Introdução à Segurança em Redes IP

Redes e Serviços

Licenciatura em Tecnologias e Sistemas de Informação
DETI-UA

universidade de aveiro
deti.ua.pt

Network Access Control

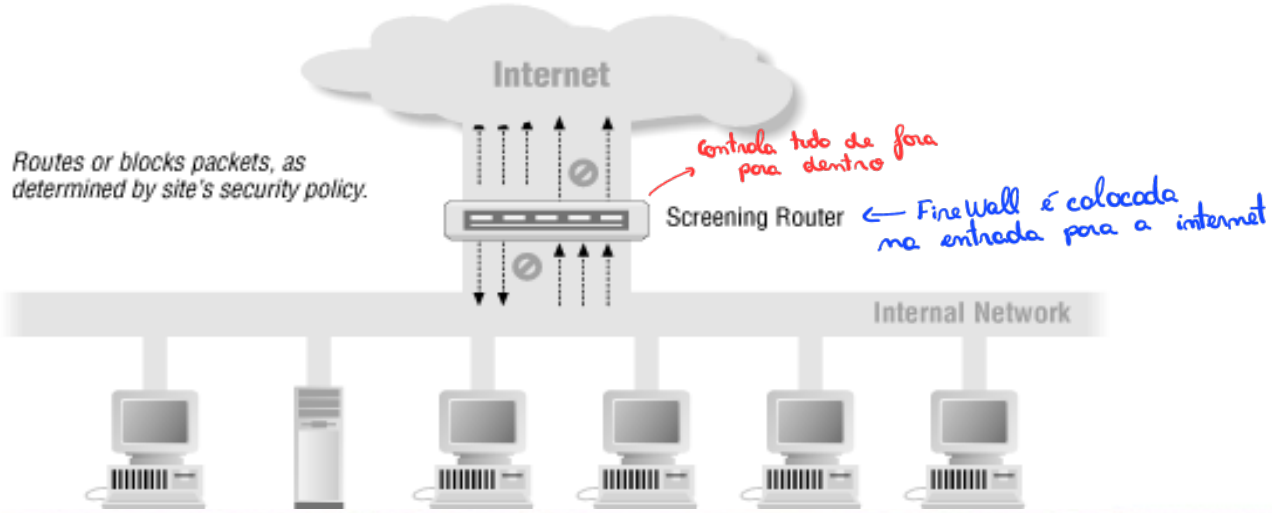
Firewall → Controla o que passa pela rede

- A firewall provides a single point of defense between networks and protects one network from the others → Podemos pôr esta barreira na entrada da nossa rede!
- System or group of systems that enforces a control policy between two or more networks (access control, flow control and content control)
- Network gateway that enforces the rules of network security
- Minimizes local vulnerabilities
- Evaluates each network packet against the policies of network security → tem de ter um bom processamento
- Can monitor all the network traffic and alert to any attempts to bypass security or to any patterns of inappropriate use
- Can be hardware or software based
- Can provide gateway services → Para redes mais movimentadas
  - NAT (Network Address Translation)
  - Proxing and application gateway → intermediário de aplicações
  - Security perimeter extension: tunneling

→ Uma firewall tem de ler todos os pacotes => MUITO Processamento

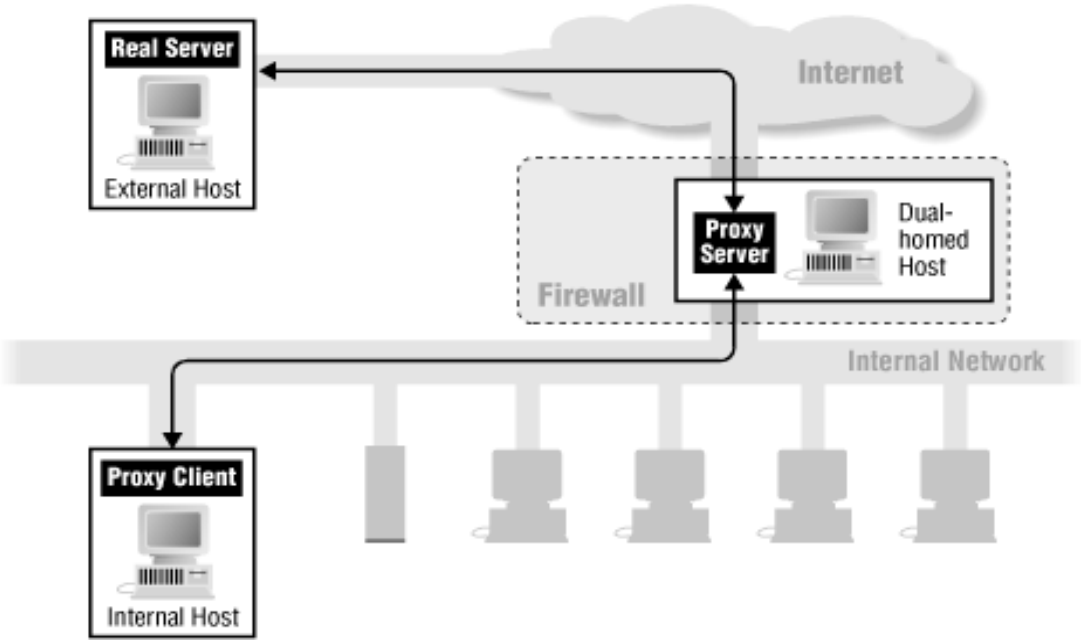
Firewall Technologies

- Packet filtering systems - Route packets between internal and external hosts, but do it selectively. The type of router used in a packet filtering firewall is known as a screening router.
- Problems:
  - Undesirable packets can be fitted to a packet rule criteria and, therefore, pass through the filter
  - Packets can pass through the filter by being fragmented
  - Complex rule sets are difficult to implement and maintain correctly



Firewall Technologies

- Proxy services - Specialized application or server programs that take users' requests for Internet services (such as FTP and Telnet) and forward them to the actual services.
- The proxies provide replacement connections and act as gateways to the services (application-level gateways).
- Problems:
  - Are a single point of failure
  - It's difficult to add new services to the firewall
  - Are CPU intensive and often perform slower under stress

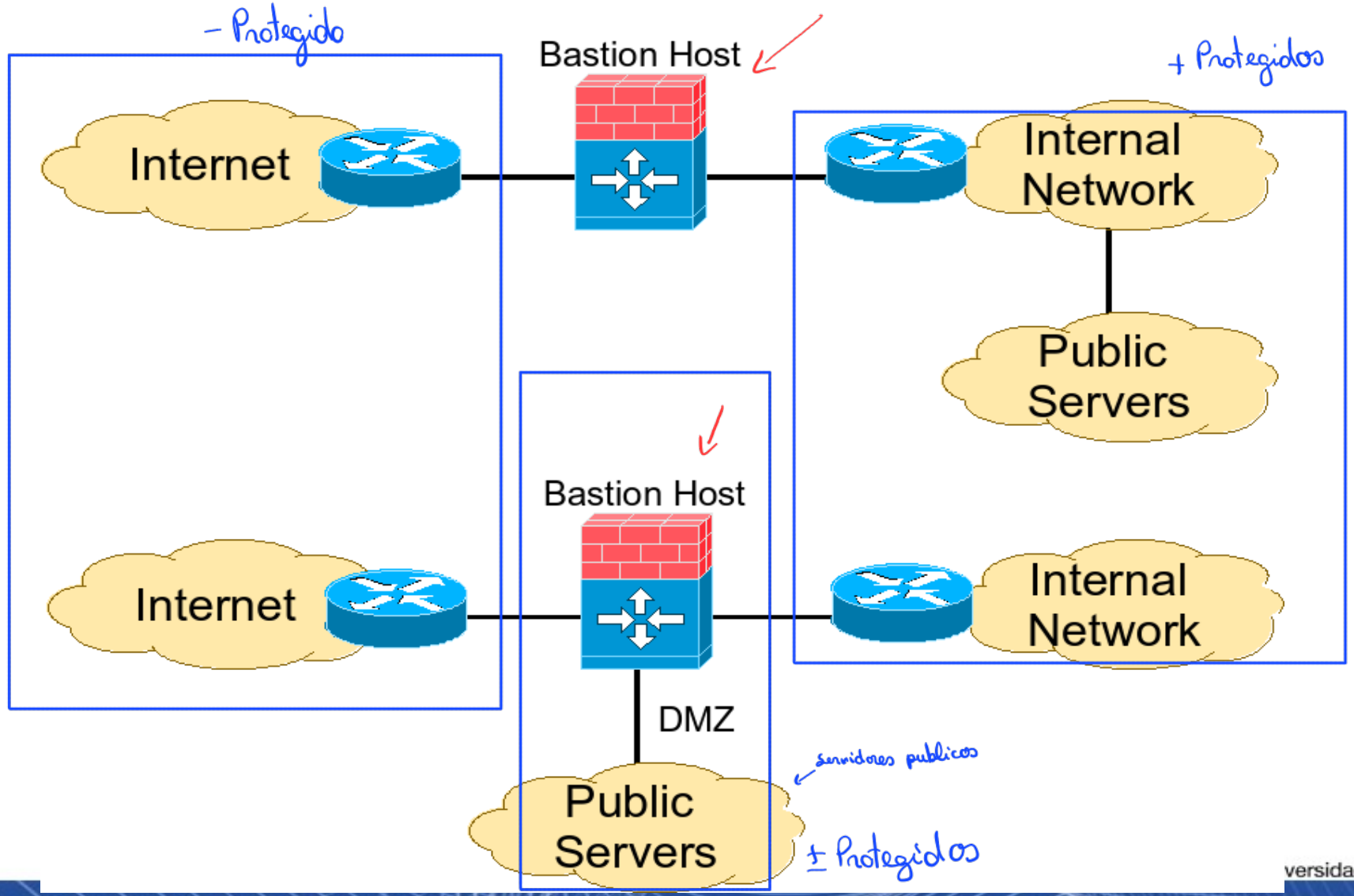


Bastion Host

- Computer that is fully exposed to attacks
- Located on the public side of the demilitarized zone (DMZ)
- Application-level gateway (redirects traffic to servers on DMZ)
- They must be designed and configured to minimize the chances of penetration
- All unnecessary services, protocols, programs, and network ports are disabled or removed
- Some bastions are deliberately exposed to potential hackers to both delay and facilitate tracking of attempted break-ins

Firewall Architectures
Most common

- Dual-Homed (without and with DMZ)



Personal firewalls

- Personal firewalls protect against external attacks by limiting access to doors
- Personal firewalls help reduce the effects of already compromised or infected computers by limiting access to outbound doors
- Can be user unfriendly
  - Many pop-up windows → acabamos por aceitar a depois corre mal ...
  - User's limited know-how
  - User tendency to accept everything/always

Cisco's Access Control Lists (ACL)

↳ Condições para aceitar/nega um pacote!

Firewall de rede!

- An access list is a sequential collection of permit and deny conditions
- IOS software tests packets against the conditions in an access list one by one
- The first match determines whether the software accepts or rejects the packet
  - Because the software stops testing conditions after the first match, the order of the conditions is critical
- If no conditions match, the software rejects the packet
- Can be applied to inbound or outbound traffic

↳ Se nada verificar, ele não passa

entrada ou saída!

ACL types

- **Standard**
  - Control traffic by the analysis of the source address of the IP packets
  - Numbered from 1 to 99
  - Example: access-list 1 permit 10.1.1.0 0.0.0.255
- **Extended**
  - Control traffic by the analysis of the source and destination addresses and protocol of the IP packets
  - Numbered from 100 to 199
  - Example: access-list 101 permit ip any 10.1.1.0 0.0.0.255
- **Named**
  - Allow standard and extended ACLs to be given names instead of numbers
  - Intuitively identify an ACL using an alphanumeric name
  - Eliminate the number limits that exist on standard and extended ACLs
  - Named ACLs provide the ability to modify ACLs without deleting and then reconfiguring them.
  - Example: ip access-list {extended | standard} name

ACL types

- Reflexive
  - Allow IP packets to be filtered based on upper-layer session information
  - Communication in one direction opens doors in the opposite direction
  - Generally used to allow outbound traffic and to limit inbound traffic in response to sessions that originate inside the network
- Context-Based Access Control (CBAC)
  - Inspects traffic to discover and manage state information for TCP and UDP sessions
  - This state information is used to create temporary openings in the firewall access lists

ACL usage

conjunto de comandos é aplicado numa interface e em que sentido "out" ou "in"

- There should be one access list per protocol per direction
- Standard access lists should be applied closest to the destination
- Extended access lists should be applied closest to the source
- The inbound or outbound interface should be referenced as if looking at the port from inside the router.
- Statements are processed sequentially from the top of the list to the bottom until a match is found. If no match is found then the packet is denied, and discarded
- There is an implicit deny any at the end of all access lists
- Access list entries should filter in the order from specific to general
- The router will send an ICMP host unreachable message to the sender of the rejected packet and will discard the packet

Cisco's Access Control Lists
Reflexive ACL

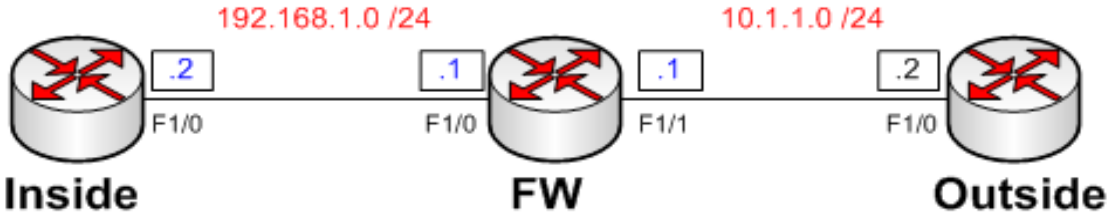
- We want to initiate telnet connections from Inside to Outside, and allow Outside to respond only if the connection was initiated from Inside. All other traffic should be denied.

```
ip access-list extended InsideACL
permit tcp 192.168.1.0 0.0.0.255 gt 1024 10.1.1.0 0.0.0.255 eq telnet reflect TelnetResponse
deny ip any any log

ip access-list extended OutsideACL
evaluate TelnetResponse
deny ip any any log

interface FastEthernet1/0
ip access-group InsideACL in

interface FastEthernet1/1
ip access-group OutsideACL in
```



- The above configuration creates an ACL named InsideACL which allows telnet traffic from Inside to Outside. Any traffic permitted by the ACL causes a temporary entry in the reflexive ACL named TelnetResponse to be created, with the source and destination addresses and port numbers reversed. All other traffic from Inside is denied and logged. An ACL named OutsideACL was also created, which first evaluates the reflexive ACL we created. Anything not permitted by the reflexive ACL is denied and logged.

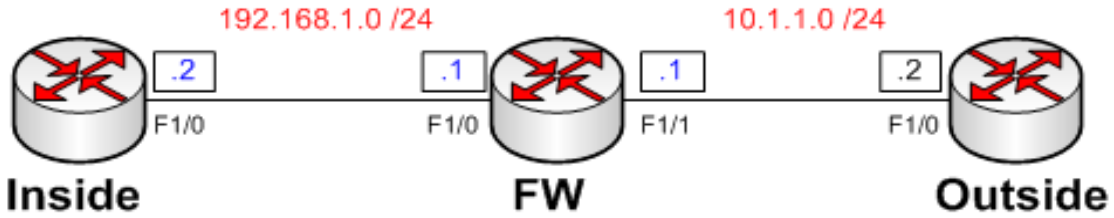
Cisco's Access Control Lists
CBAC

```
ip access-list extended InsideACL
 permit tcp 192.168.1.0 0.0.0.255 gt 1024 10.1.1.0 0.0.0.255 eq telnet
 deny ip any any log

ip access-list extended OutsideACL
 deny ip any any log
ip inspect name AllowTelnet telnet

interface FastEthernet1/0
 ip access-group InsideACL in
 ip inspect AllowTelnet in

interface FastEthernet1/1
 ip access-group OutsideACL in
```



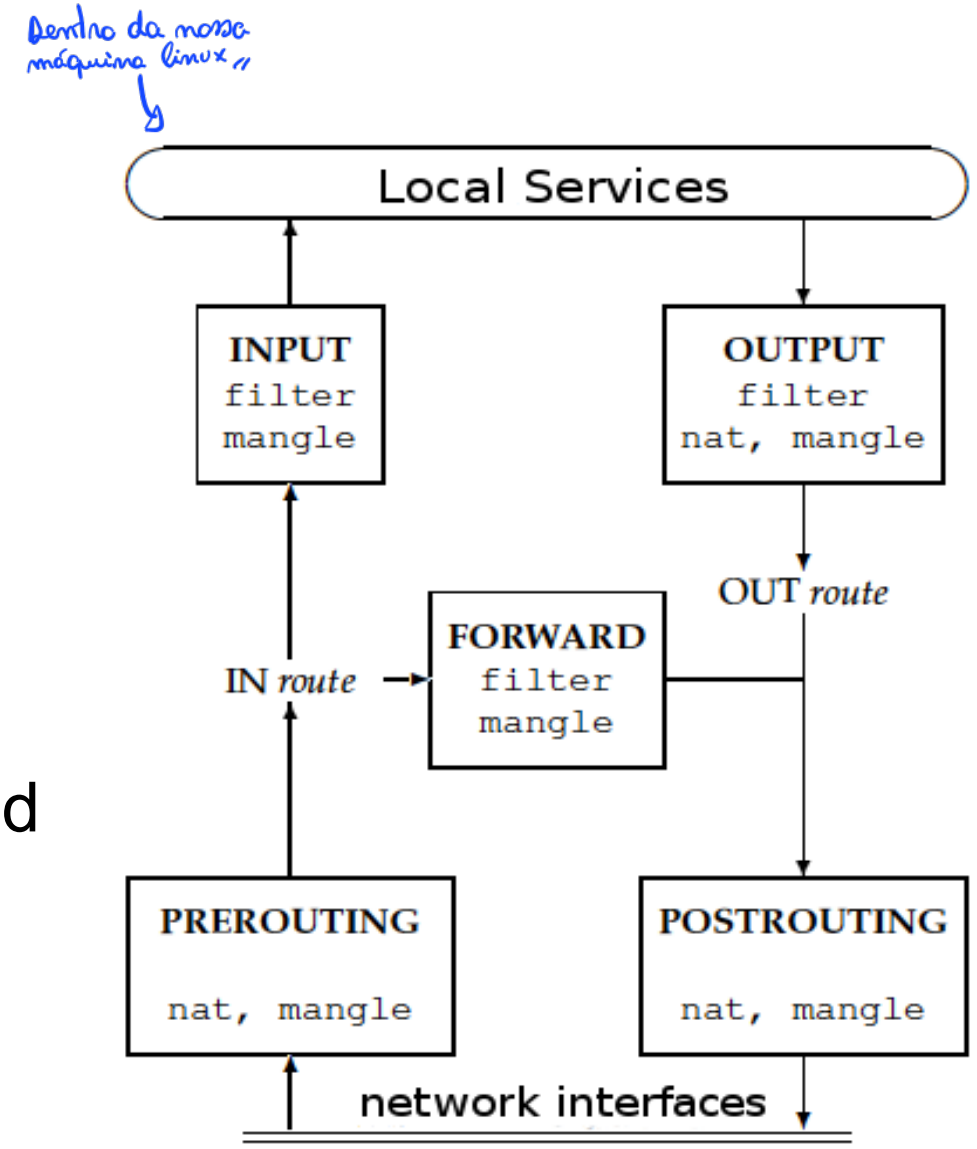
- The above configuration creates an ACL named InsideACL which allows telnet traffic from Inside to Outside and denies everything else.
- Next, it creates an ACL named OutsideACL which denies everything coming from Outside. It also creates an inspection rule named AllowTelnet which inspects Telnet traffic from Inside to Outside and allows response traffic from Outside, which our OutsideACL would have otherwise denied.

Linux IPtables ⇒ Igual à ACL da Cisco

- Name of the user space tool by which administrators create rules for the packet filtering and NAT modules
- Used to set up, maintain, and inspect the tables of IP packet filtering rules within the Linux kernel
- Has 3 default tables
  - FILTER
    - is responsible for filtering (blocking or permitting a packet to proceed)
    - every packet passes through the filter table
    - is the default table if no other is specified
  - NAT
    - is responsible for setting up the rules for rewriting packet addresses or ports
    - the first packet in any connection passes through this table: any verdicts here determine how all packets in that connection will be rewritten
  - MANGLE
    - is responsible for adjusting packet options, such as quality of service

Linux IPtables

- Each table contains chains
  - Built-in chains (INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING)
  - User-defined chains
- Connection tracking capability
- Rate-limited connection and logging capability
- Clear separation of packet filtering and NAT



Linux IPtables

- In addition to the built-in chains, the user can create any number of user-defined chains within each table, which allows them to group rules logically
- Each chain contains a list of rules
  - when a packet is sent to a chain, it is compared against each rule in the chain in order
- The rule specifies what properties the packet must have for the rule to match
  - such as the port number or IP address
- If the rule does not match then processing continues with the next rule
- If, however, the rule does match the packet, then the rule's target instructions are followed (and further processing of the chain is usually aborted)
- Some packet properties can only be examined in certain chains
  - Ex. the outgoing network interface is not valid in the INPUT chain
- Some targets can only be used in certain chains, and/or certain tables
  - for example, the SNAT target can only be used in the POSTROUTING chain of the NAT table
- The target of a rule can be the name of a user-defined chain or one of the built-in targets ACCEPT, DROP, RETURN, DNAT, SNAT and MASQUERADE
- Can think of a target in the same way as a subroutine

Firewall Limitations

↳ O problema é quando recebemos por email e abrimos algum Malware ⇒ Precisamos de monitorizar o trafego dentro da rede

- Ineffective against inside attackers or attacks from internal compromised machines (zombies)
  - Solution: Usage of multiple internal firewalls
- Can only control open traffic at the network entry point
  - Backdoor entrances: uncontrolled modems and WLAN APs
  - Cyphered traffic: VPN, IP tunnels over HTTP/ICMP/etc, SSH and IPsec Tunnels
- Hard to manage in networks with heterogeneous interests and requirements
  - Example: Universities and ISPs

IPsec

↳ Ligações seguras entre redes IP

IPSec

- Framework of security protocols and algorithms used to secure data at the network layer
- Authentication Header (AH) → Autenticação
  - Ensures data integrity
  - Does not provide confidentiality
  - Provides origin authentication
  - Uses Keyed-hash mechanisms

- Encapsulating Security Payload (ESP) → Cifra da informação
  - Provides data confidentiality (encryption)
  - Data Integrity
  - Does not protect IP header

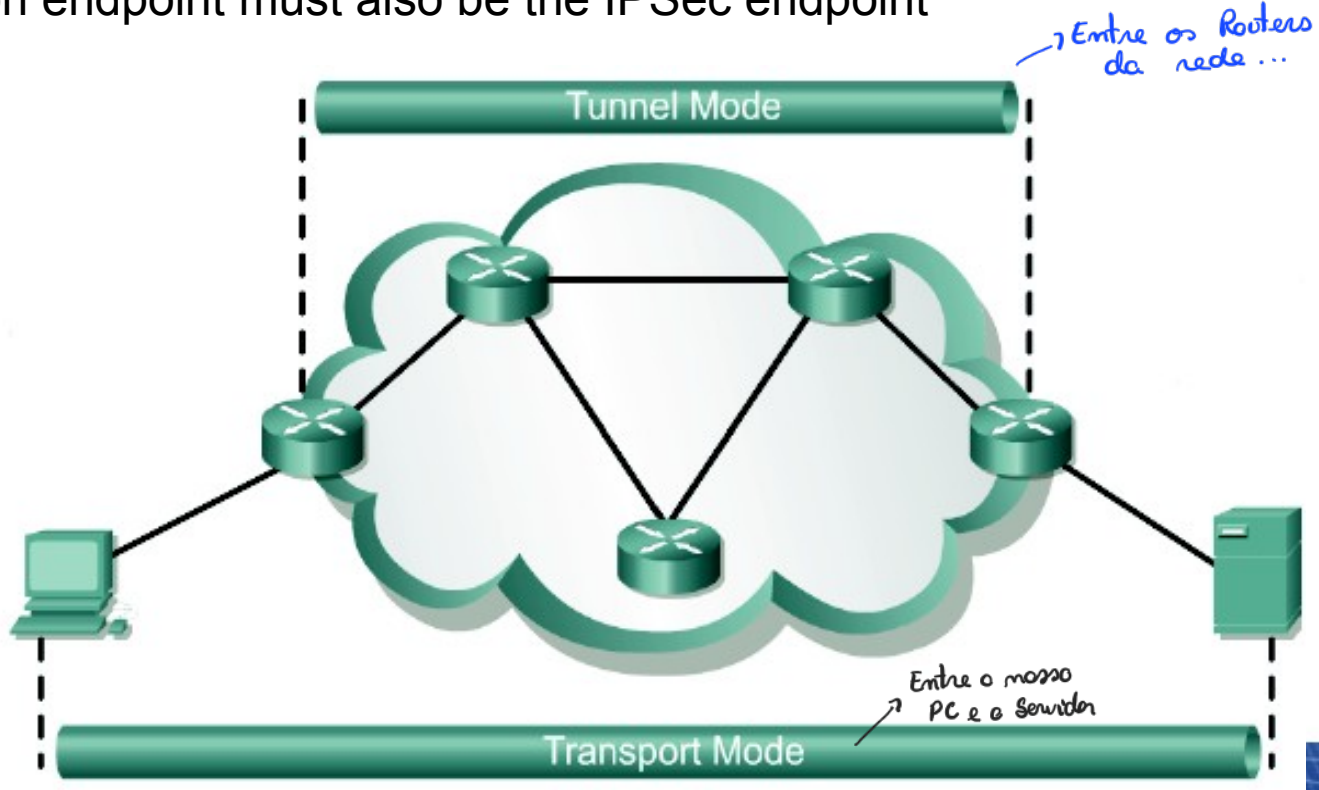
↳ Mesmo que alguem os consiga ver eles estão cifrados (...)

- AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible

Usamos o IKE primeiro para criptografia publica ...

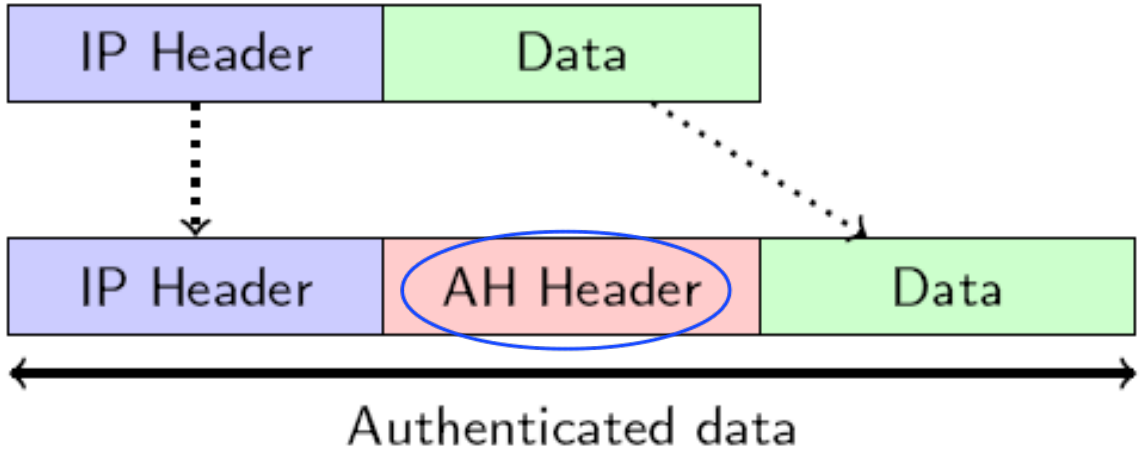
IPSec Modes

- Tunnel
  - IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels
  - End-hosts are not aware of IPSec being used to protect their traffic
  - IPSec gateways provide transparent protection over untrusted networks
- Transport ~> Tens de proteger/autenticar também o IP Header (não só a Data)
  - Each end host does IPSec encapsulation of its own data, host-to-host.
  - IPSec has to be implemented on end-hosts
  - The application endpoint must also be the IPSec endpoint

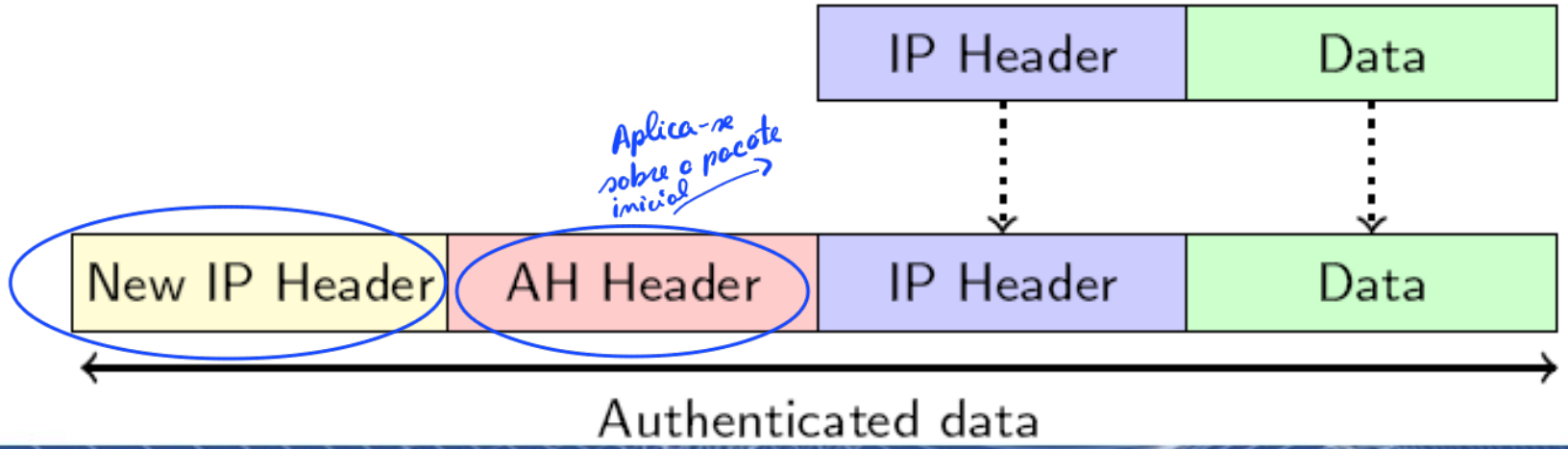


IPSec - AH header placement

- Transport mode (PC- server)

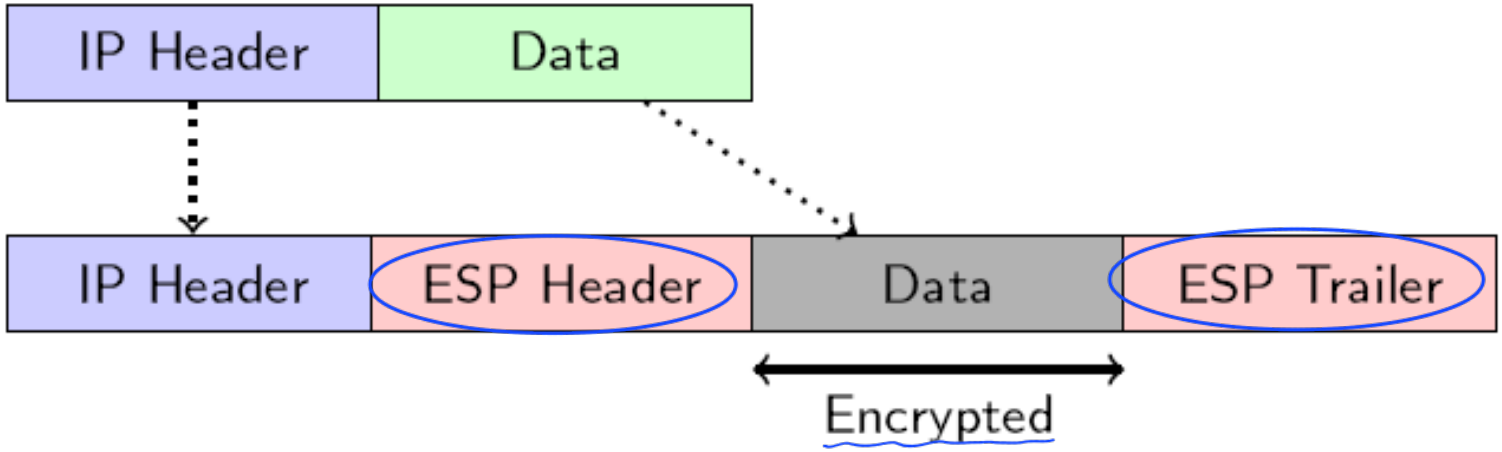


- Tunnel mode (entre Routers)

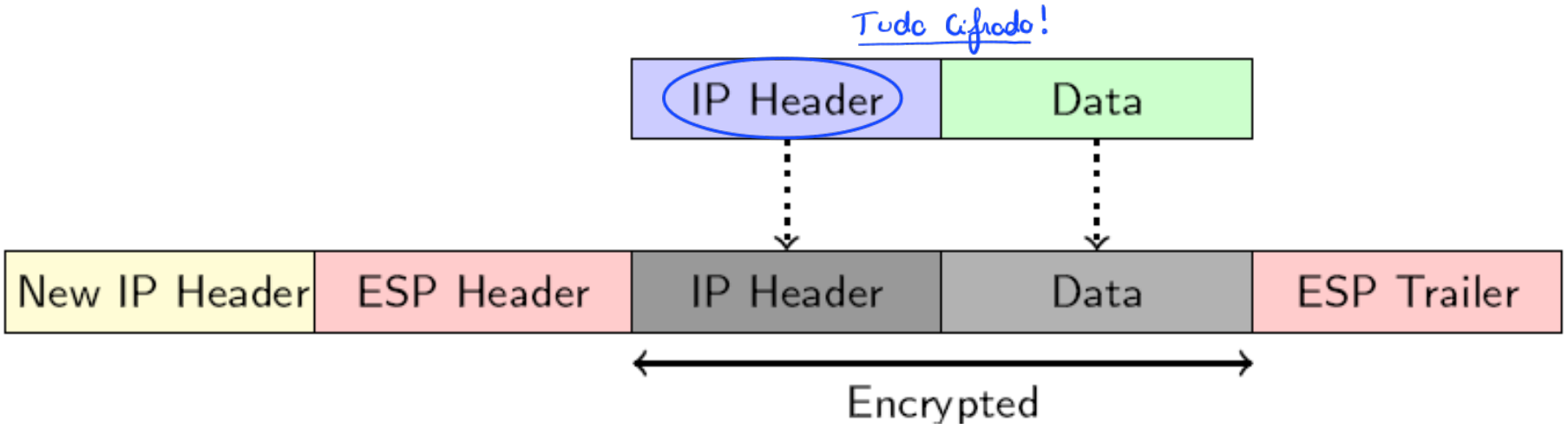


IPSec - ESP header placement

- Transport mode

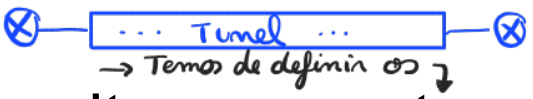


- Tunnel mode



IPSec - Security Associations

- SAs represent a policy contract between two peers or hosts
- Describe how the peers will use IPSec security services to protect network traffic



- An SA contains the following security parameters:
  - Authentication/encryption algorithm, key length and other encryption parameters (e.g. key lifetime, ...)
  - Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically
  - A specification of network traffic to which the SA will be applied (e.g. IP traffic or only TELNET sessions)
  - IPSec AH or ESP encapsulation protocol and tunnel or transport mode

IKE and IPsec

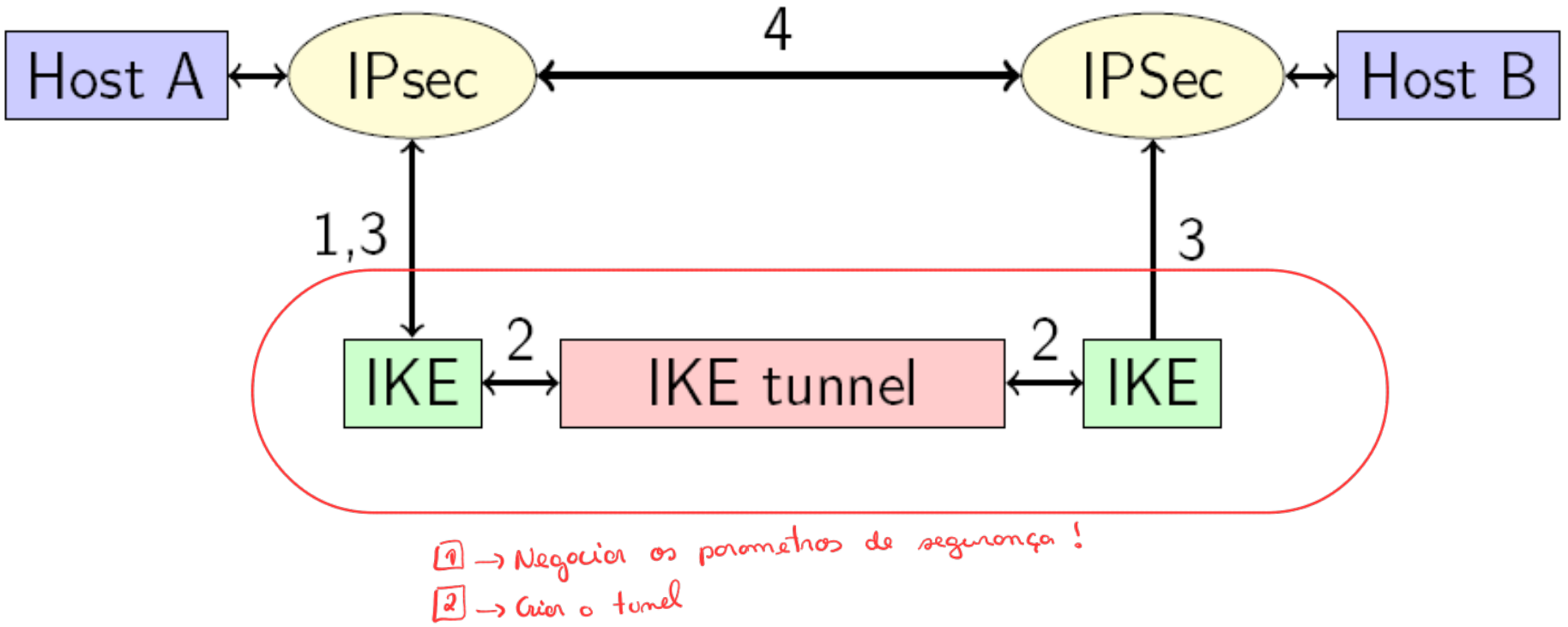
→ Negociação dos parâmetros antes de criarmos o tunel !"

- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference

→ Também tem de ser segura !"

- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certication authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE provides three methods for two-way authentication:
  - Authentication using a pre-shared secret (PSK)
  - Authentication using RSA encrypted nonces
  - Authentication using RSA signatures

IKE and IPsec



IKE and IPsec – Modes

- IKE modes control an eciency-versus-security tradeo during initial IKE key exchange
- Main mode
  - Requires six packets back and forth
  - Provides complete security during the establishment of an IPsec connection
- Aggressive mode
  - Uses half the exchanges
  - Provides less security because some information is transmitted in cleartext

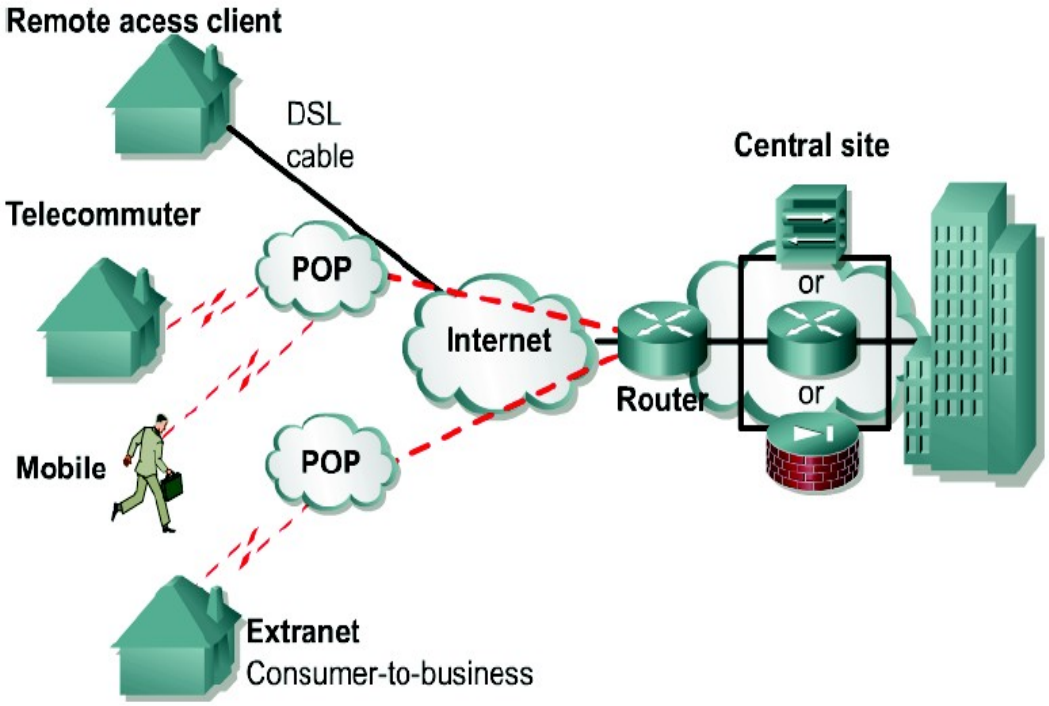
IKE and IPsec

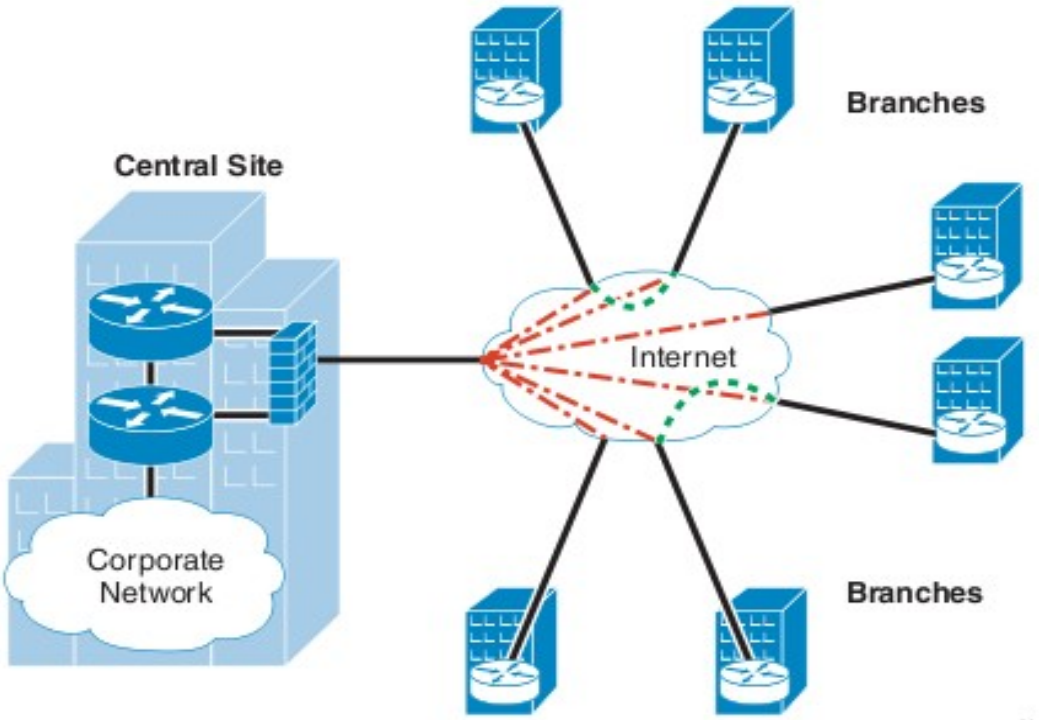
- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference
- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certication authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE provides three methods for two-way authentication:
  - Authentication using a pre-shared secret (PSK)
  - Authentication using RSA encrypted nonces
  - Authentication using RSA signatures

Virtual Private Networks

VPN - Virtual Private Networks

- Is an encrypted connection between private networks over a public network





- Remote Access VPN
- Site-to-Site VPN

VPN types

- Remote Access VPN
  - PPTP
  - L2TP/IPsec
  - SSL/TLS VPN
    - Web VPN (client-less SSL VPN) – VPN client can be a standard browser
  - SSH VPN
  - Open VPN
- Site-to-Site VPN
  - IPsec VPN
    - With static or dynamic configuration
  - IPsec + GRE VPN
    - Dynamic Multipoint VPN

Remote Access VPN - PPTP VPN

- Based on PPTP
  - PPTP packages data within PPP packets
  - Encapsulates the PPP packets within IP packets
- Uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination
- Supports authentication based on protocols PAP, EAP, CHAP, MS-CHAPv1 and MS-CHAPv2
- Uses MPPE as cipher
  - Has two different keys (one for each direction)
  - Requires MS-CHAPv2 authetication
  - Keys derived from the MS-CHAPv2's password hash and challenges
- PPTP creates a TCP control connection between the VPN client and VPN server to establish a tunnel
  - Uses TCP port 1723 for these connections
- PPTP can support only one tunnel at a time for each user

Remote Access VPN - L2TP/IPSec VPN

- Authentication can be performed with Digital Certificates (RSA) or with the same PPP authentication mechanisms as PPTP
- Provides data integrity, authentication of origin and replay protection
- Encryption provided by IPSec (ESP protocol)
- Can support multiple, simultaneous tunnels for each user
- Slower performance than PPTP

Other Remote Access VPN types

- SSL/TLS VPN
  - SSL/TLS protocol handles the VPN tunnel creation
  - SSL/TLS is much easier to implement than IPSec and provides a simple and well-tested platform
  - RSA handshake (or DH) is used exactly as IKE in IPSec
- SSH VPN
  - VPN over a SSH connection
  - SSH tunneling - port forwarding
- OpenVPN
  - Implements a SSL/TLS VPN
  - Allows PSK, certicate, and login/password based authentication
  - Encryption provided by OpenSSL (can use all ciphers available)
  - Compatible with dynamic and NAT addresses

Variants of Site-to-Site IPsec VPN

- IPsec tunnels with static configuration
  - Requires the knowledge of all peers (IP addresses and security parameters)
  - High configuration overhead
- IPsec tunnels with dynamic configuration (at the headend/hub)
  - Hub + spokes configuration
  - Generic configuration at the headend/hub
  - Easy to add new sites
- A basic IPsec tunnel can't protect multicast traffic.
- IPsec + GRE tunnels
  - Generic Routing Encapsulation (GRE) allows the protection of multicast traffic over IPsec
  - Dynamic Multipoint VPN (DMVPN)