MODULE-5: Network Security

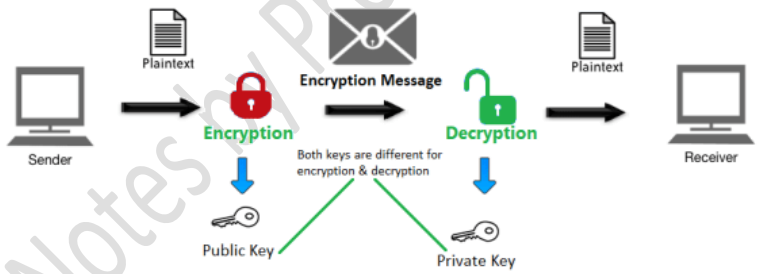
VIT | Vidyalankar Institute of Technology
Accredited A+ by NAAC

Prepared by Prof. Amit K. Nerurkar

SSL

SSL stands for Secure Sockets Layer, and it refers to a protocol for encrypting and securing communications that take place on the Internet. Although SSL was replaced by an updated protocol called TLS (Transport Layer Security) some time ago, "SSL" is still a commonly used term for this technology.
Step-by-step, here's how SSL works:
A user connects to an SSL-enabled service such as a website.

1. The user's application requests the server's public key in exchange for its own public key.
2. This public key exchange provides ways for both parties to encrypt messages that only the other party can read.
3. When the user sends a message to the server, the application uses the server's public key to encrypt the message.
4. The server receives the user's message and decrypts it using its private key. Messages sent back to the browser are encrypted in a similar way using a public key generated by the user's application.

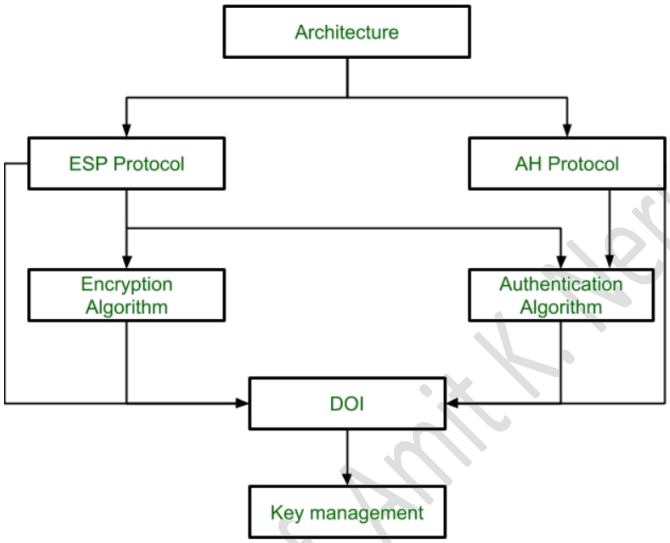


SSL creates trust by providing a secure channel for users to communicate with online services.

Users are more confident in web services since they know their data is being transmitted safely.
Enterprises see higher customer retention and trust, since their customers are more confident in their ability to safeguard data.
Users and enterprises see fewer incidents of data theft since sensitive data is no longer at risk of being intercepted.

IPSEC,

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality.



1. Architecture:

Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

2. ESP Protocol:

ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:

ESP with optional Authentication.
ESP with Authentication.

3. Encryption algorithm:

Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

4. AH Protocol:
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.

5. **Authentication Algorithm:**
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

6. **DOI (Domain of Interpretation):**
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management:
Key Management contains the document that describes how the keys are exchanged between sender and receiver.

Secure Email: PGP,

PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.

PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.

PGP is an open source and freely available software package for email security.

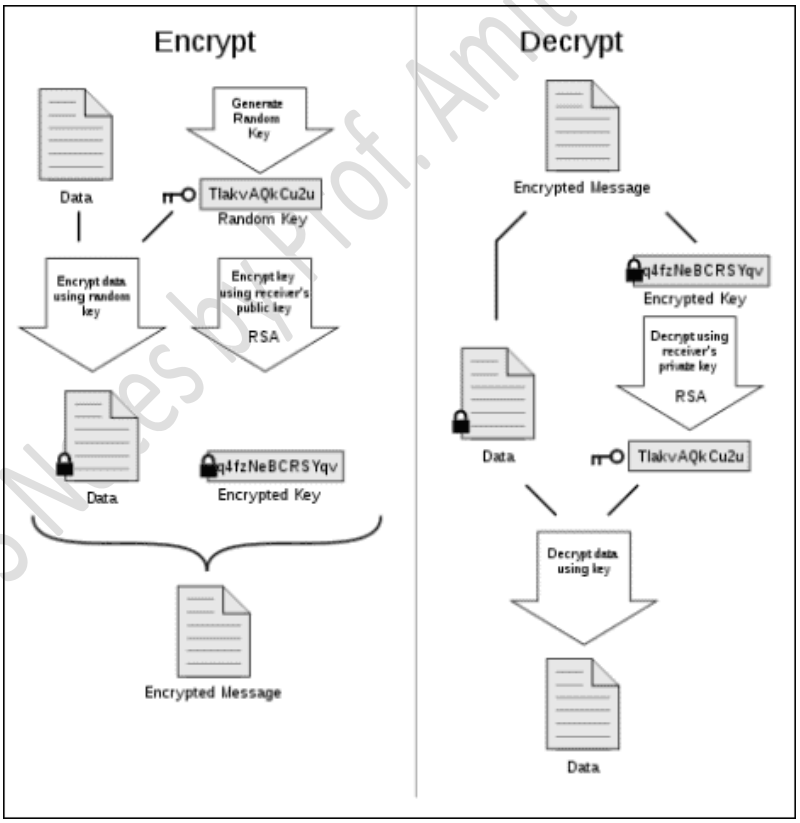
Lets first look at the common cryptography example of person A and person B. Person A wants to send a message to person B, however, there is a third party in the way, person C. Person C wants to see the message that person A is trying to send privately to person B, so person C intercepts the message before it gets to person B, reads it, then sends it back on its way.

With PGP we can prevent person C from reading the message, even if they get a hold of the message. In this situation, both person A and person B have a private

and public key. They've agreed they want to exchange messages, and both share their public keys with each other. Person A creates another key called a session key, which is never used again after the message is decrypted by person B. The message is encrypted using this session key. This session key is then also encrypted using person B's public key so that they will be able to decrypt the message once they receive the encrypted session key and message.

The session key and message are sent, and person C intercepts both. However, person C only has an encrypted session key and doesn't have the means to decrypt the key. So, person C has to send on the message without having read it.

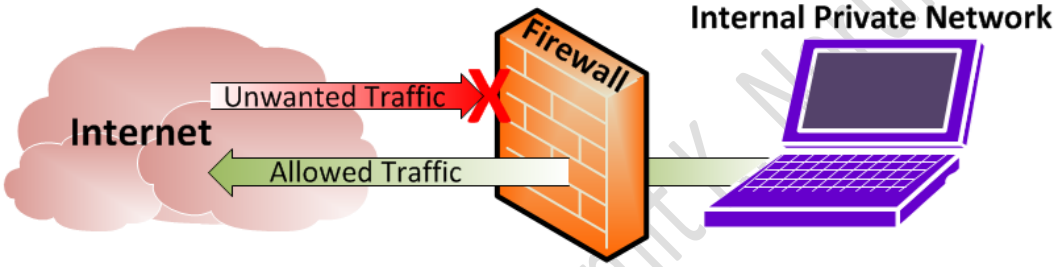
Once person B receives the session key and message, they decrypt the session key using their private key and use the session key to decrypt the message. This method allows messages to be sent between two parties without a potential third party interfering.



Firewalls

A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

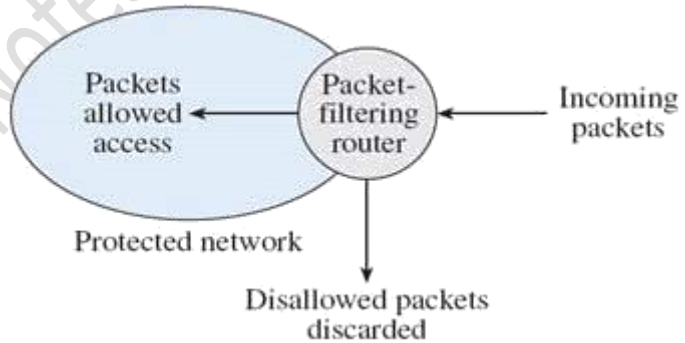
The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.



Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

Packet Filters –

It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.



For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to 'discard all packets' or to 'accept all packets'.

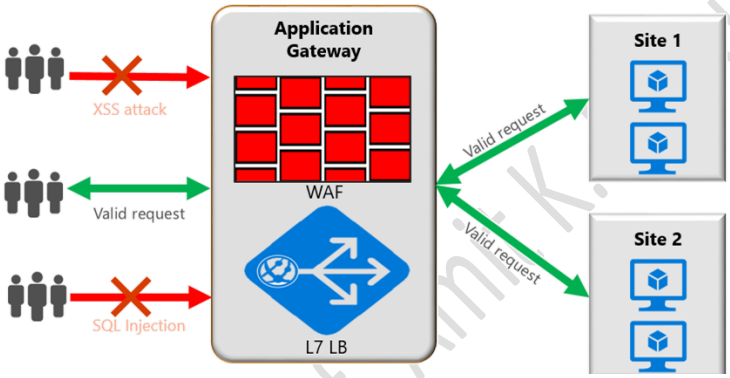
Application Gateways –

It is also known as Proxy server. It works as follows:

Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.

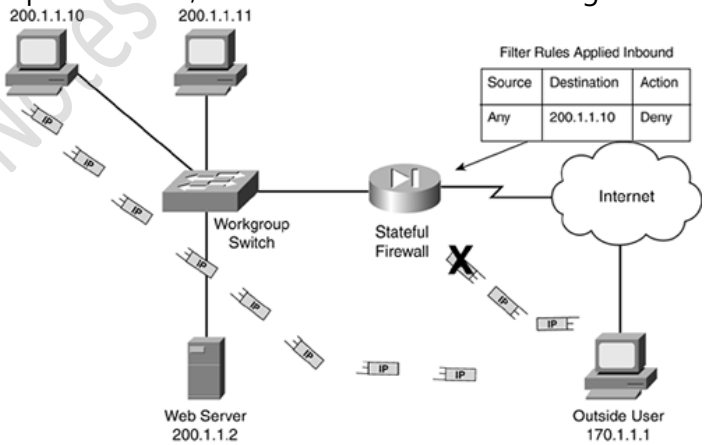
Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.



Stateful Inspection Firewalls –

It is also known as 'Dynamic Packet Filters'. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.



IDS and types

An IDS is either a hardware device or software application that uses known intrusion signatures to detect and analyze both inbound and outbound network traffic for abnormal activities.

This is done through :

- System file comparisons against malware signatures.
- Scanning processes that detect signs of harmful patterns.
- Monitoring user behavior to detect malicious intent.
- Monitoring system settings and configurations.

Upon detecting a security policy violation, virus or configuration error, an IDS is able to kick an offending user off the network and send an alert to security personnel.

Despite its benefits, including in-depth network traffic analysis and attack detection, an IDS has inherent drawbacks. Because it uses previously known intrusion signatures to locate attacks, newly discovered (i.e., zero-day) threats can remain undetected.

Furthermore, an IDS only detects ongoing attacks, not incoming assaults. To block these, an intrusion prevention system is required.

Signature-Based Intrusion Detection :

In Signature Based Intrusion Detection, the signature pattern is stored for a particular type of attack and is mapped with the attack when encountered to give related warning. A simple signature for a known attack type might be a series of TCP SYN packets sent to many different ports in succession and at times close to one another, and would cause a port scan. An intrusion detection system would probably find nothing unusual in the first SYN, say, to port 80, and then another (from the same source address) to port 25. But as more and more ports receive SYN packets, especially ports that are not open, this pattern reflects a possible port scan.

The problem with signature‐based detection is the signatures themselves. An attacker will try to modify a basic attack in such a way that it will not match the known signature of that attack.

Signature‐based IDSs cannot detect a new attack for which a signature is not yet installed in the database. Every attack starts, as a new attack at some time, and the IDS is helpless to warm of its existence.

Heuristic Intrusion Detection :

Signatures are limited to specific, known attack patterns; another form of intrusion detection is called heuristic intrusion detection that looks for uncommon behavior. For example, one user might always start the day by reading email, write many documents using a word processor, and occasionally back up files. These action would be normal. This user does not seem to use many administrator utilities. If that person tries to access sensitive system management utilities, this new behavior gives a clue that someone else was acting under the user's identity.

Stealth Mode :

An IDS is a network device and is itself potentially vulnerable to network attacks causing denial of service. To counter these problems, most IDSs run in stealth mode, where and IDS has two network interfaces; one for the network (or network segment) being mentioned and the other to generate alerts and perhaps other administrative needs. The IDS uses the mentioned interface as input only; it never sends packets out through that interface. The interface is configured so that the device has no published address through the monitored interface, that is a router cannot route anything to that address directly because the router does not know such a device exists. It is the perfect passive wiretap. If the IDS need to generate an alert, it uses only the alarm interface on a completely separate control network. Such architecture is shown in Figure.

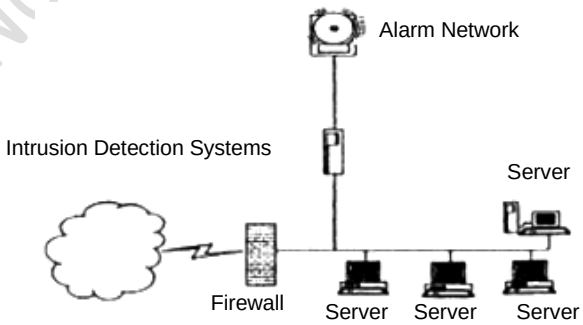


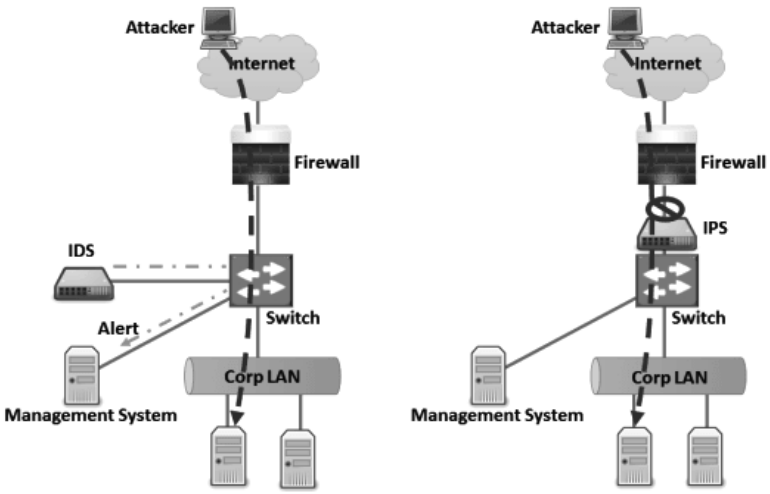
Fig.: Stealth Mode Connected in Two Network.

False Results :

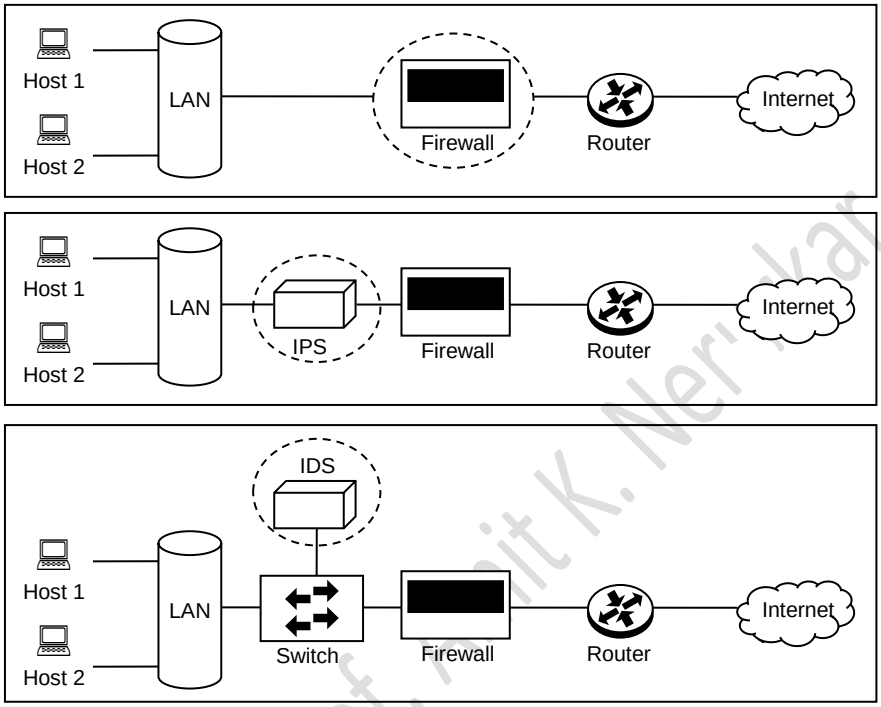
In IDS might detect an intruder correctly most of the time, it may stumble in two different ways; by raising an alarm for something that is not really an attack , or not raising an alarm for a real attack. Many false positives will make the administrator less confident of the IDS's warming's, perhaps leading to a real alarm's being ignored. But false negatives also mean that real attacks are passing the IDS without action. The degree of false positives and false negatives represents the sensitivity of the system. Most IDS implementations allow the administrator to tune the system's sensitivity, to strike an acceptable balance between false positives and negatives.

An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Whereas an Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. By blocking the attack rather than just detecting it, Intrusion Prevention allows an organization to shift from a reactive to a proactive security stance. IPS usually sits behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. IPS is placed inline (as shown in the above image) on the network i.e. in the direct communication path between source and destination, actively analyzing and taking automated actions on all traffic flows that enter the network. Unlike IDS which only detects the intrusion, IPS not only detects the Intrusion but also take actions on that like Sending an alarm to the administrator, Dropping the malicious packets, blocking traffic from the source address, Resetting the connection etc.

Intrusion Detection System **Intrusion Prevention System**

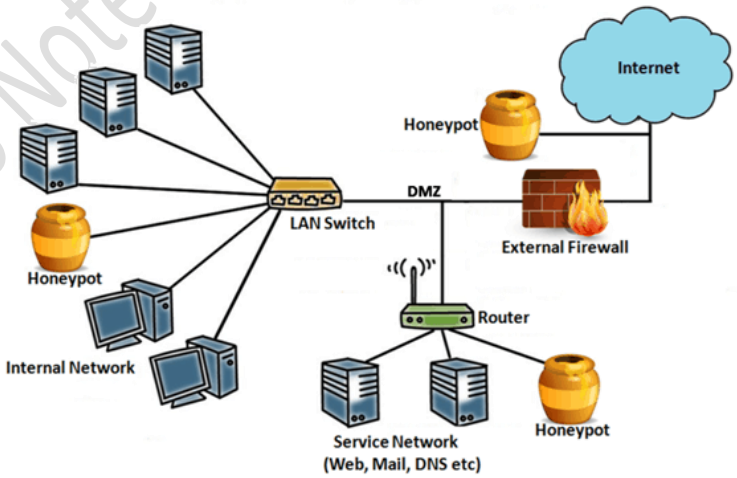


Firewall vs IDS vs IPS



Honey pots

A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate



In the real world we have seen these operations as police stings, where an undercover agent poses as a buyer of some illegal item, meets with the criminal, and with backup arrests them when they purchase of the illegal good. In cybersecurity, the same activities can occur, although the ability to arrest perpetrators is greatly diminished. In cybersecurity, honeypots are most often used to detect attacks by sophisticated hackers who may not know or recognize the targeted system is a setup. In other cases, honeypots are used to deflect attacks from legitimate targets. Honeypots are always used to gain valuable information about how cyber-criminals are operating, whom and how they are trying to attack systems.

Based on how they are built, there are three different kinds of honeypots:

Low-interaction honeypot: This type of honeypots is very easy to construct but it might look "phony" to a hacker. It runs a narrow set of services that exemplify the most prevalent attack vectors.

High-interaction honeypot: This type of honeypots employs virtual machines to ensure that potentially compromised systems are isolated.

Pure honeypot: This kind of honeypots is very time consuming and difficult to both build and manage but they are very authentic targets.

There are two primary types of honeypot designs:

Production honeypots—serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS). They deflect criminal attention from the real system while analyzing malicious activity to help mitigate vulnerabilities.

Research honeypots—used for educational purposes and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

References

1. https://www.cloudflare.com/learning/ssl/how-does-ssl-work/
2. https://blog.stackpath.com/ssl/
3. https://www.geeksforgeeks.org/ip-security-ipsec/
4. https://www.geeksforgeeks.org/ipsec-architecture/
5. https://www.javatpoint.com/computer-network-pgp
6. https://www.groovypost.com/news/apple-glass-revolutionary-or-evolutionary/
7. https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/
8. https://www.compuquip.com/blog/types-firewall-architectures
9. https://www.logsign.com/blog/what-is-a-honeypot-in-cybersecurity/
10. https://cyberhoot.com/cybrary/honeypot/