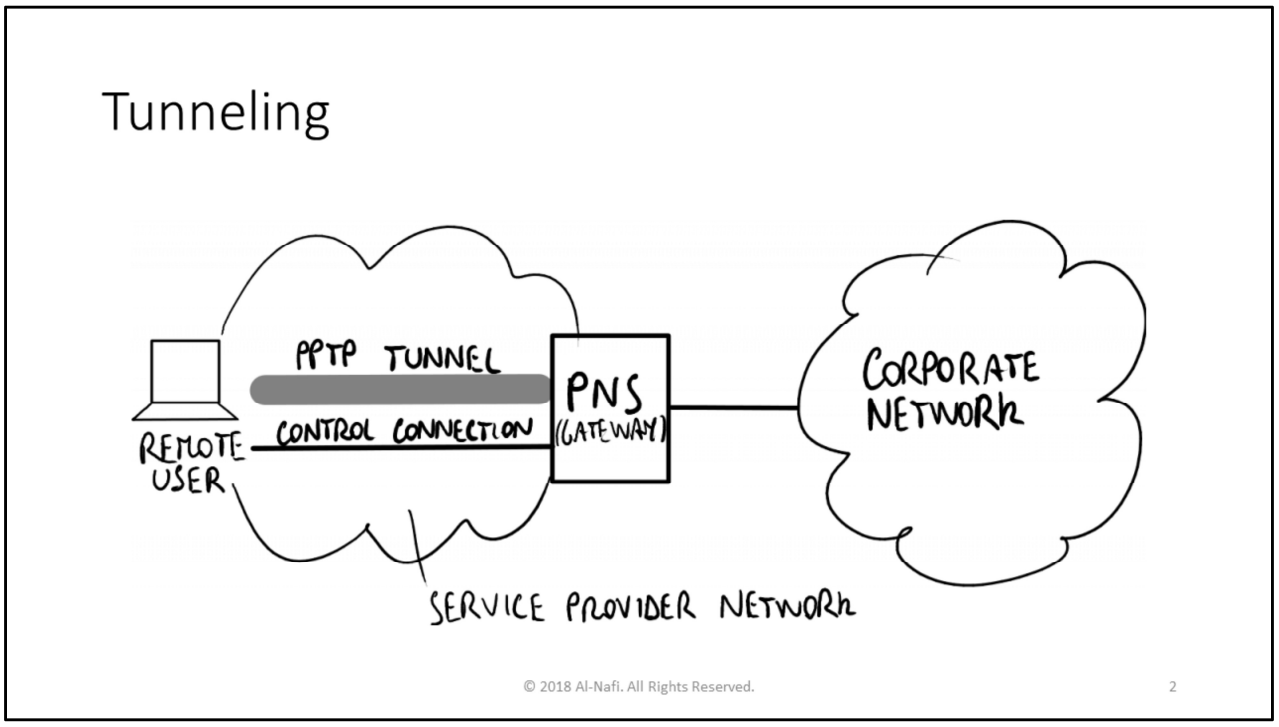
Telecommuting

Telecommuting

Common issues such as visitor control, physical security, and network control are almost impossible to address with teleworkers. Strong VPN connections between the teleworker and the organization need to be established, and full device encryption should be the norm for protecting sensitive information.

If the user works in public places or a home office the following should also be considered:

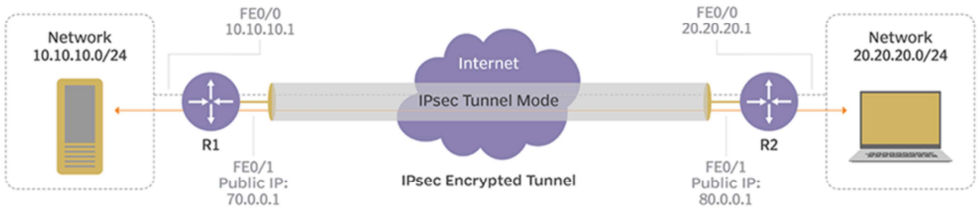
- Is the user trained to use secure connectivity software and methods such as a VPN?
- Does the user know which information is sensitive or valuable and why someone might wish to steal or modify it?
- Is the user's physical location appropriately secure for the type of work and type of information they are using?
- Who else has access to the area? While a child may seem trusted, the child's friends may not be.



Tunneling

Point-to-Point Tunneling Protocol (PPTP) Point-to-Point Tunneling Protocol (PPTP) is a tunnel protocol that runs over other protocols. PPTP relies on Generic Routing Encapsulation (GRE) to build the tunnel between the endpoints. The security architect and practitioner both need to consider known weaknesses, such as the issues identified with PPTP, when planning for the deployment and use of remote access technologies. PPTP is based on Point-to-Point Protocol (PPP), so it does offer authentication by way of password authentication protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Extensible Authentication Protocol (EAP).

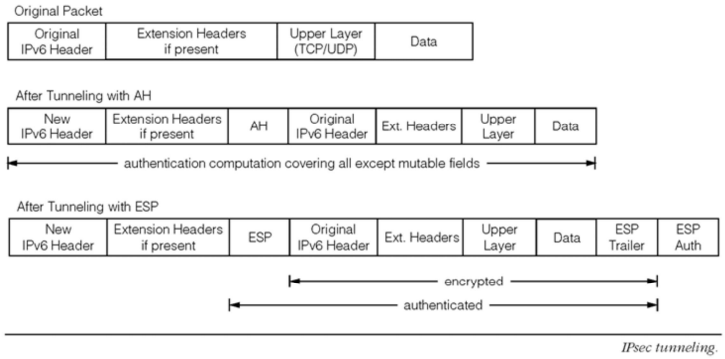
IPSEC



IP security (IPSec) is a suite of protocols for communicating securely with IP by providing mechanisms for authentication and encryption. Standard IPSec only authenticates hosts with each other. If an organization requires users to authenticate, they must employ a nonstandard proprietary IPSec implementation, or use IPSec over Layer 2 Tunneling Protocol (L2TP).

The latter approach uses L2TP to authenticate the users and encapsulate IPSec packets within an L2TP tunnel. Because IPSec interprets the change of IP address within packet headers as an attack, NAT does not work well with IPSec. To resolve the incompatibility of the two protocols, NAT Transversal (NAT-T) encapsulates IPSec within UDP port 4500 (see RFC 3948 for details. Read this RFC and search it on google please).

IPSEC tunnel continued…



IPsec tunneling.

4

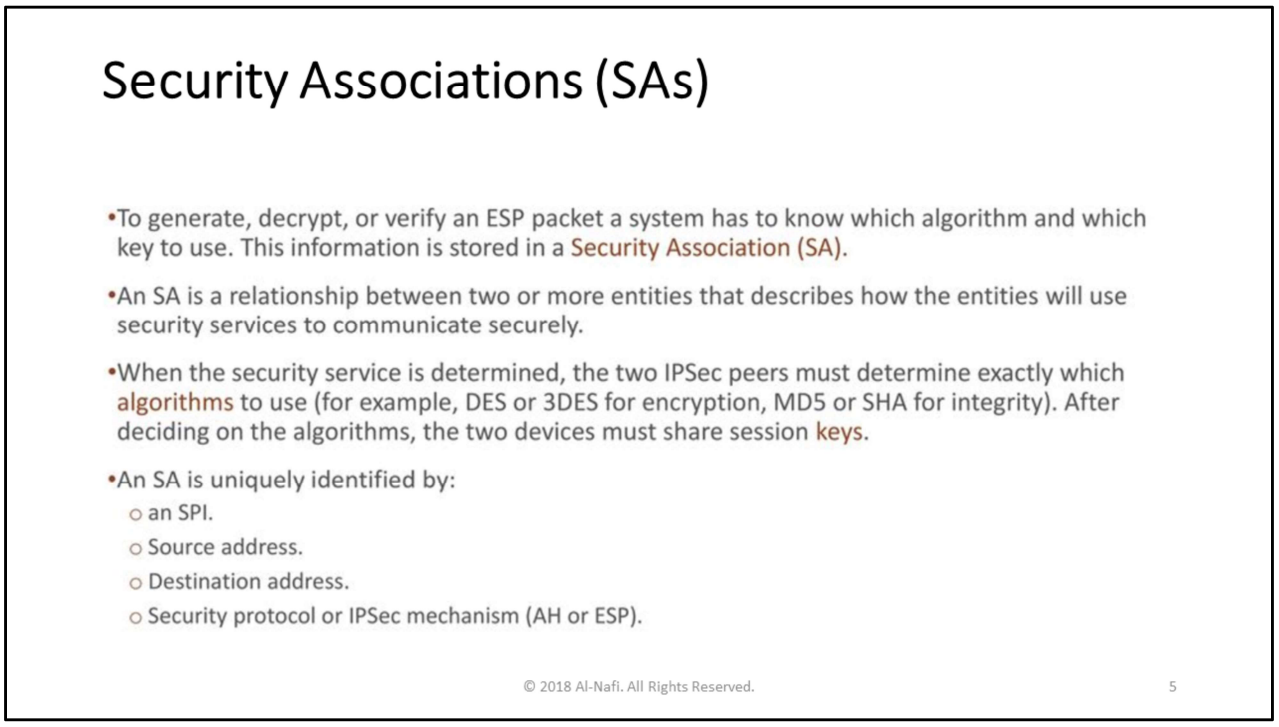
Authentication Header (AH) The Authentication Header (AH) is used to prove the identity of the origin node and ensure that the transmitted data has not been tampered with. Before each packet (headers + data) is transmitted, a hash value of the packet's contents (except for the fields that are expected to change when the packet is routed) based on a shared secret is inserted in the last field of the AH. The endpoints negotiate which hashing algorithm to use and the shared secret when they establish their security association. To help thwart replay attacks (when a legitimate session is retransmitted to gain unauthorized access), each packet that is transmitted during a security association has a sequence number that is stored in the AH. In transport mode, the AH is inserted between the packet's IP and TCP header. The AH helps ensure authenticity and integrity, not confidentiality. Encryption is implemented through the use of encapsulating security payload (ESP).

Encapsulating Security Payload (ESP)
The ESP encrypts IP packets and ensures their integrity. ESP contains four sections:

- **ESP header:** Contains information showing which security association to use and the packet sequence number. Like the AH, the ESP sequences every packet to

thwart replay attacks.

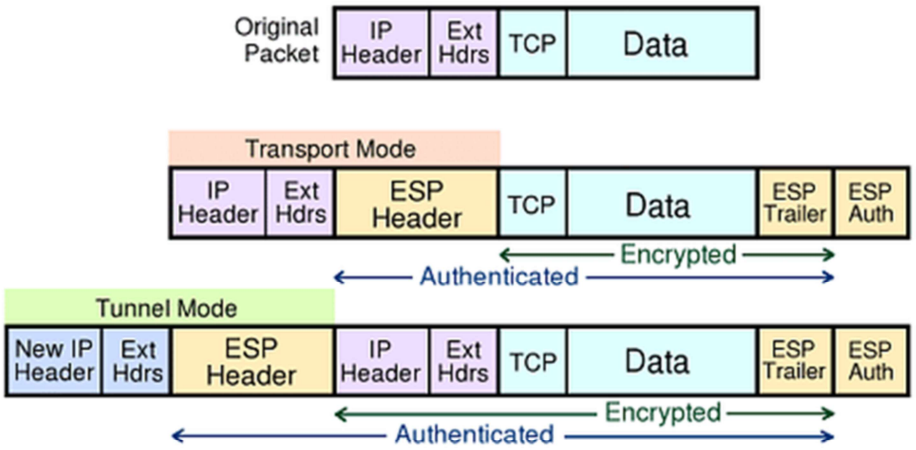
- **ESP payload:** The payload contains the encrypted part of the packet. If the encryption algorithm requires an initialization vector (IV), it is included with the payload. The endpoints negotiate which encryption to use when the security association is established. Because packets must be encrypted with as little overhead as possible, ESP typically uses a symmetric encryption algorithm.
- **ESP trailer:** May include padding (filler bytes) if required by the encryption algorithm or to align fields.
- **Authentication:** If authentication is used, this field contains the integrity check value (hash) of the ESP packet. As with the AH, the authentication algorithm is negotiated when the endpoints establish their security association.



Security Associations (SAs)

A security association (SA) defines the mechanisms that an endpoint will use to communicate with its partner. All SAs cover transmissions in one direction only. A second SA must be defined for two-way communication. Mechanisms that are defined in the SA include the encryption and authentication algorithms and whether to use the AH or ESP protocol. Deferring the mechanisms to the SA, as opposed to specifying them in the protocol, allows the communicating partners to use the appropriate mechanisms based on situational risk.

Transport Mode and Tunnel Mode



Transport Mode and Tunnel Mode

Endpoints communicate with IPSec using either transport or tunnel mode. In transport mode, the IP payload is protected. This mode is mostly used for end-to-end protection, for example, between client and server.

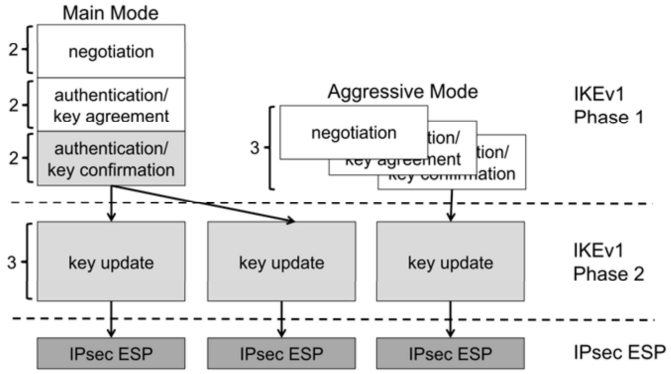
In tunnel mode, the IP payload and its IP header are protected. The entire protected IP packet becomes a payload of a new IP packet and header. Tunnel mode is often used between networks, such as with firewall-to- firewall VPNs.

Internet Key Exchange (IKE)

Described in RFC 2409

Used for Key Management in IPSec Networks

Allows automatic negotiation and creation of IPSec SAs between IPSec Peers



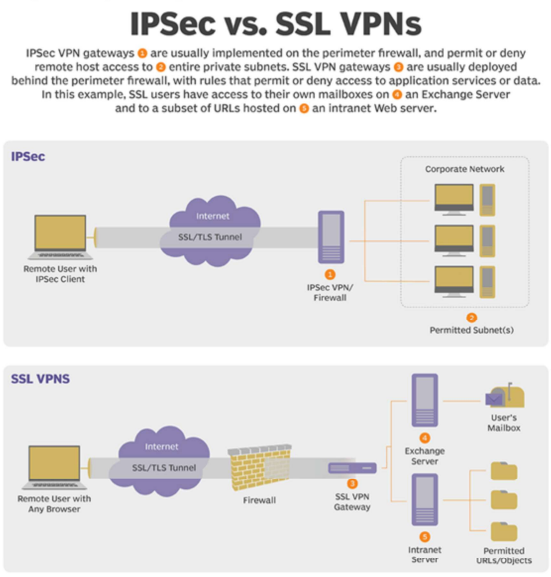
Internet Key Exchange (IKE)

Internet key exchange (IKE) allows two devices to “exchange” symmetric keys for the use of encrypting in AH or ESP. There are two ways to “exchange” keys:

1. Use a Diffie-Hellman (DH) style negotiation
2. Use public key certificates

DH would be used between devices like routers. Public key certificates would be used in an end user VPN connection.

Secure Socket Layer (SSL) Virtual Private Network VPN



SSL VPNs are another approach to remote access. Instead of building a VPN around the IPSec and the network layer, SSL VPNs leverage SSL/TLS to create a tunnel back to the home office. SSL 3.0 (Secure Socket Layer) and TLS 1.2 (Transport Layer Security) are essentially fully compatible, with SSL being a session encryption tool originally developed by Netscape and TLS 1.2 being the open standard IETF version of SSL 3.0. SSL and TSL use public key certs to authenticate each through mutual authentication.

Remote users employ a web browser to access applications that are in the organization's network. Even though users employ a web browser, SSL VPNs are not restricted to applications that use HTTP. With the aid of plug-ins, such as Java, users can have access to back-end databases, and other non-web- based applications. SSL VPNs have several advantages over IPSec. They are easier to deploy on client workstations than IPSec because they require a web browser only, and almost all networks permit outgoing HTTP. SSL VPNs can be operated through a proxy server. In addition, applications can restrict users' access based on criteria, such as the network the user is on, which is useful for building extranets with several organizations.

جزاك اللهُ

To ask questions, Join the Al Nafi Official Group

https://www.facebook.com/groups/alnafi/

(This group is only for members to ask questions)