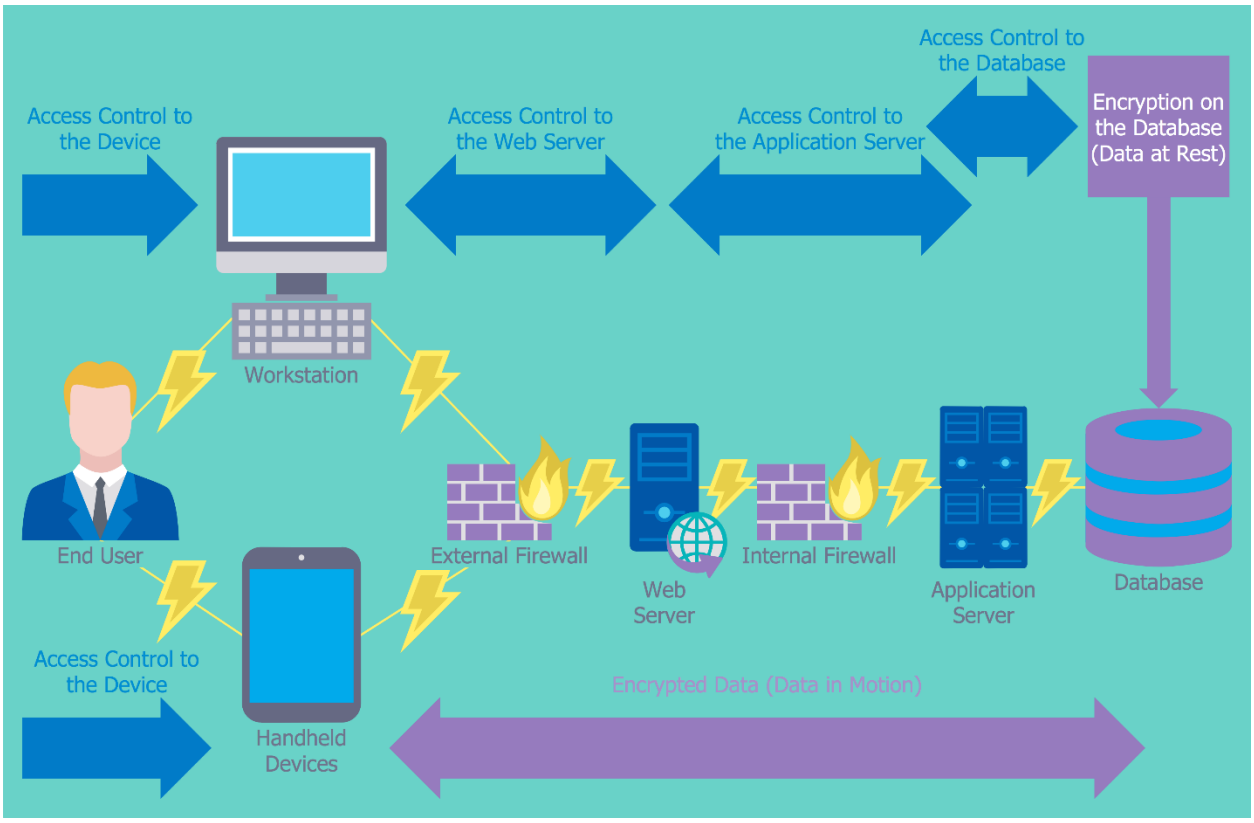


Network Security Protocols

Network security protocols implement security-related operations to ensure the security and integrity of data in transit. The network security protocols ensure the security of the data passing through the network. They implement methods that restrict unauthorized users from accessing the network. The security protocols use encryption and cryptographic techniques to maintain the security of messages passing through the network.

Network Security Devices

Network security appliances are devices that are deployed to protect computer networks from unwanted traffic and threats. These devices can be categorized into active devices, passive devices, and preventative devices. It also consists of Unified Threat Management (UTM), which combines features of all the devices



Network Security Controls

Network security controls are used to ensure the confidentiality, integrity, and availability of the network services. These security controls are either technical or administrative safeguards implemented to minimize the security risk. To reduce the risk of a network being compromised, an adequate network security plan requires implementing a proper combination of network security controls. These network security controls include:

- Access Control
- Identification
- Authentication
- Authorization
- Accounting
- Cryptography
- Security Policy

These controls help organizations with implementing strategies for addressing network security concerns. The multiple layers of network security controls along with the network should be used to minimize the risks of attack or compromise. The overlapping use of these controls ensures defense-in-depth network security.

Access Control

Access control is a method for reducing the risk of data from being affected and to save the enterprise's crucial data by providing limited access to users for accessing the computer resources. The crucial aspect of implementing access control is to maintain the integrity, confidentiality, and availability of the information. The mechanism of access control grants access to system resources to read, write, or execute to the user based on the access permissions and their associated roles.

An access control system includes:

- **File permissions**—such as create, read, edit or delete.
- **Program permissions**—such as the right to execute a program.
- **Data rights**—such as the right to retrieve or update information in a database.

There are two types of access controls: **physical** and **logical**.

1. Physical access controls affect the access to buildings, physical IT assets, etc.
2. The logical access controls affect the access to networks and data.

Access Control Terminology

The following terminologies are used to define access control on specific resources: Object

An object is an explicit resource on which access restriction is imposed. The access controls implemented on the objects further control the actions performed by the user. For example: files or hardware devices.

Access Control Principles

Access control principles deal with restricting or allowing the access controls to users or processes. The principle includes the server receiving a request from the user and authenticating the user with the help of an Access Control Instruction (ACI). The server can either allow or deny the user to perform any actions like read, write, access files, etc.

Access controls enable users to gain access to the entire directory, subtree of the directory, and other specific set of entries and attribute values in the directory. It is possible to set permission values to a single user or a group of users. The directory and attribute values contain the access control instructions.

Access control function uses an authorization database, maintained by the security admin, to check the authorization details of the requesting user.

General steps in access control:

- Step 1: Users have to provide their credentials/identification while logging into the system.
- Step 2: The system validates users with the provided credentials/identification (such as password, fingerprint, etc.) with the database.
- Step 3: Once the identification of the user is successful, the system provides the user access to use the system.

- Step 4: The system then allows the user to perform only those operations or access only those resources for which the user is authorized.

There are three main parts for an access control instruction:

1. **Target**: Permissions are set for certain attributes and entities. These attributes and entities are known as targets.
2. **Permission**: Permissions set for the target explains the actions allowed or denied for those targets.
3. **Bind Rule**: Specifies the subject to the access control instructions.

Access Control System

Administrative Access Control:

Administrative controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization. The procedures prescribed in the administrative access control ensure the authorization and authentication of personnel at all levels. The components of an administrative access control are as follows:

Security Policy and Procedures

Policies and procedures determine the method of implementing security practices in an organization. These specify the extent to which the company can accept a risk and specifies the level of actions allowed in the organization.

Personnel Controls

Personnel controls determine the methods by which the employees may handle the security principles. Personnel controls specify the steps taken in the case of any non-compliance issue. The change of security determines the steps taken from the hiring of an employee until the employee leaves or shifts to any other department.

Supervisory Structure

Supervisory structure consists of members who are responsible for the actions performed by the other employees in the organization in regards to security.

Security Awareness Training

Trains the employees in an organization about the importance of access control. The training assists the employees to limit the attacks in the network and assists them in detecting and controlling the viruses and worms.

Testing

Testing of the access controls brings out the weaknesses in the network, checks if all the access controls are working properly, and evaluates the procedures and policies aligned for the proper functioning of the organization.

Job Rotation

Job rotation improves error detection and fraud disclosures. Job rotation policy (along with separation of duties) is a good administrative access control. However, job rotation prevents employees from assuming multiple roles at a time, which adds overhead to the access control system

One needs to be aware of the impact of job rotation on the access control system. Separation of Duties Separation of duties comes into play when a single operation requires more than one person to complete it. When one individual is responsible for completing a task, it gives them more power and the security risk is high. Whereas, if the same task is accomplished by a team of people, proper checks and balances are maintained and there is less of a chance for errors.

Information Classification

Implementing access control is impossible without information classification. The information can be classified as: **public, private, secret, proprietary, confidential**, etc.

Process of Information Classification:

- Understand data classification project goals
- Build data classification policy
- Build data classification standards
- Build data classification process flow and procedures
- Create tools to support the process
- Determine application owners
- Determine data owners and data owner delegates
- Categorize information
- Define the audit process
- Save information in a repository
- Give user training
- Review and update Information classification at regular intervals

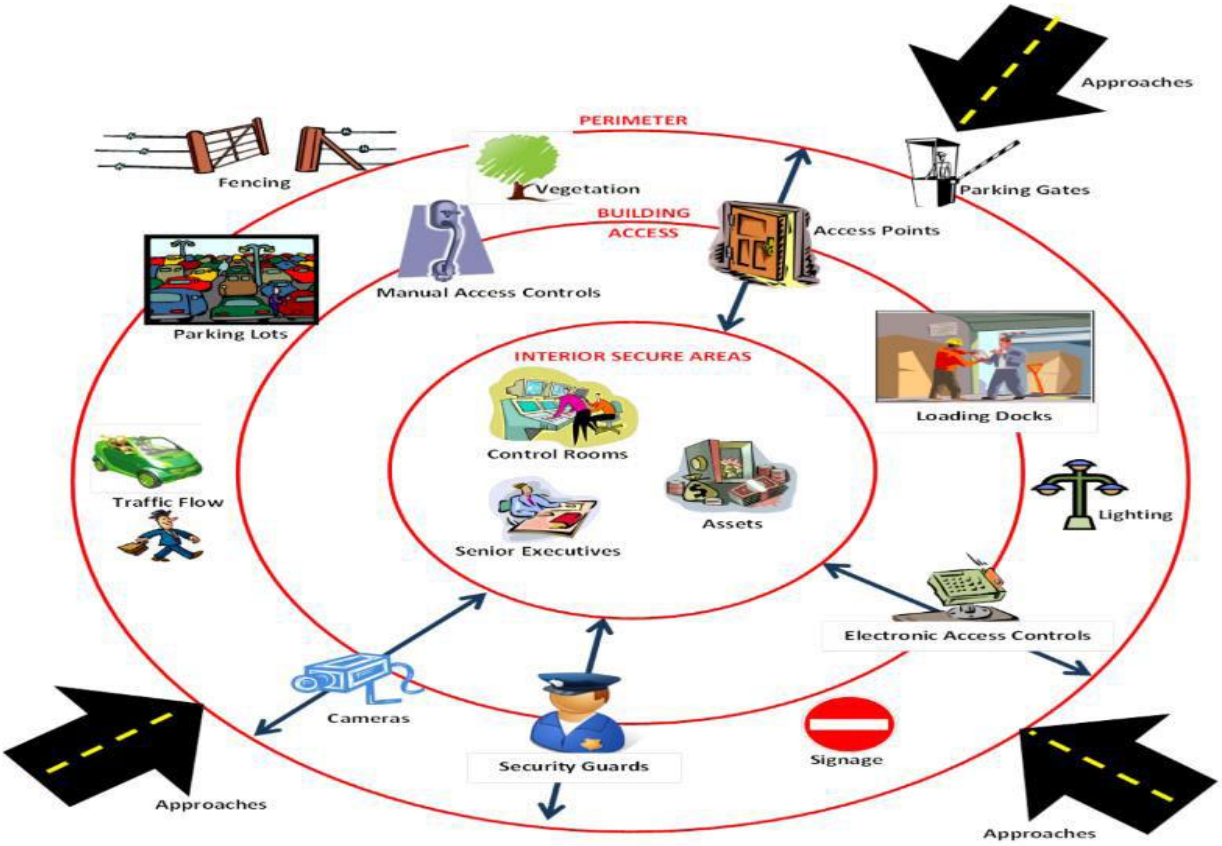
Investigation

Investigate the logs for all doubtful activities and violations and make a report for further actions. Investigate unexpected information-system-related activities. Study the investigations periodically and make changes to access authorizations.

Physical Access Controls:

Appropriate physical access controls can reduce the chances of attacks and risks in an organization. Maintaining physical access controls provides physical protection of the information, buildings, and all other physical assets of an organization.

- Fences
- Locks
- Security Guard
- Badge System
- Mantrap doors
- Lighting
- Biometric System
- Motion Detectors
- Closed-Circuit TVs
- Alarms



The physical access controls are categorized into:

Prevention Access Controls

They are used to prevent unwanted or unauthorized access to resources. It includes access controls such as fences, locks, biometrics, mantraps, etc.

Deterrence Controls

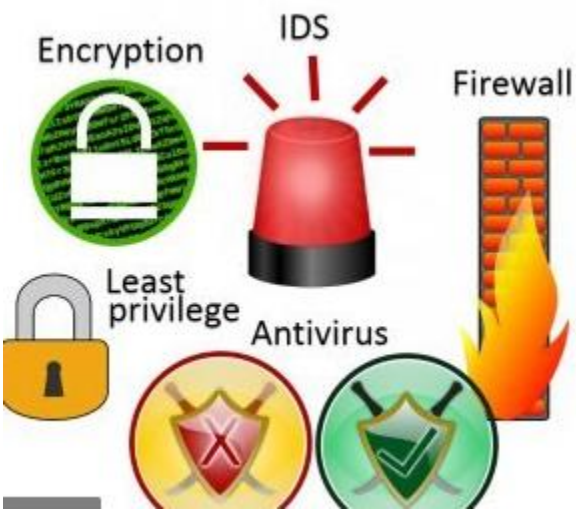
They are used to discourage the violation of security policies. It includes access controls such as security guards, warning signs, etc.

Detection Controls

They are used to detect unauthorized access attempts. It includes access controls such as CCTV, alarms, etc. An access control point can be a physical barrier, such as a door or parking gate, where an electronic access control is placed; users must enter their credentials before they get access. Using a PIN for authentication checks the identity of a user. For example, in an office, the employee must place an access card to the card reader to be able to access the premises.

Technical Access Controls:

Technical access controls affect the subject's access to an object. It involves implementing technical access controls for restricting access to devices in an organization to protect the integrity of sensitive data.



The components of technical access control include:

System Access

System access deals with restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions.

Network Access

Network access control offers different access control mechanisms for network devices like routers, switches, etc.

Encryption and Protocols

Encryption and protocols protect the information passing through the network and preserves the privacy and reliability of the data.

Auditing

Deals with tracking the activities of the network devices in a network. This mechanism helps in identifying the weaknesses in the network.

Firewalls

Firewalls are implemented to filter unwanted traffic and prevent attacks on the network.

Antivirus Software

Antivirus software is installed to prevent the system from malware infections.

Types of Access Control

Types of access control determine how a subject can access an object. The policies for determining the mechanism uses access control technologies and security.

Mandatory Access Control (MAC): • Only system owner manages access control. • End user has no control over any privileges.	**Based Access Control (RBAC):** • Provides access based on the position an individual has in an organization.
Discretionary Access Control (DAC): • Least restrictive model. • Allows an individual complete control over any objects they own.	**Rule Based Access Control (RBAC).** • Dynamically assign roles to users based on criteria defined by owner or system administrator.

The types of access control include:

1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC)
3. Role-Based Access Control (RBAC)

Discretionary Access Control (DAC)

Discretionary access controls determine the access controls taken by any possessor of an object in order to decide the access controls of the subjects on those objects. The other name for DAC is a need-to-know access model. The decision taken by the owner depends on the following measures:

- **File and data ownership**: Determines the access policies of the user.
- **Access rights and permissions**: Setting access privileges to other subjects by the possessor.

The owner can provide or deny access either to any particular user or a group of users. The attributes of a DAC include:

- The owner of an object can transfer the ownership to another user.
- Access control prevents multiple unauthorized attempts to access an object.
- Prevents unauthorized users to view details like file size, file name, directory path, etc.
- The DAC uses access control lists in order to identify and authorize users.

Disadvantages:

- It requires maintaining the access control list and access permissions for the users.

Examples of DAC include UNIX, Linux, and Windows access control.

Mandatory Access Control (MAC)

The mandatory access controls determine the usage and access policies of the users. Users can access a resource only if that particular user has the access rights to that resource. MAC finds its application in the data which is highly confidential. The network administrators impose MAC depending on the operating system and security kernel. There are two techniques to implement MAC:

1. **Rule-based access control**: Rule-based MAC specifies whether to allow or deny access to an object depending upon the levels of trust between the subject and the object.
2. **Lattice-based access control**: The lattice-based access control defines the complex controls required for multiple subjects and objects.

The advantages and disadvantages of MAC include:

- MAC provides a high level of security since the network administrators determine the access controls.
- The MAC policies minimize the chances of errors.
- The operating system, depending on the MAC, marks and labels the incoming data, thereby creating an external application control policy.

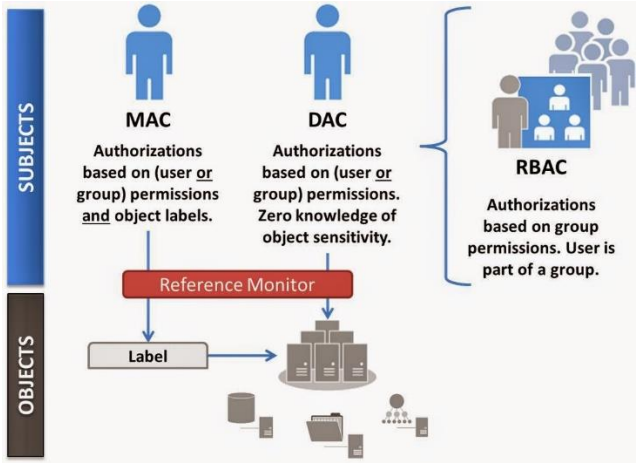
Examples of MAC include SE Linux and trusted Solaris.

Role-Based Access Control (RBAC)

In role-based access control, the access permissions are available based on the access policies determined by the system. The access permissions are out of the user's control, which means that users cannot amend the access policies created by the system. The rules for determining the role-based access controls are:

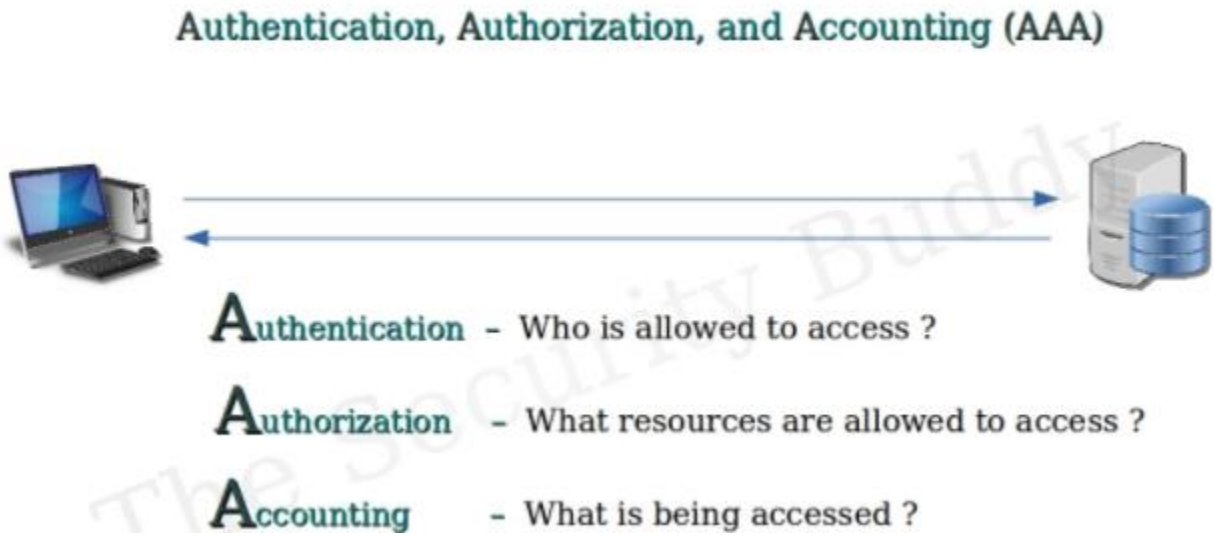
- **Role Assignment**: Assigning a certain role to a user that enables them to perform a transaction.
- **Role Authorization:** User needs to perform a role authorization in order to achieve that role.

- **Transaction Authorization**: Transaction authorization allows users to execute only those transactions for which they are authorized.



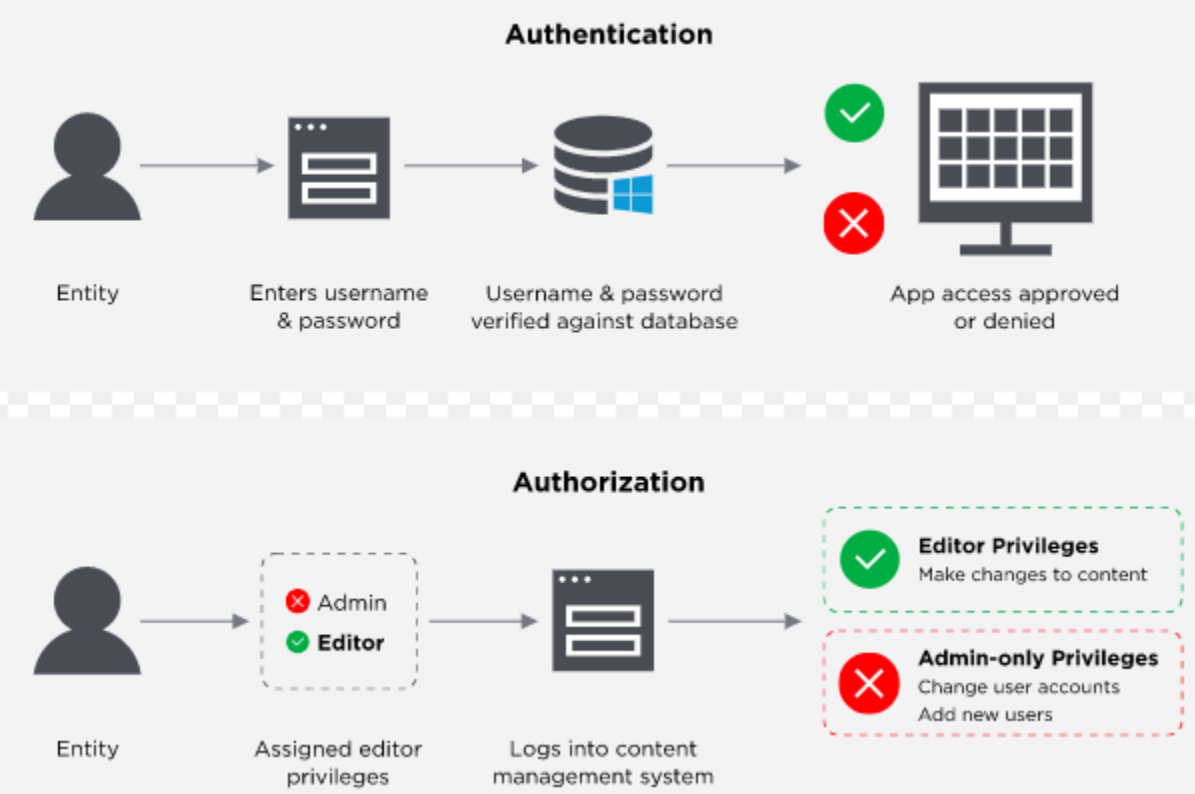
User Identification, Authentication, Authorization, and Accounting Identification

Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most common technique used in authenticating the users in the network and applications. Users have a unique user ID that helps in identifying them.



The authentication process includes verifying a user ID and a password. Users need to provide both the credentials in order to gain access to the network. The network

administrators provide access controls and permissions to various other services depending on the user IDs.



Example: Username, Account Number, etc.

Authentication

Authentication refers to verifying the credentials provided by the user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. The other forms of authentication are authenticating a website using a digital certificate and comparing the product and the label associated with it.

The factors associated with the process of authentication are:

Knowledge factors: The knowledge factors refer to the mandatory entities that a user should know while trying to log into a system or network. For example: usernames and passwords.

Possession factors: The possession factors refer to the entities that a user should have logging in. For example: one-time password token, employee ID cards, etc.

Inherence factors: The inherence factors mostly apply to the biometric factors used for authentication. For example: retina scan, fingerprint scan, etc.

Common authentication methods include:

- Passwords
- Biometrics
- Token management
- Authorization

Authorization

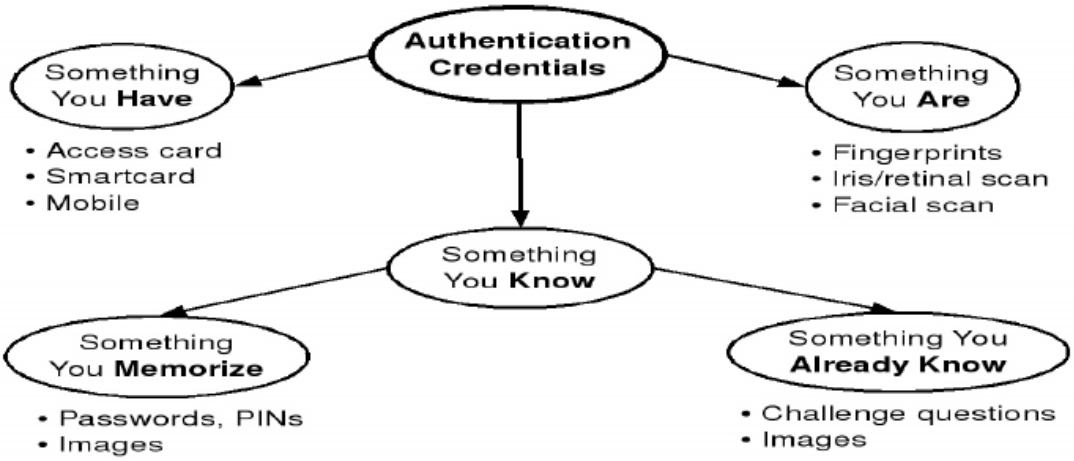
Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users, as well as verify the access permissions created for each user. In logical terms, authorization succeeds authentication. However, the type of authentication required for authorization varies. However, there are cases that do not require any authorization of the users requesting a service. For example, no user authorization is needed when a user tries to access a webpage from the Internet.

Accounting

User accounting refers to tracking the actions performed by the user on a network. This includes verifying the files accessed by the user, as well as functions like alteration or modification of the files or data.

Types of Authentication

- Password Authentication
- Two-factor Authentication
- Biometrics
- Smart Card Authentication
- Single Sign-on (SSO)



Password Authentication: In password authentication, users need to provide usernames and the passwords to prove their identity to a system, application, or network. The username and password are then matched against the list of authorized users in the database/windows active directory. Once matched, users can access the

system. The user password should follow standard password creation practices, including a mixture of alphabet letters, numbers, and special characters—and having a length greater than 8 characters (small passwords are easily guessed).

Password authentication is vulnerable to brute-force attacks (A person trying possible combinations of characters to guess the password or capture packets using a protocol "sniffer" while sending across the network as plain text). Two-factor Authentication: The two-factor authentication is a process where a system confirms the user identification in two steps. The users may use a physical entity like a security token as one of the credentials; the other credential can include security codes.

Two-factor authentication depends on two factors:

1. Something you have
2. Something you know

There are many combinations available in the two-factor authentication. Commonly found are:

- Password and Smart Card
- Password and Biometrics
- Password and OTP
- Smart Card and Biometrics

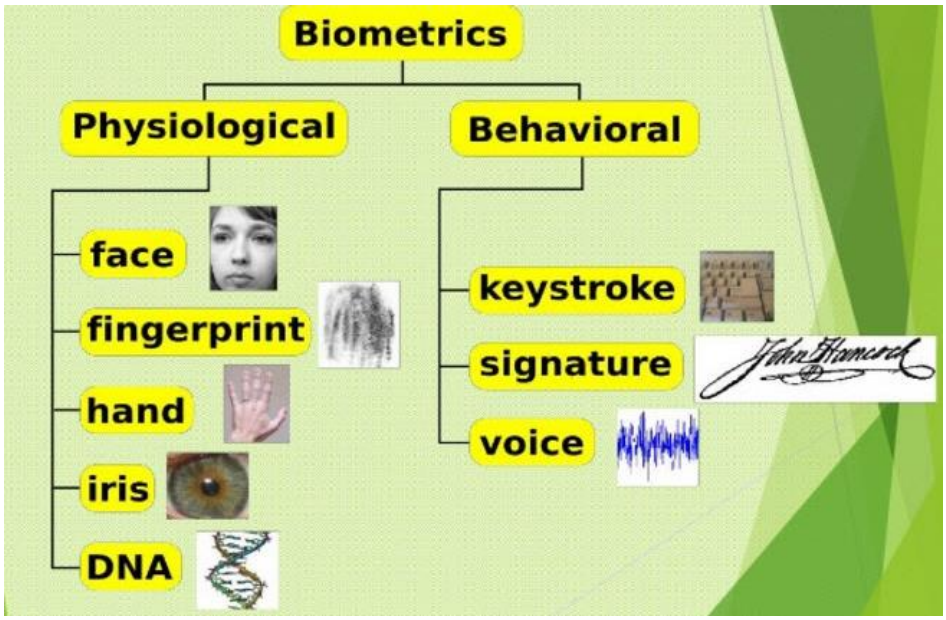
Two-factor authentication performed without the use of tokens is called token-less authentication. They can be implemented quickly across the network.

Biometrics: Biometrics are a technology that identifies human characteristics for authorizing people. The most commonly used biometrics are fingerprint scanners, retina scanners, facial recognition, DNA, and voice recognition.

Biometric authentication involves following steps:

- The reader scans biometric data
- A software converts the scanned information into a digital form and compares it against the stored data

Biometrics take the current biometric data and compares it with the biometric data stored in the database. If they match, then it confirms the authenticity of the user and allows permission.



Types of identification techniques used in biometrics are:

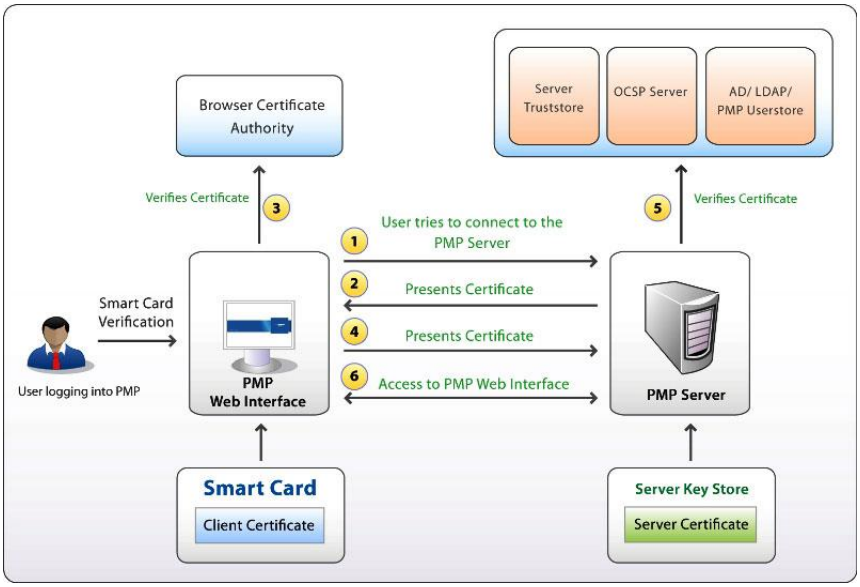
- **Fingerprint Scanning**: Compares two fingerprints for verification and identification using the patterns on the finger. The patterns depend on ridges and minutia points that differentiate each user's fingerprints.
- **Retinal Scanning**: Compares and identifies a user using the distinctive patterns of retina blood vessels.
- **Iris Scanning**: Compares and identifies the images of the iris of one or both eyes of a user. The iris pattern differs from one person to another.
- **Vein-Structure Recognition**: Compares and identifies the patterns produced by the user's veins. Each person has different patterns according to blood flow.
- **Face Recognition**: Compares and identifies a person depending on the facial patterns from an image or a video source.
- **Voice Recognition**: Compares and identifies a person according to the voice patterns or speech patterns.

Advantages of Biometrics: It is difficult to tamper with biometric details like you can with a password or username. They cannot be shared or stolen using social engineering techniques. The biometric authentication requires the presence of the user, which reduces the chances of unauthorized access.

Smart Card Authentication:

Organizations use smart card technology to ensure strong authentication. The smart technology can store password files, authentication tokens, one-time password files, biometric templates, etc. Smart card technology finds its usage with another authentication token providing a multi-factor authentication. This enables a better logical access security. Smart card technology finds its application in VPN authentication, email and data encryption, electronic signatures, secure wireless logon, and biometric authentication. Smart cards consist of a small computer chip and store

personal information of the user for identification. Smart cards are inserted into the machine for authentication along with providing the Personal Identification Number (PIN). Smart cards also help in storing public and the private keys.



The main advantage of using a smart card is that it eliminates the risk of credentials being stolen from a computer because they are stored in the card's chip itself. However, it only enables a limited amount of information to be stored in the card's microchip.

Advantages of Smart Card:

- **Uses highly secure technology**: The smart card technology uses better encryption and authentication methods, increasing the security of the card.
- **Easy to carry**: Smart cards are easy to carry and a user just needs to know the PIN of the card.
- **Reduces the chances of deception by users**: The smart card enables users to store information like fingerprints and other biometric details, thereby allowing organizations to recognize their employees.

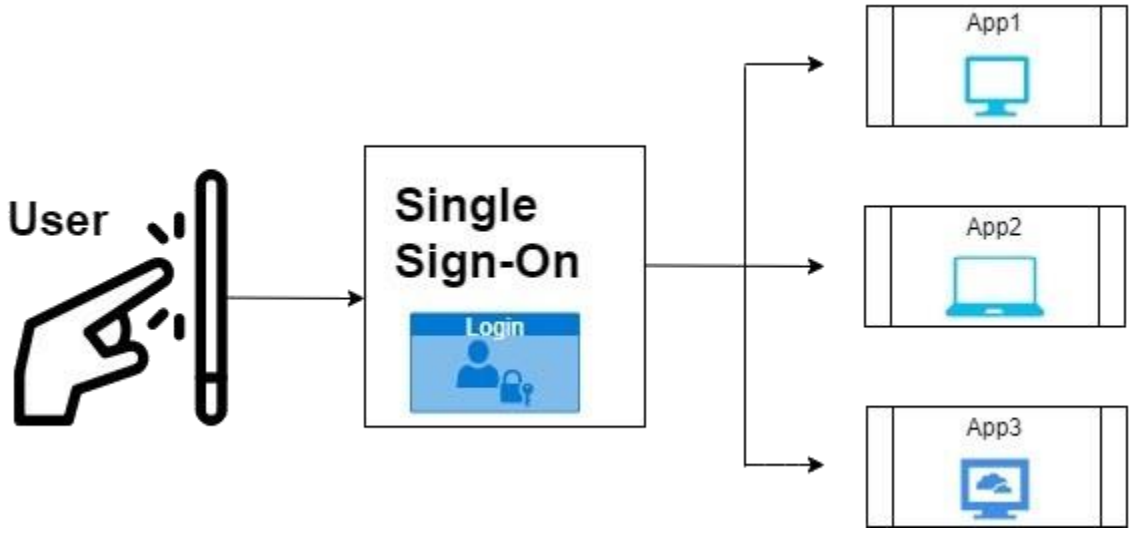
Disadvantages of Smart cards:

- **Can be easily lost**: Since the smart cards are small in size, the chances of losing it are very high.
- **Security issues**: Losing a smart card puts its owner's information and identity at great risk.
- **High cost for production of smart cards**: Since smart cards have microchips and other encryption technologies, its production cost is high.

Single Sign-on (SSO):

As the name suggests, it allows users to access multiple applications using a single username and password. The SSO stores the credentials of a user in an SSO policy server. An example for SSO is Google applications. Users can access all Google applications using a single username and password combination. Consider Google as a

central service. The central service creates a cookie for all users logging in for the first time in any of the applications present in the central service. When a user attempts to access other applications of the central service, it eliminates the need for the user to enter the credentials again due to the cookie that is already created. The system checks the credentials using the cookie created.



Advantages of SSO:

- Reduces the chances of re-authentication, thereby increasing the productivity.
- Removes the chances of phishing.
- Provides better management of applications due to a centralized database.

Disadvantages of SSO:

- Losing credentials have a higher impact, as all the applications of the central service become unavailable.
- There are many vulnerability issues related with the authentication to all the applications.
- It is an issue in multi-user computers and requires certain security policies implemented to ensure security.

Types of Authorization Systems

Network authorization can take different forms based on the organization's need.

- Centralized Authorization
- Decentralized Authorization
- Implicit Authorization
- Explicit Authorization

Centralized Authorization

The need for centralized authentication came into existence when it became difficult to implement the authorization process individually for each resource. It uses a central authorization database that allows or denies access to users. The decision depends on

the policies created by the centralized units. This enables easy authorization for users accessing different platforms. The centralized authorization units are easy to handle and have low costs. A single database provides access to all applications, thereby enabling better security.

The centralized database also provides an easy method of adding, modifying, and deleting the applications from the centralized unit.

Decentralized Authorization

The decentralized authorization maintains a separate database for each resource. The database contains the details of all users permitted to access that resource. The decentralized authorization process enables users to provide access to other users as well. This increases the flexibility level of the users in using the decentralized method. However, certain issues related to the decentralized authorization are cascading and cyclic authorizations.

Implicit Authorization

Implicit authorization provides the access to resources indirectly. The task is possible after the user gets authorization for a primary resource through which the access to the requested resource is possible. For example, the user requesting a webpage has permission to access the main page, as well as all pages linked to the main page. Hence, the user is gaining indirect access to the other links and documents attached to the main page. The implicit authorization provides a level of better granularity.

Explicit Authorization

The explicit authorization maintains separate authorization details for each resource request. The explicit authorization technique is simpler than the implicit technique; however, this technique makes use of more storage space due to the storage of all authorization details.

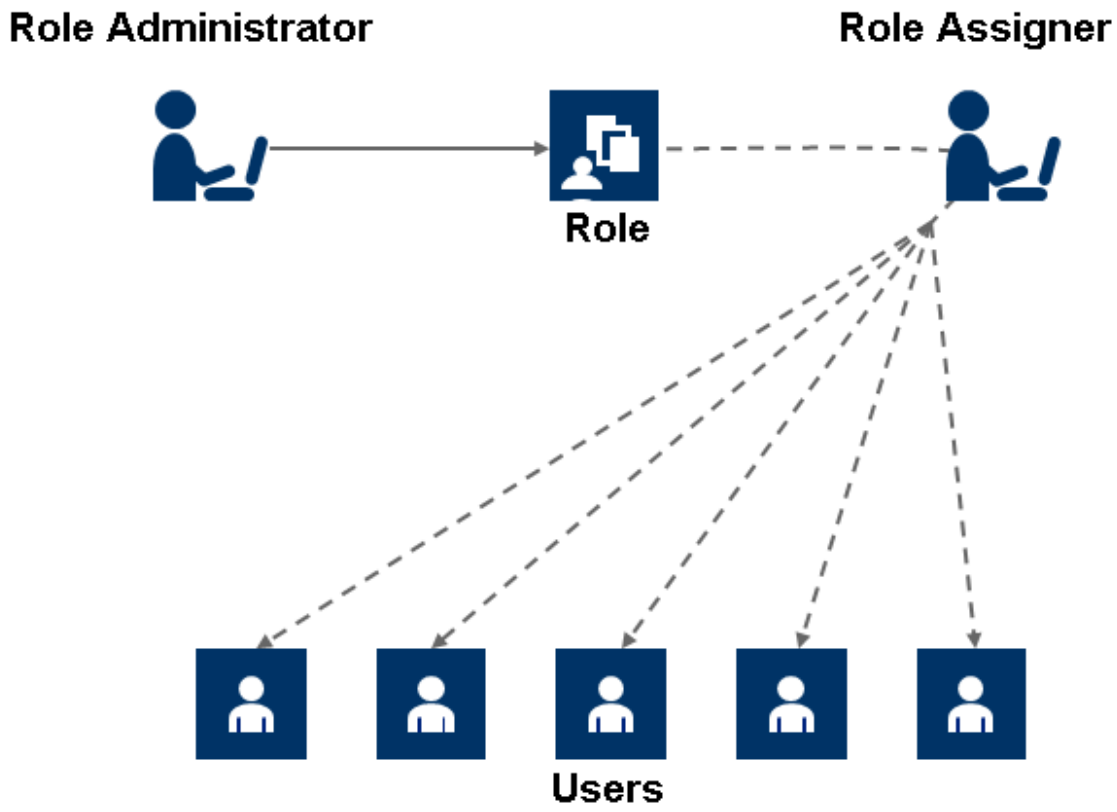
Authorization Principles

The authorization principle describes in detail the access permission levels of users. Enabling an authorization process ensures the security of the processes and resources. The process of authorization should be based on the following principles:

Least Privilege

Least privilege provides access permissions to only those users who really need the access and resources. The permission granted depends on the roles and responsibilities of the user requesting the access. There are two underlying principles involved in the least privilege method: less secure and less risk. According to these principles, users need to complete the task using the limited amount of resources in a limited amount of time provided to the users. This approach reduces unauthorized access to the system resources

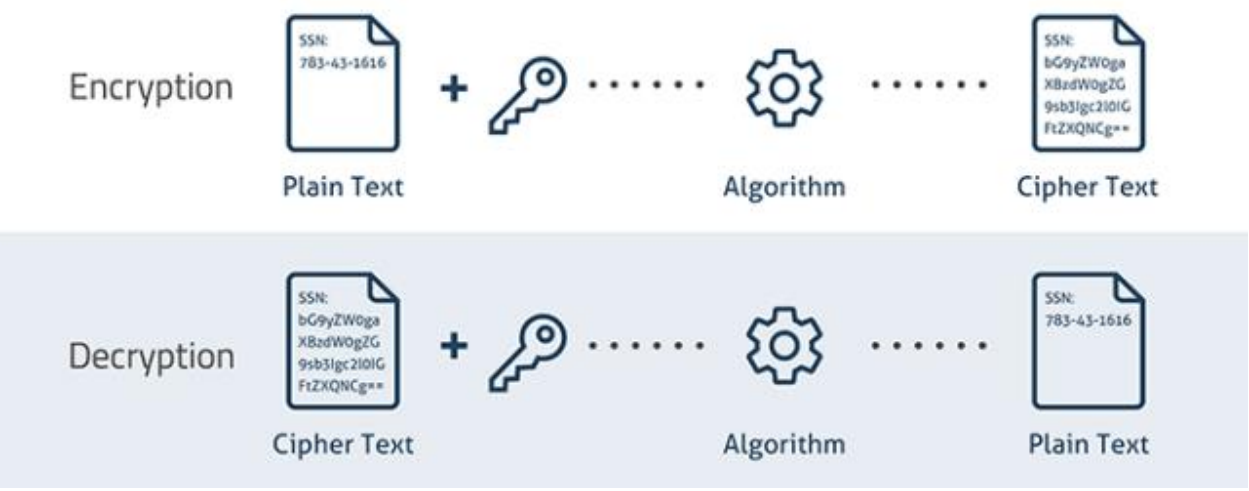
Separation of Duties



It involves breaking the authorization process into various steps. Different privileges are assigned to each step for individual subjects requesting a resource. It ensures that no one individual has authorization rights to perform all functions and, at the same time, does not allow access to all the objects for one individual. This division makes sure that one person is not responsible for a larger process. For example, granting webserver administrator rights to only configure a webserver without granting administrative rights to other servers.

Encryption

Encryption is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. Encryption guarantees confidentiality and integrity of organizational data—at rest or in transit. The encryption algorithm encrypts the plain text with the help of an encryption key. The encryption process creates a cipher text that needs decrypting with the help of a key.



The process of decryption involves the same steps, except for the usage of keys in the reverse order. Common encryption algorithms used to encrypt data include RSA, MD5, SHA, DES, AES, etc. The encryption process finds its application while transmitting data through a network, mobile phones, wireless transmission, and Bluetooth devices.

Types of Encryption

1. Symmetric Encryption
2. Asymmetric Encryption

Symmetric Encryption: Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key. The sender uses a key to encrypt the plain text and sends the resulting cipher text to the recipient, who uses the same key to decrypt the cipher text into plain text. Symmetric encryption is also known as secret-key cryptography, as it uses only one secret key to encrypt and decrypt the data. This kind of cryptography works well when you are communicating with only a few people.

Advantages:

- Easy to encrypt and decrypt the message.
- Faster than asymmetric encryption.

Disadvantages:

- The communicating parties need to share the key used for transmission of data.
- Unauthorized access to the symmetric key compromises data at both ends.

Asymmetric Encryption:

The introduction of asymmetric encryption (also known as public-key cryptography) was to solve key-management problems. Asymmetric encryption involves a public key and a private key. The public key is publicly available, but the sender keeps the private key a secret.

Asymmetric encryption uses the following sequence to send a message:

1. An individual finds the public key of the person they want to contact in a directory.

2. This public key is used to encrypt a message that is then sent to the intended recipient.

3. The receiver uses the private key to decrypt the message and read it.

Advantages:

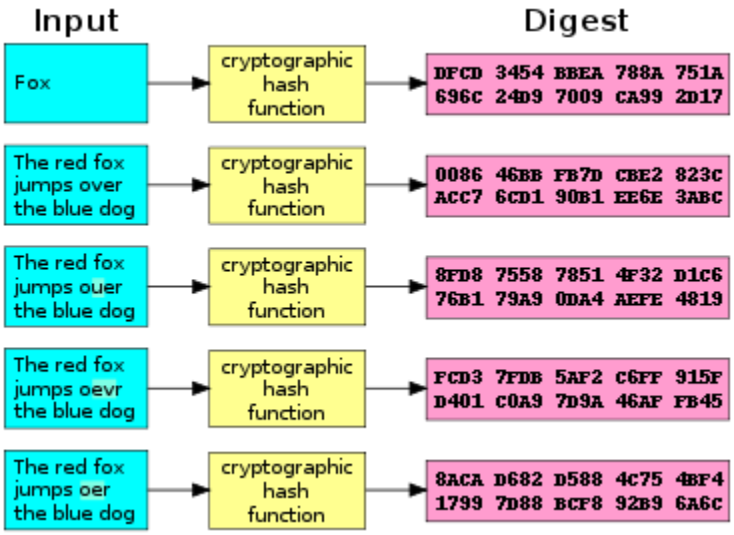
- More secure than symmetric encryption.
- No need to distribute the keys.

Disadvantages:

- It takes a longer time than symmetric encryption because it involves various combinations of the secret keys and the public keys.
- Various complex algorithms involved in the process of asymmetric encryption also increase the time taken to implement it.

Hashing: Data Integrity

Hashing is a method to generate a fixed-length string of random characters for a message using an algorithm. It involves the conversion of the original message into a short fixed-length value or a key that carries the original information.



Hashing finds its application in:

Secure Storage of Passwords: Passwords are hashed before being stored in the database. Every time the user enters the password to login, it is first hashed and the generated hash is matched with the hash stored in the database. If both the hashes match, the user is granted access. Hashing secures passwords from attackers who gain access to the database. The stored hash is useless until the attacker is able to generate the password using a reverse algorithm.

Monitoring File Integrity: Hashing helps identify if a downloaded file is tampered with. A hash of the downloaded file is generated and matched with the one provided by the website. If both hashes match, it is assumed that the file is in its original form.

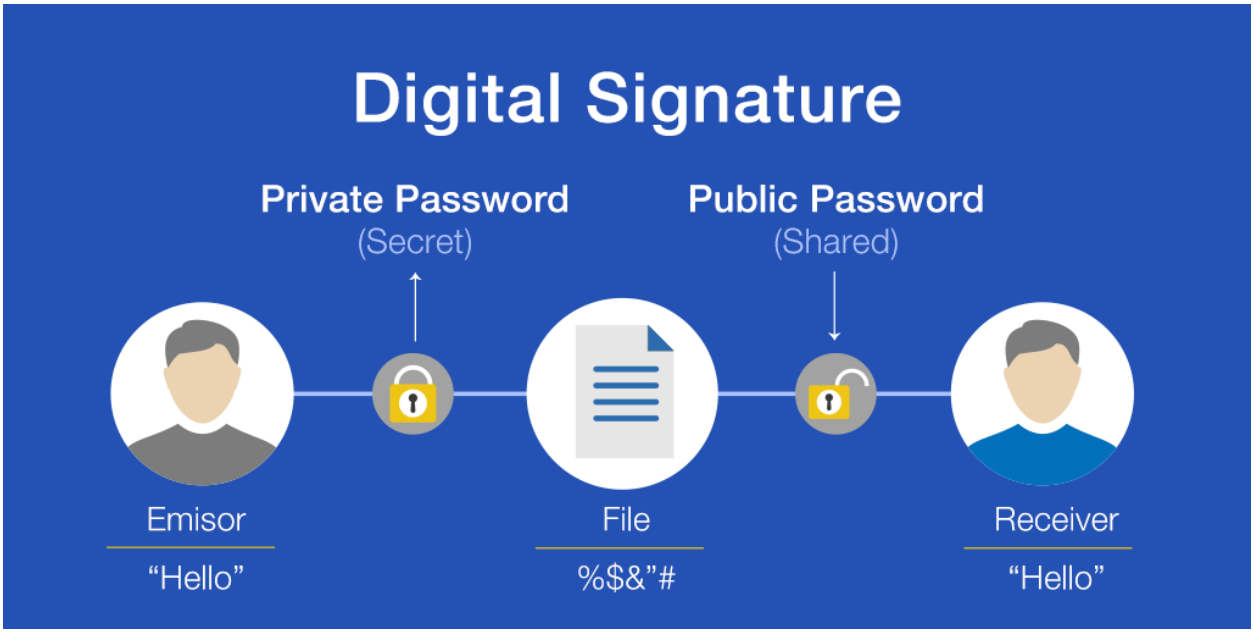
Monitoring Message Integrity: Hashing ensures that the transmitted messages are not tampered with. An encrypted hash is sent along with the message to the receiver who decrypts the message and hash, and then generates a hash from the decrypted hash. If the sent hash and the generated hash are same, the message is assumed to have been transmitted safely.

Common hashing functions:

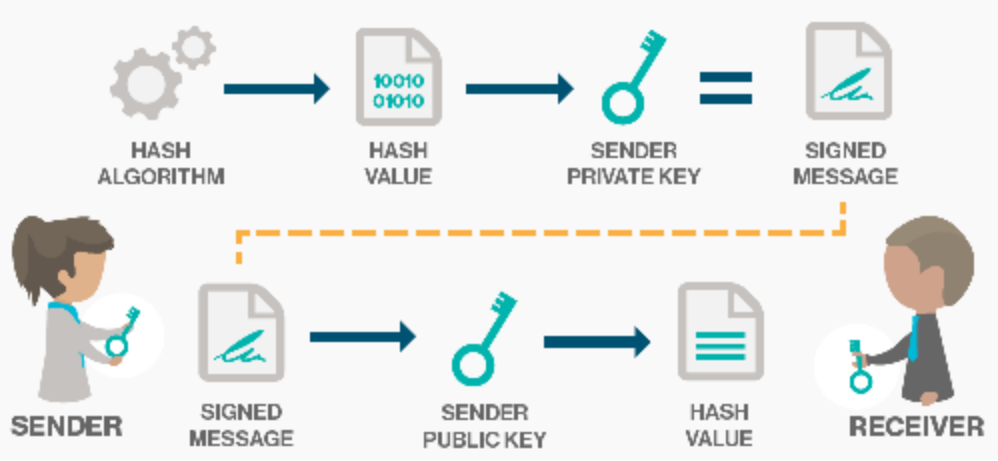
- **MD5 (Message Digest 5):** Generates hashes of 128 bits in length (expressed as 32 hexadecimal characters).
- **SHA (Secure Hashing Algorithm):** Considered a more secure hashing algorithm. SHA SHA-1 generates hashes of 160 bits in length (expressed as 40 hexadecimal characters).
- **SHA-256**: Generates hashes of 256 bits in length (expressed as 64 hexadecimal characters).

Limitations of hashing: Since a hash is a fixed-length string, it may result in collision (generating same hash for different data). Hashes of a smaller length are more prone to collision compared to fixed-length.

Digital Signatures:

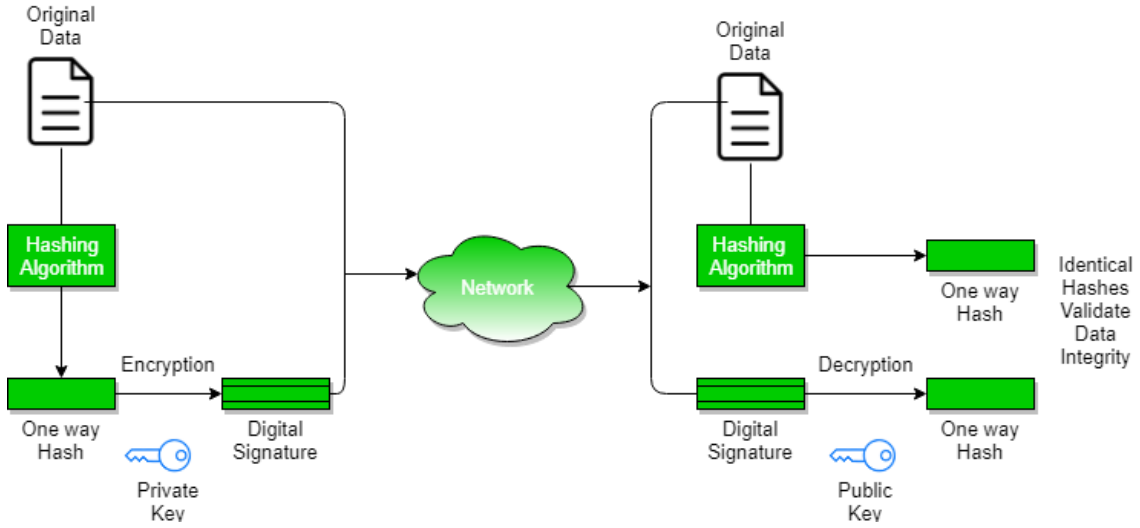


A digital signature is a cryptographic means of authentication. Public-key cryptography uses asymmetric encryption and helps the user to create a digital signature.



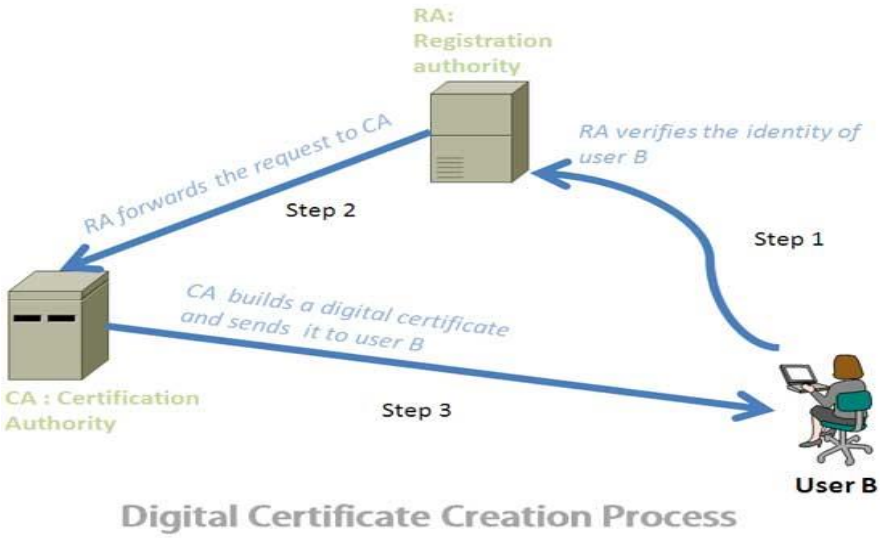
Digital Certificates:

Digital certificates allow the secure interchange of information between a sender and a receiver. This enables the use of a public key by the sender to the receiver. The sender applies for a digital certificate from the Certificate Authority (CA). The CA along with the encrypted message and the public key provides other identity validating information. The receiver accepts the encrypted message and uses the CA's public key to decode the digital certificate. This allows the receiver to identify the digital signature and then obtain the sender's public key and other identification details. The digital certificate can hold information like the name of the sender who applied for the certificate, expiration date, and copy of the sender's public-key digital signature from the CA. The receivers accepting the digital certificate can check the validity of the certificate using the signature attached from the approved authorities with the private key of the authority. Each operating system and web browser carries authorized certificates from the CA, which enables easy validation. The main aim in implementing a digital certificate is to ensure non-repudiation. Most of the SSL/TLS protocols use certificates in order to prevent attackers from changing or modifying the data. The certificates find application in email servers and code signing.



Digital Certificate Attributes

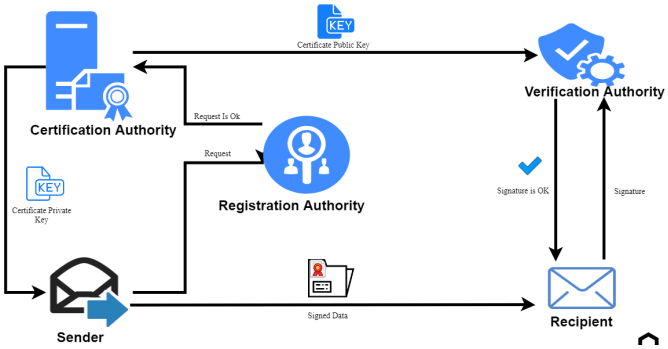
- **Serial number**: Represents the unique certificate identity
- **Subject**: Represents the owner of the certificate, who may be a person or an organization
- **Signature algorithm**: States the name of the algorithm used for creating the signature
- **Key-usage**: Specifies the purpose of the public key—whether it should be used for encryption, signature verification, or both
- **Public key**: Used for encrypting the message or verifying the signature of the owner
- **Issuer**: Provides the identity of the intermediary that issued the certificate
- **Valid to:** Denotes the date until which the certificate is valid
- **Thumbprint algorithm**: Specifies the hashing algorithm used for digital signatures
- **Thumbprint**: Specifies the hash value for the certificate, which is used for verifying the certificate's integrity



Digital Certificate Creation Process

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a security architecture developed to increase the confidentiality of information exchanged over the Internet. It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a Certificate Authority (CA).



PKI is a comprehensive system that allows the use of public-key encryption and digital signature services across a wide variety of applications. PKI authentication depends on digital certificates (also known as public-key certificates) that CAs sign and provide. The digital certificate is a digitally signed statement with a public key and the subject (user, company, or system) name on it.

Public-key infrastructure is widely recognized as a best practice for ensuring digital verification of electronic transactions. This is the most effective method for providing verification while enabling electronic transactions. The digital signatures supported by PKI include the following:

- With whom are you dealing (identification)?
- Who is authorized to access what information (entitlements)?
- A verifiable record of the transaction (verification)

Components of PKI

- A certificate authority (CA) that issues and verifies digital certificates
- A registration authority (RA) that acts as the verifier for the certificate authority
- A certificate management system for generation, distribution, storage, and verification of certificates
- One or more directories where the certificates (with their public keys) are stored

Uses of PKI

PKI does not serve as a business function only; it provides the foundation for other security services. The primary use of PKI is to allow the distribution and use of public keys and certificates with security. The security mechanisms that are based on PKI include email, chip card application, value exchange with e-commerce, home banking, and electronic postal systems. PKI enables basic security services for varied systems:

- Uses SSL, IPsec, and HTTPS protocols for communication security.
- Uses S/MIME and PGP protocols for email security.
- Uses SET protocol for value exchange.

The following are the key benefits of PKI:

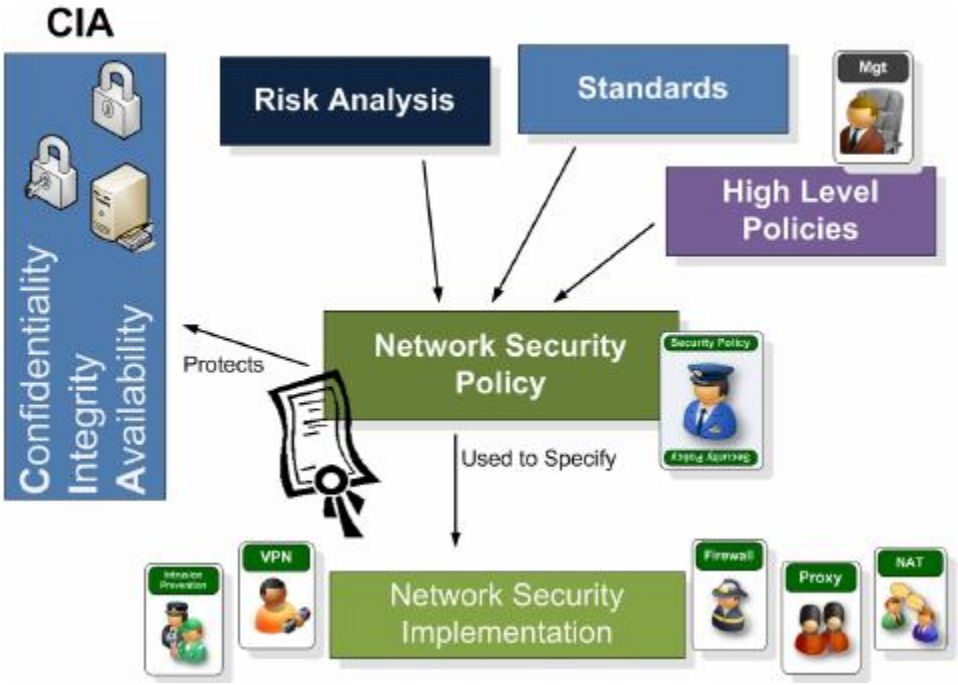
- Reduces the transactional processing expenses.
- Reduces risk.

- Improve efficiency and performance of systems and networks.
- Reduces the difficulty of security systems with binary symmetrical methods.

Network Security Policy

Value of Network Security Policy Development	Explanation/Implication
Identification/Authentication	Want to be assured that users can be accurately identified and that only authenticated users are allowed access to corporate resources
Access Control/Authentication	Want to be assured that even authenticated users are only allowed access to those information and network resources that they are supposed to access
Privacy/Confidentiality	Want to be assured that network based communication is private and not subject to eavesdropping
Data Integrity	Want to be assured that data is genuine and cannot be changed without proper controls
Nonrepudiation	Want to be assured that users cannot deny the occurrence of given events or transactions

Network security policy is a document describing the various policies used to build the network security architecture of the organization. The security policies generally examine the data access, web-browsing methods, and encryption processes. It also helps in restricting unauthorized users and malicious users from the organization.



A security policy should include the type of services that are available and the probability of damage to these services. The security policies decide the access permissions of users and security of the network. Security policies enable permissions

to the minimal level of resources, which is enough to complete the task. Organizations need to monitor the policies and confirm they meet their security needs.

Network Security Devices

Firewalls

A firewall is a secure, reliable, and trusted device placed between private and public networks. It helps in protecting a private network from the users of a different network. It has a set of rules to trace the incoming and outgoing network traffic and is also responsible for allowing or denying the traffic to pass through.

- Protect the private network applications and the public network, by defending services on the internal network from unauthorized traffic.
- Restrict the access of the hosts on the private network and the services of the public network.
- Support network address translation, which helps in using the private IP addresses and to share a single Internet connection.

Proxy Server

A proxy server is an application that can serve as an intermediary when connecting with other computers.

1. A proxy server is a dedicated computer or a software system virtually located between a client and the actual server

2. It is a sentinel between an internal network and the open Internet

3. It serves client requests on behalf of actual severs, thereby preventing actual servers from exposing themselves to the outside world

4. It intercepts and filters all the requests going to the real server

5. It provides an additional layer of defense to the network and can protect against some OS and webserver-specific attacks

6. Network administrators should deploy a proxy server to intercept malicious or offensive web content and computer viruses hidden in the client requests

A proxy server is used:

- As a firewall and to protect the local network from outside attacks.
- As an IP address multiplexer, allowing a number of computers to connect to the Internet when you have only one IP address (NAT/PAT).
- To anonymously surf the web (to some extent).
- To filter out unwanted content, such as ads or "unsuitable" material (using specialized proxy servers).
- To provide some protection against hacking attacks.
- To save bandwidth.

Working of proxy servers

Initially, when you use a proxy to request a particular webpage on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on behalf of your request: it mediates between you and the actual server to send and respond to the request.

Advantages of using Proxy Servers

The following are some more benefits of using a proxy server in the network

- Acts as security protector between user devices and server.
- Enhances the security and privacy of client devices.
- Improves browsing speed.
- Provides advanced logging capabilities for user activities.
- Used to control access to specific types of restricted services.
- Helps the organization to hide its internal IP address.
- Reduces the chances of modifying cookies in the browser configuration and protects from any kind of malware.
- Filters requests from external sites.
- Improves delivery of the requested webpages to the users.
- Enables authentication for the proxy servers before it handles the user requests and services.

Proxy Tool: Proxy Workbench

Proxy Workbench is a proxy server utility that displays the passage of data in real time. It allows getting details like saving data, viewing history, and viewing the socket diagram

of a socket connection for a particular TCP/IP connection. The socket connection diagram displays the graphical history of all the previous events that took place in that socket connection.

Advantages:

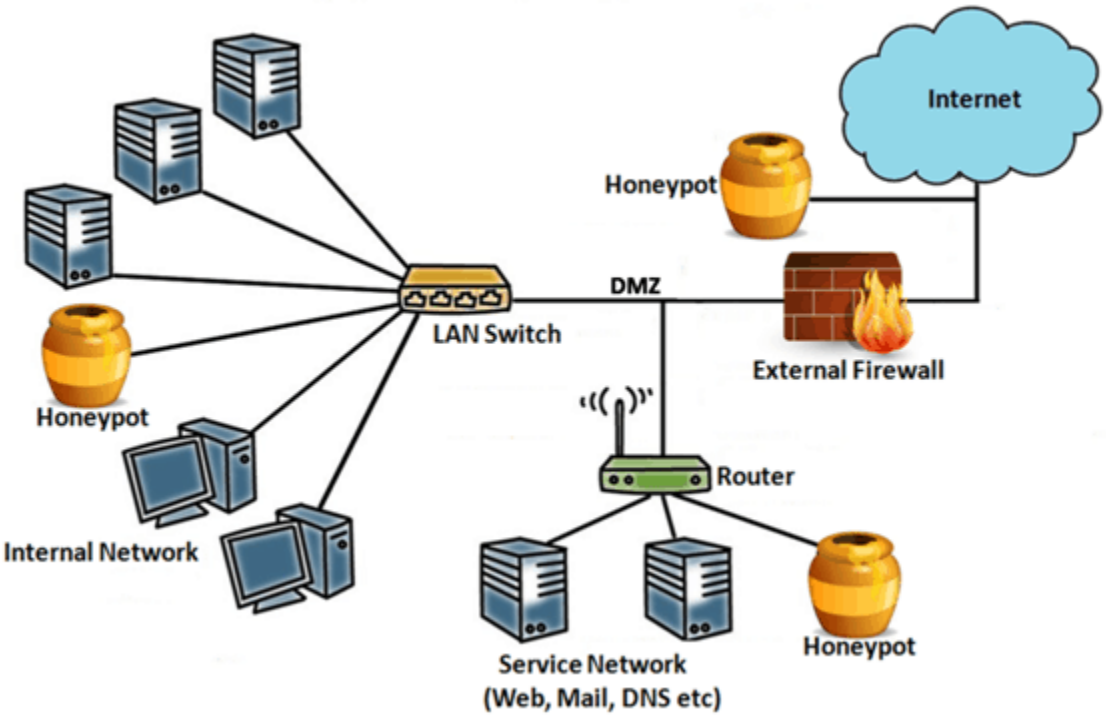
- Displays an animated view of the socket connection.
- Handles POP3 and HTTPS (secure sockets).
- Displays real-time logging of data.

Proxy workbench is mainly used by:

- People interested in web browsing, sending and receiving emails, etc.
- Programmers
- IT training industry
- Internet security practitioners

Honeypot

A honeypot is a computer system on the Internet intended to attract and trap people who attempt unauthorized or illicit utilization of the host system. It is a fake proxy run in an attempt to frame attackers by logging traffic through it, and then sending complaints to victim ISPs. Whenever there is any interaction with a honeypot, it is most likely a malicious activity. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tool with many different security applications. Some honeypots help in preventing attacks. Others can be used to detect attacks or be used for information gathering and research. It requires a considerable amount of attention to maintain a honeypot.



To set up a honeypot:

- Install a system on the network with no particular purpose other than to log all attempted access.
- Install an older, unpatched operating system on a network.
- Ensure that the attacker cannot easily delete system data intended to be in the honeypot.

The main intention of implementing a honeypot is to:

- Track the activities performed by the attackers, thereby allowing the network administrators to build countermeasures for those attacks.
- Collect forensic information that can be used for the further investigation of the attack.

There are two types of honeypots classified based on their deployment:

1. **Production Honeypot**: Normally placed inside a production network along with the other production servers, thereby giving attackers the impression that it contains real and valuable data. The organization evaluating the traffic through the honeypot can now understand the activities performed by an attacker. Honeypots also allow the organization to identify the attackers and bring charges against them.
2. **Research Honeypot**: Research honeypots enable an organization to closely evaluate each step taken by the attackers while attacking the network. This enables the organization to understand each step carefully in order to develop the measures required for each attack. The use of a honeypot also enables the organization to easily track the data stolen by the attackers.

The further classification of honeypots available based on their design:

Pure Honeypots: The presence of pure honeypots makes it possible to track the activities of an attacker in a complete manner. It places a small tap in between the honeypot's link to the network.

Low-interaction Honeypots: As the name suggests, low-interaction honeypots generally fake those services which are frequently requested by the attacker. They are essentially a single machine with multiple virtual machines.

High-Interaction Honeypots: High-interaction honeypots stage a lot of services and activities performed by the real production systems, tricking the attackers into believing that they are accessing a real production system. Multiple honeypots on a single machine is possible by implementing a virtual machine. High-interaction honeypots are highly secure and examine each activity of the attacker. However, the disadvantage with this honeypot is that they are very costly to maintain and implement. Honeypots implemented need to look as genuine as any other original production system. It should contain information that can attract the attackers and persuade them to perform activities.

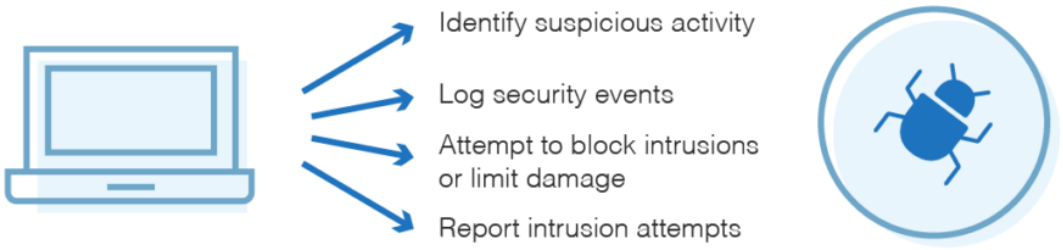
Advantages of using honeypots

The following are some security benefits of implementing honeypots in the network:

- **Simplicity**: Honeypots are simple to implement since they do not contain complex algorithms.
- **Detect Inside attacks**: Honeypots help detect insiders (employees) misusing the system.
- **Reduce False Positive**: Any connection to a honeypot is considered a hostile attack. Any information sent from the honeypot represents an intrusion.
- **Identify False Negatives**: Since any activity with the honeypot is considered abnormal, they help capture new attacks or activity against them easily.
- **Data Collection**: Honeypots collect little high-value data when interacted which is valued and tranquil to analyze.
- **Resources**: Since honeypots capture less activity, they do not come across a resource exhaustion issue.
- **Encryption**: Honeypots capture the activity even if they are encrypted.
- **IPv6**: Honeypots are capable of detecting, capturing, and logging all IP activity.
- **Incident response:** Allows the organization to detect and prevent attacks by taking the necessary steps
- **Warning system**: Provides alerts regarding threats in the network.
- **Ability to mislead**: Easy to mislead attackers.
- **Stores information**: Information collected by honeypots is considered highly beneficial.
- Honeypots appear to be easy to compromise, so the attackers focus on the honeypots first.
- The sole purpose of honeypots is to track the attacks so they can easily identify any newly created viruses and worms.
- Honeypots are easy to deploy, configure, and maintain.
- Honeypots can be used to identify zero-day attacks.
- It is difficult to identify an internal attack attempted within the organization's firewall monitoring space. Honeypots can resolve this.
- Honeypots provide high value and limited data compared to firewalls, system logs, and IDSs.
- Due to a limited data monitoring feature, honeypots rarely face a resource exhaustion problem.
- Honeypots need less equipment, so the investment in them is less.
- Honeypots confuse attackers and keep them occupied.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) performs an evaluation of the network traffic for illegal activities and policy violations. Intrusion detection uses vulnerability assessment for ensuring the security of the network.



Features of Intrusion Detection include:

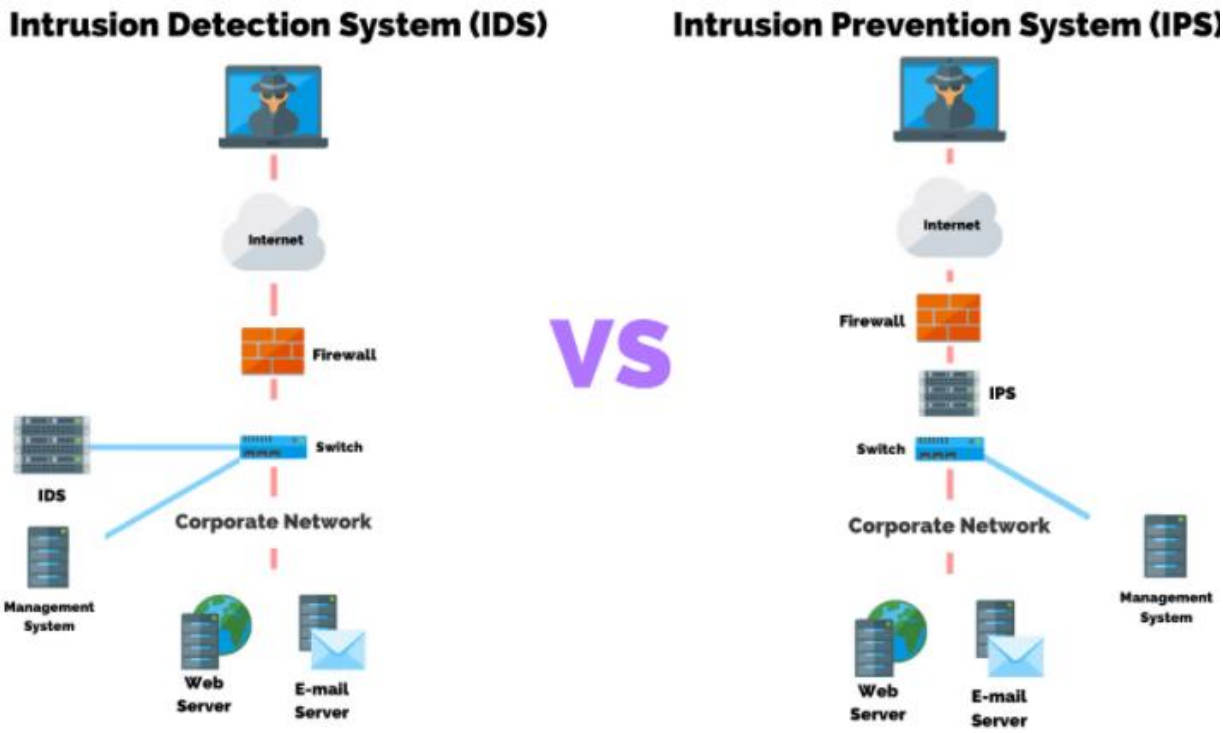
- Evaluating the system and network activities.
- Analyzing vulnerabilities in the network.
- Measuring the system and file reliability.
- Identifying the possibilities of attacks.
- Monitoring irregular activities in the network and system.
- Evaluating the policy violations.

Organizations can identify the presence of attacks or intrusions from outside the network, as well as the intrusions or misuse within the network. Mostly, the intrusion detection systems use vulnerability assessment or scanning in order to identify the vulnerabilities in the network and to monitor the security of the network.

Firewalls prevent intrusions within the network, but do not actually provide alerts regarding the intrusion or attack. IDS systems can monitor and identify the intrusions within the network, as well as signal an alarm to the network administrator.

Advantages and disadvantages of IDS:

- The IDS allows continuous monitoring and tracking of all intrusions and attacks in the network.
- The IDS provides an extra layer of security to the network.
- The IDS can also provide a log or data regarding the attack or intrusion that can be used later for investigation of the incident.
- The IDS requires more maintenance when compared to the firewalls.
- It is not always possible for the IDS to detect the intrusions.
- IDS requires properly trained and experienced users to maintain it.
- IDS can raise false alarms to the network administrator.



Intrusion Prevention System (IPS)

Intrusion Prevention Systems (IPS) work similar to an IDS. Like an IDS, an IPS monitors the network traffic for any intrusion or attack. IPS systems have the capability to carry out quick action against any kind of intrusion. An IPS takes actions based on certain rules and policies configured into it. In other words, the IPS system can identify, log, and prevent the occurrence of any intrusions or attacks in the network

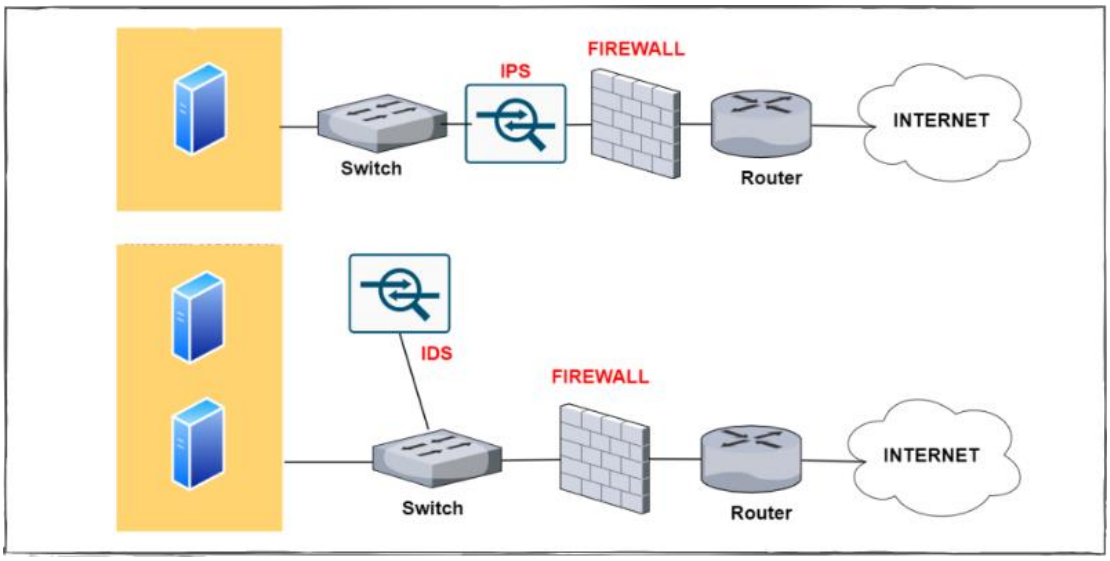
The features of an IPS include:

- Identify illegal activities.
- Record information about any illegal activity.
- Restrict the attack across the network.
- Report the attack to the network administrator.

An IPS may include firewalls or antivirus software in order to deny access to intruders in the network.

Advantages of IPS over IDS:

- Unlike an IDS, the IPS systems can block as well as drop illegal packets in the network.
- An IPS can be used to monitor activities occurring in a single organization.
- An IPS prevents the occurrence of direct attacks in the network by controlling the amount of network traffic.



Network Protocol Analyzer

A network protocol analyzer is a computer hardware device or software that monitors and analyzes data passing through a network. A network protocol analyzer can complement a firewall, an antivirus program, and spyware in a network. It analyzes the raw data in each packet and identifies the content in each packet passing through the network. It reduces the probability of an attack in a network and also provides immediate response to an attack on the network. It is an efficient network sniffer for capturing and logging traffic between an organization's server and its users. Protocol analyzers usually place a NIC in promiscuous mode in order to see and capture all the packets on the network. It includes a timing chart, which indicates the interaction of the packet flow between the organization's server and the user's browser by time. A protocol analyzer is often referred to as a packet analyzer, network analyzer, sniffer, etc.

Features of a network protocol analyzer include:

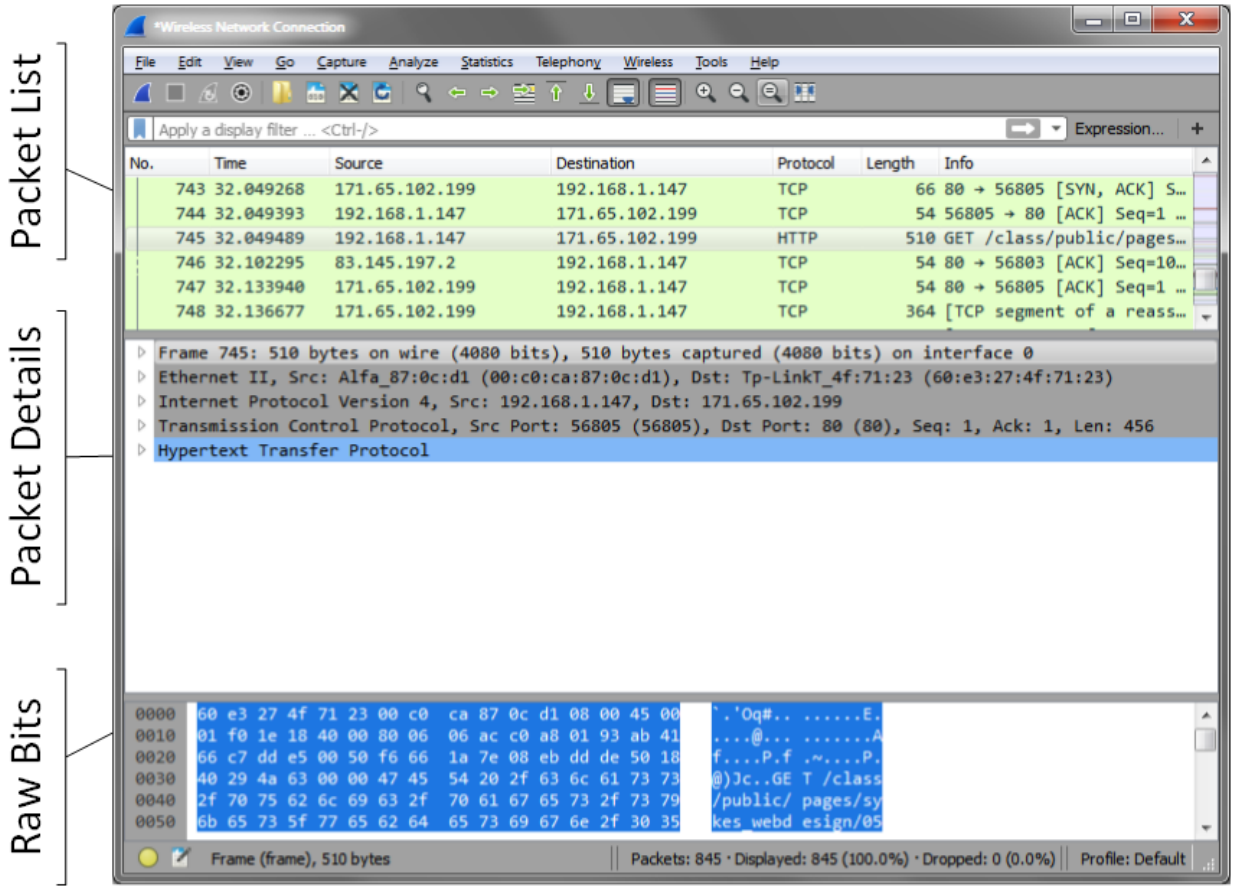
- Detailed description of activities in a network.
- Network traffic analysis.
- Packet data analysis.
- Alarms for threats in the network.
- Bandwidth analysis.

A network protocol analyzer enables the network administrator to gain a snapshot of the traffic in the network.

How it Works

The analyzer works on the host machine. After starting the analyzer in promiscuous mode, the NIC on the host captures all traffic passing through it. The analyzer then forwards the captured traffic into the packet-decoder engine of the analyzer. Here, the decoder engine monitors the behavior of the traffic and splits the packets into their respective layers. The analyzer software will now verify these packets and later display

the packet information on the host screen of the analyzer. The analyzer also enables filtering of the packet depending on the product capability.



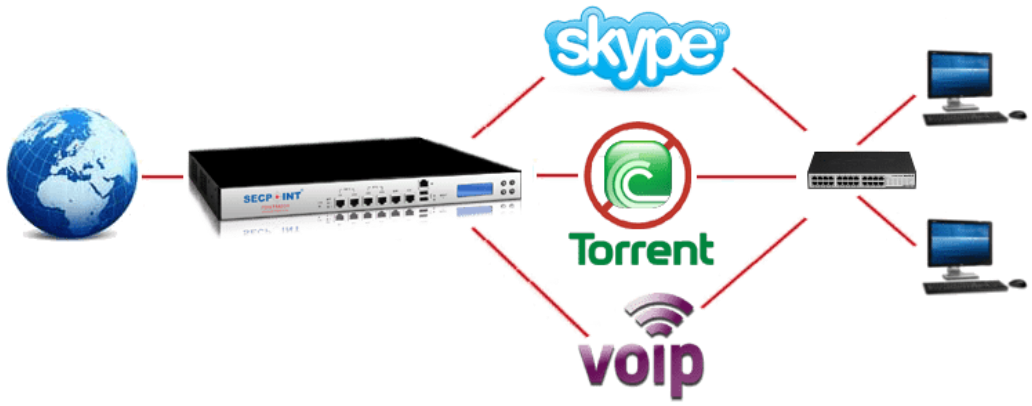
Advantages of using a Network Protocol Analyzer

The following are some benefits of using a Network Protocol Analyzer in the network:

- It can be used as a network troubleshooting and debugging tool. It helps in figuring out the reason for performance issues, identifying protocol errors, investigating why the DHCP stopped working, reasons for virtual network not routing traffic correctly, and various other related problems.
- It is used to identify implementation and configuration errors while applying a new service or altering an existing one.
- It helps in improving the performance of security products like firewalls and intrusion-detection systems. By analyzing the packets using the protocol analyzer, reasons for access issues (like the passing of malicious traffic and the restriction of authorized packets) can be identified.
- It is used to analyze attacks like a denial-of-service (DoS) attack.
- It generates application statistics such as average HTTP traffic transaction time, DNS query and SQL Server response time, retransmission rates, and top talkers and listeners on the network.
- It provides all the current and latest updates of the activities occurring in the network.

- It verifies the occurrences of any irregularity in the network traffic and checks if there is any variation in the features of a data packet.
- It records details that later assist in the forensic investigation of any incident. This minimizes the risk of users gaining information related to a previous incident.
- It can inquire about any particular data string in a given packet.
- It can disable any unwanted protocols.
- Gets details about the untrusted contents in a packet.
- Monitors other network users.
- Helps in reinstating client-server communications.
- Helps in debugging network protocol applications.
- Blocks all unwanted traffic in the network or, in other words, blocks all traffic that is not required for analyzing.

Internet Content Filter



Content filters block deceptive webpages or emails. It protects the network from malware and other systems that are unreceptive and interfering. A content filter allows the organization to block certain web sites. Organizations can implement different types of Internet filtering:

- Browser-based filters
- Email filters
- Client-side filters
- Content-limited filters
- Network-based filtering
- Search engine filters

Advantages of using Internet Content Filters

Controls the productivity

It is often difficult to manage employee activities in a large organization. The Internet content filter can assist the organization by restricting the employees from using any social networking sites or any illegitimate sites. Network administrators can block sites

not related to work—thereby increasing the efficiency and productivity of the organization.

High-level of protection

Internet content filters normally provide protection from malware programs and software.

Restricts all kinds of liability issues

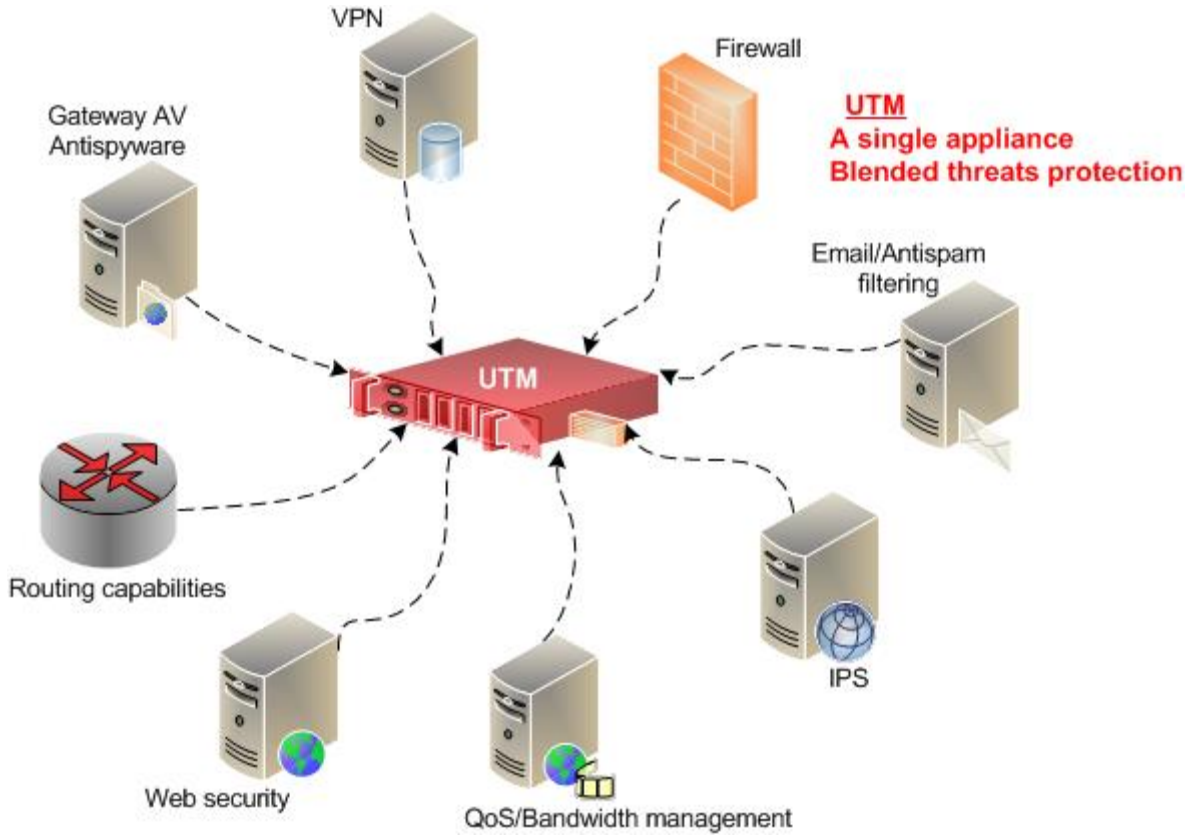
Content-filtering software can prevent users from sharing files and other documents outside the organization.

Highly flexible

It enables the organization to decide on the sites that need to be blocked. It also provides the organization the ability to change the site-blocking setting at any time. Increased speed Using Internet content filtering allows the organization to control the bandwidth of the Internet connection by blocking sites. This, in turn, increases the speed of the Internet.

Unified Threat Management (UTM)

Unified Threat Management (or UTM) is a security management method that enables the administrator to evaluate and examine security-related applications and other components through a single console. UTM helps in minimizing the complexity of the network by protecting users from blended threats.



Advantages of UTM:

- **Lower cost**: Reduces the cost of buying multiple devices. UTM needs only a single console that can manage the whole network.
- **Low maintenance cost**: Since only a single console is used, it needs little maintenance.
- **Easy installation and management:** UTM involves the use of only a single console that requires minimum wiring and other installation requirements.
- **Fully integrated:** UTM is a complete console that incorporates every feature required for protecting a network.

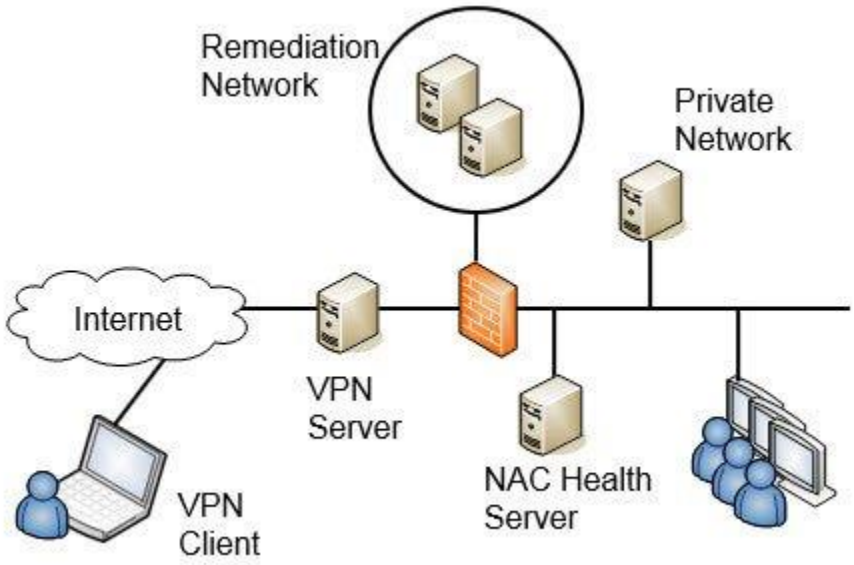
Disadvantages of UTM:

- **Less specialization**: As UTM is a single console managing the whole security of the network, there are chances of it missing certain features that are required to maintain the security. This can be avoided by using dedicated devices for each feature.
- **Single point-of-failure**: UTM involves the use of a single console with all features included in it. Failure of one feature can affect the performance of the other features and the inner workings of the UTM.
- **Possible performance constraints**: The single console in the UTM performs various tasks at the same time. There are chances that all the tasks or features do not get adequate CPU time. This situation may lead to many attacks on the system.

Network Access Control (NAC)

Network Access Control (also known as Network Administration Control) deals with restricting the availability of a network to the end user depending on the security policy. It mainly restricts systems without antivirus or intrusion prevention software from accessing the network.

NAC allows you to create policies for each user or systems and define policies for networks in terms of IP addresses.



What NAC does?

- Authentication of users connected to network resources
- Defining a connection point of network devices
- Identification of devices, platforms, and operating systems
- Development and application of security policies
- NAC implements detection programs using the following points:
- Searching for an antivirus program and examining whether it is updated or not.
- Checking if the end system has a configured firewall or Intrusion Prevention Software.
- Looking for any viruses on the network and checking if the operating system is updated.

NAC performs the following actions:

- Evaluate unauthorized users, devices, or behaviors in the network. It provides access to authorized users and other entities.
- NAC helps in identifying users and devices on a network. Also determines whether these users and devices are secure or not.
- Examines the system integration with the network according to the security policies of the organization.

NAC helps in maintaining security policies for increased control of the network. An organization must look into the threats to its network while considering the cost of implementing a NAC. Organizations need to have plans to rectify the faults in the policies while implementing a NAC.

Organizations may consider the following points:

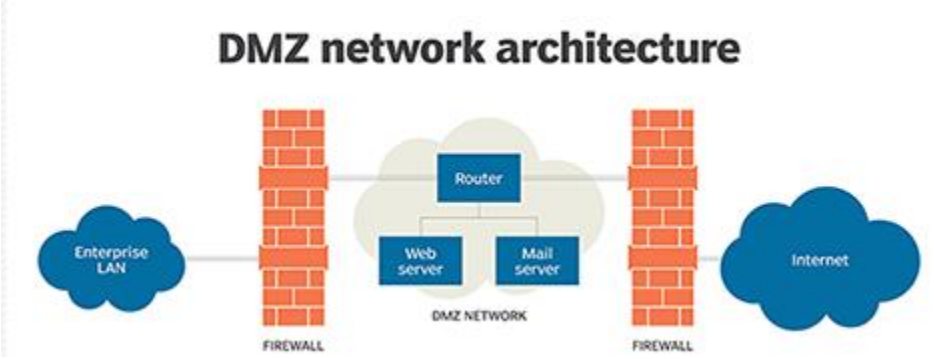
- Do the NAC policies authenticate users?
- How well is the NAC implemented?
- Is NAC properly integrated with the device?
- Does the NAC tool check if the end user is blocked?

Organizations need to consider the following resources while implementing a NAC:

- **Network Infrastructure**: Incorporate network access control policies within the network infrastructure.
- **Security**: Manage the infrastructure.
- **Human Resources**: Report the network policies to the employees in an organization.
- **Operations**: Management of response, procedures, and actions.
- **Management**: Decides the priority of the policies and the effect of the policies on the organization, as well as manages the budget issues.

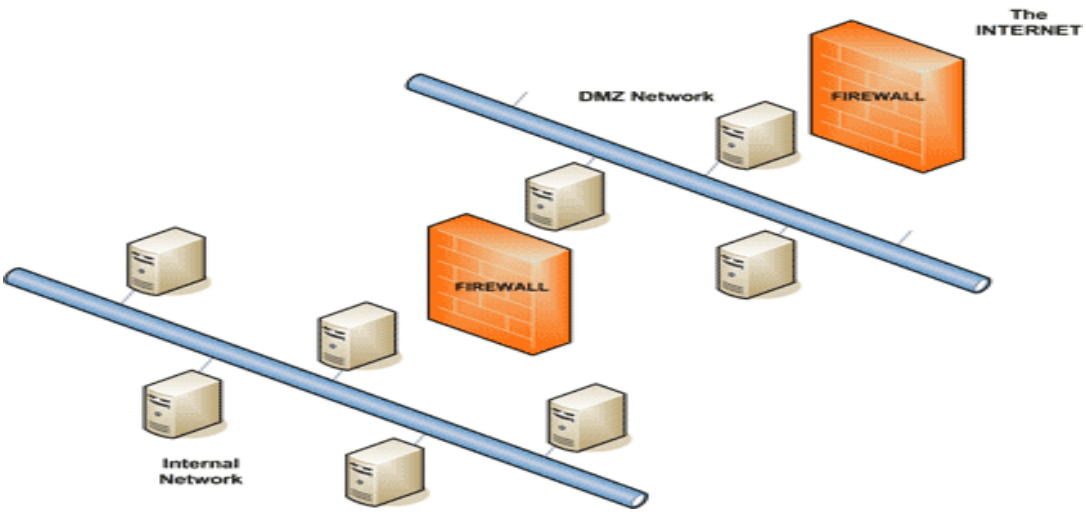
Demilitarized Zone (DMZ)

A DMZ is a small network that is placed between the organization's private network and an outside public network. It prevents the outsider from getting direct access to the organization's server. For example, if an attacker uses the public network to access the DMZ host and penetrates it, then only the information on that host will be compromised. In this way, a DMZ acts as an additional security layer for networks and lowers the threat of intrusion in the internal network.



A DMZ contains the following servers, which need to be accessible from outside the network:

- Webservers
- Email servers
- DNS servers



Two basic methods of designing a network with a DMZ are using a single firewall (three-legged model) and using dual firewalls. It is also possible to extend these configurations according to the network requirements.

Single Firewall: In this model, the network architecture containing the DMZ consists of three network interfaces. The first network interface connects the ISP to the firewall forming the external network, whereas the second interface forms the internal network. The third interface forms the DMZ. The firewall acts as the single point of failure and should be able to manage all the traffic to the DMZ.

Dual Firewall: The dual firewall approach uses two firewalls to create a DMZ. The first firewall allows only sanitized traffic to enter the DMZ and the second firewall double-checks it. The dual approach is the most secure approach in implementing a DMZ.

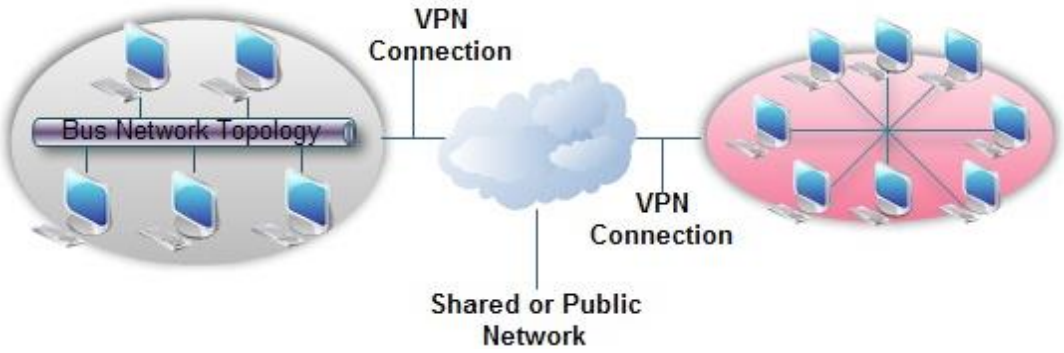
Any server that needs exposure to the public network can be placed in the demilitarized zone. It is possible for the network administrator to place servers (like a webserver, DNS server, email server, FTP server, etc.) in the DMZ and enable access for internal and external clients

Advantages of a DMZ:

- Separation of the DMZ from the LAN enables the high level protection of LAN.
- Provide an increased control of resources.
- It uses multiple software-and hardware-based products of different platforms in order to provide an additional layer of protection.
- Provides a high level of flexibility for Internet-based applications like email, web services, etc.

Virtual Private Network (VPN)

A VPN uses public networks, such as the Internet, and assures secure transfer of data between systems over them. Certain tunneling protocols employed by the VPN help to achieve encryption, data integrity, and authentication. A VPN ensures scalability in organizing to support new clients, organizations, and applications. It ensures solutions to business problems with its embedded technology.



A VPN enables a virtual connection between users and the public network. A packet that is transmitted is encapsulated inside a new packet along with a new header. The header facilitates packet traversal in the network. The path through which the encapsulated packet traverses is known as a tunnel. The encapsulated packet, after reaching the end point of the tunnel, is de-encapsulated so that the original packet is forwarded to the final destination.

The tunnel needs to carry the same tunneling protocols that operate at layer 2 (data link layer) or layer 3 (network layer) of the OSI layer. Commonly used tunneling protocols are: IPsec, PPTP, L2TP, and SSL.

Network Security Protocols

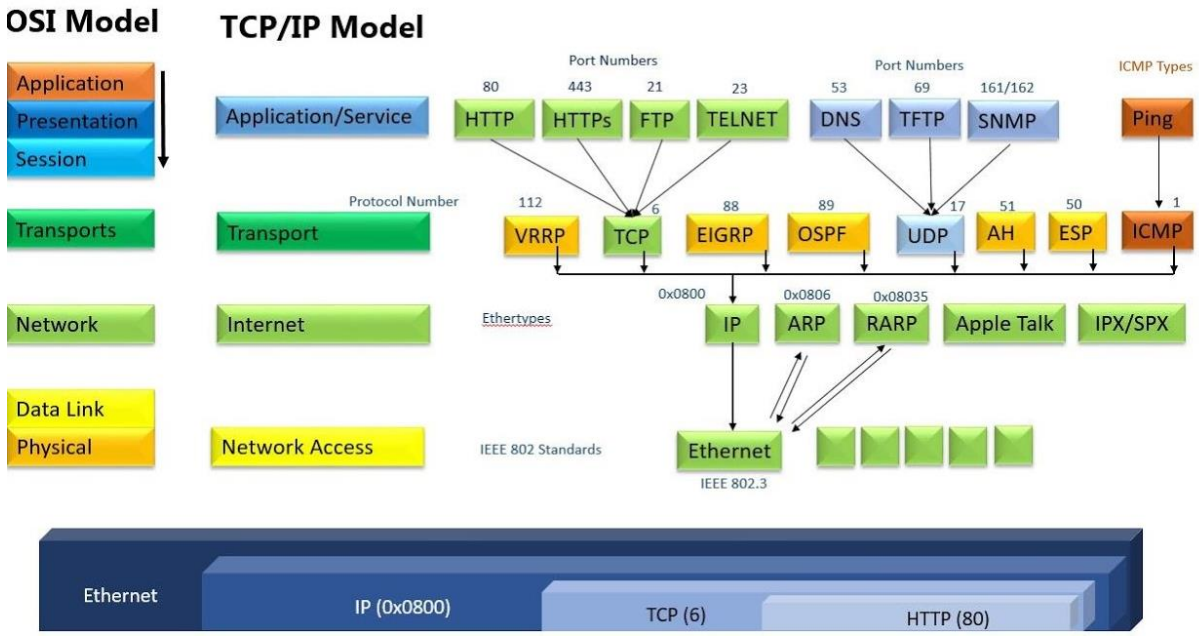
There are various security protocols that work at data link, network, transport, and application layers. These protocols help organizations in enhancing the security of their data and communication against different types of attacks. The security protocols that work at the transport layer are as follows:

Transport Layer Security (TLS): The TLS protocol provides security and dependability of data between two communicating parties

Secure Sockets Layer (SSL): The SSL protocol provides security to the communication between a client and a server.

The security protocols that work at the network layer are as follows:

Internet Protocol Security (IPsec): The IPsec protocol authenticates the packets during the transmission of data.



The security protocols that work at the application layer are as follows:

- **Pretty Good Service (PGP) protocol**: The PGP protocol provides security to the data through the method of encryption and decryption.
- **S/MIME Protocol**: Commonly known as Secure/Multi-Purpose Internet Mail Extensions, it provides security to emails.
- **Secure HTTP**: Secure HTTP provides security to the data traversing through the world wide web.
- **Hyper Text Transfer Protocol Secure (HTTPS):** The HTTPS protocol ensures the security of data in the network.
- **KERBEROS**: The Kerberos protocol provides security using a client-server model.

The security protocols that work at the data link layer are as follows:

- **RADIUS**: The RADIUS protocol provides security to the remote access servers to communicate with a central server.
- **TACACS+:** The TACACS+ provides security using a client-server model

RADIUS

RADIUS stands for Remote Authentication Dial-In User Service. It was developed by Livingston Enterprises as a networking protocol that provides centralized authentication, authorization, and accounting for remote access servers to communicate with a central server. RADIUS has a client-server model, which works on the application layer of the OSI model by using UDP or TCP as a transport protocol. The RADIUS protocol is the de facto standard for remote user authentication and it is documented in RFC 2865 and RFC 2866.

Radius Authentication Steps:

1. The client initiates the connection by sending an Access-Request packet to the server.

2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the Accept-Accept message along with the Access-Challenge to the client for additional authentication; otherwise, it sends back an Accept-Reject message.

3. Client sends the Accounting-Request message to the server to specify accounting information for a connection that was accepted.

Radius Accounting Steps

Client sends the Accounting-Request message to the server to specify accounting information for a connection that was accepted.

The server receives the Accounting-Request message and sends back the Accounting-Response message confirming the successful establishment of the network

The RADIUS protocol is an AAA protocol that works on both mobile and local networks. It uses PAP, CHAP, or EAP in order to authenticate the users communicating with the servers.

The components of a RADIUS AAA protocol are as follows:

- Access clients
- Access servers
- RADIUS proxies
- RADIUS servers
- User account databases

RADIUS messages are sent as UDP messages and allow only one RADIUS message in the UDP payload section of the RADIUS packet. RADIUS messages consist of a RADIUS header and other RADIUS attributes.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol developed by Cisco. It is derived from the TACACS protocol. It performs authentication, authorization, and accounting separately (unlike RADIUS). It is primarily used for device administration.

- Terminal Access Controller Access-Control System Plus is a network security protocol used for authentication, authorization, and accounting for a network device (like switches, routers, and firewalls) through one or more centralized servers.
- TACACS+ encrypts the entire communication between the client and server, including the user's password, which protects from sniffing attacks.
- It Is a client-server model approach where the client (user or network device) requests a connection to the server, then the server authenticates the user by examining the credentials

Authentication of TACACS+

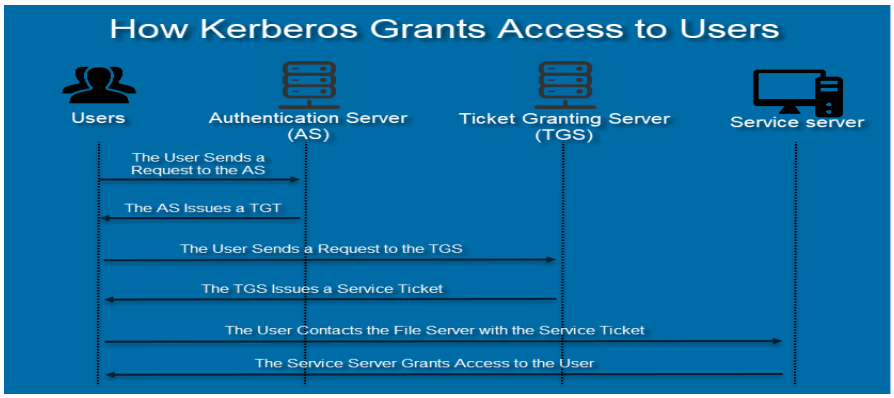
Consider the following example of authentication where a laptop user is connecting to a NAS (router). The TACACS+ authentication involves the following steps:

- Step 1: User initiates the connection for authentication.
- Step 2: Router and user exchange authentication parameters.
- Step 3: Now, the router sends the parameters to the server for authentication purposes.
- Step 4: Server responds with the REPLY message based on the provided information.

Radius	TACACS+
UDP 1812, 1645 (Authentication), 1813, 1646 (Accounting)	TCP 49
Created by IETF, Open Standard	Created by Cisco, Open Standard
Password Only	Full Packet Encryption
Uniderectional CHAP	Bidirectional CHAP
Low resource dependent	Requires more resources
No command logging	Full logging of commands
Used for network access	Supports administration
Authentication and Authorization is combined. Accounting is seperate	Authorization, Authentication, and accounting are separate
Extensive accounting	Limited Accounting
Priviledge mode is supported	15 priviledge modes are supported

Kerberos

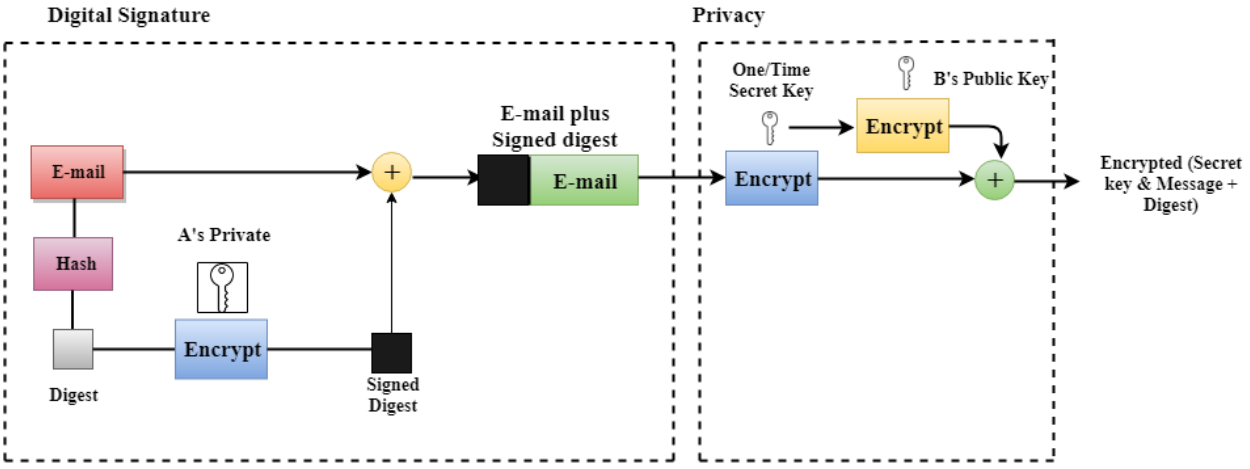
Kerberos is a network authentication protocol for authenticating requests in computer networks. It is based on a client-server model, which uses an encryption technology and a “Ticket” mechanism to prove the identity of a user on a non-secure network. Kerberos protocol messages protect the network from replay attacks and eavesdropping. It commonly uses public-key cryptography while authenticating users attempting to access the server.



- Step 1: The user sends the credentials to the authentication server.
- Step 2: The AS (authentication server) hashes the password of the user and verifies the credentials in the active directory database. If the credential matches, then the AS (which consists of the Ticket Granting Service) sends back the TGS Session Key and ticket, granting the ticket to the user to create a session.
- Step 3: Once the user authenticates, they send the ticket, granting the ticket to request a service ticket to the server or TGS for accessing services.
- Step 4: The TGS authenticates the TGT and grants a service ticket to the user. The service ticket consists of a ticket and a session key.
- Step 5: The client sends the service ticket to the server. The server uses its key to decrypt the information from the TGS and the client is authenticated to the server

(PGP) Protocol

PGP (Pretty Good Privacy) is an encryption and decryption computer program that is used to provide confidentiality and validation during communication. PGP enhances the security of emails.



- PGP is an application-layer protocol that provides cryptographic privacy and authentication for network communication.
- It encrypts and decrypts email communication, as well as authenticates messages with digital signatures and encrypts stored files.

Working of PGP

Every user has a public encryption key and a private key. Messages are sent to another user after encryption using the public key. The receiver decrypts the message using their private key. PGP compresses the message, which increases the security of the message in the network. PGP creates a session key that is used only once. PGP encrypts the message using the session key (along with the encryption algorithm). The session key is encrypted by the recipient's public key. The session key encrypted by public key is sent to the recipient along with the encrypted message. The recipient uses their private key to decrypt the session key and to decrypt the entire message.

There are two versions of PGP:

1. Rivest-Shamir-Adleman Algorithm
2. Diffie-Hellman Algorithm

PGP creates a hash code from the user's name and signature to encrypt the sender's private key. The receiver uses the sender's public key to decrypt the hash code.

S/MIME Protocol

S/MIME (Secure/Multipurpose Internet Mail Extensions) is an application-layer protocol used to send digitally signed and encrypted email messages. It uses the Rivest-Shamir-Adleman encryption (RSA) system for email encryption. Administrators need to enable S/MIME-based security for mailboxes in their organizations.

Difference between PGP and S/MIME

S/MIME is used to send digitally signed and encrypted messages. It allows you to encrypt the email messages and then digitally sign them to ensure confidentiality, integrity, and non-repudiation for messages. It provides cryptographic security services such as:

- Authentication
- Message Integrity
- Non-Repudiation
- Privacy
- Data Security

S/MIME ensures email security and has been included in the latest versions of browsers. It uses a RSA encryption method and provides details including encryption and digital signatures in the message.

Secure HTTP

Secure HTTP ensures a secured interchange of data on the World Wide Web. It implements application-level security that offers encryption and digital signatures for the message. S-HTTP verifies the user by using a certificate. S-HTTP provides many cryptographic algorithms and modes of operations. The S-HTTP protocol uses a client-server protocol to determine the security conditions for a client-server communication. It allows the client to send a certificate in order to authenticate a user. There are many

webservers that support the S-HTTP protocol, which allows them to communicate without the need for any encryption.

HTTP	HTTPs
It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
It is not secure & unreliable.	It is secure & reliable.
HTTP URLs begin with http://.	HTTPs URLs begin with https://.
It uses port 80 by default .	It was use port 443 by default.
It is subject to man-in-the-middle & eavesdropping attacks.	It is designed to withstand such attacks & is considered secure against such attacks.

Hyper Text Transfer Protocol Secure (HTTPS)

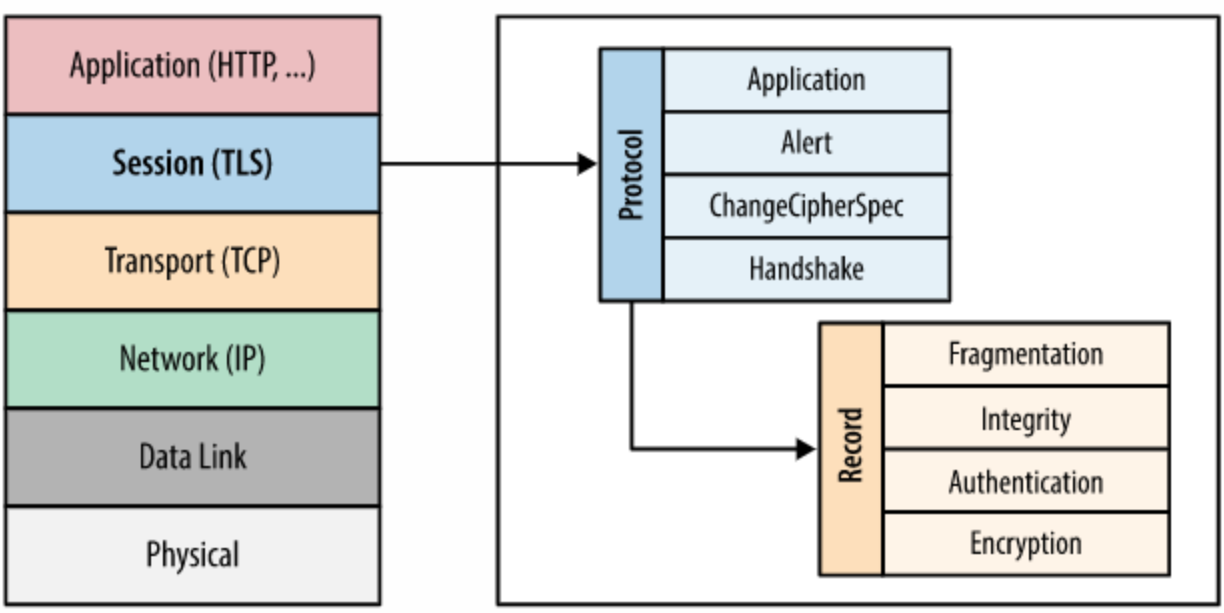
It is a protocol used to ensure secure communication in the network. It uses protocols such as TLS (Transport layer security) and Secure Sockets Layer (SSL) to ensure secure transmission of data. HTTPS confirms the verification of the websites and preserves the confidentiality and reliability of the messages passed over the Internet.

HTTPS mainly uses SSL in order to protect the website, making it easier for users to access the website. SSL has the following advantages:

- Encrypts confidential information during the exchange of data.
- Maintains a record of the details regarding the certificate owner.
- A certificate authority checks the owner of the certificate while issuing it

Transport Layer Security (TLS)

TLS provides secure communication of data in addition to confidentiality and reliability between the communicating parties



A secure TLS connection includes the following properties:

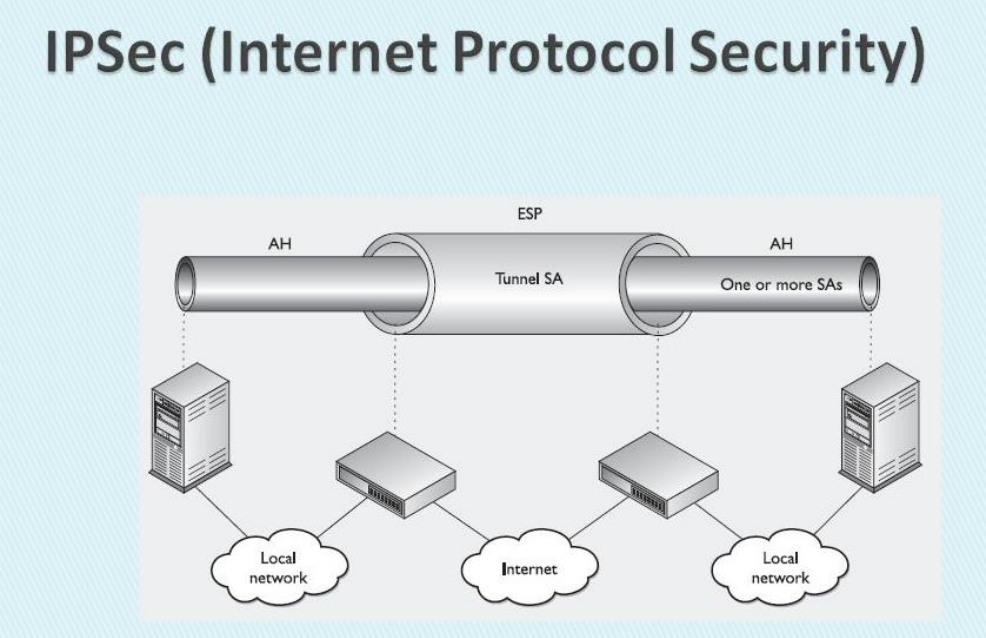
- Ensured confidentiality and reliability of data during communication between client and server using symmetric cryptography.
- Authenticates communication applications using public-key cryptography.
- Authentication codes can maintain the reliability of the data.

TLS consists of two protocols:

1. **TLS Record Protocol**: Provides security using an encryption method.
2. **TLS Handshake protocol**: Provides security using authentication of the client and the server before communication.

Internet Protocol Security (IPsec)

IPsec ensures secure communications over the Internet Protocol (IP) network. It works at the application layer of the communications model. It makes use of cryptographic security services to ensure secure communication. It allows authenticating the IP packets during communication of data. IPsec finds its applications in Virtual Private Networks and remote user access. IPsec is used between a pair of hosts, a pair of security gateways, or between a security gateway and a host. The IPsec consists of two security services: Authentication Header (AH) and Encapsulating Security payload (ESP). The AH allows authentication of the sender; whereas, the ESP allows authentication of the sender as well as encryption of the data.



It provides secure communication for network-level peer authentication, data origin authentication, and ensures data integrity, data confidentiality (encryption), and replay protection IPsec consists of two encryption modes: transport and tunnel.

- In transport mode, the data portion or the payload is encrypted.
- In tunnel mode, the entire IP is encrypted.