4. Virtual Private Networks

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

- This section provides an overview of IP security (IPsec) and an introduction to the IPsec architecture. It explains the problem solved by IPSec and its features. Further, it explains how the different IPSec protocols work in different modes (transport and tunnel). Additionally, the section overview about features of different VPN solutions.

Overview

At the end of this lesson, you will be able to;

- Explain the need of VPN technology
- Explain the difference between VPN and Secure VPN
- Explain the difference between transport mode and tunnel mode.
- Understand the concept of the security association
- Explain the difference between the security association database and the security policy database.
- Summarize the traffic processing functions performed by IPsec for out- bound packets and for inbound packets.
- Present an overview of Encapsulating Security Payload.
- Summarize the alternative cryptographic suites approved for use with IPsec.

Overview

4.1. Introduction to Virtual Private Networks

- 4.1.1. Requirement of Remote Access and Private Communication
- **Remote access**
  - Accessing organizations resources remotely and most of the time the access is ubiquitous.
- **Site-to-Site access**
  - **Intranet based**
    - Connecting several branches of the same organization : E.g. Head office of a bank with its branches
  - **Extranet based**
    - Connecting between two different organizations : E.g. Bank give access to the software development company

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **Dedicated network link owned and maintained by you**
  - Not scalable
  - Expensive investment
  - Not flexible for remote connectivity only for short range site-to-site connectivity
  - You are on your own (no maintenance or support otherwise)
  - Upgrade cost would be very high

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **What is a Virtual Private Network (VPN)?**
  - Virtual Private Network can be described as a logical communication link that carries private traffic over public network.
  - In an VPN:
    - Access to communication should only be for the defined users
    - Communication should be private and not necessarily be encrypted: e.g. MPLS
    - Communication should be abstracted from physical substrate (Virtual) i.e. does not change when physical layer technology changes.

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **Practical VPN applications**
  - Ubiquitous access to the cooperate resources : e.g. Working while traveling.
  - Need of accessing private cooperate services from remote locations: e.g. Cooperate financial system
  - Controlled/Private Access needed from many locations by different parties : e.g. software vendor accessing from their site
  - Long distance where leased lines are not feasible : e.g. international employees / clients
  - Infrastructure requirements such as extended LANs (PROD to DR) : e.g. Oracle DB deployments

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **VPN implementations**
  - MPLS - Multi-Protocol Label Switching (no security)
  - GRE Tunnels - Generic Routing Encapsulation (no security)
  - PPTP - Point-to-Point Tunnelling Protocol (secure but considered vulnerable now, Use GRE for encapsulation)
  - L2TP - Layer 2 Tunnelling Protocol (no security)
    Use GRE for encapsulation and no security unless IPSec is incorporated
  - IPSecurity (secure and de facto protocol for secure VPN implementations)
  - TLS (SSL VPN) - Transport Layer Security VPNs (secure)

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **MPLS - Multi-Protocol Label Switching**
  - Not secure
  - Use a labelling mechanism to isolate the network from other networks
  - Can be implemented as a full mesh (not limited as leased lines)
  - Within the service provider network and difficult to find service providers with global partnerships

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **GRE Tunnels - Generic Routing Encapsulation**
  - Not secure
  - Use encapsulation to isolate the network from other networks
  - Can be used to forward multicast traffic where other VPN protocols does not support

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **PPTP - Point-to-Point Tunnelling Protocol**
  - Introduced by Microsoft way back and there were few versions
  - Supported by many Operating Systems : Microsoft Windows, Mac OS, GNU/Linux
  - Authentication is done using MS-CHAP
  - Keys to encrypt payload is communicated during the authentication process
  - Secure but considered vulnerable
  - Use GRE for encapsulation and encryption vary by the implementation
  - Point-to-Point connectivity
  - Works only on IP networks
  - A data link layer protocol

4.1. Introduction to Virtual Private Networks

- 4.1.2. Private Communication Technologies and Evolution
- **L2TP - Layer 2 Tunnelling Protocol**
  - L2TP provides the functionality of PPTP, but it can work over networks other than just IP
  - L2TP does not provide any encryption or authentication services
  - Need to combined with IPSec if encryption and authentication services are required
  - The processes that L2TP uses for encapsulation are similar to those used by PPTP
  - A data link layer protocol

4.1. Introduction to Virtual Private Networks

- 4.1.3. VPN vs Secure VPN
- Secure VPNs give you confidentiality, integrity and authentication for your communication.
- Example protocols
  - PPTP
  - IP Security
  - SSL/TLS VPN
  - SSH Tunnels

4.2. IP Security Overview

- 4.2.1 Applications of IPsec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security

4.2. IP Security Overview

- 4.2.2 Benefits of IPsec
  - When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security related processing.
  - IPsec in a firewall is resistant to bypass if all traffic from the outside must use IPsec and the firewall is the only means of entrance from the Internet into the organization
  - IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.
  - IPsec can be transparent to end users.
  - IPsec can provide security for individual users if needed.

4.2. IP Security Overview

- 4.2.3 Routing Applications
  - IPsec can assure that
    - A router advertisement (a new router advertises its presence) comes from an authorized router.
    - A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) comes from an authorized router.
    - A redirect message comes from the router to which the initial IP packet was sent.
    - A routing update is not forged.

4.2. IP Security Overview

- 4.2.4 IPsec Services
- IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.
- Two protocols are used to provide security:
    - **Authentication Header (AH)**
        - an authentication protocol designated by the header of the protocol
    - **Encapsulating Security Payload (ESP)**
        - a combined encryption/authentication protocol designated by the format of the packet for that protocol

4.2. IP Security Overview

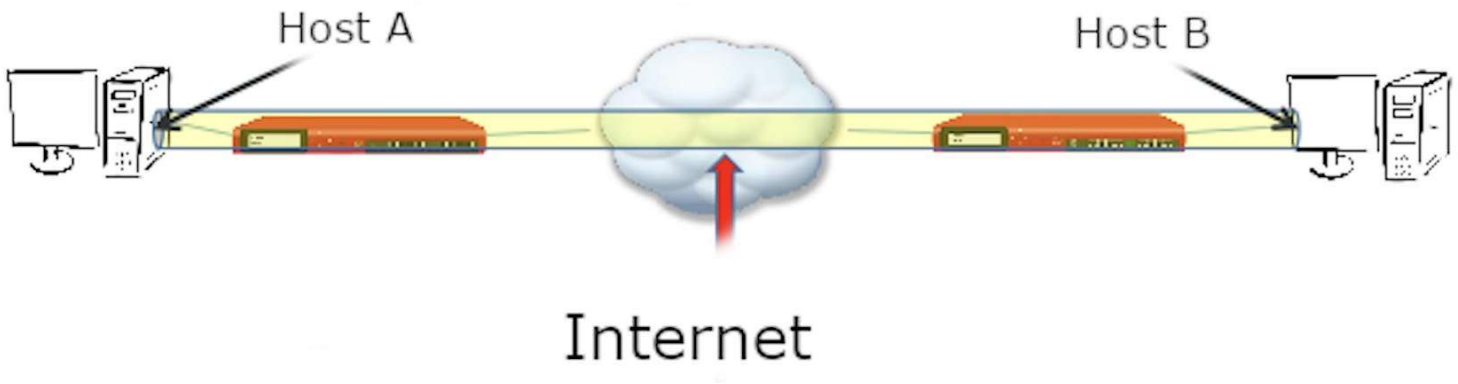
- 4.2.4 IPsec Services
- RFC 4301 lists the following services:
    - Access control
    - Connectionless integrity
    - Data origin authentication
    - Rejection of replayed packets (a form of partial sequence integrity)
    - Confidentiality (encryption)
    - Limited traffic flow confidentiality

4.2. IP Security Overview

- 4.2.5 Transport and Tunnel Modes
- Both AH and ESP support two modes of use: transport and tunnel mode

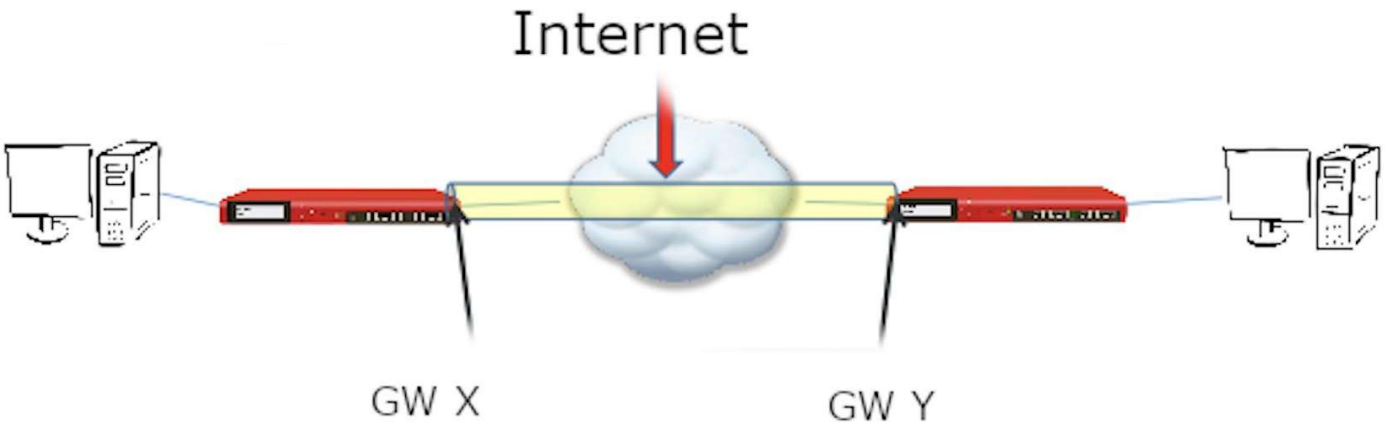
4.2. IP Security Overview

- 4.2.5.1 Transport Mode
- Transport mode is used for end-to-end communication between two hosts
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- AH in transport mode authenticates the IP payload and selected portions of the IP header.



4.2. IP Security Overview

- 4.2.5.2 Tunnel Mode
- Tunnel mode is used to protect communication between site-to-site / network-to-network
- Tunnel mode provides protection to the entire IP packet
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header



4.3. IP Security Policy

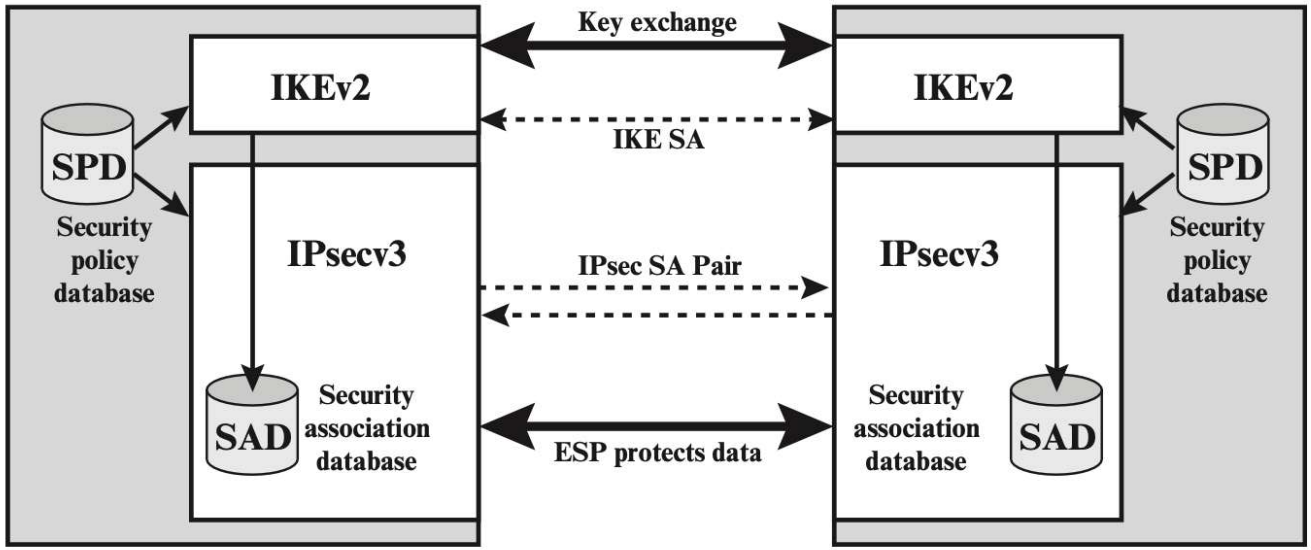
- IPsec policy is determined primarily by the interaction of two databases, the Security Association Database (SAD) and the Security Policy Database (SPD)

4.3. IP Security Policy

- 4.3.1. Security Associations
  - An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.
  - If a peer relationship is needed for two-way secure exchange, then two security associations are required.
  - A security association is uniquely identified by three parameters.
    - Security Parameters Index (SPI)
    - IP Destination Address
    - Security Protocol Identifier

4.3. IP Security Policy

- 4.3.2. IPSec Architecture



4.3. IP Security Policy

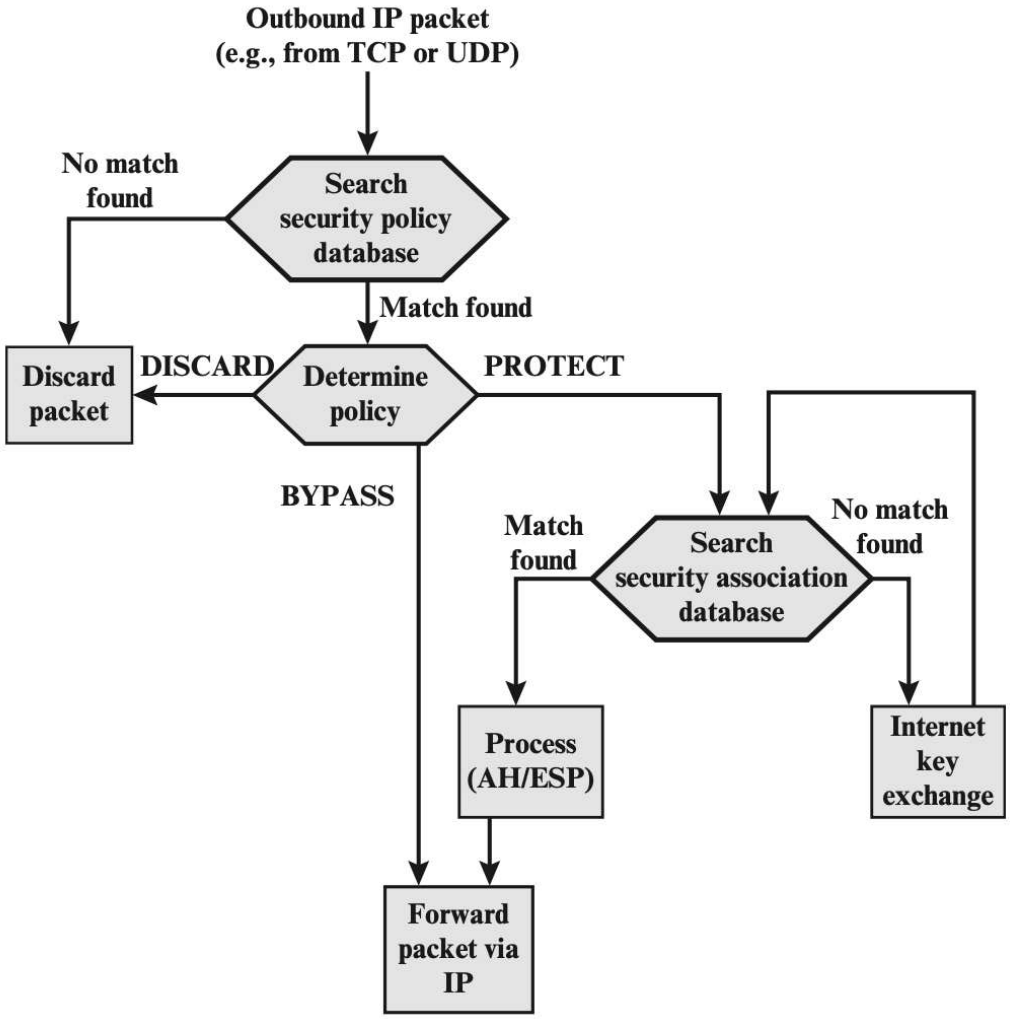
- 4.3.3. Security Association Database
  - Security Association Database that defines the parameters associated with each SA
  - A security association is normally defined by the following parameters in an SAD entry
    - Security Parameter Index
    - Sequence Number Counter
    - Sequence Counter Overflow
    - Anti-Replay Window
    - AH Information
    - ESP Information
    - Lifetime of this Security Association
    - IPsec Protocol Mode
    - Path MTU

4.3. IP Security Policy

- 4.3.4. Security Policy Database
  - The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) is the nominal Security Policy Database (SPD)
  - The following selectors determine an SPD entry
    - Remote IP Address
    - Local IP Address
    - Next Layer Protocol
    - Name
    - Local and Remote Ports

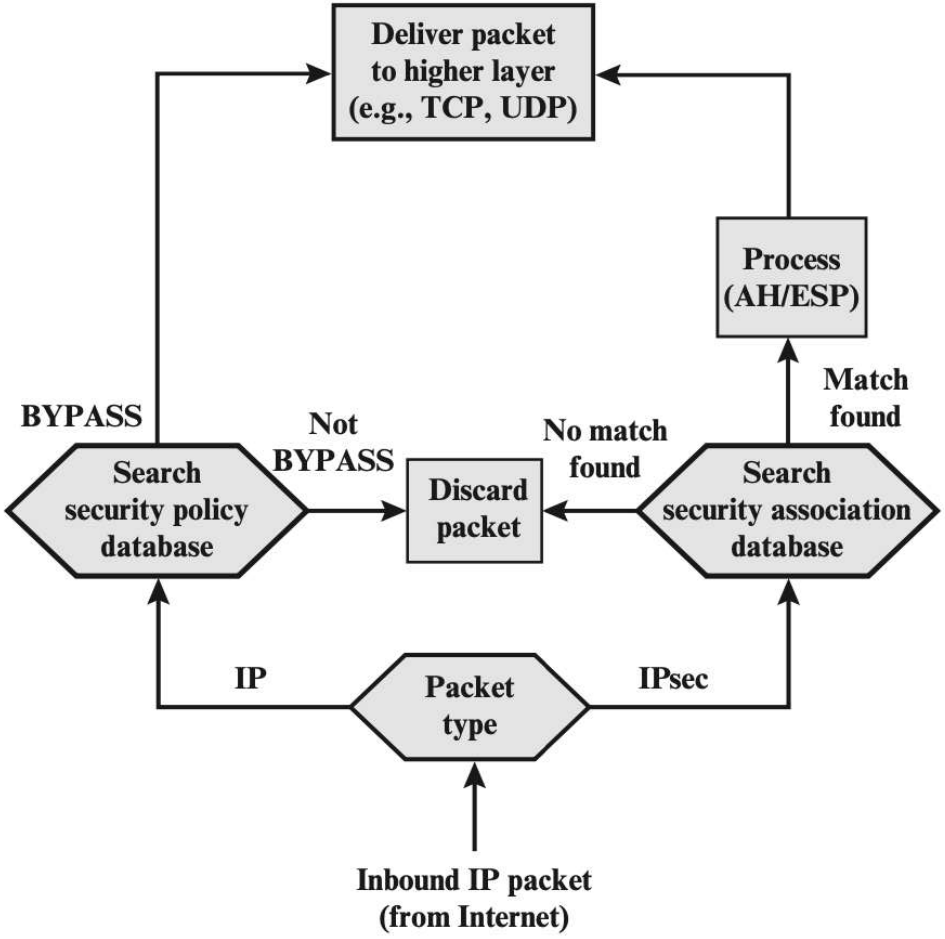
4.3. IP Security Policy

- 4.3.5. IP Traffic Processing - Outbound packets



4.3. IP Security Policy

- 4.3.5. IP Traffic Processing - Inbound packets



4.4. Encapsulating Security Payload

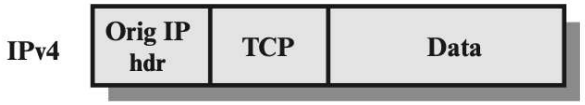
- ESP can be used to provide
  - confidentiality
  - data origin authentication
  - connection- less integrity
  - anti-replay service
  - traffic flow confidentiality

4.4. Encapsulating Security Payload

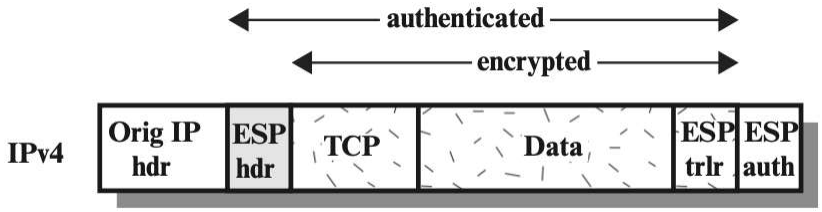
- ESP Format
- Encryption and Authentication Algorithms
- Padding
- Anti-Replay Service

4.4. Encapsulating Security Payload

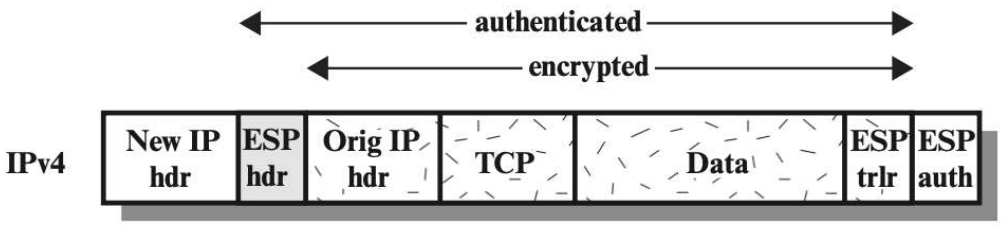
- Packet structure before applying ESP



- Packet structure after applying ESP Transport mode



- Packet structure after applying ESP tunnel mode



4.5. Internet Key Exchange

- The key management portion of IPsec involves the determination and distribution of secret keys.
- IPsec Architecture document mandates support for two types of key management:
  - Manual
  - Automated
- The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the following elements:
  - Oakley Key Determination Protocol
  - Internet Security Association and Key Management Protocol (ISAKMP)

4.6. Cryptographic Suites

- Cryptographic suite is a set of cryptographic algorithms, variety of parameters, key sizes to define a suite.

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP