UNIT-6

Syllabus: IP Security & Intrusion Detection Systems

IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating
Security Payload, Combining Security Associations and Key Management. Intrusion detection: Overview, Approaches for IDS/IPS, Signature based IDS, Host based IDS/IPS.

6.1 IP SECURITY OVERVIEW:

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and it includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit.

IPSEC SECURITY FEATURES:

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- Authentication: Verifies that the packet received is actually from the claimed sender.
- Integrity: Ensures that the contents of the packet did not change in transit.
- Confidentiality: Conceals the message content through encryption.

IPSEC ELEMENTS:

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP):** Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH):** Provides authentication and integrity.
- **Internet Key Exchange (IKE):** Provides key management and Security Association (SA) management.

APPLICATIONS OF IPSEC:

IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following:

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- **Establishing extranet and intranet connectivity with partners**: IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- **Enhancing electronic commerce security:** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

BENEFITS OF IPSEC:

- IPSec provides strong security within and across the LANs.

- Firewall uses IPSec to restrict all those incoming packets which are not using IP. Since firewall is the only way to enter into an organization, restricted packets cannot enter.
- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications.
- There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper layer software, including applications, is not affected.
- IPSec can be transparent to end users.
- IPSec can provide security for individual users if needed.

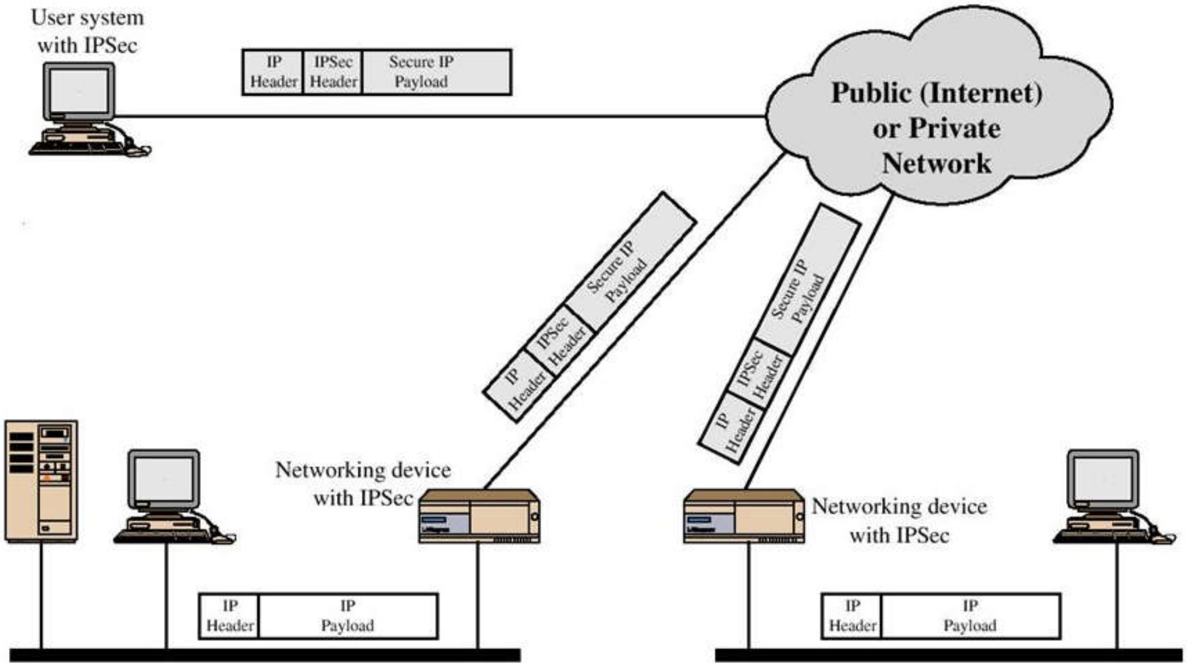


Figure. An IP Security Scenario

6.2 IP SECURITY ARCHITECTURE:

Mainly the IPSec is constituted by three major components.

- IPSec Documents
- IPSec Services
- Security Associations(SA)

IPSec Documents:

The IPSec specification consists of numerous documents. The most important of these, issued in November of 1998, are RFCs 2401, 2402, 2406, and 2408:

υ RFC 2401: An overview of a security architecture

υ RFC 2402: Description of a packet authentication extension to IPv4 and IPv6

υ RFC 2406: Description of a packet encryption extension to IPv4 and IPv6

υ RFC 2408: Specification of key management capabilities

The header for authentication is known as the Authentication header (AH); that for encryption is known as the **Encapsulating Security Payload (ESP)** header. The documents are divided into seven groups, as depicted in Figure.

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology.
- **Encapsulating Security Payload (ESP):** Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.

- **Authentication Header (AH):** Covers the packet format and general issues related to the use of AH for packet authentication.
- **Encryption Algorithm:** A set of documents that describe how various encryption algorithms are used for ESP.
- **Authentication Algorithm:** A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.
- **Key Management:** Documents that describe key management schemes.
- **Domain of Interpretation (DOI):** Contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

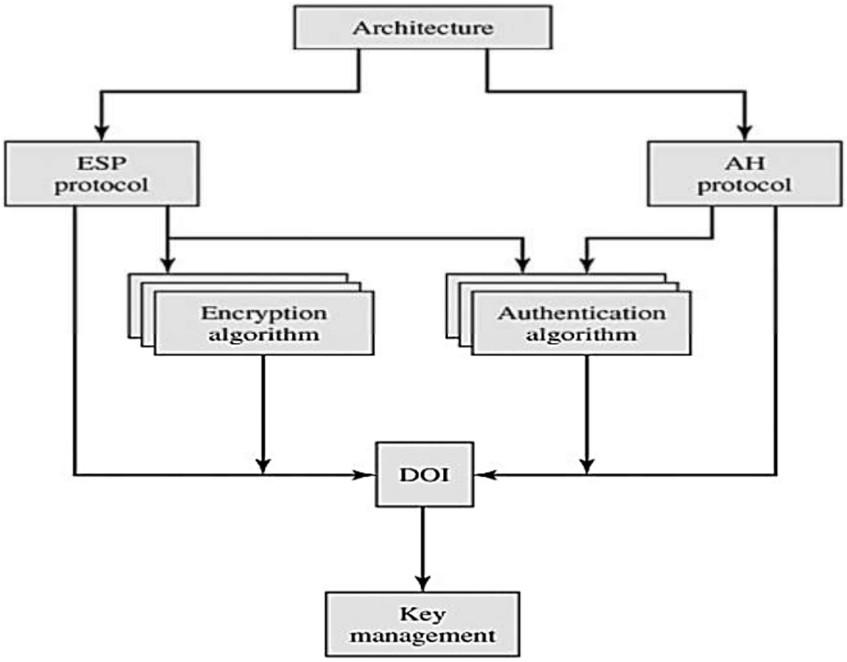


Figure. IPSec Document Overview

IPSec Services:

IPSec provides security services at the IP layer by selecting required security protocols, algorithms and cryptographic keys as per the services requested.

Two protocols are used to provide security:

♣ An authentication protocol designated by the header of the protocol, **Authentication Header (AH)**

♣ A combined encryption/authentication protocol designated by the format of the packet for that protocol, **Encapsulating Security Payload (ESP).**

The services are

υ Access control

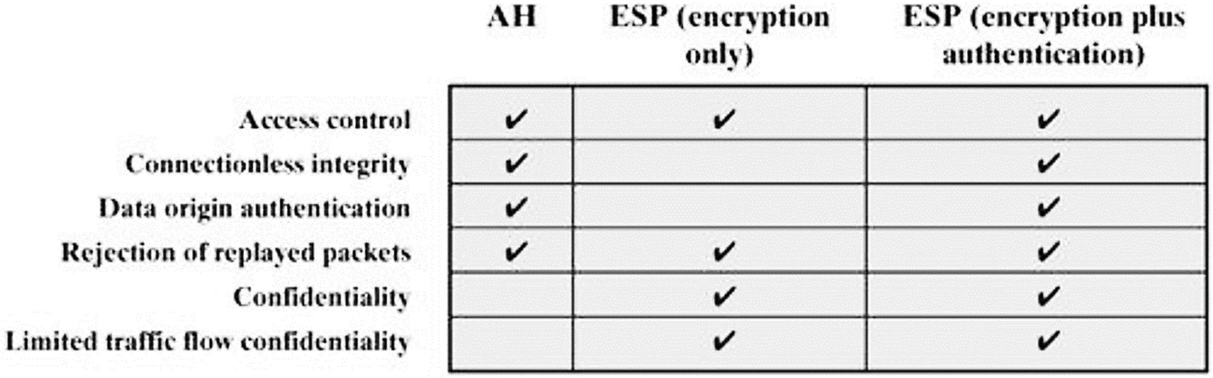
υ Connectionless integrity

υ Data origin authentication

υ Rejection of replayed packets

υ Confidentiality

υ Limited traffic flow confidentiality



	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

Security Associations:

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both.

A security association is uniquely identified by three parameters:

- **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. SPI is located in AH and ESP headers. SPI enables the receiving system under which the packet is to process.
- **IP Destination Address:** It is the end point address of SA which can be end user system or a network system.
- **Security Protocol Identifier:** security protocol identifier indicates whether the associations is an AH or ESP.

SA Parameters:

The implementation of IPSec contain SA database which identifies the parameters related to SA.

- **Sequence Number Counter**: A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow**: A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA.
- **Anti-Replay Window**: Used to determine whether an inbound AH or ESP packet is a replay
- **AH Information**: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.
- **ESP Information**: Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).
- **Lifetime of This Security Association**: A time interval or byte count after which an SA must be replaced with a new SA or terminated.
- **IPSec Protocol Mode:** This parameter represents the type of mode used for IPSec implementation. The mode may be a Tunnel or transport.
- **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted).

SA Selectors:

- IPSec provides flexibility in providing services to the users according to their needs. For this purpose, SA's are used. Different combinations of SA's can give different user configurations. IPSec is also capable of differentiating traffic i.e., which traffic is allowed to pass and which traffic should be forwarded the IPSec protection. The property of IPSec requires the traffic to be associated with a security association. To associate a particular SA to IP traffic IPSec maintains a database called Security Policy Database (SPD).
- SPD is table entries which maps a set of IP traffic to a single or more SAs.
- Selectors are basically used to define policy that specifies which packet should be forwarded and which packet should be rejected to filter outgoing traffic.

A sequence of steps is performed on the outgoing traffic,

- Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
- Determine the SA if any for this packet and its associated SPI. **Security Parameter Index (SPI**) is one of the fields of IPSec header which is a unique identifier to identify a security association.
- Do the required IPSec processing (i.e., AH or ESP processing).

The following selectors determine an SPD entry:

- **Destination IP Address:** This may be a single IP address, an enumerated list or range of addresses.
- **Source IP Address:** This may be a single IP address, an enumerated list or range of addresses.
- **UserID:** A user identifier from the operating system. This is not a field in the IP or upper-layer headers but is available if IPSec is running on the same operating system as the user.
- **Data Sensitivity Level:** Used for systems providing information flow security (e.g., Secret or Unclassified).
- **Transport Layer Protocol:** Obtained from the IPv4 Protocol or IPv6 Next Header field. This may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers.
- **Source and Destination Ports:** These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port.

Transport and Tunnel Modes:

- Both AH and ESP support two modes of use: **transport and tunnel mode**.
- The operation of these two modes is best understood in the context of a descri ption of AH and ESP.

Transport Mode:

Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. Transport mode is used for end-to-end communication between two hosts. ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel Mode:

Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new "outer" IP packet with a new outer IP header. The entire original, or inner, packet travels through a "tunnel" from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security.

Tunnel mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPSec. ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header. AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

6.3 AUTHENTICATION HEADER(AH):

The Authentication Header provides support for data integrity and authentication of IP packets. Data integrity service insures that data inside IP packets is not altered during the transit. The authentication feature enables an end system to authenticate the user or application and filter traffic accordingly. It also prevents the **address spoofing attacks** (A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP **address** indicating that the message is coming from a trusted host).Authentication is based on the use of a message authentication code (MAC)i.e.; two communication parties must share a secret key.

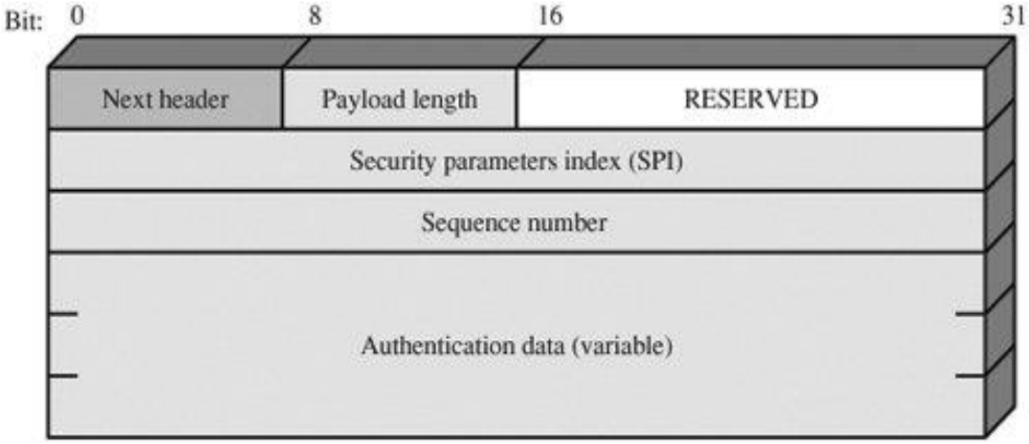

Bit: 0
8
16
31
Next header
Payload length
RESERVED
Security parameters index (SPI)
Sequence number
Authentication data (variable)

Figure. IPSec Authentication Header

The Authentication Header consists of the following fields

1. **Next Header (8 bits):** Identifies the type of header that immediately following the AH.
2. **Payload Length:** Length of Authentication Header in 32-bit words.
3. **Reserved (16 bits):** For future use.
4. **Security Parameters Index (32 bits):** Identifies a security association.
5. **Sequence Number (32 bits):** A monotonically increasing counter value.
6. **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value (ICV), or MAC, for this packet.

Anti-Replay Service:

A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence. The **Sequence Number** field is designed to stop such attacks.

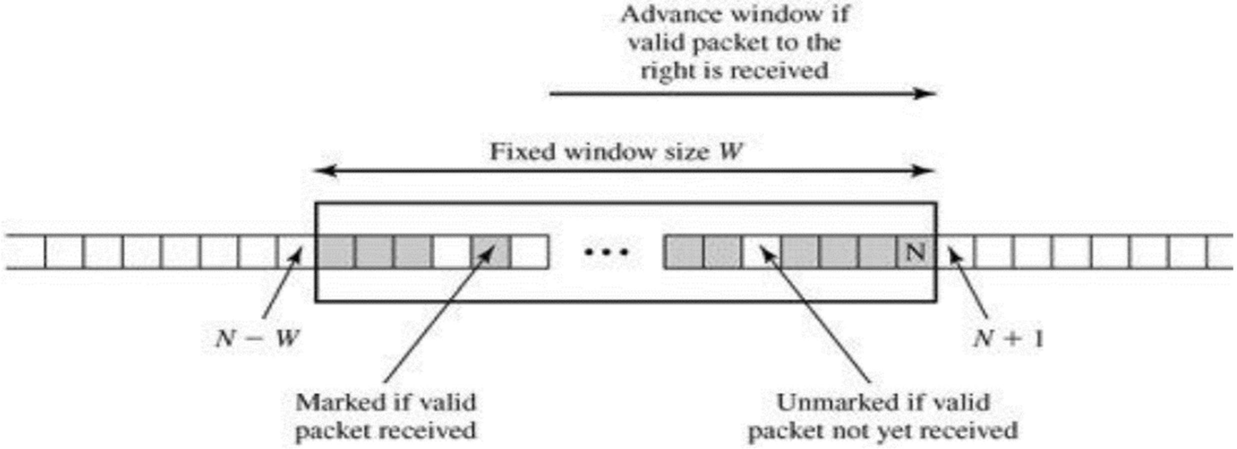

Advance window if valid packet to the right is received
Fixed window size W
N
N − W
N + 1
Marked if valid packet received
Unmarked if valid packet not yet received

Figure. Antireplay Mechanism

When a new SA is established, the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field. Thus, the first value to be used is 1. If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 2_{32}-1 back to zero. Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 2_{32}-1 is reached, the sender should terminate this SA and negotiate a new SA with a new key. IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered. Therefore, the IPSec authentication document dictates that the receiver should implement a window of size W, with a default of W = 64. The right edge of the window represents the highest sequence number, N, so far received for a valid packet. For any packet with a sequence number in the range from N-W+ 1 to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked (Figure).

Inbound processing proceeds as follows when a packet is received:

1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
3. If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

Integrity Check Value:

The Authentication Data field holds a value referred to as the Integrity Check Value. The ICV is a message authentication code or a truncated version of a code produced by a MAC algorithm.

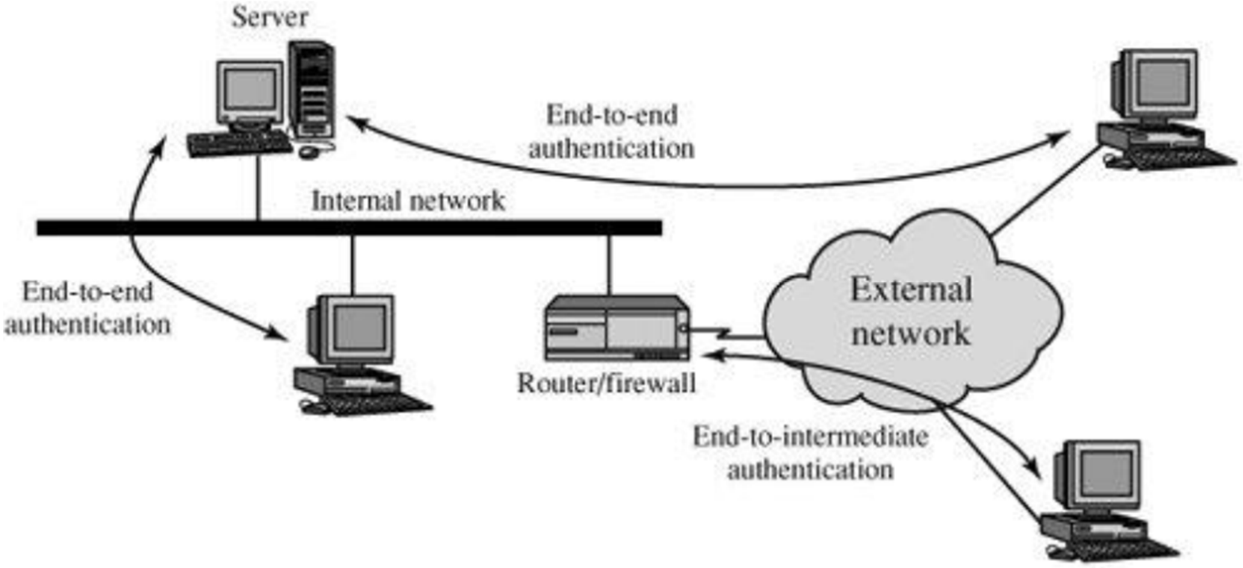

Server
End-to-end authentication
Internal network
End-to-end authentication
Router/firewall
External network
End-to-intermediate authentication

Figure. End-to-End versus End-to-Intermediate Authentication

Transport and Tunnel Modes:

There are two ways in which the IPSec authentication service can be used. In one case, **authentication is provided directly** between a server and client workstations; the workstation can be either on the same network as the server or on an external network. As long as the workstation and the server share a protected secret key, the authentication process is secure. This case uses a **transport mode SA**. In the other case, a **remote workstation authenticates itself to the corporate firewall**, either for access to the entire internal network or because the requested server does not support the authentication feature. This case uses a **tunnel mode SA**.

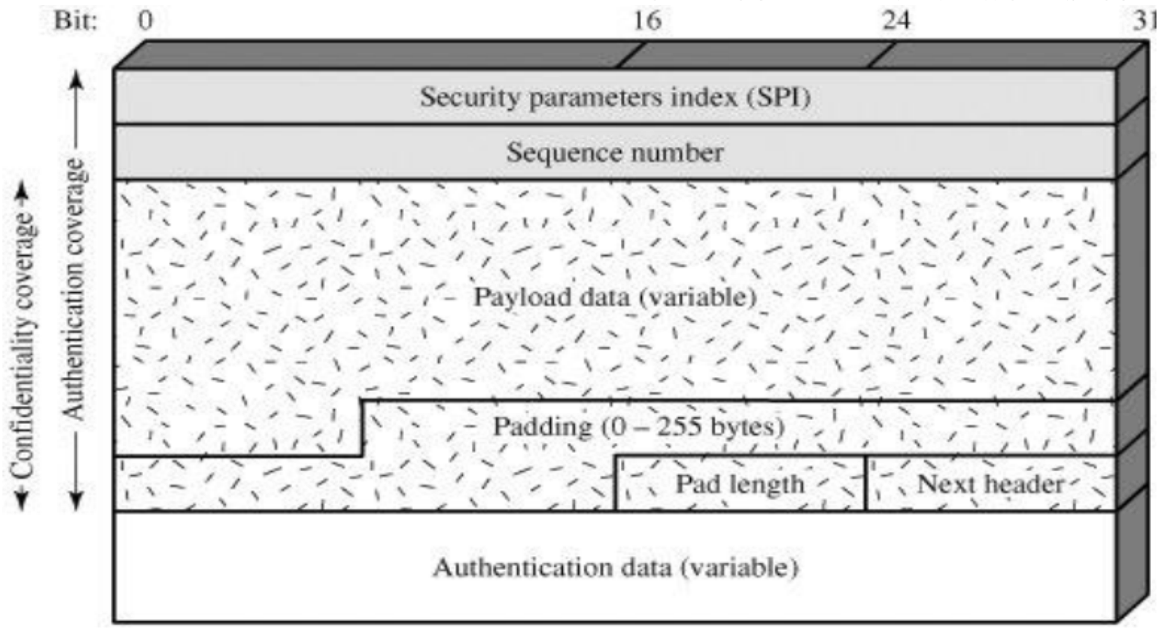
6.4. Encapsulating Security Payload(ESP):

The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide an authentication service.

ESP Format:

It contains the following fields:

1. **Security Parameters Index (32 bits):** Identifies a security association.
2. **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an antireplay function, as discussed for AH.
3. **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. **Padding (0-255 bytes):** The purpose of this field is discussed later.
5. **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
6. **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that.
7. **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field.



Encryption and Authentication Algorithms:

The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP. Various algorithms used for encryption are: Three-key triple DES, RC5, IDEA, Three-key triple IDEA, CAST, Blowfish

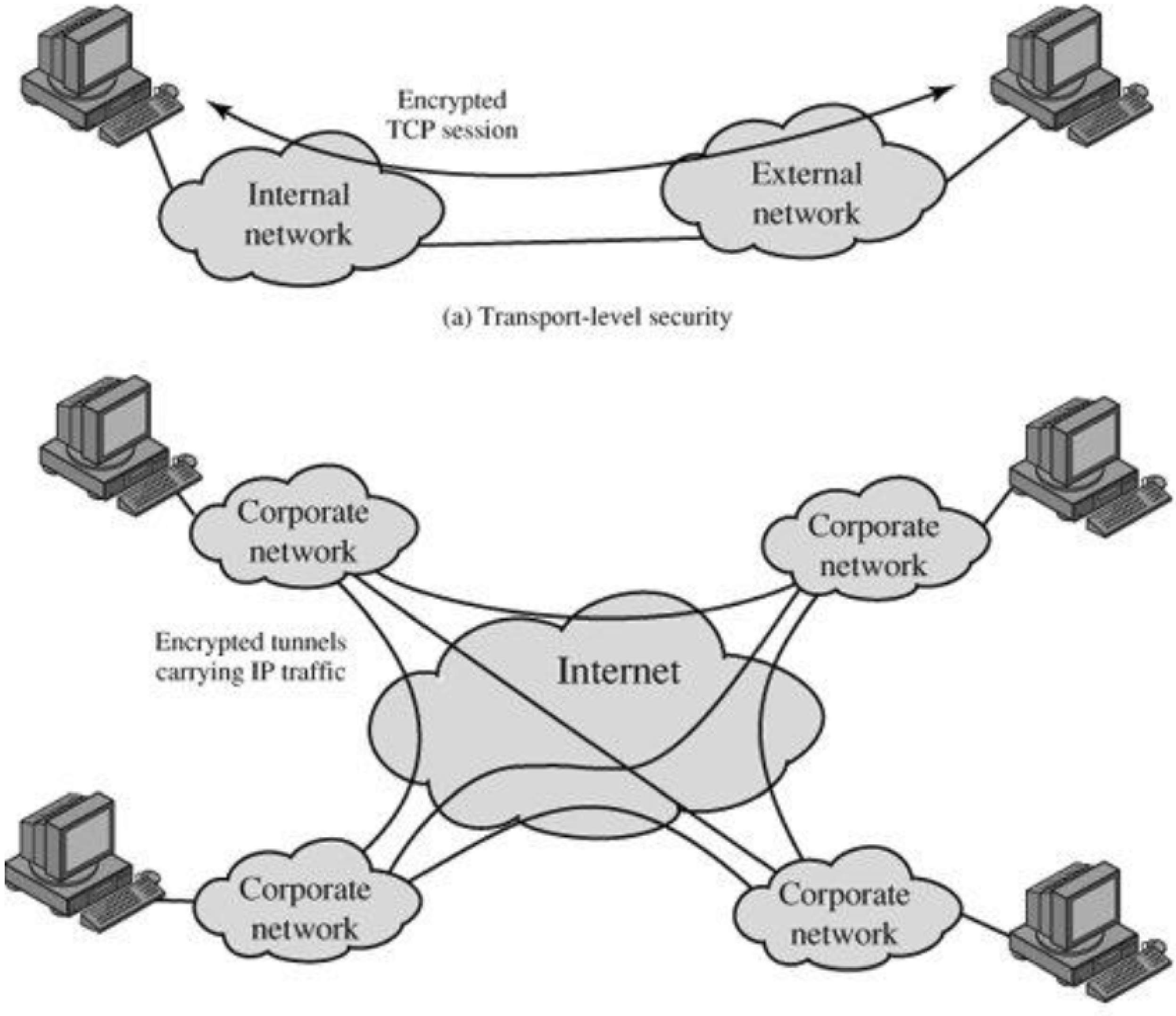
Padding:

The Padding field serves several purposes:

1. If an encryption algorithm requires the plaintext to be a multiple of some number of bytes. The Padding field is used to expand the plaintext to the required length.
2. The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.
3. Additional padding may be added to provide partial traffic flow confidentiality by concealing the actual length of the payload.

Transport and Tunnel Modes:

Figure shows two ways in which the IPSec ESP service can be used. In the upper part of the figure, encryption (and optionally authentication) is provided directly between two hosts. Figure(b) shows how tunnel mode operation can be used to set up a *virtual private network*. In this example, an organization has four private networks interconnected across the Internet. Hosts on the internal networks use the Internet for transport of data but do not interact with other Internet-based hosts. By terminating the tunnels at the security gateway to each internal network, the configuration allows the hosts to avoid implementing the security capability. The former technique is support by a transport mode SA, while the latter technique uses a tunnel mode SA.



(a) Transport-level security

(b) A virtual private network via tunnel mode

6.5 COMBINING SECURITY ASSOCIATIONS:

An individual SA can implement either the AH or ESP protocol but not both. Sometimes a particular traffic flow will call for the services provided by both AH and ESP. Further, a particular traffic flow may require IPSec services between hosts and, for that same flow, separate services between security gateways, such as firewalls. In all of these cases, multiple SAs must be employed for the same traffic flow to achieve the desired IPSec services. The term ***security association bundle*** refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPSec services.

Security associations may be combined into bundles in two ways:

υ **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet, without invoking tunneling.

υ **Iterated tunneling:** Refers to the application of multiple layers of security protocols effected through IP tunneling.

6.6 KEY MANAGEMENT:

The key management portion of IPSec involves the determination and distribution of secret keys. A typical requirement is four keys for communication between two applications: transmit and receive pairs for both AH and ESP.

The IPSec Architecture document mandates support for two types of key management:

- **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems. This is suitable for small, relatively static environments.
- **Automated:** An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system.

The default automated key management protocol for IPSec is referred to as ISAKMP/Oakley and consists of the following elements:

1. **Oakley Key Determination Protocol**
2. **Internet Security Association and Key Management Protocol (ISAKMP)**

Oakley Key Determination Protocol:

Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.

The Diffie-Hellman algorithm has **two** attractive features:

1. Secret keys are created only when needed.
2. The exchange requires no preexisting infrastructure other than an agreement on the global parameters. However, there are a number of weaknesses to Diffie-Hellman, as pointed out in.
3. It does not provide any information about the identities of the parties.
4. It is subject to a man-in-the-middle attack

It is computationally intensive. As a result, it is vulnerable to a clogging attack, in which an opponent requests a high number of keys.

Oakley is designed to retain the advantages of Diffie-Hellman while countering its weaknesses.

Features of Oakley:

The Oakley algorithm is characterized by five important features:

- It employs a mechanism known as cookies to thwart clogging attacks.
- It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange.
- It uses nonces to ensure against replay attacks.
- It enables the exchange of Diffie-Hellman public key values.
- It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

Internet Security Association and Key Management Protocol (ISAKMP):

ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

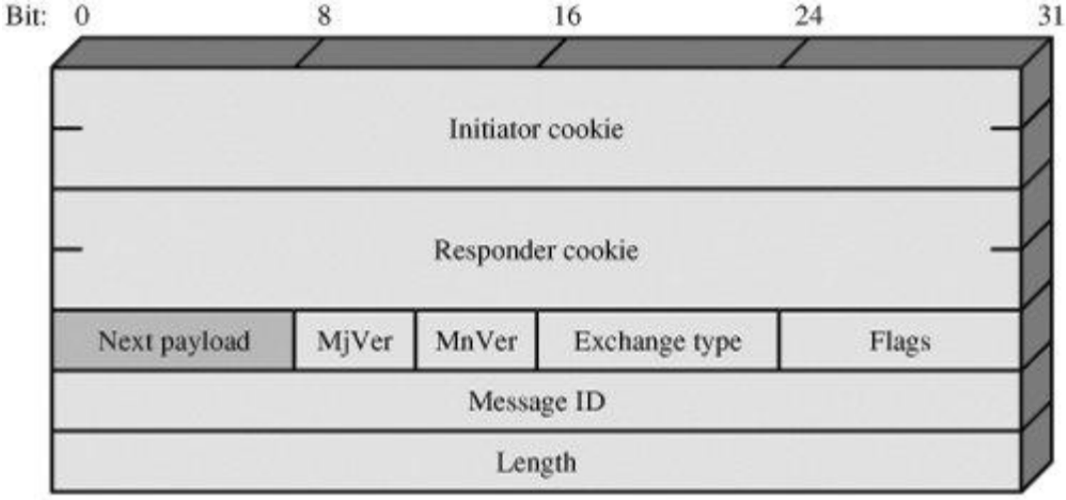
ISAKMP Header Format:

An ISAKMP message consists of an ISAKMP header followed by one or more payloads. All of this is carried in a transport protocol. The specification dictates that implementations must support the use of UDP for the transport protocol.

It consists of the following fields:

1. **Initiator Cookie (64 bits):** Cookie of entity that initiated SA establishment, SA notification, or SA deletion.

2. **Responder Cookie (64 bits):** Cookie of responding entity; null in first message from initiator.
3. **Next Payload (8 bits):** Indicates the type of the first payload in the message
4. **Major Version (4 bits):** Indicates major version of ISAKMP in use.
5. **Minor Version (4 bits):** Indicates minor version in use.
6. **Exchange Type (8 bits):** Indicates the type of exchange.
7. **Flags (8 bits):** Indicates specific options set for this ISAKMP exchange.
8. **Message ID (32 bits):** Unique ID for this message.
9. **Length (32 bits):** Length of total message (header plus all payloads) in octets.



(a) ISAKMP header

6.7. Intrusion Detection/Prevention System:

Intrusion

A set of actions aimed to compromise the security goals, namely Integrity, confidentiality, or availability, of a computing and networking resource. It is act of gaining unauthorized access to a system so as to cause loss.

Intrusion detection

The process of identifying and responding to intrusion activities

Intrusion prevention

Extension of ID with exercises of access control to protect computers from exploitation

Terminology:

- **True Positives**: These are alerts that something is not right when it is actually not right.
- **True negatives**: these are alerts that something is right when it is actually right.
- **False positives**: these are alerts indicating that something is not right with a packet when actually it is right.
- **False Negatives**: these are alerts that something is right when actually it is wrong.

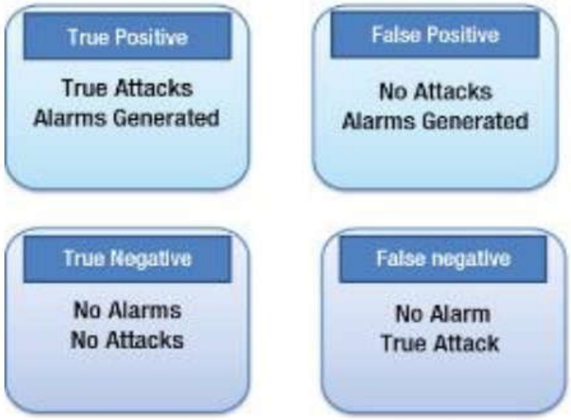
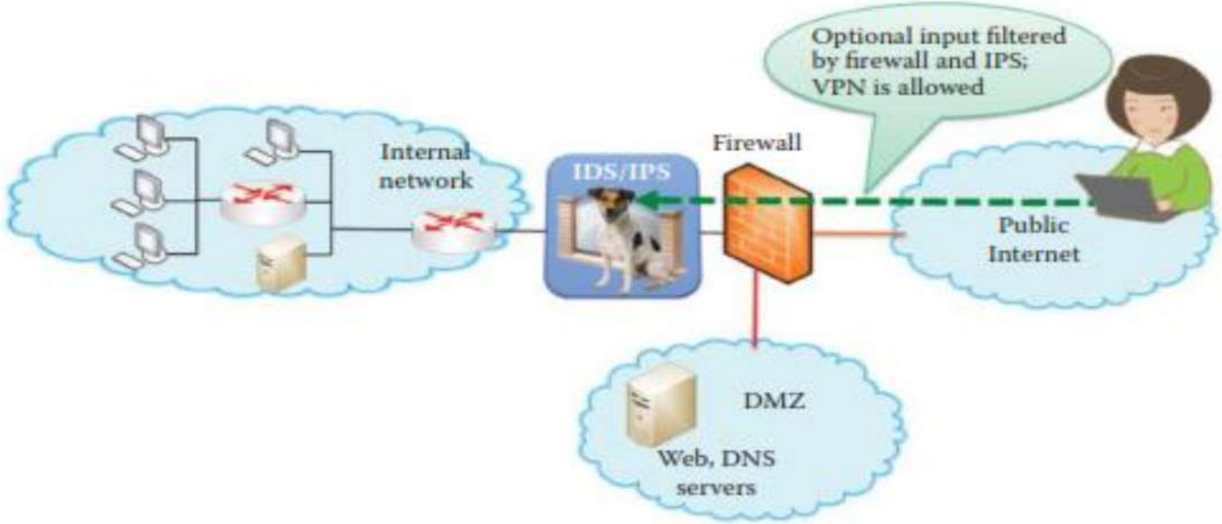


Figure 11-1. Definitions of IDS/IPS Alerts

6.8 OVERVIEW:

An intrusion detection/prevention system (IDS/IPS) is another element in which it employed to provide deep packet inspection at the entrance of important network. Intrusion Detection System/Intrusion Prevention System is positioned behind the firewall, as shown in Figure.



The IDS/IPS provides deep packet inspection for the payload, IDS is based on out-of-band detection of intrusions and their reporting, and IPS is in-band filtering to block intrusions. IDS is performed through a wiretap, and is clearly an out-of-band operation. In contrast, IPS is performed inline. And by preventing intrusions, IPSs eliminate the need for keeping and reading extensive intrusion-incident logs, which contributes to IDSs' considerable CPU, memory, and I/O overhead.

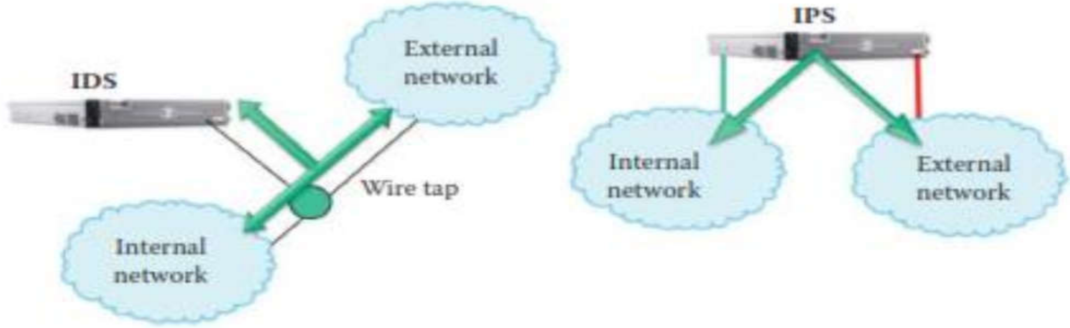


FIGURE 19.2 An illustration of out-of-band IDS vs. in-band IPS.

IDS/IPS BUILDING BLOCKS:

A block diagram that outlines the functions of an IDS/IPS system is shown in Figure. As indicated, the observable activities are preprocessed and forwarded to the detection engine that uses a Signature/Anomaly model. This information is then forwarded to the classification decision engine that uses classification algorithms to provide the alerts or blocking actions.

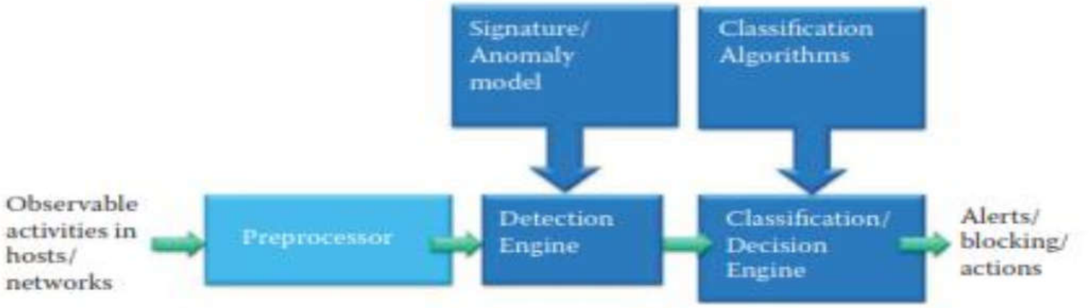


FIGURE 19.3 An IDS/IPS system processes activities and generates alerts and blockings.

HOST-BASED OR NETWORK-BASED IDS/IPS:

IDS/IPS can be either **host-based or network-based**, in which case it is labeled as HIDS/HIPS or NIDS/NIPS, respectively. In the HIDS/HIPS case, the **monitoring and blocking activity is performed on a single host**. HIDS/HIPS has the advantage that it provides better visibility into the behavior of individual applications running on that host. HIDS/HIPS monitoring also includes attacks by genuine users/insiders. These include illegitimate use of root privileges; unauthorized access to resources and data. In the NIDS/NIPS, it is often located behind a router or firewall that provides the guarded entrance to a critical asset. At this location traffic is monitored and packet headers and payloads are examined using the knowledge base in NIDS/NIPS. The advantage of this location is that a single NIDS/NIPS can protect many hosts as well as detect global patterns.

There are **various types of IPS products**.

- **Host-based application** firewalls perform the IPS function independently of the operating system and block the entry of application-level and web based intrusions, much like network firewalls bar entry to unwanted traffic.
- A **network-based IPS** blocks network-level intrusions, such as denial-of-service attacks, and may use anomaly detection to recognize threats based on their behavior.
- Combining network- and host-based IPSs provides the best protection against all types of intrusions.

6.9 THE APPROACHES USED FOR IDS/IPS:

The approaches to **intrusion detection** can generally be classified as either **anomaly/behavior based** or **signature-based**.

- Anomaly-based detectors generate the normal behavior/pattern of the protected system, and deliver an anomaly alarm if the observed behavior at an instant does not conform to expected behavior.
- Anomaly-based IDS/IPS are more likely to generating false positives due to the dynamic nature of networks, applications and exploits.
- According to the type of processing, anomaly detection techniques can be classified into three main categories: **statistical-based, knowledge-based, and machine learning-based**.

STATISTICAL-BASED IDS/IPS:

In the statistical-based IDS/IPS, the behavior of the system is represented from the **captured network traffic activity** and a profile representing its stochastic behavior is created. This profile is based on metrics such as the **traffic rate, the number of packets for each protocol, the rate of connections, the number of different IP addresses**, etc. This method employs the collected profile that relates to the behavior of genuine users and is then used in statistical tests to determine if the behavior under detection is genuine or not. During the anomaly detection process, one corresponding to the currently captured profile is compared with the previously trained statistical profile. As the network events occur, the current profile is determined and an anomaly score estimated by comparison of the two behaviors. The score normally indicates the degree of deviation for a specific event.

Advantages

- First, they do not require prior knowledge about the normal activity of the target system; instead, they have the ability to learn the expected behavior of the system from observations.
- Second, statistical methods can provide accurate notification of malicious activities occurring over long periods of time.

Drawbacks

- Setting the values of the thresholds, parameters/metrics that is a difficult task, especially because the balance between false positives and false negatives is affected.
- Not all behaviors can be modeled by using stochastic methods.

KNOWLEDGE-/EXPERT-BASED IDS/IPS:

Knowledge-based IDS/IPS captures the **normal behavior from available information, including expert knowledge, protocol specifications, network traffic instances,** etc. The normal behavior is represented as a **set of rules**. Attributes and classes are identified from the training data or specifications. Then a set of classification rules, parameters or procedures are generated. The rules are used for detecting anomaly behaviors. Specification-based anomaly methods require that the model is manually constructed by human experts in terms of a set of rules (the specifications) that describing the system behavior. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as other anomaly detection methods in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. The most significant advantages of knowledge/expert-based detection are the low false alarm rate and the fact that they may detect zero-day and mutated attacks. The main drawback is that the development of high-quality rules is time-consuming and labor-intensive.

MACHINE LEARNING-BASED IDS/IPS:

Machine learning IDS/IPS schemes are based on the establishment of an explicit or implicit model that allows the patterns analyzed to be categorized. Machine learning is different from statistical-based methods because machine learning discovers the characteristics for building a model of behaviors. As more learning is performed, the model will become more accurate. The discovery and learning process is the advantage of machine learning; however, it requires a significant amount of computational resources.

6.10. SIGNATURE BASED IDS:

This mechanism proceeds against known threats. A signature is a known pattern of a threat, such as:

♣ An e-mail with an attachment containing a malware with an interesting subject.

♣ A “remote login" by an admin user, which is a clear violation of an organization's policy.

Signature-based detection is the simplest form of detection because it just the traffic with the signature database. If a match found then the alert is generated, if a match is not found then the traffic flows without any problem. In signature-based detection, detection is based on comparing the traffic with the known signatures for possible attacks. They can only detect known threats and hence, are not efficient in detecting unknown threats. To detect an attack, the signature matching has to be precise, otherwise, even if the attack has a small variation from the known threat signature, then the system will not detect. Hence, it is very easy for the attackers to compromise and breach into the trusted network.

Signature database needs to be updated constantly, almost on a daily basis from the anti –virus labs. If the signature is not up to date, chances are that the IDS systems will fail to detect some of the intrusion attacks. The other disadvantage is that they have very little information about previous requests when processing the current ones.

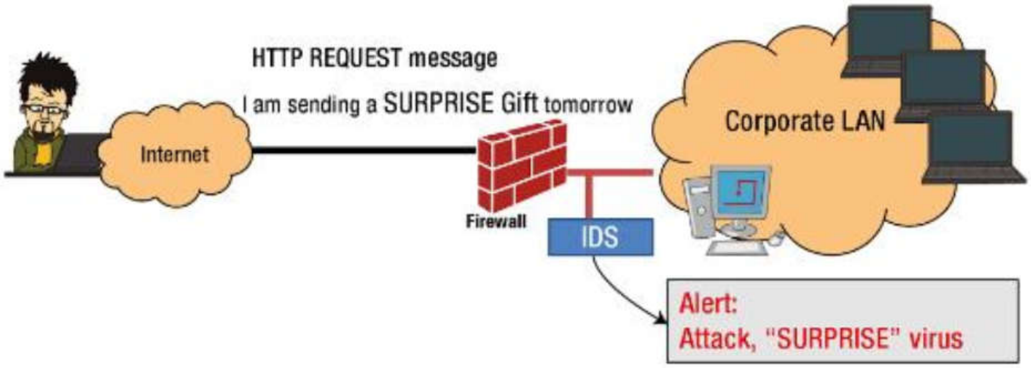


Figure: Signature based detection

Signature based detection can offer very specific detection threats by comparing network traffic with the threat signature database. The detection can be enhanced if the network traffic inside the network can be made to learn specific patterns, thus reducing false positives. Signature detection engines tend to degrade in performance over a period of time as more and more signatures are added to the database. It takes more time for engine to do a pattern search as the signature database is always growing as more and more definitions are added to it. Hence a robust platform is needed for signature detection considering this growth.

6.11. HOST-BASED IDS:

Host-based Intrusion Detection System refers to the detection intrusion Single system. This is normally software-based deployment where an agent, as shown in Figure, is installed on the local host that monitors and reports the application activity. HIDS monitors the access to the system and its application and sends alerts for any unusual activities. It **constantly monitors event logs, system logs, application logs**, user policy enforcement, rootkit detection, file integrity and other intrusions to the system. **It constantly monitors these logs and creates a baseline.** If any log entries appear, HIDS Checks the data against the baseline and if entries are found outside of this baseline. HIDS triggers an alert, if any unauthorized activity is detected, HIDS can alert the user or block the activity or perform any other decision based the policy that is configured on the system.

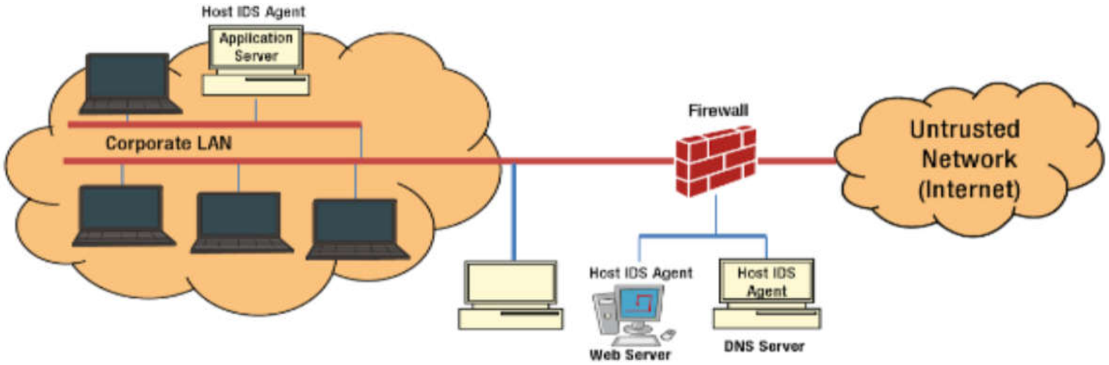


Figure: Host – Based Intrusion Detection System

Most of the HIDS products have ability to prevent attacks also. However, it is initially deployed in the monitor mode and then there is of the System activity, a baseline is and then HIDS is deployed prevention mode. The functionality HIDS depends the logs generated by the System and the fact that the intruders leave evidence of their activities. Generally, hackers get access to the System and install malicious tools so that future access becomes easier. If these tools change the operating system configurations, or entries of some windows registry, it is logged in the systems/event log, thus triggering an alert by the HIDS system. HIDS is generally installed on servers, or end point devices to protect the system from intrusion. The function of HIDS solely depends on the audit trails generated by the system, If hackers manage to turn off these logs, if you have a HIDS agent running. it may not trigger any alerts. This is the biggest disadvantage of HIIDS.

Advantages of HIDS are:

- System level protection. Protects from attacks directed to the system
- Any unauthorized activity on the system (configuration changes, file changes, registry changes, etc.) are detected and an alert is generated for further action

Disadvantages

- HIDS functionality works only if the Systems generate logs and match against the pre – defined policies. If for some reason, Systems do not generate logs, HIDS may not function properly.
- If hackers bring down the HIDS server, then HIDS is of no use. This is true for any vulnerability Software.

HOST-BASED IDS/IPS:

Many host security products contain integrated host-based IDS/IPS systems (HIDS/HIPS), antimalware and a firewall. These HIDS/HIPS systems have both advantages and weaknesses. They are capable of protecting mobile hosts from an attack when outside the protected internal network, and they can defend local attacks, such as malware in removable devices. They also protect against attacks from network and encrypted attacks in which the encrypted data stream terminates at the host being protected. They have the capability of detecting anomalies of host software execution, e.g., system call patterns. HIDS/HIPS builds a dynamic database of system objects that can be monitored.

On the negative side, if an attacker takes over a host, the HIDS/HIPS and NAC (Network Access Control) agent software can be compromised and disabled, and the audit logs are modified to hide the malware. In addition, HIDS/HIPS has only a local view of the attack, and host-based anomaly detection has a high false alarm rate.