Unit 4: E-Commerce Security and Fraud Issues and Protections

(Part-B)

Contents:

4.5 EC defense Strategy: access control (Authorization and Authentication, Biometric Systems), encryption and PKI (Symmetric Key Encryption, Asymmetric Key Encryption, Certificate Authority (CA), Secure Socket Layer (SSL).
4.6 Securing e-commerce networks: Firewalls, Virtual Private Networks, Intrusion Detection Systems (IDS), intrusion prevention System (IPS)

4.5 EC defense Strategy

EC security needs to be addressed by the organization. An EC security framework defines the high level categories of assurance and their controls. The major categories are regulatory, financial, and marketing operations. Only the key areas are listed in bellow:

1. Defending access to computing systems, data flow, and EC transactions.

This includes three topics:

i) Access control (including biometrics),
ii) encryption of contents, and
iii) public key infrastructure (PKI).

These line of defense provides comprehensive protection when applied together. Intruders that by-pass the access control will face encrypted material even if they pass a firewall.

2. **Defending EC networks**.

This includes mainly protection by **firewall**. The firewall isolates the corporate network and computing devices from the Internet that are poorly secured.

To make the Internet more secured, we can use **virtual private network (VPN)**.

In addition to these measures, it is wise to use **intrusion detection system** (IDS).

A protected network means securing the incoming e-mail, which is usually unencrypted. It is also necessary to protect against viruses and other malware that are transmitted via the networks.

3. **General, administrative, and application controls.** These are a variety of safeguards that are intended to protect computing assets by establishing guidelines, checking procedures, and so forth.

4. **Protection against social engineering and fraud**. Several defense methods are used against spam, phishing, and spyware.

5. **Disaster preparation, business continuity, and risk management**. These topics are managerial issues that are supported by software.

6. **Implementing enterprise-wide security programs**. To deploy the abovementioned defense methods, one needs to use appropriate implementation strategy.

7. **Conduct a vulnerability assessment and a penetration test**.

8. **Back up the data**.

Access Control

Access control determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how).

Authorization and Authentication

Access control involves authorization (having the right to access) and authentication, which is also called user identification (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that differentiates it from other users. Typically, user identification is used together with a password.

Authentication

After a user has been identified, the user must be authenticated. Authentication is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.

To maintain a secure network, an organization must authenticate users attempting to access the network by requiring them to:

- enter a username and password;
- insert a smart card and enter the associated PIN;
- biometrics (provide a fingerprint, voice pattern sample, or retina scan)

The policy makers in security system at present recommends a **two-factor authorization**. This approach adds another identity check along with the password system.

A number of multifactor authentication schemes can be used, such as biometrics, one-time passwords (OTP), or hardware tokens that plug into a USB port on the computer and generate a password that matches the one used by a bank's security system.

Biometrics System

A biometric authentication is a technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals. Biometric systems can identify a previously registered person by searching through a database for a possible match based on the person's observed physical, biological, or behavioral traits, or the system can verify a person's identity by matching an individual's measured biometric traits against a previously stored version.

Examples of biometric features include fingerprints, facial recognition, DNA, palm print, hand geometry, iris recognition (retina scan), and even odor/scent. Behavioral traits include voice ID, typing rhythm (keystroke dynamics), and signature verification.

Thumbprint or fingerprint. A thumb- or fingerprint (finger scan) of users requesting access is matched against a template containing the fingerprints of authorized.

Retina scan. A match is sought between the patterns of the blood vessels in the retina of the access seekers against the retinal images of authorized people stored in a source database.

Voice ID (voice authentication). A match is sought between the voice pattern of the access seekers and the stored voice patterns of the authorized people.

Facial recognition. Computer software that views an image or video of a person and compares it to an image stored in a database (used by Amazon.com and Alibaba).

Signature recognition. Signatures of access seekers are matched against stored authentic signatures.

The use of biometric technology has been slow to develop due to cost and privacy concerns. However, MasterCard recently announced it will begin rolling out its new MasterCard Identity Check service that allows users to take an initial ID photo that will be used to create a digital map of their face, which will be stored on MasterCard's servers. When the user wants to make a payment using a smartphone, the MasterCard app will capture his or her image, which, along with a user-entered password, will be authenticated against the stored image before the transaction is approved. MasterCard's system also offers a fingerprint sensor that can be used to verify purchases.

Apple's new Apple Pay system makes use of the fingerprint sensors on newer iPhones. Consumers paying with Apple Pay, which is tied to a credit or debit card, just hold their iPhone close to the contactless reader with their finger on the Touch ID button.

Encryption and PKI

The word "**cryptography**" derives from the Greek word for "secrete writing".

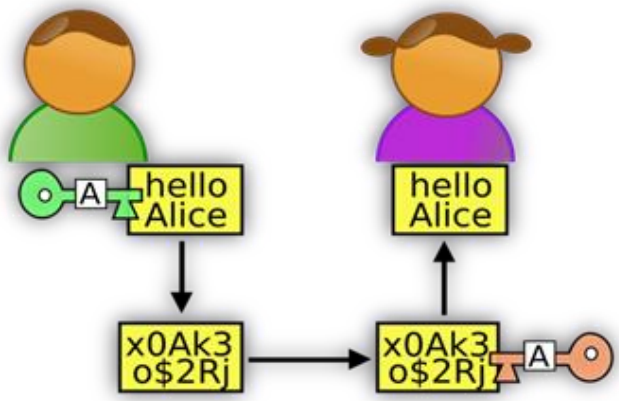
Cryptography is a process associated with changing **plaintext** (ordinary text, or cleartext) into **ciphertext** (a process called **encryption**), and then backs again (known as **decryption**).

It is the conversion of data into a secret code for protection of privacy using a specific algorithm and a secret key.

It is used to protect e-mail messages, credit card information, and corporate data.

The primary goal of cryptography is to conceal (hide) data to protect it against unauthorized third-party access by applying encryption.

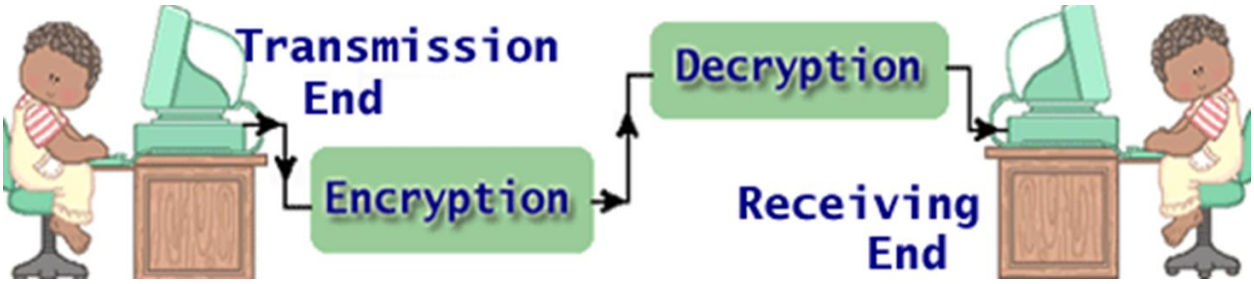
The more theoretical or mathematical effort is required for an unauthorized third party to recover data, the stronger is the encryption.

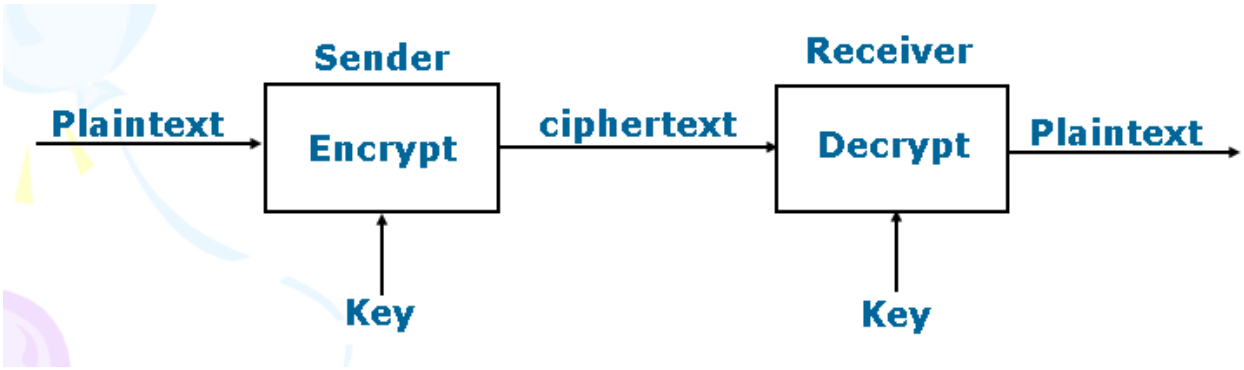


Encryption and decryption in cryptography

Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver. Encryption is done by using encryption key.

Decryption is the process of taking encrypted text or cipher text and converting it back into original text (plain text) that we can read and understand. It is done by using decryption key.





The purpose of encryption is to:

(a) To secure stored information

(b) To secure information transmission

Plaintext is ordinary text or clear text which is able to read and understand by computer and human being.

Cipher text/cypher text- text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver.

A **key** is a piece of information that allows only those that hold it to encode and decode a message.

How does algorithm work?

Substitution cipher – every occurrence of a given letter is replaced systematically by another.

"HELLO" → "JGNNQ"

Transposition cipher- the ordering of the letters in each word is changed in systematic way

"HELLO" → "OLLEH"

General Requirement of encryption and decryption

Consider an e-commerce scenario where Alice, a purchasing agent, wants to order some products from Bob, her supplier.

Requirements for the transaction:

1. Alice wants to be sure that she is really dealing with Bob and not an impostor (**authentication**).
2. Bob wants to know that Alice is really Alice and not an impostor (**authentication**), because Alice gets special prices as negotiated.
3. Alice wants to keep the order secret from her competitors; and Bob does not want other customers to see Alice's special prices (**privacy**).
4. Alice and Bob both want to be sure that crackers cannot change the price or quantity (**integrity**).
5. Bob wants to ensure that Alice cannot later claim that she did not place the order (**non-repudiation**).

Benefits of encryption and decryption

- Provides secured communication.
- Allows users to carry data on their laptops, mobile devices, and storage devices (e.g., USB flash drives)
- Protects backup media while people and data are offsite.
- Allows for highly secure virtual private networks.
- Enforces policies regarding who is authorized to handle specific corporate data.
- Ensures compliance with privacy laws and government regulations and reduces the risk of lawsuits.
- Protects the organization's reputation and secrets.

It enables organizations to share sensitive sales data, promotion plans, new product designs, and project status data among employees, suppliers, contractors, and others with a need to know.

Encryption enables physicians and patients to share sensitive healthcare data with labs, hospitals, and other health treatment facilities as well as insurance carriers.

To complete such transactions, sensitive data—including names, physical addresses, email addresses, phone numbers, account numbers, health data, financial data, passwords, and PINs—must be sent and received.

Type of Cryptography

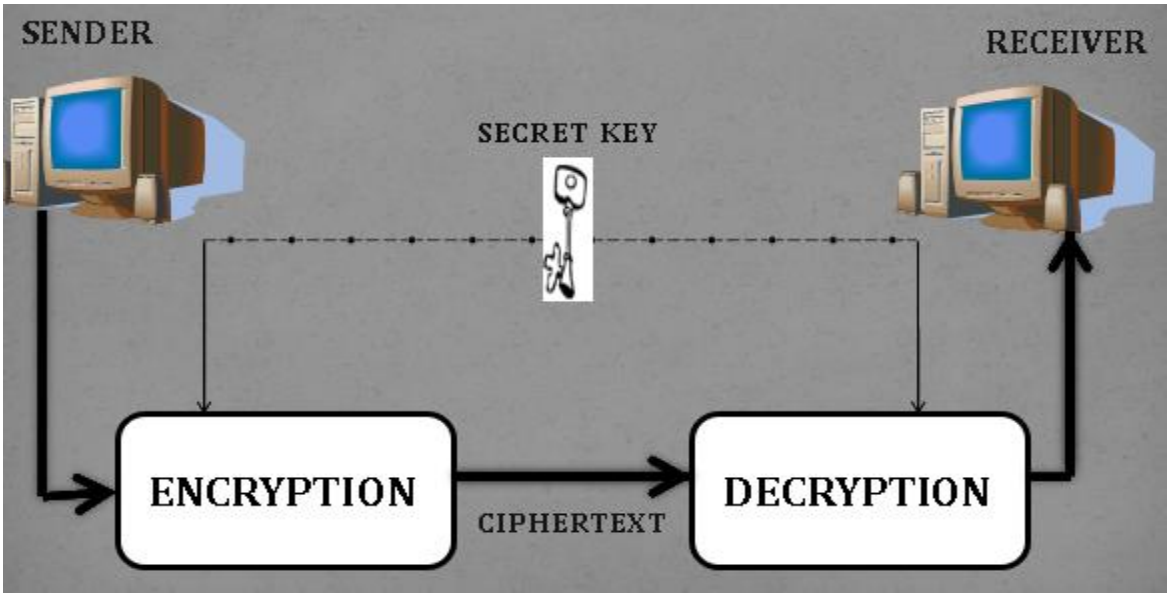
There are several ways of classifying cryptographic algorithms.

According to number of keys used for encryption and decryption, can be classified into following types:

1) **Secret/Symmetric** Key Cryptography: Uses a single key for both encryption and decryption.
2) **Public/Asymmetric** Key Cryptography: Uses one key for encryption and another for decryption.

Secret/Symmetric key Cryptography

- The message (plaintext) is encrypted into ciphertext using a key.
- The resulting ciphertext is sent to the recipient, who will decrypt it using the **same key.**
- Hence, the same key must be known to both parties.
- The best known secret-key system is the Data Encryption Standard (DES).
- This method is easy and fast to implement but has weaknesses;
- The algorithm that is used to encode the message is easier for attackers to understand, enabling them to more easily decode the message.



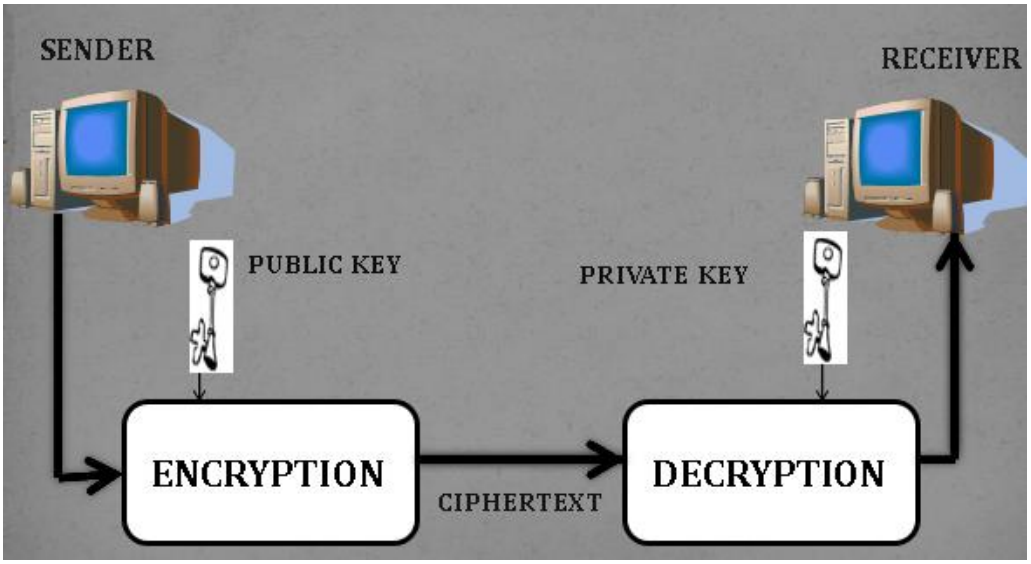
Advanced Encryption Standard (AES) is the most widely used symmetric algorithm. Wireless Protected Access 2 (WPA2), which is the most commonly used security protocol for wireless networks today, employs the AES encryption algorithm.

Some of the common secret key cryptography methods used are:

1. Advanced Encryption Standard (AES) – 128, 192, 256 bits
2. Data Encryption Standard (DES)
3. Triple Data Encryption Standard (TripleDES) – advanced form of DES
4. Twofish - 128 bits – successor of Blowfish
5. Rivest Cipher 4 (RC4)
6. QUAD (Cipher)

Public/Asymmetric key Cryptography

- The **public key** can only be used to encrypt the message and the **private key** can only be used to decrypt it.
- This allows a user to freely distribute his or her **public key** to people who are likely to want to communicate with him or her without worry of compromise because only someone with the **private key** can decrypt a message.
- To secure information between two users, the sender encrypts the message using the **public key** of the receiver. The receiver then uses the **private key** to decrypt the message.
- The best-known public-key cryptosystem is RSA, named after its inventors: Rivest, Shamir, and Adleman.



Some of the common public key cryptography methods used are:

1. Rivest-Shamir-Adleman (RSA)
2. Elliptic Curve Cryptography (ECC)
3. ElGamal Encryption

Differences between symmetric and asymmetric key cryptography

Characteristics	**Symmetric Key Cryptography**	**Asymmetric Key Cryptography**
Key used for encryption/decryption	Same key is used for encryption and decryption	One key is used for encryption and another, different key is used for decryption
Complexity	Simple	Complex, due to use of two different keys
Speed of encryption/decryption	Very fast	Slower
Size of the resulting encrypted text	Usually same as or less than the original plain text size	More than the original plain text size
Key length	Smaller key lengths are used to encrypt the data (e.g. 128 - 256 bits)	Usually uses longer keys lengths (e.g. 1024 – 4096 bits)
Key agreement/exchange	A big issue	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of the participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption/decryption (confidentiality). Cannot be used for digital signatures.	Can be used for encryption/ decryption as well as for digital signatures (integrity and non-repudiation)
Ideal use	Applications where a large number of data are to be encrypted	Applications where small amount of data are to be encrypted, digital signatures.

Examples	DES, AES, TDES, RC4, QUAD	RSA, ECC, ElGamal, Digital Signature algorithms

Digital Signature or E-signature

- A digital signature is an electronic signature that can be used to **authenticate** the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged (**Integrity**).
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily **repudiate** it later.
- A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.
- Digital Signatures are a cryptographic technique and are one of the most important application of asymmetric public-key cryptography.

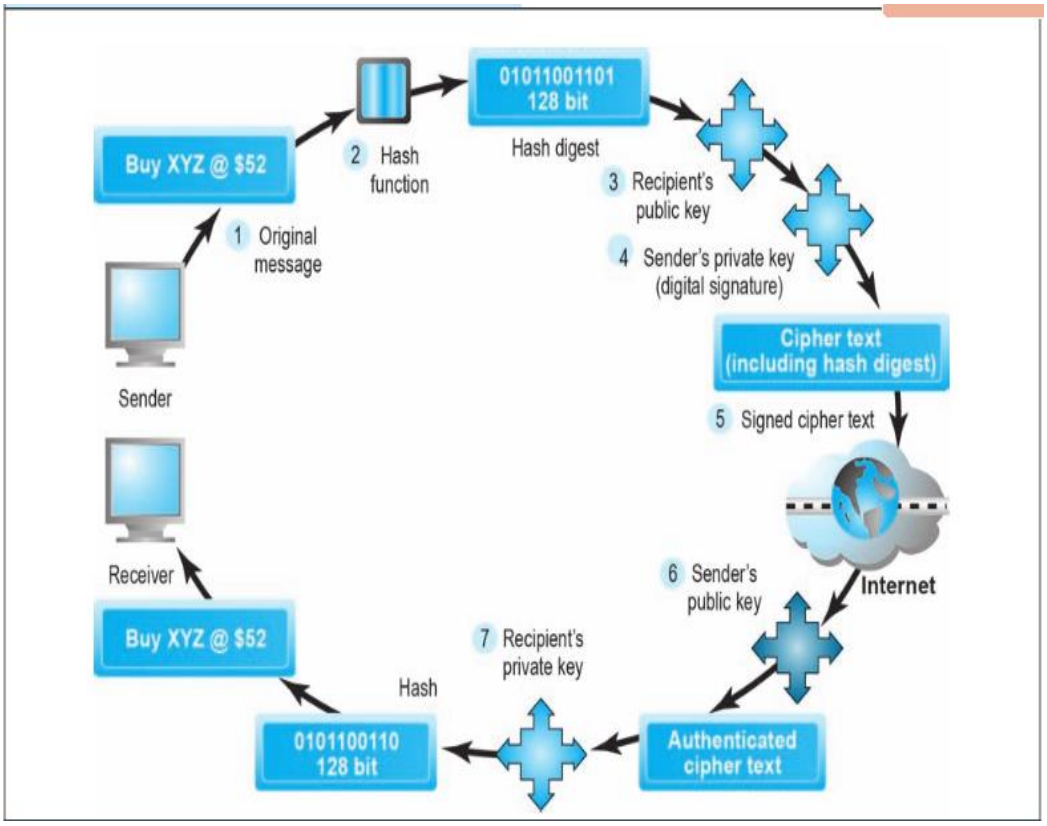
Digital Signatures features

- Easily transportable.
- Cannot be imitated by someone else
- Can be automatically generated.

How does Digital Signature Work?

FIGURE 5.7 PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES

STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result using recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using his or her private key.
4. The sender encrypts the result, again using his or her private key.	The sender's private key is a digital signature. There is only one person who can create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packets.
6. The receiver uses the sender's public key to authenticate the message.	Only one person can send this message, namely, the sender.
7. The receiver uses his or her private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensures the message was not changed in transit.



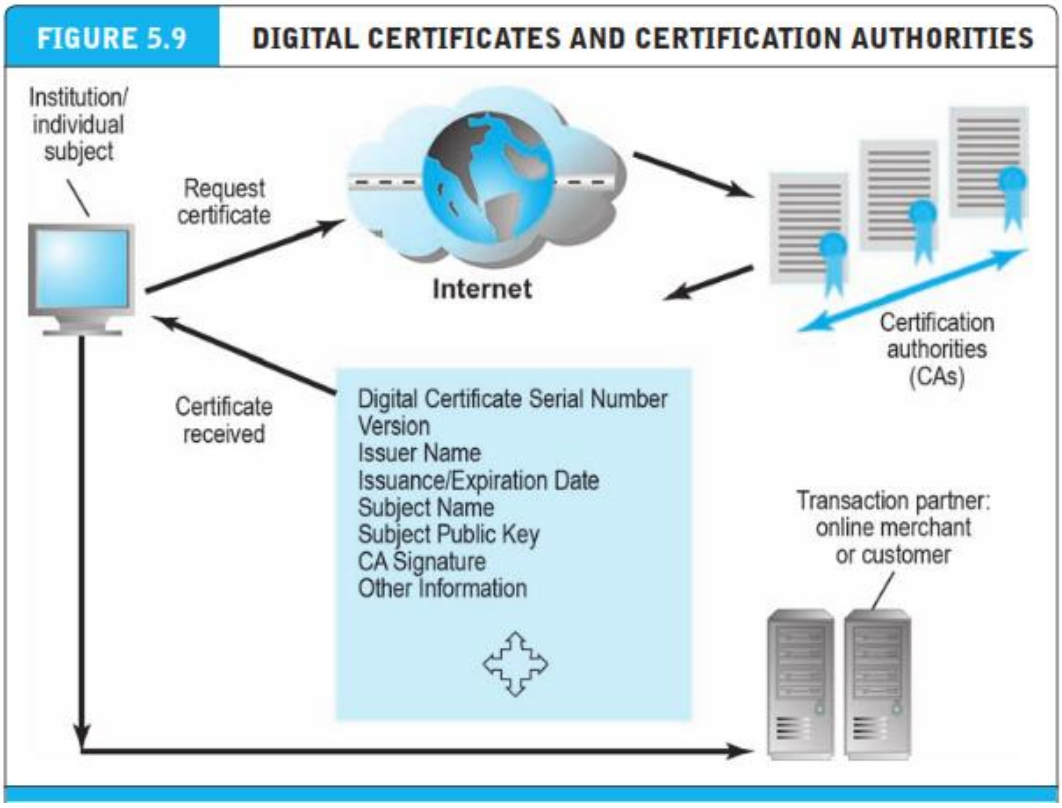
Digital Certificate and Certification authority

Digital certificate a digital document issued by a certification authority that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority, and other identifying information.

A digital certificate is a digital document issued by a trusted third-party institution known as a **Certification authority** (CA) that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority (the name of the CA encrypted using the CA's private key),and other identifying information.

Certification authorities issue, verify, and guarantee digital certificates that are used in e-commerce to assure the identity of transaction partners.

Public key infrastructure (PKI) refers to the CAs and digital certificate procedures that are accepted by all parties. When you sign into a "secure" site, the URL will begin with "https" and a closed lock icon will appear on your browser. This means the site has a digital certificate issued by a trusted CA. It is not, presumably, a spoof site.



Certificates are used in e-commerce in different ways.

- Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt it using the merchant's public key to obtain both the message digest and the certificate as issued. If the message digest matches the certificate, then the merchant and the public key are authenticated.
- The merchant may in return request certification of the user, in this case the user would send the merchant his or her individual certificate.
- There are many types of certificates: personal, institutional, Web server, software publisher, and CAs themselves.

Digital signatures vs Digital certificate

Digital signatures are electronically generated and can be used to ensure the integrity and authenticity of some data, such as an e-mail message and protect against non-repudiation.

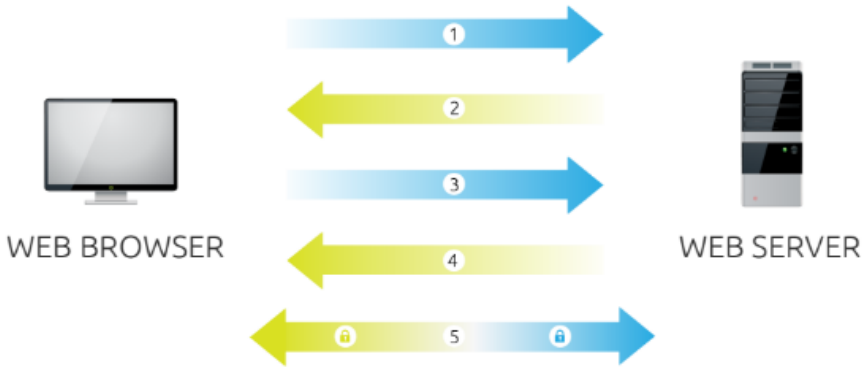
Digital certificate is a form of an electronic credential for the Internet. Similar to a driver's license, employee ID card, a Digital certificate is issued by a trusted third party to establish the identity of the certificate holder. The third party who issues the Digital Certificate is known as the Certifying Authority (CA).

Secure Sockets Layer (SSL)

- The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- E-commerce web sites use SSL (Secure Sockets Layer) to protect important information such as credit card numbers as they travel across the network.
- SSL creates a private communication path between the web browser and the web server, encrypting all information that goes between the systems.

- Most common web browsers have SSL support built in and e-commerce companies can purchase or get freely available web servers that support SSL.
- SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.
- More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

How does (SSL) work?



1. Browser connects to a web server (website) secured with SSL (https). Browser requests for the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Browser checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Browser now encrypt all transmitted data with the session key.

4.6 Securing e-commerce networks

Virtual Private Network (VPN)

A **virtual private network** (**VPN**) is a computer network that uses the Internet to provide remote offices or individual users with secure access to their organization's network by creating an encrypted path to that network.

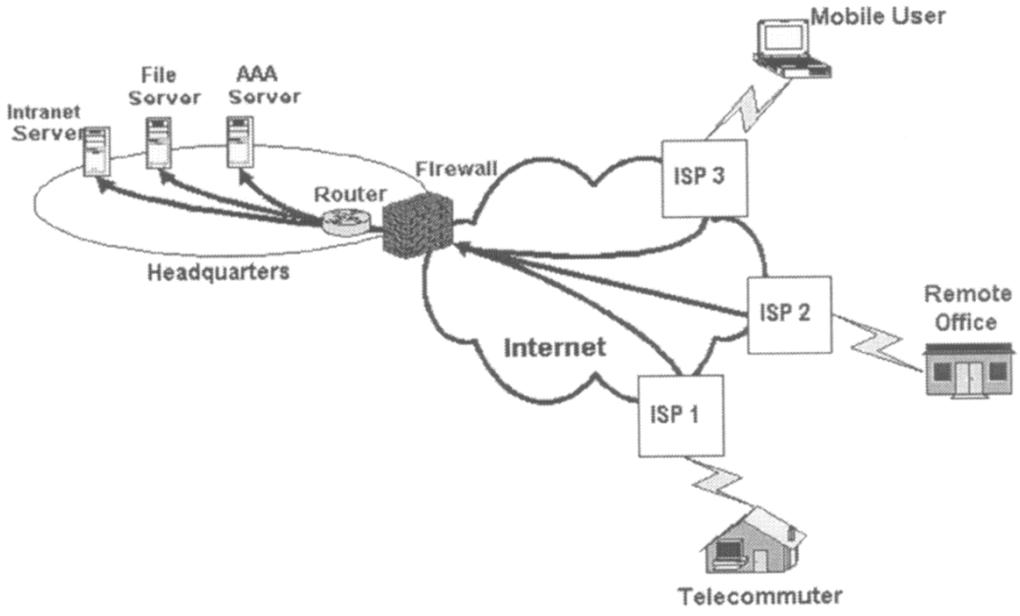
Virtual private networks help distant colleagues work together, much like desktop sharing.

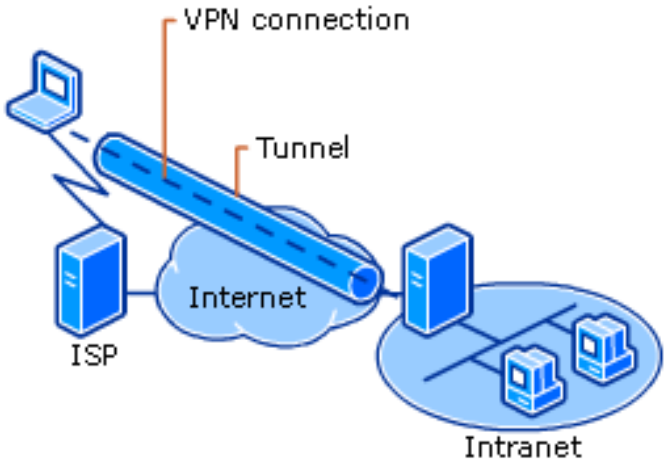
VPNs use both authentication and encryption to secure information from unauthorized persons. Authentication prevents spoofing and misrepresentation of identities. A remote user can connect to a remote private local network using a local ISP.

Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

It allows remote users to securely access internal networks via the Internet, using the Point-to-Point Tunneling Protocol (PPTP)

A virtual private network (VPN) is a secure way of connecting to a private Local Area Network at a remote location, using the Internet or any unsecure public network to transport the network data packets privately, using encryption. The VPN uses authentication to deny access to unauthorized users, and encryption to prevent unauthorized users from reading the private network packets. The VPN can be used to send any kind of network traffic securely, including voice, video or data.

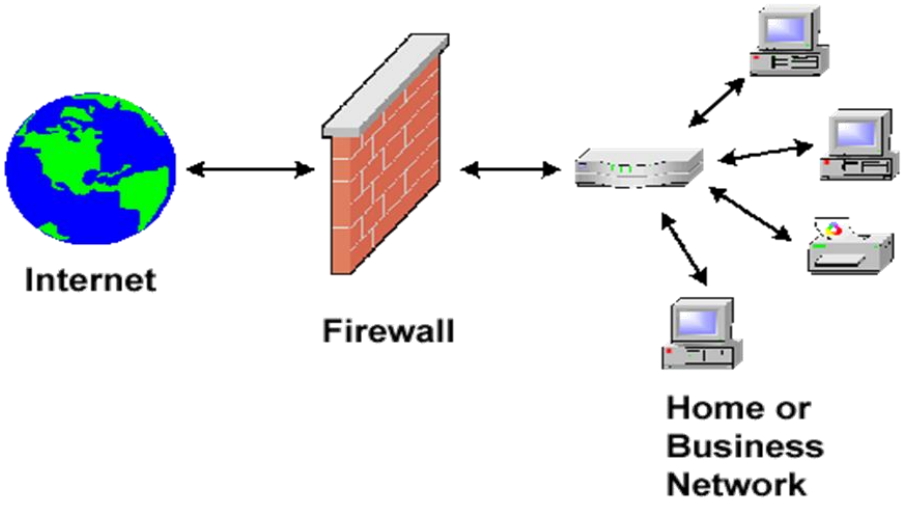




Firewall

A **firewall** is a hardware or software designed to permit or deny network transmissions based upon a set of rules and is frequently used to **protect networks from unauthorized access** while permitting legitimate communications to pass.

A Firewall is hardware, software, or a combination of both which is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.



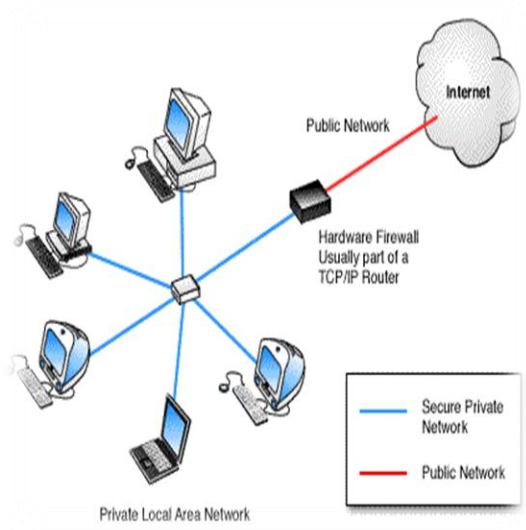
Hardware vs Software Firewall

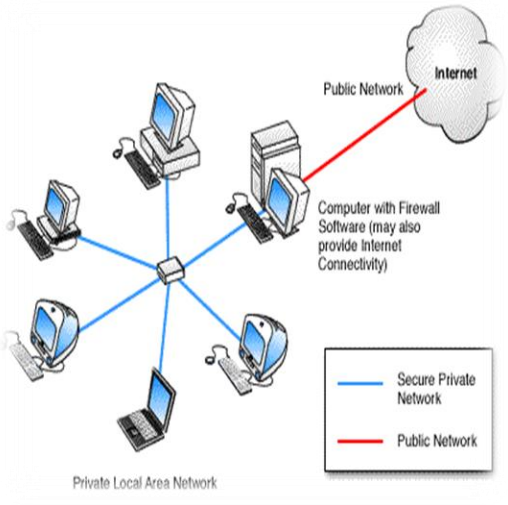
Hardware Firewalls

- Protect an entire network
- Implemented on the router level
- Usually more expensive, harder to configure

Software Firewalls

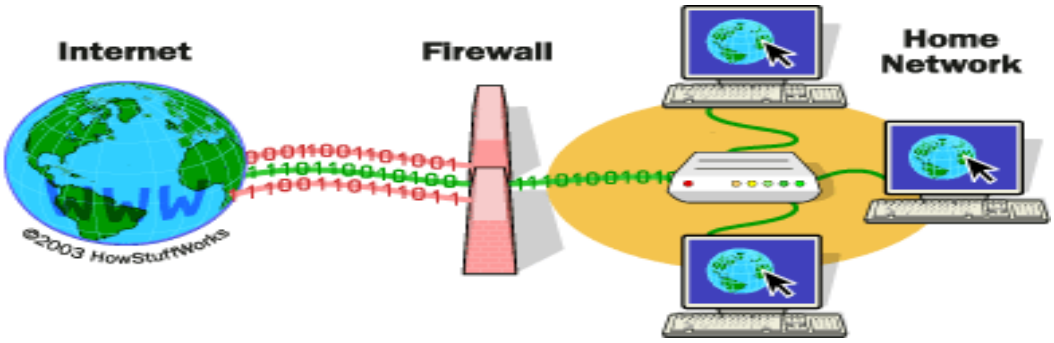
- Install in a single computer and protect all
- Usually less expensive, easier to configure





How does a software firewall work?

- Inspects each individual “packet” of data as it arrives at either side of the firewall.
- Determines whether it should be allowed to pass through or if it should be blocked.



Firewall Rules

Allow – traffic that flows automatically because it has been deemed
Block – traffic that is blocked because it has been deemed dangerous to your computer
Ask – asks the user whether or not the traffic is allowed to pass through

Characteristics of firewall

- Service control - Determines the types of Internet services that can be accessed, inbound or outbound.
- Direction control - Determines the direction in which particular service requests are allowed to flow.
- User control - Controls access to a service according to which user is attempting to access it
- Behavior control - Controls how particular services are used (e.g. filter e-mail)
- All traffic from inside to outside must pass through the firewall.
- Only authorized traffic will be allowed to pass.

What Can a Firewall Do?

- Focus for security decisions - Stop hackers from accessing your computer
- Can enforce security policy - Protects your personal information
- Limits your exposure - Blocks “pop up” ads and certain cookies
- Can log Internet activity efficiently - Determines which programs can access the Internet

What Can't a Firewall Do?

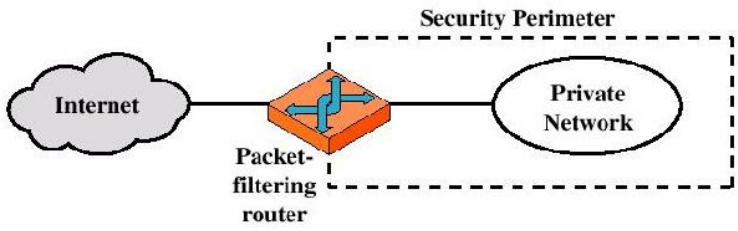
- Cannot protect against internal threats - For example, an angry employee deleting files Or, an employee cooperating with an outside attacker
- Cannot protect against attacks that bypass the firewall
- Can't protect against completely new threats
- Can't protect against viruses, different operating systems and applications inside the network - Need to scan all incoming data…impractical, perhaps impossible

Types of firewalls

Packet-filtering Router

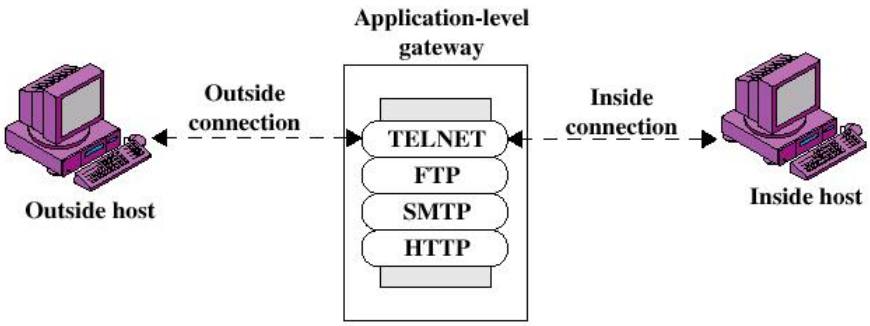
- Applies a set of rules to each incoming IP packet and then forwards or discards the packet

- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)
- Advantages: Transparency to users, High speed
- Disadvantages: Difficulty of setting up packet filter rules, Lack of Authentication



Application-level Gateway

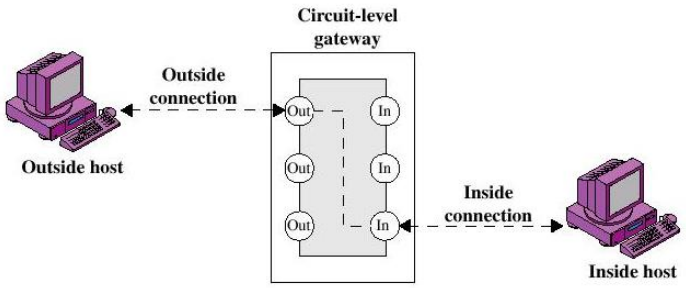
- Also called proxy server
- Acts as a relay of application-level traffic
- User contacts gateway through an application (e.g., telnet or FTP)
- User must authenticate and provide name of remote host
- Gateway connects to remote host and relays data back to the user
- If code for an application is not implemented, gateway will not support that application
- May be configured to support only certain features of an application
- Advantages: Higher security than packet filters, Only need to scrutinize a few allowable applications, Easy to log and audit all incoming traffic
- Disadvantages: Additional processing overhead on each connection (gateway as splice point)



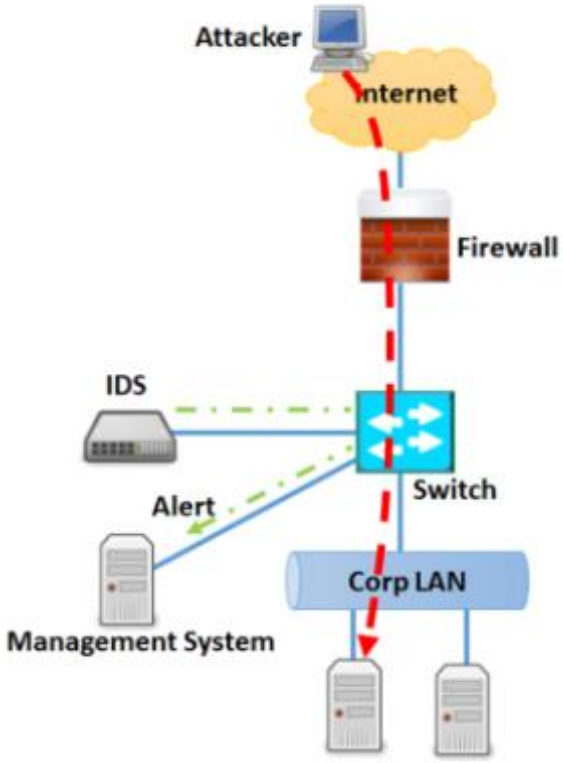
Circuit-level Gateway

It provides session-level control over network traffic. Circuit-level gateways are host based and reside on individual clients and servers inside the network, rather than on a dedicated machine as they do with other types of firewalls. It examines incoming IP packets at the session level and act as relays by handing off incoming packets to other hosts. It monitors TCP handshaking between packets to determine whether a requested session is legitimate.

Circuit-level gateways are rarely used as a stand-alone firewall solution; instead, they are typically used in combination with application layer proxy services and packet filtering features in dedicated firewall applications.



Intrusion Detection System (IDS)



An intrusion detection system (IDS) is a device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems.

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Types of IDS:

Network Intrusion Detection System (NIDS):

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

Host Intrusion Detection System (HIDS):

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

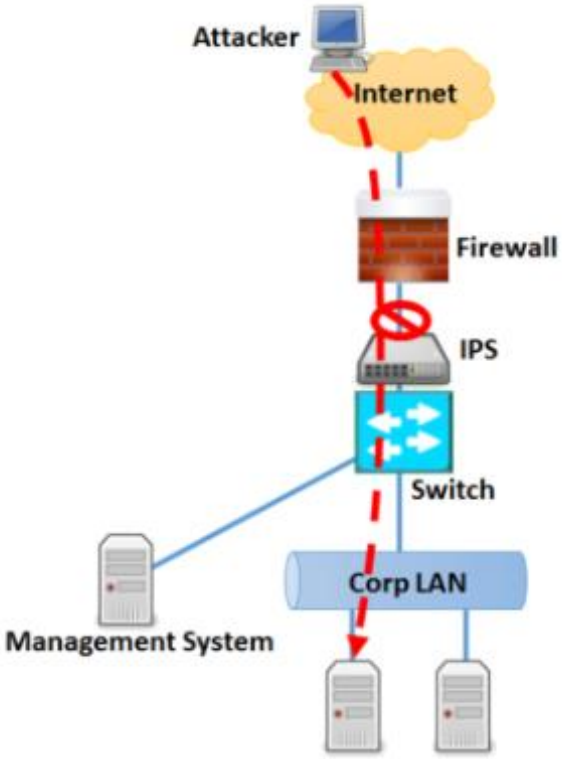
Hybrid Intrusion Detection System:

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Intrusion Prevention System (IPS)

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity.

Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.



Comparison of IPS with IDS:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

Types of IPS:

Network-based intrusion prevention system (NIPS): It monitors the entire network for suspicious traffic by analyzing protocol activity.

Wireless intrusion prevention system (WIPS): It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Network behavior analysis (NBA): It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

Host-based intrusion prevention system (HIPS): It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

PARAMETER	IPS	IDS
Abbreviation for	Intrusion Prevention System	Intrusion Detection System
System Type	Active (monitor & automatically defend) and/ or passive	Passive (monitor and Notify)
Detection mechanism	Statistical anomaly based detection Signature detection: Exploit-facing signatures, Vulnerability-facing signatures	Signature detection: Exploit-facing signatures
Placement	Inline to data communication	Out of band from data communication
Anomaly response	Drop, alert or clean malicious traffic	Sends alarm/alert of detecting malicious traffic
Network performance impact	Slows down network performance due to delay caused by inline IPS processing	Does not impact network performance due to non-line deployment of IDS.
Benefits	Preferred by most organizations since detection and prevention are automatically performed	Does not block legitimate traffic which might be blocked by IPS at times.

Practice Questions:

1. How you define network security?
2. Explain the Network security goal with example.
3. Differentiate between authorization and authentication.
4. Why firewall is required in organization.
5. What are the limitation of firewall?
6. What is DDOS attack?
7. Explain the working mechanism of Anti-virus software.
8. Explain the public/private cryptography in detail.
9. What is digital signature?
10. How does digital signature work?
11. Define the term 'Certification authority' and its role in e-commerce.
12. What is PKI?
13. Explain the limitation of encryption.
14. Differentiate between digital signature and digital certificate.
15. What do you mean by Third party authentication in e-commerce?
16. What is SSL? Explain the working mechanism of SSL in e-commerce web site.
17. What is VPN? Write three applications of VPN.
18. Explain EC security requirement in details.
19. Explain basic terminology of EC Security.
20. What is technical attack? Explain five technical attack on EC Application.
21. What is ransomware? Explain defense technic of ransomware.
22. What is digital signature? Explain the requirements of digital signature in secure transaction.
23. Explain the working mechanism of digital signature.
24. What is CA? Explain the working mechanism of CA.
25. Explain working mechanism of Secure Sockets Layer (SSL)
26. Explain the Securing e-commerce networks.
27. How does a VPN work and how does it benefit users?
28. List the basic types of firewalls and briefly describe each.