CRYPTOGRAPHY AND NETWORK SECURITY

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.

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. IPSecprovides datasecurity at the IP packet level. A packet is a data bundle that is organized fortransmission across a network, and it includes aheaderand payload (the data in the packet). IPSecemerged 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 datawhilein 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 messagecontent through encryption.

IPSEC ELEMENTS:

IPSeccontains 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:

IPSecprovides thecapability to securecommunications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following:

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

www.Jntufastupdates.com

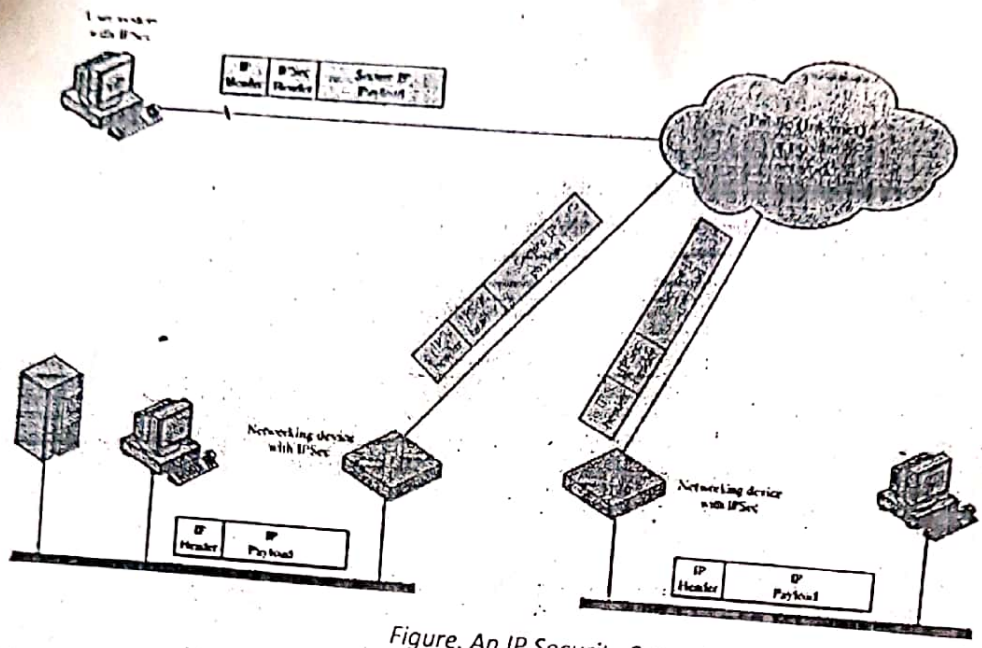


Figure. An IP Security Scenario

BENEFITS OF IPSEC:

- IPSecprovides 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 enterinto an organization, restricted packets cannot enter.
- IPSecis 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 thefirewall orrouter.Even if IPSecis implemented in end systems,upper-layersoftware, including applications, is not affected.
- IPSeccan be transparent to end users.
- IPSeccan provide security for Individualusers if needed.

IP SECURITY ARCHITECTURE:

Mainly the IPSecis constituted by three majorcomponents.

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

IPSec Documents:

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

- RFC 2401: An overview of asecurity architecture
- RFC 2402: Description of apacket authentication extension to IPv4 and IPv6
- RFC 2406: Description of apacket encryption extension to IPv4 and IPv6
- 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

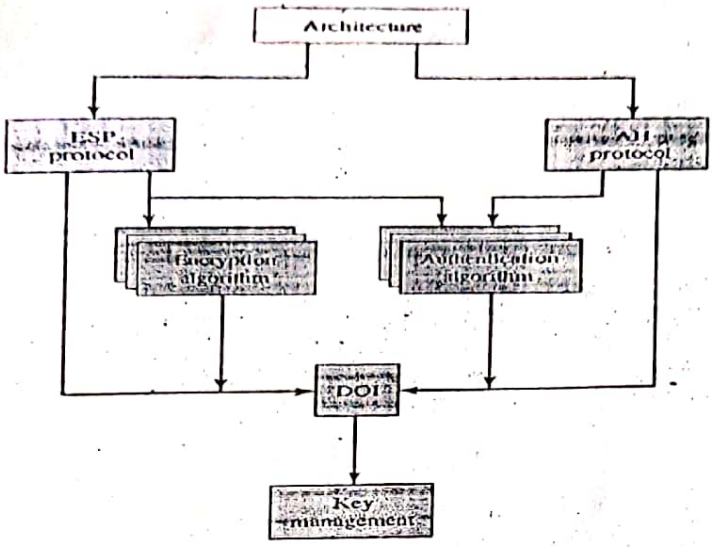


Figure. IPSec DocumentOverview

- **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms definingIPSectechnology.
- **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 forpacketauthentication.
- **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 forthe 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. Theseinclude identifiers forapprovedencryptionand authentication algorithms, as well as operational parameters such as key lifetime.

IPSec Services:

IPSecprovides security services at the IP layerby selecting requiredsecurityprotocols, algorithms and cryptographickeys as per the services requested.

Two protocols are used to provide security:

- an authentication protocoldesignated by the headerof the protocol, **Authentication Header (AH)**
- and a combined encryption/authentication protocol designated by the format of the packet for that protocol, **Encapsulating Security Payload (ESP).**

www.Jntufastupdates.com

The services are

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality
- Limited trafficflow 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 trafficcarried on it. If a peerrelationship is needed, fortwo-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 underwhich the packet is toprocess.
- **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 whetherthe associationsis an AH or ESP.

SA Parameters:

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

- **Sequence Number Counter:** A 32-bit value usedto generatethe Sequence Numberfield 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 whetheran inbound AHor ESP packet is a replay
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used withAH.
- **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 orbyte count afterwhich an SA must be replaced with a new SA or terminated.

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 oneorboth ends of an SA are asecurity gateway, such as afirewall or routerthat implements IPSec. ESP in tunnel modeencrypts 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.

AUTHENTICATION HEADER(AH):

The Authentication Headerprovides support fordata integrity and authentication of IP packets. Data integrity service insures that datainside IP packets is not altered during the transit. The authentication feature enables an end system to authenticate the useror application and filter trafficaccordingly. 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 asecret key.

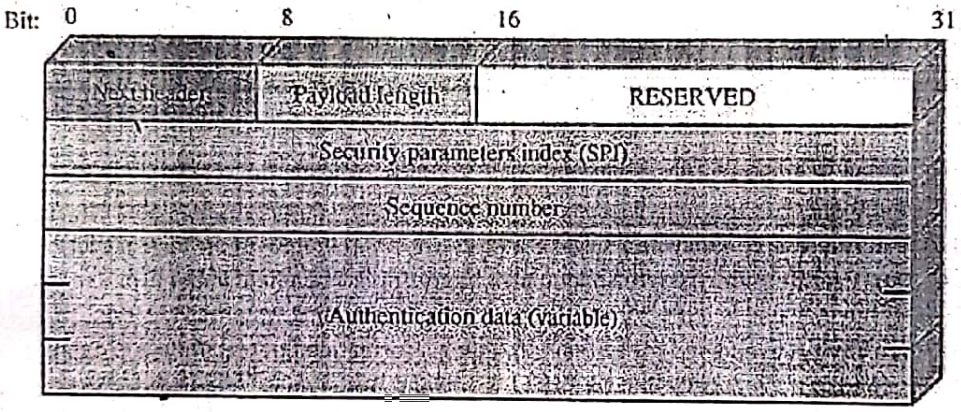


Figure. IPSec Authentication Header

The Authentication Headerconsists of the following fields

1. **Next Header (8 bits):** Identifies the type of headerthat immediately following the AH.
2. **Payload Length:** Length of Authentication Headerin 32-bit words.
3. **Reserved (16 bits):** For future use.
4. **Security Parameters Index (32 bits):** Identifies asecurity association.
5. **Sequence Number(32 bits):** A monotonically increasing countervalue.
6. **Authentication Data (variable):** A variable-length field (must be an integral numberof 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 intendeddestination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some otherundesired consequence. The **Sequence Number** fieldis designed to stop such attacks.

www.Jntufastupdates.com

- **IPSec Protocol Mode:** This parameter represents the type of mode used for IPSec implementation. The mode may be a Tunnel ortransport.
- **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 userconfigurations. IPSec is also capable of differentiating traffic i.e., which traffic is allowed to pass and which trafficshould be forwarded the IPSecprotection. The property of IPSecrequires 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 aset of IP trafficto a single ormore 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 theappropriatefields in thepacket (theselectorfields) against the SPD to find a matching SPDentry, 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 IPSecprocessing (i.e., AHor ESP processing).

The following selectors determinean SPDentry:

- **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 orrange of addresses.
- **UserID:** A useridentifierfrom the operating system. This is not a field in the IP or upper-layer headers but is available if IPSecis 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 Headerfield.This may be an individualprotocol number, a list of protocol numbers, orarange of protocol numbers.
- **Source and Destination Ports:** These may be individual TCP or UDP port values, an enumerated list of ports, ora 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 optionallyauthenticates 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:

www.Jntufastupdates.com

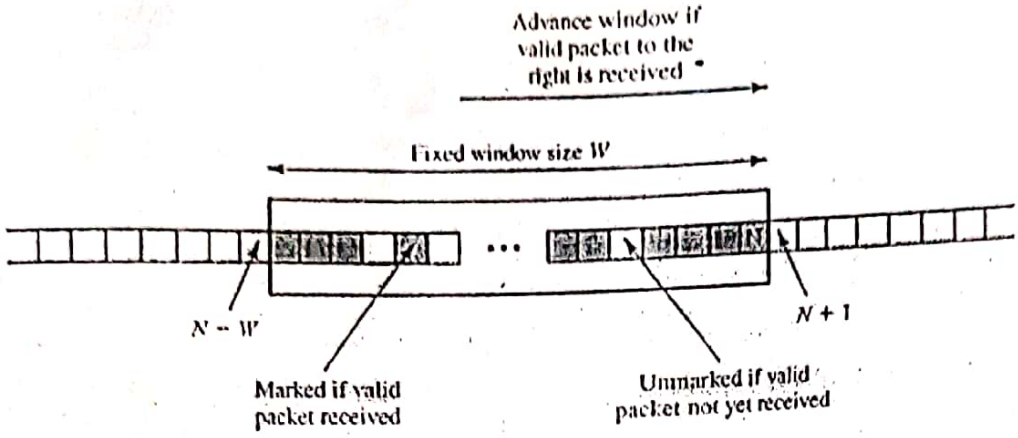


Figure. Antireplay Mechanism

When a new SA is established, the senderinitializes asequence numbercounterto 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 numberin the range from N-W+ 1 to N that has been correctly received (i.e., properly authenticated), the corresponding slot in the windowis marked (Figure).

Inbound processing proceeds as follows when apacket is received:

1. If the received packet falls within the windowand 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 packetis 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 ora truncated version of a code produced by a MAC algorithm.

Transport and Tunnel Modes:

There are two ways in which the IPSecauthenticationservice 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 serveroron an externalnetwork.As long as the workstation and the servershare a protected secret key, the authentication process is secure. This case uses a transport mode SA. In the othercase, a remote workstation authenticates itself to the corporate firewall, eitherforaccess to the entire internal network or because the requested server does not support the authentication feature. This case uses a tunnel mode SA.

www.Jntufastupdates.com

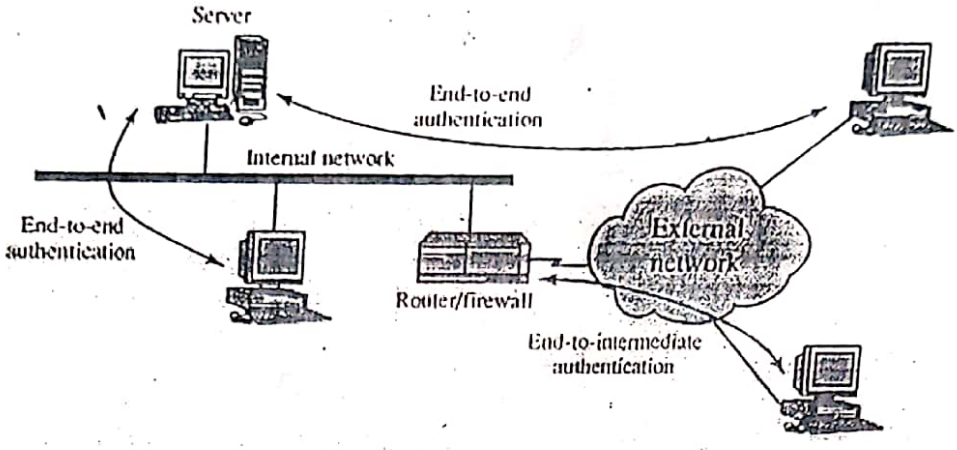


Figure. End-to-End versus End-to-Intermediate Authentication

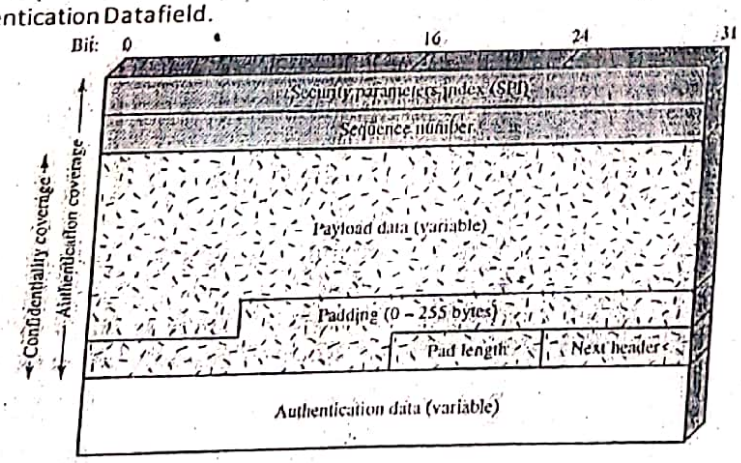
Encapsulating Security Payload(ESP):

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.
   Sequence Number(32 bits): A monotonically increasing countervalue; this provides an anti-replay function, as discussed for AH.
2. **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
3. **Padding (0-255 bytes):** The purpose of this field is discussed later.
4. **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
5. **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that.
6. **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 Headerfields are encrypted by the ESP.

Various algorithms used for encryption are: Three-key triple DES, RC5, IDEA, Three-key triple IDEA, CAST, Blowfish

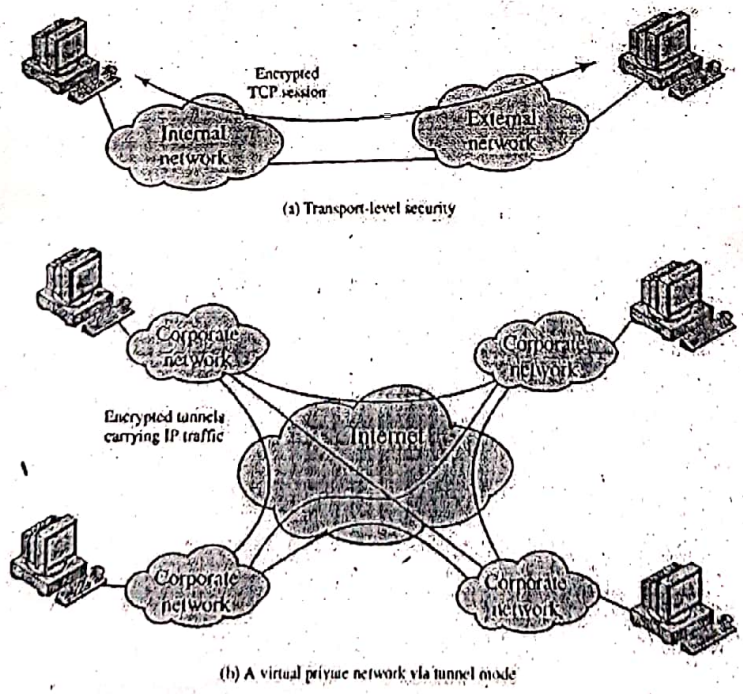
Padding:

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 allgned within a 32-bit word. Equivalently, the ciphertext must be an integermultiple of 32 bits. The Padding field is used to assure this alignment.
3. Additional padding may be added to provide partial trafficflow 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 thesecurity capability.The formertechniqueis support by atransport mode SA, while the lattertechnique uses atunnel mode SA.



(a) Transport-level security

(b) A virtual private network via tunnel mode

www.Jntufastupdates.com

COMBINING SECURITY ASSOCIATIONS:

An individual SA can implement either the AH or ESP protocol but not both. Sometimes a particular trafficflow willcall forthe services providedby both AHand ESP. Further, aparticulartrafficflow 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 forthe same traffic flow to achieve the desired IPSecservices. The term ***securityassociation bundle*** refers to a sequence of SAs through which trafficmust be processed to provide adesired set of IPSecservices.

Security associations may be combined into bundles in two ways:

- **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet, without invoking tunneling.
- **Iterated tunneling:** Refers to the application of multiple layers of security protocols effected through IP tunneling.

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 fortwo types of key management:

- **Manual:** A system administratormanually 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 IPSecis 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 akey exchangeprotocolbasedon the Diffie-Hellman algorithmbut providingadded security. Oakley is generic in that it does not dictate specificformats.

The Diffie-Hellman algorithm has two attractive features:

1. Secret keys are created only when needed.
2. The exchange requires no preexisting infrastructure otherthan an agreement on the global parameters.

However, there are anumberof 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

www.Jntufastupdates.com

It is computationally intensive. As aresult, it is vulnerable to a clogging attack, in which an opponent requests ahigh numberof keys.

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

Features of Oakley:

The Oakley algorithm is characterized by five important features:

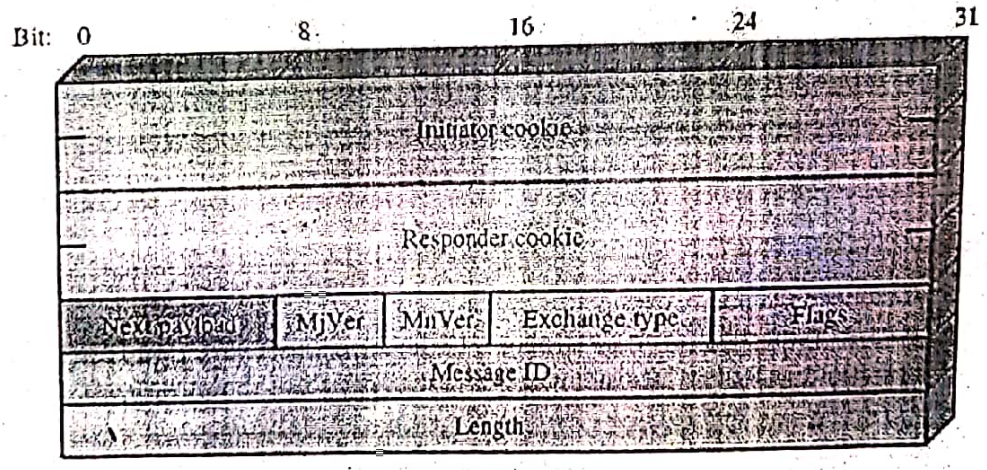
- It employs amechanism known as cookies to thwart clogging attacks.
- It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange.
- It uses nonces to ensure against replay attacks.
- It enables the exchangeof Diffie-Hellman publickey 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, fornegotiation 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.



(a) ISAKMP header

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; nullin 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 majorversion of ISAKMP in use.
5. **Minor Version (4 bits):** Indicates minorversion in use.
6. **Exchange Type (8 bits):** Indicates the type of exchange.
7. **Flags (8 bits):** Indicates specific options set forthis ISAKMP exchange.
8. **Message ID (32 bits):** Unique ID for this message.
9. **Length (32 bits):** Length of total message (headerplus all payloads) in octets.

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 IDwith exercises of access control to protect computers from exploitation

Terminology:

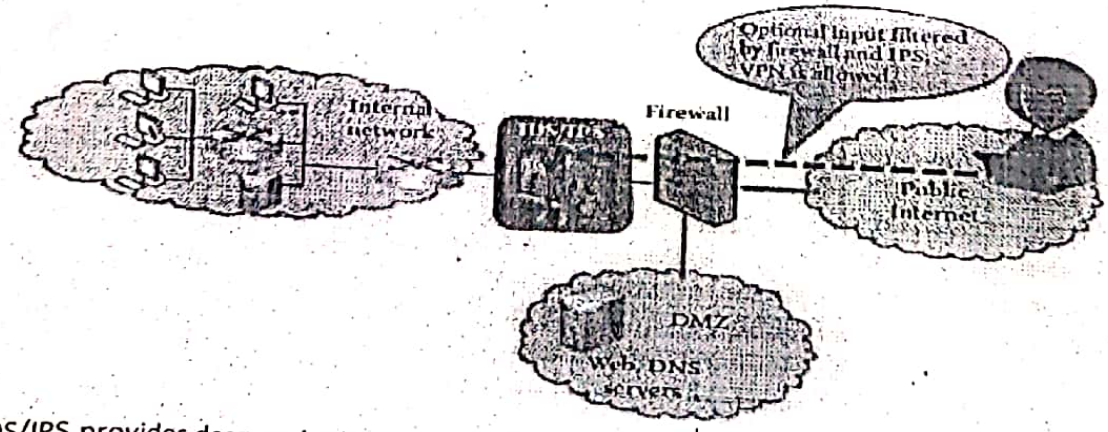
- **True Positives:** These are alerts that something is not right when it is actually not right.
- **True negatives:** these are alerts that something is right when it is actually right.
- **False positives:** these are alerts indicating that something is not right with a packet when actually it is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



Figure 11-1. Definitions of IDS/IPS Alerts

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 packetinspectionforthe payload,IDS is based on out-of-band detection of intrusions and theirreporting, and IPS is in-band filtering to block intrusions. IDS is performedthrough

www.Jntufastupdates.com

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.

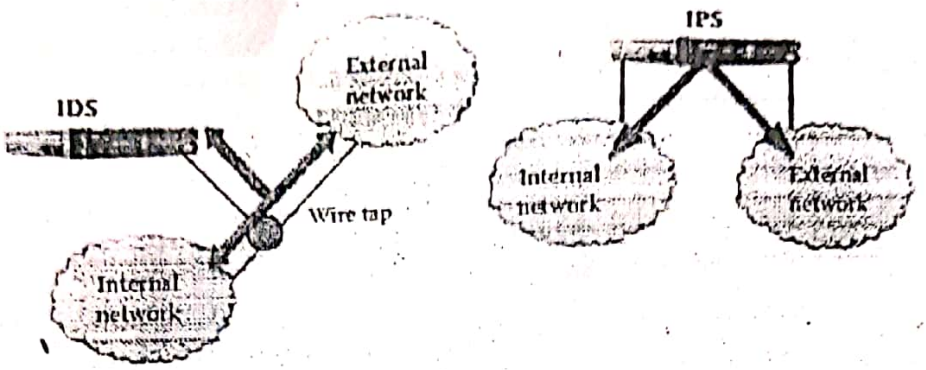


FIGURE 19.2 An illustration of out-of-band IDS vs. in-band IPS.

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 orblocking actions

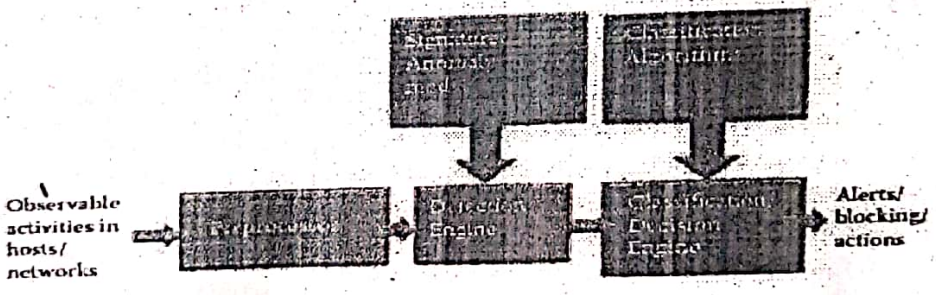


FIGURE 19.3 An IDS/IPS system processes activities and generates alerts and blockings.

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 includeillegitimate 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.

www.Jntufastupdates.com

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 barentry 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 theirbehavior.
- Combining network- and host-based IPSs provides the best protection against all types of intrusions.

THE APPROACHES USED FOR IDS/IPS:

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

- Anomaly-based detectors generatethe normalbehavior/pattern of theprotected system, and deliveran anomalyalarm if the observed behaviorat an instant does not conform to expected behavior.
- Anomaly-based IDS/IPSare more likely to generating false positives dueto the dynamicnature of networks, applications and exploits.
- According to the type of processing, anomaly detection techniques can be classifiedinto three main categories: statistical-based, knowledge-based, and machine learning-based.

STATISTICAL-BASED IDS/IPS:

In the statistical-based IDS/IPS, the behaviorof 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 behaviorof genuine users and is then used in statistical tests to determine if the behaviorunder detection is genuine or not. During theanomalydetection process, onecorresponding 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 degreeof deviation foraspecificevent.

Advantages

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

Drawbacks

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

KNOWLEDGE-/EXPERT-BASED IDS/IPS:

Knowledge-based IDS/IPS capturesthe normal behaviorfromavailable 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

www.Jntufastupdates.com

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-BASEDIDS/IPS:

Machine learning IDS/IPSschemes 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 machinelearning discovers the characteristics forbuilding amodel of behaviors. As more learning is performed, the modelwillbecome moreaccurate. The discovery and learning process is the advantage of machine learning; however, it requires a significant amount of computational resources.

SIGNATURE BASED IDS:

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

- An e-mail with an attachment containing amalware 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 becauseit just the trafficwith the signature database. Ifamatch found then thealert is generated, ifamatch is not found thenthe 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 needsto be updatedconstantly, almost on adaily basis from theanti -virus labs. If the signature is not up to date, chances are that the IDS systems will failto detect some of the intrusion attacks. The other disadvantage is that they have very little information about previous requests when processing the current ones.

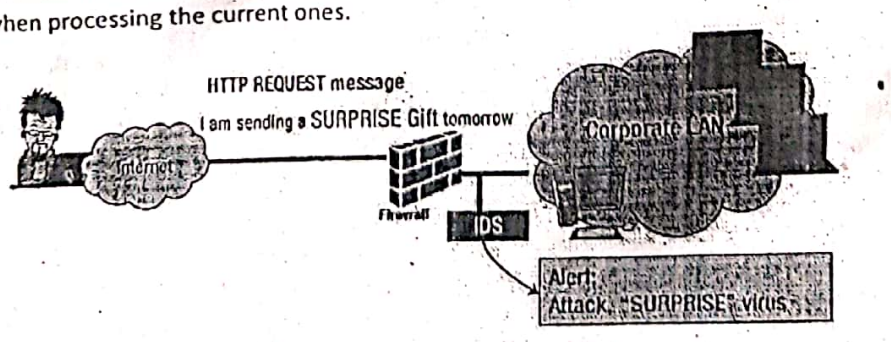


Figure. Signature baseddetection

Signature based detection can offer very specificdetection threats by comparing network trafficwith the threat signature database. Thedetection can be enhanced if thenetwork traffic insidethenetwork can be made to learn specificpatterns, thus reducing false positives. Signaturedetection enginestend

www.Jntufastupdates.com

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 definitionsare added to it. Hencearobust platform is neededforsignature detection considering this growth.

HOST-BASED IDS:

Host-based Intrusion Detection System refers to the detection intrusion Single system. This is normally software-baseddeployment where an agent, as shownin Figure, is installed on the localhost that monitors and reports the application activity. HIDS monitors the access to the system and its application and sendsalerts forany unusual activities. It constantly monitors eventlogs, systemlogs, application logs, user policy enforcement, rootkit detection, file integrity and otherintrusions 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 otherdecision based the policy that is configured on the system.

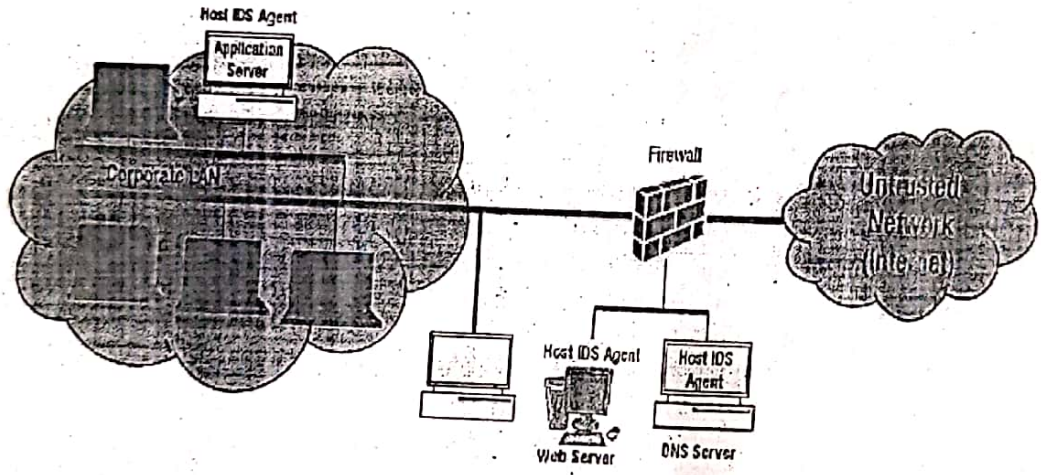


Figure 11-2. Host Based Intrusion Detection System

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 functionalityHIDS dependsthe logs generated by the System and the fact that the intruders leave evidence of theiractivities. 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 triggerany 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 forfurtheraction

www.Jntufastupdates.com

Disadvantages

- HIDS functionality works only if the Systems generatelogs and match against the pre-defined policies. If forsome 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 forany vulnerability Software.

HOST-BASED IDS/IPS:

Many host security products contain integrated host-based IDS/IPS systems (HIDS/HIPS), anti-malware 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 internalnetwork, and they can defend local attacks, such as malwarein removable devices.They also protect against attacks from network and encrypted attacks in which the encrypted datastream 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 adynamicdatabase 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.