IP SECURITY AND SYSTEM SECURITY

Syllabus: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management. **System Security**

IP SECURITY

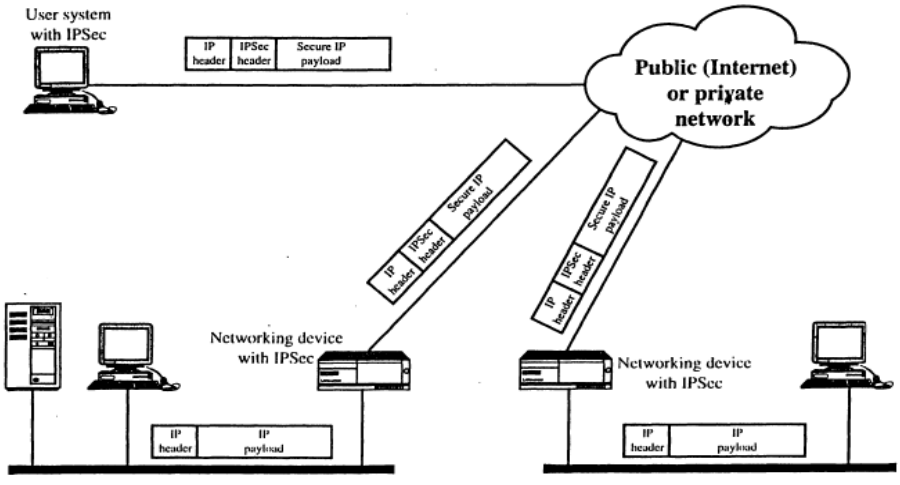
In 1994, the Internet Architecture Board issued a report entitled 'Security in the Internet Architecture". In the year 2001, CERT, Computer Emergency and Response Team analysed 52,000 types of attacks on the Internet. The most serious types of attacks are IP spoofing, eavesdropping and packet sniffing.

IP spoofing: Intruders create packets with false IP addresses and exploit applications that use authentication based on IP

Packet Sniffing: Attackers read transmitted information, including logon information and database contents.

Applications of IP Security:

IP security provides capability to secure communications across a LAN, across private and public WANs, and across the Internet.



An IP Security Scenario.

- **Secure Branch Office connectivity over the Internet:** A company can build a secure virtual private network over the Internet or over a public WAN. This enables the company to rely on the Internet and reduce its need for private networks.

- **Secure Remote access over the Internet**: An end user whose system is equipped with IP Security protocols can make a local call to an Internet Service Provider(ISP) and gain secure access to a company network.
- **Establishing extranet and Intranet connectivity with Partners**: IPSec can be used to secure communications with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- **Enhancing Electronic Commerce Security**: Even though some web and e-commerce applications have built in security protocols, by using IPSec enhances that security.

Benefits of IP Security:

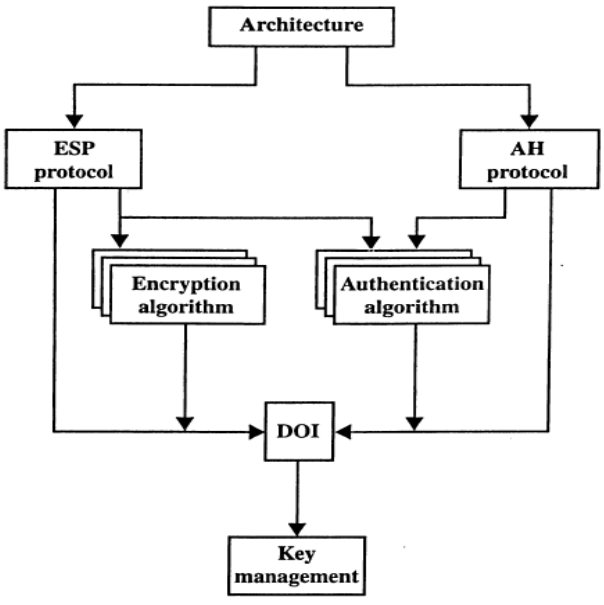
- When IPSec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- Using IPSec, a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below transport layer and so it is transparent to applications and end users.

Routing Applications:

In addition to supporting end users and protecting premises systems and networks IPsec can play a vital role in the routing architecture required for internetworking.

- A router advertisement and neighbour advertisement comes from an authorized router
- A redirect message comes from the router to which the initial packet was sent
- A routing update is not forged.

IP SECURITY ARCHITECTURE:



IPSec Document Overview.

IP Security contains the following documents:

- IPSec 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 the use of 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 if 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 documents relate to each other. These include identifiers for encryption and authentication algorithms.

IPSec Services: IPSec provides services at the IP layer by enabling a system to select required security protocols, determine the algorithms to use for the service. Two protocols are used to provide security: an authentication protocol (AH) and a combined protocol for encryption/authentication (ESP). the services are:

- Access Control
- Connectionless Integrity
- Data Origin Authentication
- Rejection of replayed packets
- Confidentiality
- Limited Traffic flow confidentiality

The following table lists various services provided by AH and ESP

IPSec Services

	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 presents in both the authentication and confidentiality mechanisms for IP is the security association (SA). It is a one-way relation between a sender and a receiver that affords security services to the traffic carried on it. A security association is uniquely identified by three parameters:

- Security Parameter Index (SPI): A bit string associated to this SA. This filed is present in AH and ESP.
- IP Destination Address: Only unicast addresses are allowed. This is the destination address of SA. Destination may be an end system, network system, firewall or router
- Security Protocol Identifier: Indicates whether the association is an AH or ESP.

SA Parameters:

In each IPSec implementation there is a nominal security association database that define the parameters associated with each SA:

- Sequence Number Counter: A 32-bit value is used to generate the sequence number field in AH or ESP headers.
- Sequence Counter Overflow: A flag which indicates the overflow of sequence numbers
- Anti-Replay Window: Used to find whenther an inbound AH or ESP packet is a replay.
- AH Information: Authentication algorithm, keys, key lifetimes and related parameters in AH
- ESP Information: Encryption and Authentication algorithms, keys, initialization values, key lifetimes, and related parameters.
- Lifetime of this Security Association: A time interval for each SA
- IPSec protocol Mode: Tunnel, transport, or wild card.
- Path MTU: maximum size of a packet.

SA Selectors: IPSec services are applied to IP traffic. Each SA has SPD(Security Policy Database. Each SPD is defined by a set of IP and upper layer protocol field values. The following selectors determine an SPD entry:

- Destination IP Address
- Source IP Address
- User ID: A user id from OS.
- Data Security Level: Used for systems providing information flow security(secret or unclassified)
- Transport Layer protocol:
- IPSec Protocol: (AH, ESP, AH/ESP)

- Source and Destination Ports
- IPV6 class: collected from IPV6 Header
- IPV6 flow Label
- IPV4 Type of Service(TOS)

Transport and Tunnel Modes: Both AH and ESP supports two modes.

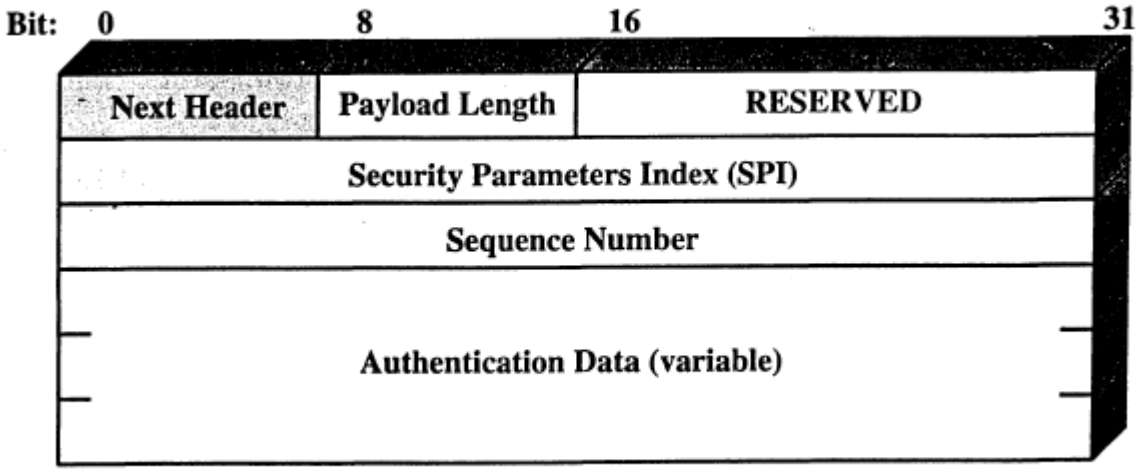
Transport Mode:

- Provides protection for upper layer protocols.
- That is transport mode protection extends to the payload of an IP packet. Ex: TCP,UDP,ICMP
- Transport mode is used to provide end-to-end communication between hosts

Tunnel Mode:

- Provides protection to the entire IP packet.
- After AH, ESP, these headers are added to the IP packet. So that the entire IP packet plus security files is treated as the payload of a new "outer" IP packet.
- The entire original, or inner packet travels through a tunnel from one peer to another peer

Authentication Header (AH): The AH provides support for data integrity and authentication of IP packets. The data integrity feature ensures that undetected modification to a packet's content in transit is not possible. The authentication feature enables an end system or network device to authenticate the user or application and filter traffic. It also prevents the address spoofing attacks. AH also guards against the replay attacks. Authentication is based on Message Authentication Code (MAC). The Authentication Header contains:

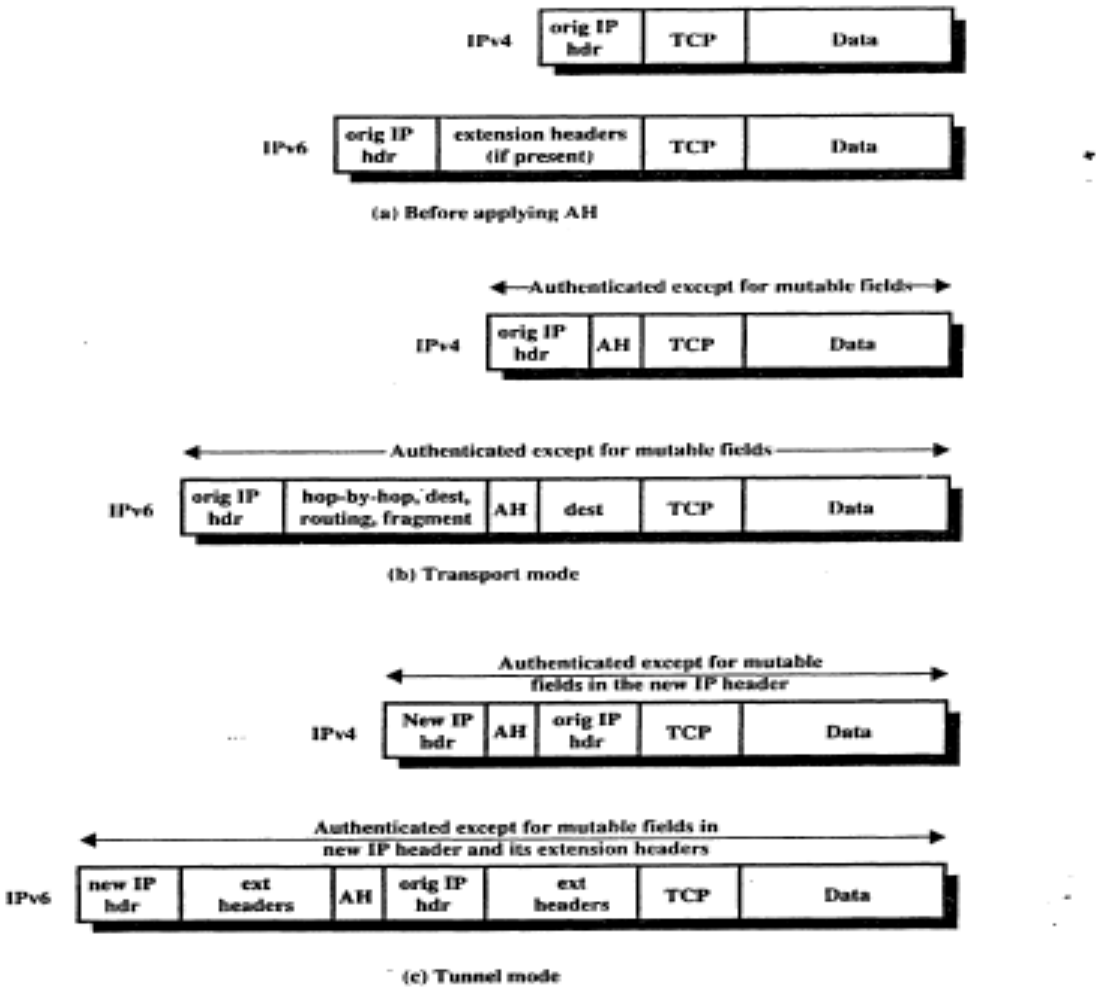


IPSec Authentication Header.

- Next Header (8 bits): Identifies the type of heard immediately following this header
- Payload Length (8 bits): Length of Authentication Header in 32 bit words.
- Reserved (16 bits): These 16 bits are reserved for future purpose.
- Security Parameter Index (32 bits): Identifies a Security Association (SA)
- Sequence Number (32 bits): A 32 bit increasing counter value
- 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 the corresponding packet.

AH in Transport and Tunnel Modes:

For transport mode AH using IPv4, the AH is inserted after the original IP header and before the IP payload. Authentication covers the entire packet, excluding mutable fields in the IPv4 header. In IPv6, the AH is viewed as an end-to-end payload; that is, it is not examined or processed by intermediate routers. Therefore, AH appears after IPv6 base header and hop-by-hop, routing and fragmentation extension headers. The destination options header can appear before or after the AH header.

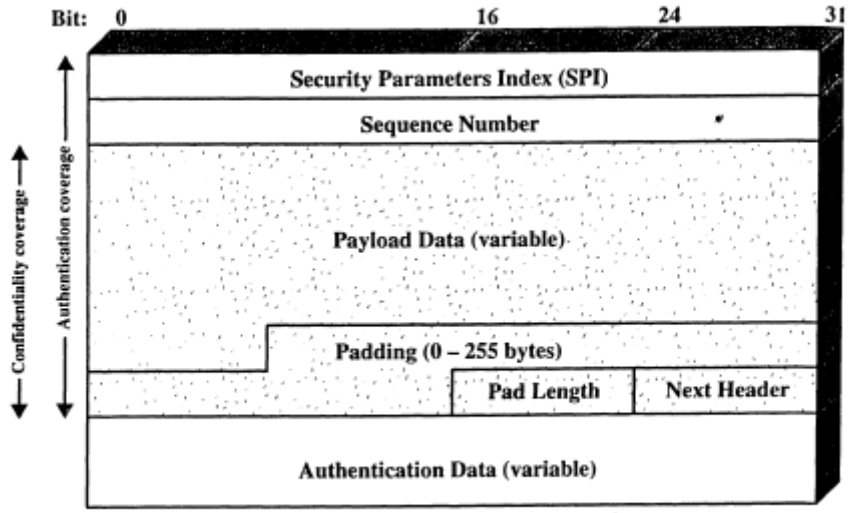


Scope of AH Authentication.

For tunnel mode AH, the entire original IP packet is authenticated and the AH is inserted between the original IP header and a new router IP header. The inner IP header carries the ultimate source and destination addresses, while an outer IP header contain different IP addresses (firewalls or other security gateways). Therefore, with tunnel mode entire inner IP packet, including the entire inner IP header, is protected by AH. The outer IP header is protected except for mutable and unpredictable fields.

Encapsulating Security Payload: ESP provides confidentiality services including traffic flow confidentiality. ESP can also provide same authentication services as AH.

ESP Format: It contains the following fields:



IPSec ESP Format.

- Security Parameter Index (32 bits): Identifies a security association
- Sequence Number (32 bits): An increasing counter value which provides an anti-replay function.
- Payload Data (variable): This is a transport level segment (transport mode) or IP packet (tunnel mode) protected by encryption.
- Padding: This is of length 0 to 255 bytes
- Pad length (8 bits): Indicates the number of pad bytes immediately preceding this field.
- Next Header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload.
- Authentication Data (variable): A variable-length field that contains the Integrity Check Value compared over the ESP packet minus the Authentication Data Field.

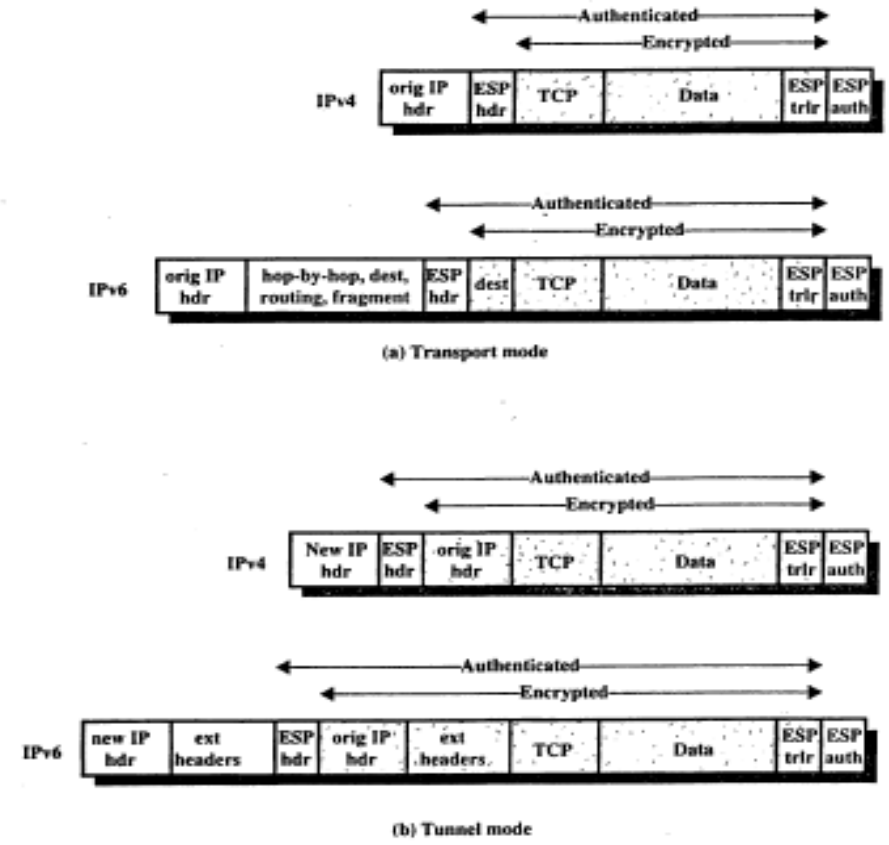
Encryption and Authentication Algorithms in ESP:

Encryption: 3DES, RC5, IDEA, 3key triple IDEA, CAST, Blowfish

Authentication: MAC, HMAC with MD5, HMAC with SHA I

Transport and Tunnel Modes:

Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP(e.g., a TCP segment). For this mode using IPv4, the ESP header is inserted into the IP packet immediately prior to the transport-layer header and an ESP trailer is placed after the IP packet; if authentication is selected, the ESP authentication data field id added after the ESP trailer. The entire transport layer segment plus the ESP trailer are encrypted. Authentication covers all of the cipher text plus the ESP header. In IPv6, the ESP is viewed as an end-to-end payload; that is, it is not examined or processed by intermediate routers. Therefore, ESP appears after IPv6 base header and hop-by-hop, routing and fragmentation extension headers. The destination options header can appear before or after the ESP header. For IPv6 encryption covers the entire transport level segment plus the ESP trailer plus the destination options header if it covers after ESP.

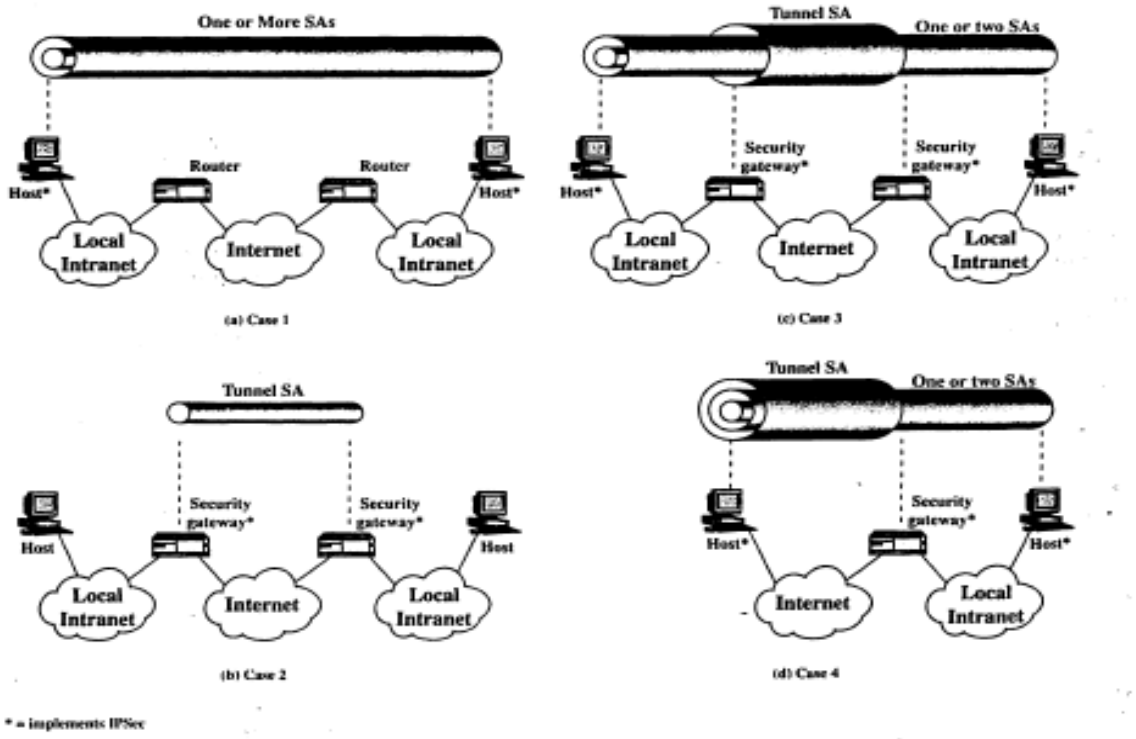


Scope of ESP Encryption and Authentication.

Tunnel mode ESP is used to encrypt an entire IP packet. For this mode, ESP header is prefixed to the packet and then packet plus the ESP trailer is encrypted. This method can be used to counter traffic analysis.

Basic combinations of security Associations:

IPSec architecture lists four examples of combinations of SAs that must support by IPSec hosts. The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs, the mode may be either transport or tunnel; otherwise it must be tunnel mode.



Basic Combinations of Security Associations.

Case 1: Security is provided between end systems that implement IPSec. For any two end systems to communicate via an SA, they must share the appropriate secret keys. The following are the possible combinations:

- AH in transport mode
- ESP in transport mode
- AH followed by ESP in transport mode
- Any one of a, b, or c inside an AH or ESP in tunnel mode

Case 2: Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPSec. It implements simple virtual private network support. The tunnel could support AH, ESP or ESP with its authentication.

Case 3: Built on case 2 by adding end-to-end security. The same combinations used in case 1 and case 2 are allowed here. The gateway-to-gateway tunnel provides either authentication or confidentiality or both for all traffic between end systems.

Case 4: Provides support for a remote host that uses the Internet to reach an organization's firewall and then gain access to some server or workstation behind the firewall. Only tunnel mode is required between the remote host and the firewall.

Key Management: It 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. There are two types of ley management:

- Manual: A system admin manually configures each system with its own keys and with the keys of other communicating systems. This is practical for small relatively static environments.
- Automated: Enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed systems.

The default key management protocol for IPSec is referred to as ISAKMP/Oakley and contains the following elements.

1. **Oakley Key Determination Protocol**: A key exchange protocol based on the Diffie-Hellman algorithm.
2. **Internet Security Association Key Management Protocol (ISAKMP)**: Provides a framework for Internet Key management and provides specific protocol support.

Oakley Key Determination Protocol: This is a refinement on Diffie Hellman Algorithm.

- Select a largest prime number q
- Select an integer α which is a primitive root of q

These two will be considered as global public key parameters.

- User A selects a random integer X_A as its private key
- User A calculates his public key $Y_A = \alpha^{xa} \bmod q$ and transmits to B

Similarly B also generates his public and private key pair

- User B selects a random integer X_B as its private key
- User A calculates his public key $Y_B = \alpha^{xb} \bmod q$ and transmits to A

Each user can now compute the session key:

$$K=(Y_B)^{XA} \bmod q = (Y_A)^{XB} \bmod q$$

The Diffie-Hellman has two attractive features:

- Secret keys are created only when needed. There is no need to store secret keys for a long period of time.
- The exchange requires no pre-existing infrastructure.

However, there are number of weaknesses in Diffie-Hellman:

- It does not provide any information about the identities of parties
- It is subject to a man-in-the middle attack in which a third party C can impersonate B while communicating with A, and impersonates like while communicating with B.
- The man-in-the-middle attack proceeds as follows:
    a) B sends his public key Y_B in a message addressed to A
    b) The enemy E intercepts this message. E saves B's public key and send a message to A, that has B's user Id and E's public key Y_E. A receives E's message and stores E's public key with B's user ID. Similarly E sends a message to B with E' public key and A user ID.
    c) B computes a secret key K1 based on B's private key and Y_E. A computes a secret key K2 based on A's private key and E's public key Y_E. E computes K1 using E's secret key X_E and Y_B, and computes k2 using X_E and Y_A.
    d) From now onwards, E is able to relay messages from A to B ad from B to A, appropriately encipher, decipher the messages and forwards to A and B in such a way that neither A nor B will know that they share their communication with E.

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

Features of Oakley:

1. It employs a mechanism known as cookies to thwart clogging attacks.
2. It enables the two parties to negotiate a group, and global parameters of Diffie-Hellman.
3. It uses nonces to ensure against replay attacks.
4. It enables the exchange of Diffie-Hellman pulbi key values..
5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

Three different authentication methods can be used with Oakley:

- Digital Signatures
- Public key encryption
- Symmetric Key Encryption

Oakley Key Exchange Example:

$I \rightarrow R$: CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, $S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

$R \rightarrow I$: CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, $S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^y \| g^x \| EHAS]$

$I \rightarrow R$: CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, $S_{KI}[ID_I \| ID_R \| N_I \| N_R \| GRP \| g^x \| g^y \| EHAS]$

Notation:

I	=	Initiator
R	=	Responder
CKY_I, CKY_R	=	Initiator, responder cookies
OK_KEYX	=	Key exchange message type
GRP	=	Name of Diffie-Hellman group for this exchange
g^x, g^y	=	Public key of initiator, responder; g^{xy} = session key from this exchange
EHAO, EHAS	=	Encryption, hash, authentication functions, offered and selected
NIDP	=	Indicates encryption is not used for remainder of this message
ID_I, ID_R	=	Identifier for initiator, responder
N_I, N_R	=	Random nonce supplied by initiator, responder for this exchange
$S_{KI}[X]$, $S_{KR}[X]$	=	Indicates the signature over X using the private key (signing key) of initiator, responder

Example of Aggressive Oakley Key Exchange.

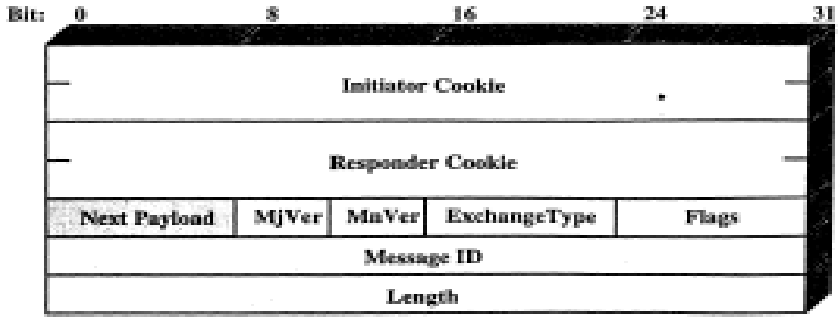
ISAKMP (Internet Security Association Key Management Protocol):

It defines procedures and packet formats to establish, negotiate, modify, and delete security associations. To establish SA, ISAKMP defines payloads for exchanging key generation and authentication data. These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism.

ISAKMP Header Format: It consists of one or more payloads. All these payloads are carried by Transport protocol.

- Initiator Cookie (64 bits): Cookie of entity that initiates SA establishment, SA notification or SA deletion.
- Responder cookie (64 bits): Cookie of responding entity: null in first message form initiator.
- Next Payload (8 bits): Indicates the type of first payload in the message.
- Major Version (4 bits): indicates major version of ISKMP in use
- Minor version (4 bits): Indicates minor version in use.
- Exchange Type (8 bits): Indicates the type of exchange.

- Flags (8 bits): Indicates specific option set for this ISKMP exchange.
- Message Id (32 bits): Unique ID for this message
- Length (32 bits): Length of the total message (header plus all payloads) in bytes.



ISAKMP Formats.

ISAKMP Payload Types: All ISAKMP payloads begin with the same generic payload header. The next payload field has a value of zero if this is the last payload in the message; otherwise its value is the type of next payload. Payload length fields defines the length of payload in bytes. Hers is a list of payloads:

ISAKMP Payload Types

Type	Parameters	Description
Security Association (SA)	Domain of Interpretation, Situation	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Transform #, Transform-ID, SA Attribute	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Key Exchange Data	Supports a variety of key exchange techniques.
Identification (ID)	ID Type, ID Data	Used to exchange identification information.
Certificate (CERT)	Cert Encoding, Certificate Data	Used to transport certificates and other certificate-related information.

Certificate Request (CR)	# Cert Types, Certificate Types, # Cert Auths, Certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Hash Data	Contains data generated by a hash function.
Signature (SIG)	Signature Data	Contains data generated by a digital signature function.
Nonce (NONCE)	Nonce Data	Contains a nonce.
Notification (N)	DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data	Used to transmit notification data, such as an error condition.
Delete (D)	DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid.

ISAKMP Exchange Types: It provides a framework for message exchange, with the payload types serving as building blocks. There are five default exchange types:

Base Exchange: Allows key exchange and authentication material to be transmitted together. It minimizes the number of exchanges and do not protects the identities. The first two messages provide cookies and establish an SA with accepted protocol and transforms using a nonce value to ensure against replay attacks. The last two messages exchange the key material and user IDs with the ATUH payload used to authenticate keys, identities with the nonces from the first two messages.

Exchange	Note
(a) Base Exchange	
(1) **I** → **R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R** → **I:** SA; NONCE	Basic SA agreed on
(3) **I** → **R:** KE; ID_I; AUTH	Key generated; Initiator identity verified by responder
(4) **R** → **I:** KE; ID_R; AUTH	Responder identity verified by initiator; Key generated; SA established

The Identity Protection Exchange: It expands the Base Exchange to protect the user identities. The first two message establish the SA. The next two messages perform key exchange, with noces for replay protection. Once the session key has been computed, the two parties exchange encrypted messages that contain authentication information, such as digital signatures and optionally certificates which validate the public keys.

(b) Identity Protection Exchange	
(1) **I** → **R:** SA	Begin ISAKMP-SA negotiation
(2) **R** → **I:** SA	Basic SA agreed on
(3) **I** → **R:** KE; NONCE	Key generated
(4) **R** → **I:** KE; NONCE	Key generated
(5)* **I** → **R:** ID_I; AUTH	Initiator identity verified by responder
(6)* **R** → **I:** ID_R; AUTH	Responder identity verified by initiator; SA established

Authentication Only Exchange: It is used to perform mutual authentication, without a key exchange. The first two messages establish the SA. In addition, the responder uses the second message to convey its ID and uses authentication to protect the messages. The initiator sends the third message to transmit its authenticated ID.

(c) Authentication Only Exchange	
(1) **I** → **R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R** → **I:** SA; NONCE; ID_R; AUTH	Basic SA agreed on; Responder identity verified by initiator
(3) **I** → **R:** ID_I; AUTH	Initiator identity verified by responder; SA established

Aggressive Exchange: It minimizes the number of exchanges. It also do not protects the identities. In the first message, the initiator proposes an SA with associated offered protocol and transform options. The initiator also begins with key exchange and provides its ID. In the second message, the responder indicates its acceptance of the SA, with a particular protocol and transform, computes the key exchange and authenticates the transmitted information. In the third message, the initiator transmits an authentication result that covers the previous information, encrypted using the shared secret session key.

(d) Aggressive Exchange	
(1) **I** → **R:** SA; KE; NONCE; ID_I	Begin ISAKMP-SA negotiation and key exchange
(2) **R** → **I:** SA; KE; NONCE; ID_R; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* **I** → **R:** AUTH	Responder identity verified by initiator; SA established

Information Exchange: It used for one-way transmittal of information for SA management mostly to notify the status, errors and deletion

(e) Informational Exchange	
(1)* **I** → **R:** N/D	Error or status notification or deletion

SYSTEM SECURITY

Intruders: An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

Password Capture:

- another attack involves **password capture**
  - watching over shoulder as password is entered
  - using a trojan horse program to collect
  - monitoring an insecure network login
    - eg. telnet, FTP, web, email
  - extracting recorded info after successful login (web history/cache, last number dialed etc)
- using valid login/password can impersonate user
- users need to be educated to use suitable precautions/countermeasures

Password Guessing:

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests)
  - exhaustively searching all possible passwords
- check by login or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

Password Management:

- front-line defense against intruders
- users supply both:
  - login – determines privileges of that user
  - password – to identify them
- passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - more recent systems use crypto hash function
- should protect password file on system

Password Studies:

- Purdue 1992 - many short passwords
- Klein 1990 - many guessable passwords
- conclusion is that users choose poor passwords too often
- need some approach to counter this

Managing Passwords-Education:

- can use policies and good user education
- educate on importance of good passwords
- give guidelines for good passwords
    - minimum length (>6)
    - require a mix of upper & lower case letters, numbers, punctuation
    - not dictionary words
- but likely to be ignored by many users

Computer Generated Passwords:

- let computer create passwords
- if random likely not memorisable, so will be written down (sticky label syndrome)
- even pronounceable not remembered
- have history of poor user acceptance
- FIPS PUB 181 one of best generators
    - has both description & sample code
    - generates words from concatenating random pronounceable syllables

Managing Passwords: Reactive Checking

- reactively run password guessing tools
    - note that good dictionaries exist for almost any language/interest group
- cracked passwords are disabled
- but is resource intensive
- bad passwords are vulnerable till found

Managing Passwords- Proactive Checking:

- most promising approach to improving password security
- allow users to select own password
- but have system verify it is acceptable
    - simple rule enforcement (see earlier slide)
    - compare against dictionary of bad passwords
    - use algorithmic (markov model or bloom filter) to detect poor choices

Intruders are classified into 3 categories

- **Masquerador:** An individual who is not authorized to use the computer and who penetrates a system's access conrols to exploit a legitimate user's account.
- **Misfeasor:** A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- **Clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Intrusion Techniques:

- aim to gain access and/or increase privileges on a system
- basic attack methodology
    - target acquisition and information gathering
    - initial access
    - privilege escalation
    - covering tracks
- key goal often is to acquire passwords
- so then exercise access rights of owner

Intrusion Detection:

- inevitably will have security failures
- so need also to detect intrusions so can
    - block if detected quickly
    - act as deterrent
    - collect info to improve security
- assume intruder will behave differently to a legitimate user
    - but will have imperfect distinction between
- statistical anomaly detection
    - threshold
    - profile based
- rule-based detection
    - anomaly
    - penetration identification

Audit Records:

- fundamental procedure for intrusion detection
- native audit records
    - part of all common multi-user O/S

- already present for use
- may not have info wanted in desired form

- detection-specific audit records
  - created specifically to collect wanted info
  - at cost of additional overhead on system

Statistical Anomaly Detection:

- threshold detection
  - count occurrences of specific event over time
  - if exceed reasonable value assume intrusion
  - alone is a crude & ineffective detector
- profile based
  - characterize past behavior of users
  - detect significant deviations from this
  - profile usually multi-parameter

Analysis:

- foundation of statistical approaches
- analyze records to get metrics over time
  - counter, gauge, interval timer, resource use
- use various tests on these to determine if current behavior is acceptable
  - mean & standard deviation, multivariate, markov process, time series, operational
- key advantage is no prior knowledge used

Rule-Based Intrusion Detection:

- observe events on system & apply rules to decide if activity is suspicious or not
- rule-based anomaly detection
  - analyze historical audit records to identify usage patterns & auto-generate rules for them
  - then observe current behavior & match against rules to see if conforms
  - like statistical anomaly detection does not require prior knowledge of security flaws
- rule-based penetration identification
  - uses expert systems technology
  - with rules identifying known penetration, weakness patterns, or suspicious behavior
  - compare audit records or states against rules
  - rules usually machine & O/S specific
  - rules are generated by experts who interview & codify knowledge of security admins

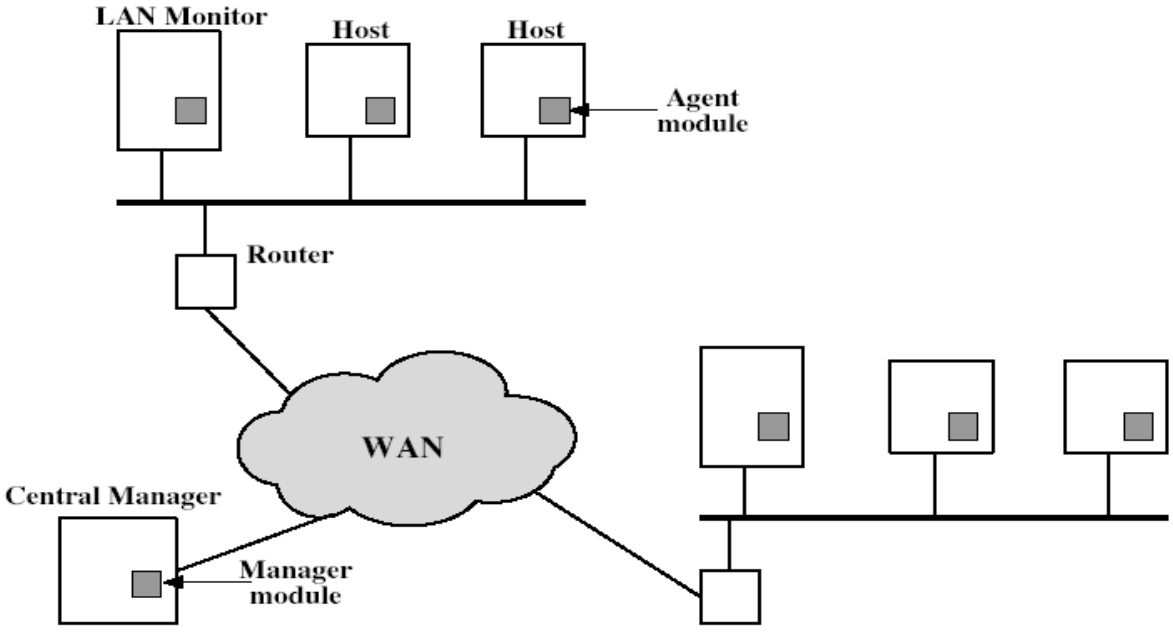
quality depends on how well this is done

Base Rate Fallacy:

- practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
  - if too few intrusions detected -> false security
  - if too many false alarms -> ignore / waste time
- this is very hard to do
- existing systems seem not to have a good record

Distributed Intrusion Detection:

- traditional focus is on single systems
- but typically have networked systems
- more effective defense has these working together to detect intrusions
- issues
  - dealing with varying audit record formats
  - integrity & confidentiality of networked data
  - centralized or decentralized architecture



Host Agent Module: Collects data on security related events on the host and transmit these to the central manager.

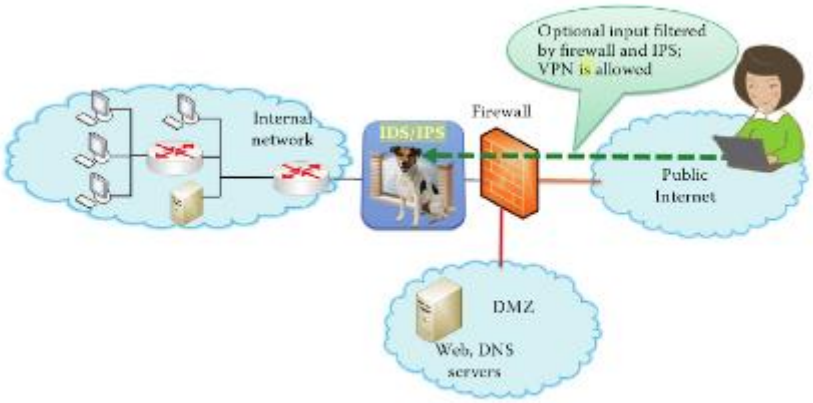
LAN Monitor agent module: Operates like a host agent module except that it analyses LAN traffic and reports the results to the central manager.

Central Manager Module: Receives reports from LAN monitor and host agents processes and correlates these reports to detect intrusion.

Honeypots:

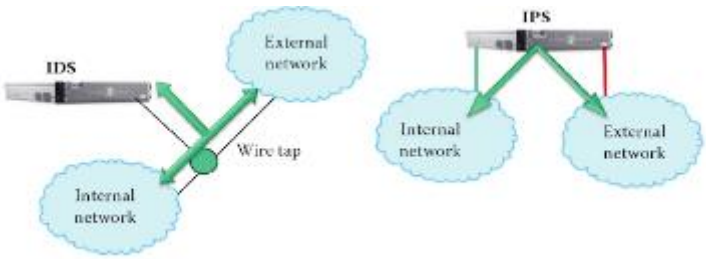
- decoy systems to lure attackers
  - away from accessing critical systems
  - to collect information of their activities
  - to encourage attacker to stay on system so administrator can respond
- are filled with fabricated information
- instrumented to collect detailed information on attackers activities
- single or multiple networked systems
- cf IETF Intrusion Detection WG standards

An Intrusion Detection/Prevention system provides a deep packet inspection at the entrance of network. This system is positioned behind the firewall as shown in the following diagram.



Positioning IDS/IPS in a system.

VPN (virtual private network) is permitted to pass firewall and IDS/IPS, since traffic is normally encrypted and authenticated. It provides deep inspection for the pay loads. IDS is based on out-of-band detection of intrusions and their reporting, and IPS in in-band-filtering to block intrusions. The following figure shows the difference between IDS and IPS.



Differences between IDS and IPs:

IDS is performed through a wiretap, and is clearly an out-of-band operation. IPS is performed in-line.

Difference between IDS and IPS systems: IDS and IPS are originally developed for addressing requirements of lacking in most firewalls. IDS are basically used to detecting the threats or intrusions in network segment. But IPS is focused on identifying those threats or intrusions for blocking or dropping their activities.

The IDS and IPS are list of similar functions like packet inspection, stateful analysis, TCP segment reassembly, deep packet inspection, protocol validation, and signature matching.

The best example of security gate in term of difference of IDS and IPS is, An IDS works like a patrol car within the border, monitoring activities and looking for abnormal situations. But an IPS operates like a security guard at the gate of allowing and denying access based on credentials and some predefined rule set, or policy. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks.

Intrusion Detection System (IDS): The IDS is software or an appliance that detects a threat, unauthorized or malicious network traffic. IDS has their own predefined rule sets, through that it can inspect the configuration of endpoints to determine whether they may be susceptible to attack (this is known as host-based IDS), and also it can record activities across a network and compare it to known attacks or attack patterns (this is called network-based IDS). The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network malicious activities.

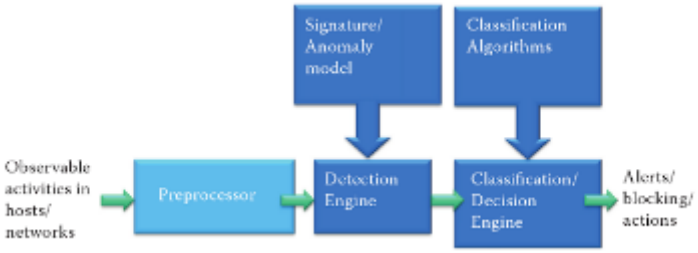
- Preventing network attacks
- Identifying the intruders
- Preserving logs in case the incident leads to criminal prosecution

Intrusion Prevention System (IPS): The IPS are not only detect the bad packets caused by malicious codes, botnets, viruses and targeted attacks, but also it can take action to prevent those network activity from causing damage on network. The attacker's main motive is to take sensitive data or intellectual property, through that they interested 4 in whatever they can get from customer data like employee information, financial records etc. The IPS is specified to provide protection for assets, resources, data, and networks.

- IPS stops the attack itself
- IPS changes the security environment

IDS/IPS Building Blocks:

The following block diagram outlines the functions of an IDS/IPS system. The observable activities re pre-processed 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 alerts or blocking actions.



The knowledge used by detection, including signature and anomaly model, can be provided by captured signature or by training algorithms which is shown in the following diagram.

The Approaches used for IDS/IPS:

The approaches to Intrusion detection can generally be classified as either anomaly /behaviour based or signature based.

1. **Anomaly-Based Detection Methods:**
    - Anomaly based detectors generate the normal behaviour/pattern of the protected system, and deliver an anomaly alarm if the observed behaviour at any point of time does not matches with the expected behaviour.
    - These are more prone to generating false positives due to the dynamic natures of networks, applications and exploits.
    - Due to the difficulty in manual setting of the profiles for complicated and dynamic traffic, anomaly-detection systems should be applied on various levels of traffic aggregation such as single server, a server farm, an operation unit or an enterprise in order to achieve the accurate protection.

- Legitimate traffic in network contains anomalies. For example, protocol anomalies arise from custom application that use off-the-shelf protocol libraries, but employ them in an unexpected manner, and behaviour anomalies come from exceptional. But often critical business processes.
- Based on the type of processing anomaly detection techniques are further classified into three main categories
    a) Statistical-based,
    b) Knowledge-based,
    c) Machine learning-based.

a) **Statistical-based IDS/IPS:** In this system, the behaviour is represented from the captured network traffic activity and a profile representing its-stochastic behaviour is created. This profile is based on metrics such as:

- 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 behaviour of legitimate users and is then used in statistical tests to find if the behaviour under detection is legitimate or not. During the anomaly detection process, one corresponding to the currently captured profile is compared with the previously trained statistical profile. These behaviours are compared using threshold detection and profile detection methods.

The threshold detection uses thresholds that are independent of users for examining the frequency of occurrence of events. Network security managers can utilize pre-programmed limits based on the types of traffic to ensure the servers will not become overloaded.

In contrast, the profile detection uses a profile of activity of each user/device to detect abnormal behaviour. Profiles can be established at both global and granular session levels for short and long periods. When a statistical distribution relationship exists among the different types of TCP packets like: 3-way handshake, 4-way close, and data transfer, the relationship can be learned to establish profiles. These profiles are established based on statistical measures of date and time of traffic. These profiles can be used to detect DOS and DDOS.

Statistical approaches use three types of models like uni variate (Gaussian random variables) and multi variate(use correlation between one or more metrics). Time series

models use interval timer, an event counter or resource measure take into account the order and the inter-arrival times of the activities.

Advantages of Statistical approaches:

- They do not require prior knowledge about the normal activity of the target system
- They have the ability to learn the expected behaviour of the system from observations
- They can provide accurate notification of malicious activities occurring over long periods of time.

b) **Knowledge/Expert Based IDS/IPS:** These systems capture the normal behaviour from available information, including the expert knowledge, protocol specifications, and network traffic instances. The normal behaviour is represented as set of rules. Attributes and classes are identified from the training data or specifications. Then a set of classification rules, parameters are generated. These rules will be used to detect anomaly behaviours.

Specification based anomaly methods require that the model is manually constructed by human experts in terms of a set of rules that describe the system behaviour. These techniques have shown to produce a low rate of false alarms, but are not as effective as other anomaly detection methods in detecting novel attacks like network probing and DOS attacks. Protocol anomaly is abed on the inspection of layers 2-7 by specifications-generated rules:

- A protocol or service is used for a non-standard purpose or on a non-standard port
- IP defragmentation overlaps and suspicious IP options
- Unusual TCP fragmentation overlaps and illegal TCP options and usage
- Application protocol include illegal field values and command usage.

c) **Machine Learning-Based IDS/IPS:** These schemes are based on the establishment of an explicit or implicit model that allows the patterns analysed to be categorized. Machine learning is different from statistical based methods because it discovers the characteristics for building a model of behaviours. The discovery and learning process is the advantage of machine learning. Machine learning methods for generating IDS/IPS rules are;

- Bayesian Networks
- Neural Networks
- Genetic Algorithms
- Fuzzy Logic
- Clustering
- Nearest Neighbour Analysis
- Data Mining

- Markov Chains and hidden Markov analysis
- Spectral anomaly detection
- Association rule discovery

2.Signature-Based IDS/IPS: This is sued to detect patterns of specific known exploits and vulnerabilities. The exploits include patterns of codes, scripts, registration-key-modification and buffer overflow. The vulnerabilities include payload content or requests to a known vulnerability, which is used to create vulnerability based signatures. Content signature is often a string of characters that appear in the payload of packets as part of the attack. Once a new vulnerability is disclosed, signatures are developed by researchers to counter threats. Signature based system take a look at he payload and identify whether it contains a matched signature. It has usually a lower false positive rate, it may not detect zero-day and mutated attacks. Malware can be stealthy by embedding its communications into protocols that are likely to be present in normal network operations or incorporate polymorphism and metamorphism to avoid a fixed signature. A Botnet might coordinate with its C&C at irregular intervals and at low rates to avoid generating significant anomalies.

The major challenges in these are the size of the signature database and the processing time of packets against all entries in the signature database. These can make the IDS vulnerable to DOS attacks.

3.Adaptive Profiles: The profile of normal behaviour consists of a comprehensive list of parameters and values for target being monitored. During IDS/IPS installation, the administrator can select an appropriate profile based on the network zone's mission or service types. A profile/policy template, provided by the IDS/IPS vendor, is a collection of policy construction rules that the IDS/IPS uses to create the zone policies during the policy construction phase of the learning process. The IDS/IPS uses the policies to monitor the zone traffic for anomalies that indicate an attack on the zone. The zone policies are configured to take action against a particular traffic flow if the flow exceeds the policy thresholds.

The self- learning capability supports learning the patterns of network usage and traffic patterns that take place during normal network operations. Thus, adaptive profiles can reflect the normal network traffic pattern evolution, and avoids raising false alarms. For example, the combination of threshold based detection and self-learning (adaptive) capability can accurately detect DoS/DDoS attacks. When one activates anomaly detection in IDS/IPS, an administrator can invoke self-learning using the following options:

- **Detect :** IDS/IPS analyses the zone traffic and begins producing dynamic filters when it detects a traffic anomaly or when the flow exceeds the zone policy thresholds and

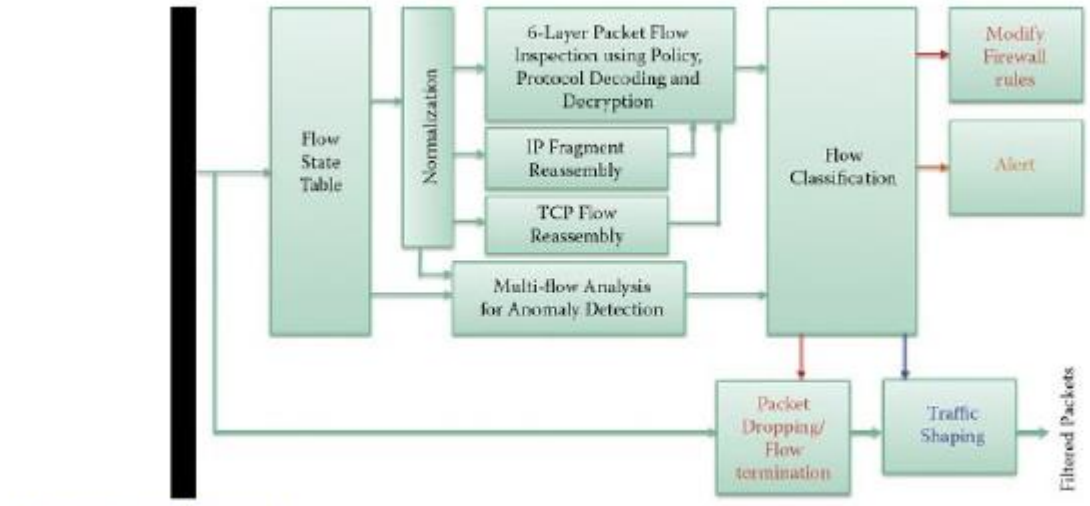
continuously adapts this set of filters to the zone traffic and the type of DDoS attack. Dynamic filters apply protection to the traffic flow and define how to handle the attack. The dynamic filter contains source and destination IPs and port numbers, fragmentation settings of the traffic flow, filter action and traffic rate.

- **Detect and Learn**: IDS/IPS analyses zone traffic for traffic anomalies and at the same time begins the threshold-tuning phase of the learning process. While analysing the traffic for the threshold-tuning phase, the IDS/IPS can automatically adjust the policy thresholds of the zone configuration.

An administrator can configure the IDS/IPS to detect traffic anomalies in a zone using either automatic detect mode or Interactive detect mode.

Network-Based IDS/IPS (NIDS/NIPS):

The incoming packets enter the flow state table, where state information is maintained. The maintenance of state information permit sensors to obtain the context for attack detection. The entire content of the data packet is inspected and state information is captured and updated in real time. This state information provides basis for layers2-7 detection. Multiple token matches are utilized to capture attack signatures and behaviours that span packet boundaries or exist in an our-of-order packet stream. This process permit the system to determine if a state transition should be allowed or not, and thus detects a blocks malware, Trojans, Key loggers, P2P, botnets and worms.



The IDS/IPS block diagrams.

The normalization function involves both TCP normalization and IP normalization, which are used to make comparisons with normal behaviour. With TCP, normalization, invalid or suspect conditions are inspected (SYN from client to server and SYN+ACK from server to client). The following types of network attacks are blocked: insertion and evasion attacks. Insertion attacks occur when the

inspection module accepts a packet that is rejected by the end host system. Evasion attacks occur when the inspection module rejects a packet although the end host system accepts it. Segments are discarded that contain bad checksum, TCP header or payload length, suspect TCP flags (SYN/FIN, SYN/URG). TCP normalization is configured by assembling various TCP commands into a parameter map for filtering as a policy.

The IP normalization process inspects packets using a configured parameter map for such things as general security checks, ICMP security checks, fragmentation security checks, IP fragment reassembly and IP fragmentation if packet size exceeds maximum length(MTU).

The final blocks illustrate actions taken by IPS, not IDS. In addition to dropping packets and terminating sessions, there are other important operations. For example:

- Firewall rules need to be adjusted to block suspicious hosts.
- Traffic shaping may be involved and involve slowing down less critical traffic such as P2P and video.

NIDS/NIPS may not detect encrypted traffic since some portions of data and some header information are encrypted. Malware are exploring this weakness of NIDS/NIPS by encrypting packets.

EX: SNORT It is an open source network IDS/IPS developed by Source Fire. It has the benefits of signature and anomaly-based inspection. It is the most widely deployed IDS/IPS world wide. It supports both inline IPS and offline IDS. IT has separate versions for Linux, Unix, Windows. Unix based NIDS passively monitors network traffic and looks for suspicious activity.

HOST Based IDS/IPS: Many host based security products contain integrated host-based IDS/IPS systems, anti-malware and a firewall. They have both advantages and weaknesses.

Advantages:

- They are capable of protecting mobile hosts from an attack when outside protected internal network can defend local attacks such as malware in removable devices.
- They also protect from 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 in host software execution (system call patterns).

Weaknesses:

- If an attacker takes over a host, the HIDS/HIPS and NAC agent s/w can be compromised and disabled and the audit logs are modified to hide the malware.
- HIDS/HIPS has only a local view of the attack, and a host-based anomaly detection has a high false alarm rate.

Ex: OSSEC is an open source host-based intrusion detection system. It performs log analysis, file integrity checking, policy monitoring, root kit detection, real time alerting and active response. It runs on most operating systems including windows, Linux, MacOS X, FreeBSD, Solaris, HP-UX and AIX.

With some modification of the host's kernel. A HIDS/HIPS can monitor all system calls and evaluate system calls against either known attack signatures or anomaly rules. The HIDS/HIPS detect and prevent attacks on host computers, including web servers and database servers. The inputs to HIDS/HIPS are network packets, system logs, system events and hardware information. Combined signatures and anomaly based methods detect and block abnormal activity patterns and generate system alarms and event reports.