In the Name of Allah

Virtual Private Network

Present by

Ali Fanian

Virtual Private Networks

- Introduction
- What security problems do VPNs solve ?
- What security problems are not solved by VPNs ?
- VPN Principles of operation: tunneling, encapsulation, encryption and authentication
- VPN Technologies: Microsoft PPTP, L2TP and IPsec

History and background of VPNs 1

Internet multi-site organisations operated private networks using leased lines. This approach was expensive and inflexible.

It became cheaper to use shared Internet than dedicated.

Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate

VPNs enabled more flexible use of larger networks by removing network geography constraints from shared-insider LAN/Intranet associations and services.

With cryptography as part of a VPN, a travelling saleseman could communicate with head office at lower risk from spying competitors etc.

What problems do VPNs solve ?

- Avoiding costs of fixed lines.
- Extending security context of LAN across sites, regardless of geography, including to mobile users.
- Authentication: knowing who your users are.
- Encryption: preventing monitoring of use of insecure client server applications at the network level.

What security problems do VPNs not solve ?

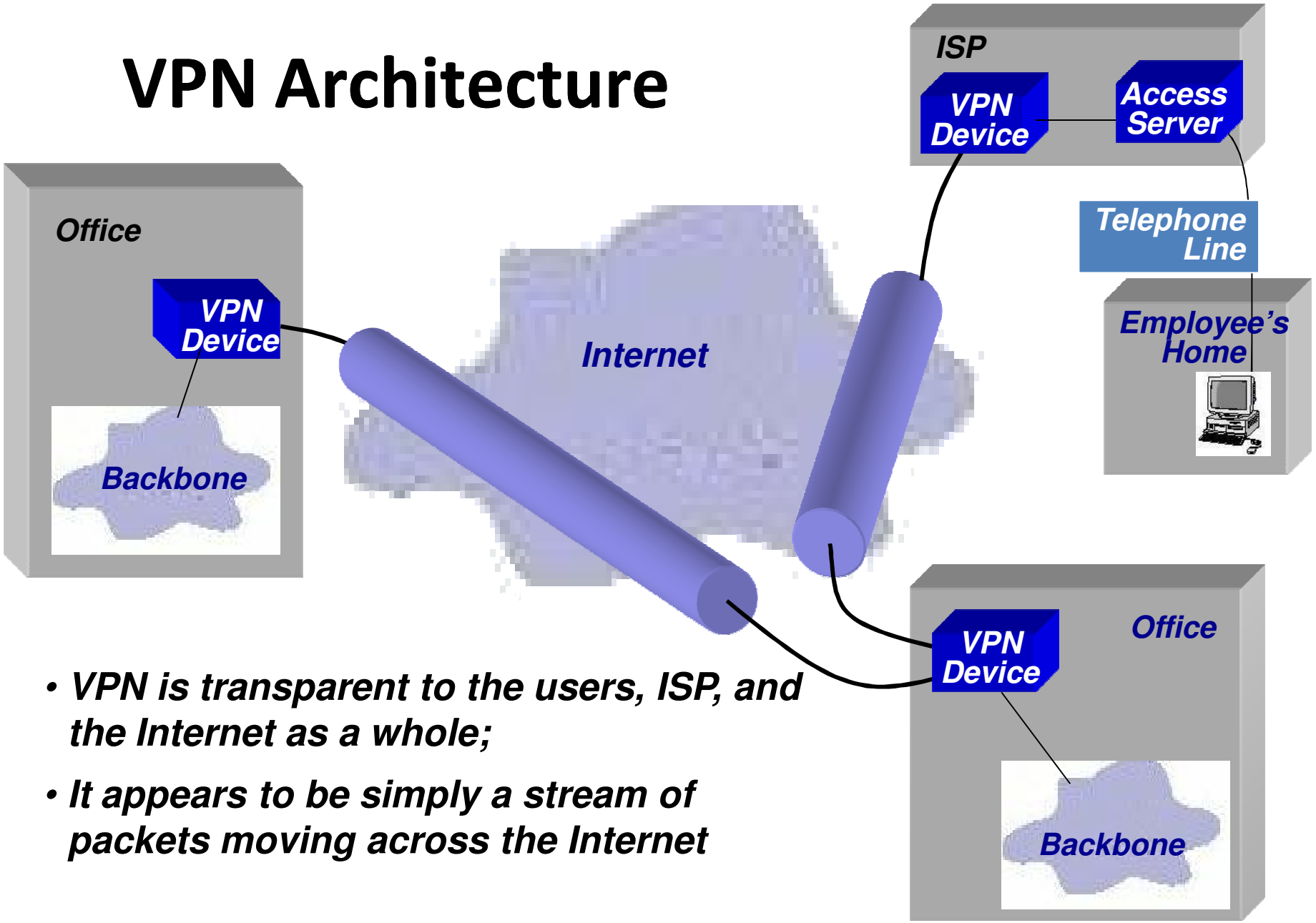
- Having a VPN which isn't secure and not knowing this is probably worse than having no VPN
- Traffic analysis: monitoring of packet sizes, network usage times, endpoints of conversation etc.
- VPNs can be used to pierce firewalls, by encapsulating traffic prohibited by organisation policy within a firewalled perimeter which the firewall can't inspect or control.

Tunneling

Typically a VPN consists of a set of point to point connections tunnelled over the Internet.

The routers carrying this traffic over the Internet see each P2P connection externally as a sequence of packets routed between endpoints.

VPN Architecture



- *VPN is transparent to the users, ISP, and the Internet as a whole;*
- *It appears to be simply a stream of packets moving across the Internet*

Encapsulation

In order to achieve tunnelling, the packets including payloads, to and from addresses, port numbers and other standard protocol packet headers are encapsulated as the payload of packets as seen by the external routers carrying the connection.

Authentication

A digital signing scheme is typically used to enable verification of the VPN principals. Note that both the client and the server need to authenticate each other.

Message authentication codes, hashes or checksums are typically used to authenticate message contents.

Encryption

To protect the privacy of the connection from external snooping, the payload of the packets visible externally will be encrypted.

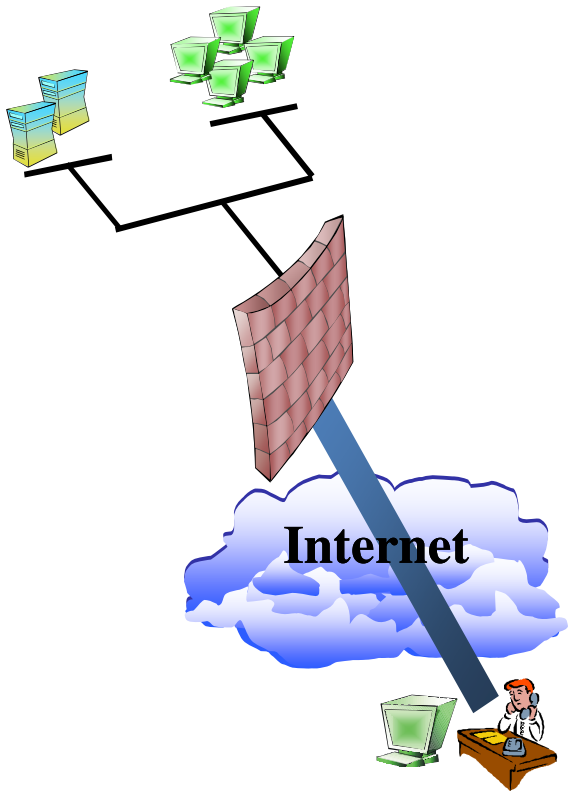
To enable routing over conventional networks, the packet headers of the encapsulating packets are not encrypted, but the packet headers of the encapsulated packets are encrypted along with their contents.

VPN Topology: Types of VPNs

- Remote access VPN
- Site-to-Site VPN

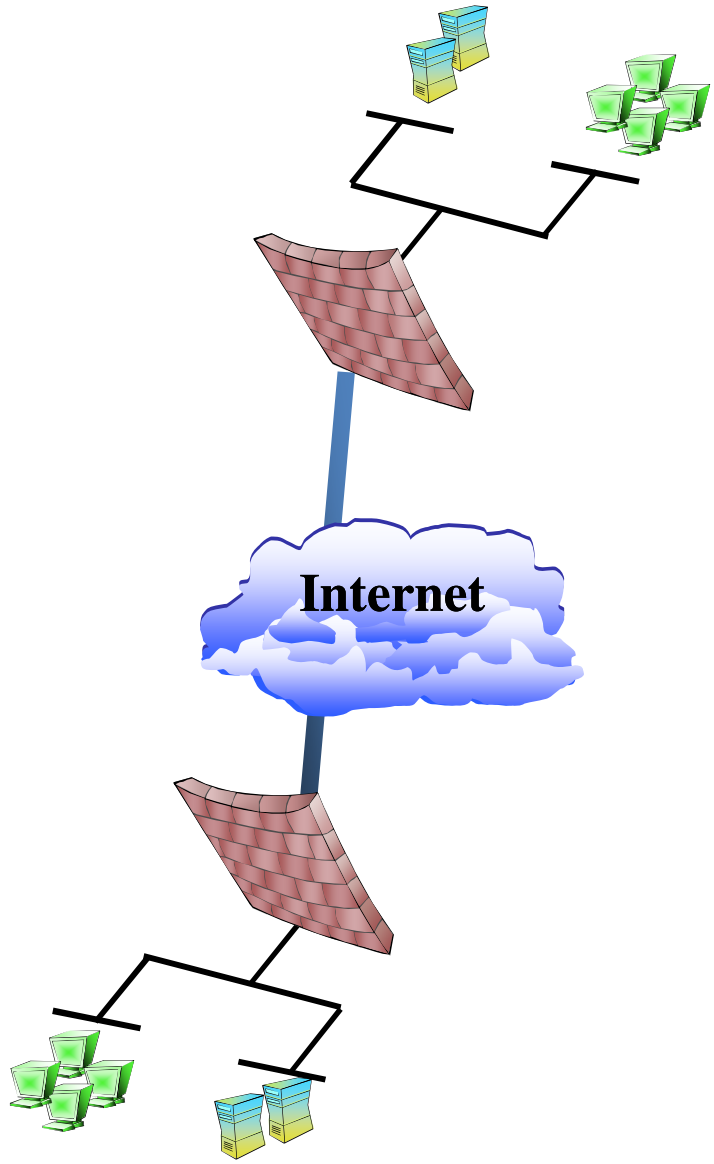
Types of VPNs

- **Remote Access VPN**
  - Provides access to internal corporate network over the Internet.
  - Reduces long distance, modem bank, and technical support costs.



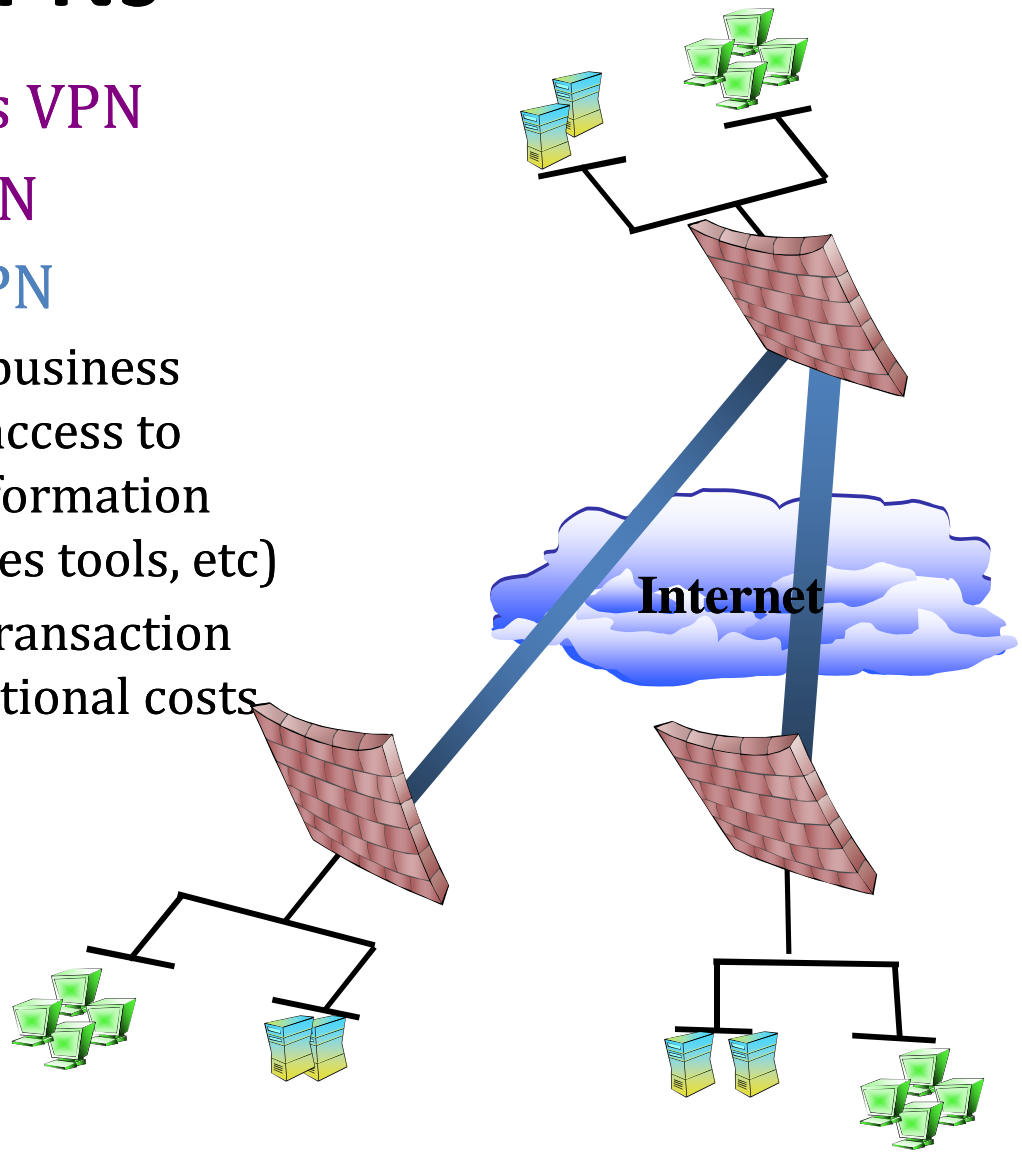
Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
  - Connects multiple offices over Internet
  - Reduces dependencies on frame relay and leased lines



Types of VPNs

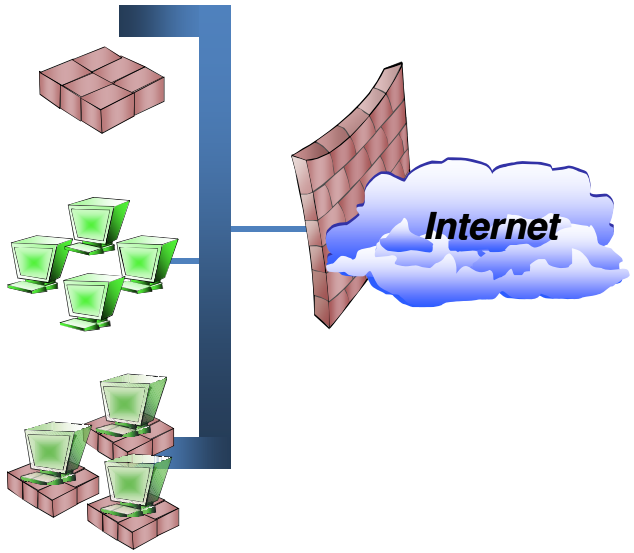
- Remote Access VPN
- Site-to-Site VPN
  - Extranet VPN
    - Provides business partners access to critical information (leads, sales tools, etc)
    - Reduces transaction and operational costs



Types of VPNs

- Remote Access VPN
- Site-to-Site VPN
  - Extranet VPN
  - Intranet VPN:

Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.



VPN Topology: How it works

- Operates at layer 2 or 3 of OSI model
  - Layer 2 frame – Ethernet
  - Layer 3 packet – IP

VPN Components: Protocols

- IP Security (IPSec)
  - Transport mode
  - Tunnel mode
- Point-to-Point Tunneling Protocol (PPTP)
  - Uses PPP (Point-to-Point Protocol)

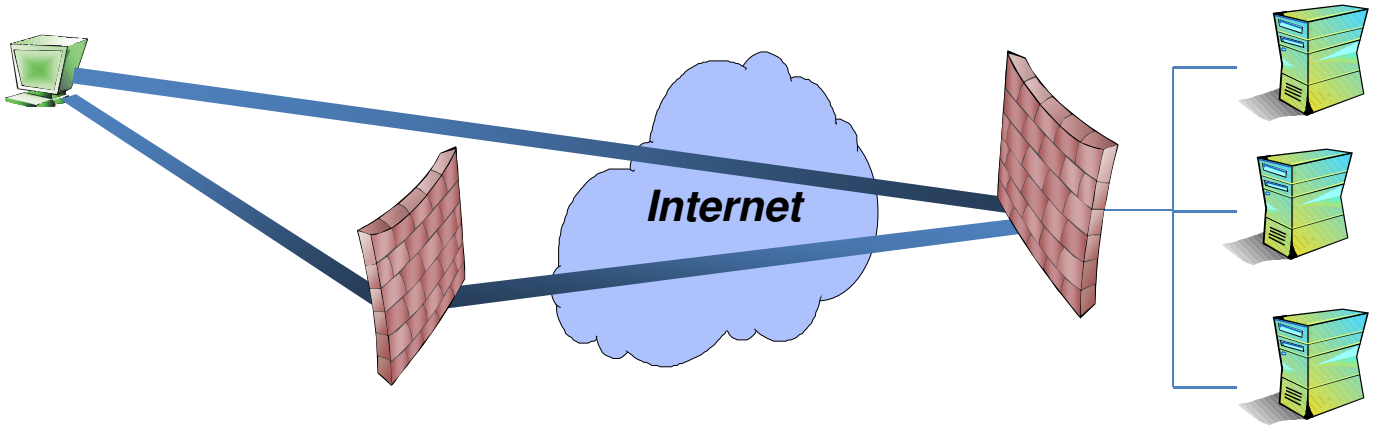
VPN Components: Protocols

- Layer 2 Tunneling Protocol (L2TP)
  - Exists at the data link layer of OSI
  - Composed from PPTP and L2F (Layer 2 Forwarding)
  - Compulsory tunneling method

Point-to-Point Tunneling Protocol (PPTP)

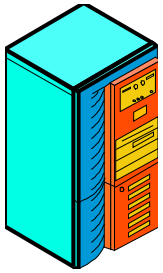
- Layer 2 remote access VPN distributed with Windows product family
  - Based on Point-to-Point Protocol (PPP)

- Uses proprietary authentication and encryption
- Limited user management and scalability



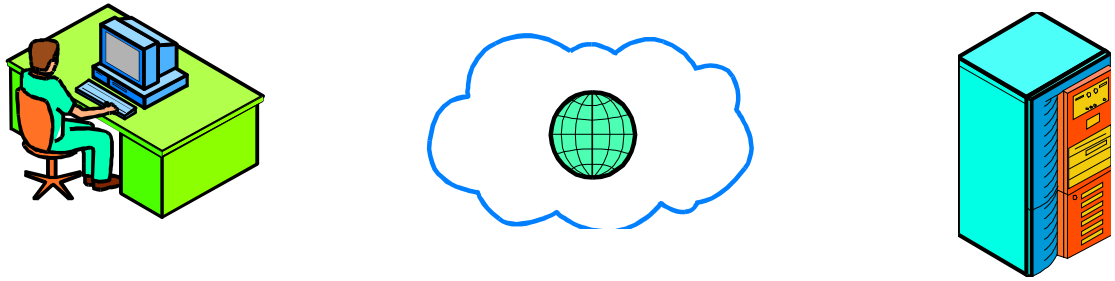
PPP

- *Point-to-Point Protocol (PPP)*
  - PPP was created for dialing into a local RAS server
  - But the site's RAS may be far away
  - Long-distance calls are expensive



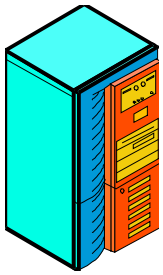
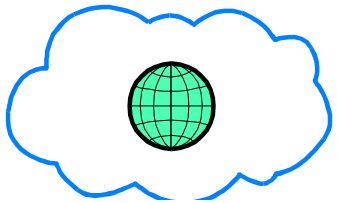
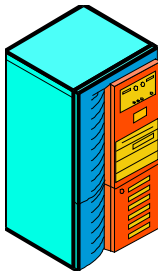
PPTP

- Point-to-Point Tunneling Protocol (PPTP)
  - We would like PPP to work over the Internet to avoid long-distance telephone charges
  - But PPP is only a data link layer protocol
  - It is only good for transmission within a subnet (single network)



PPTP

- The Point-to-Point Tunneling Protocol (PPTP) makes this possible
  - Created by Microsoft
  - Widely used

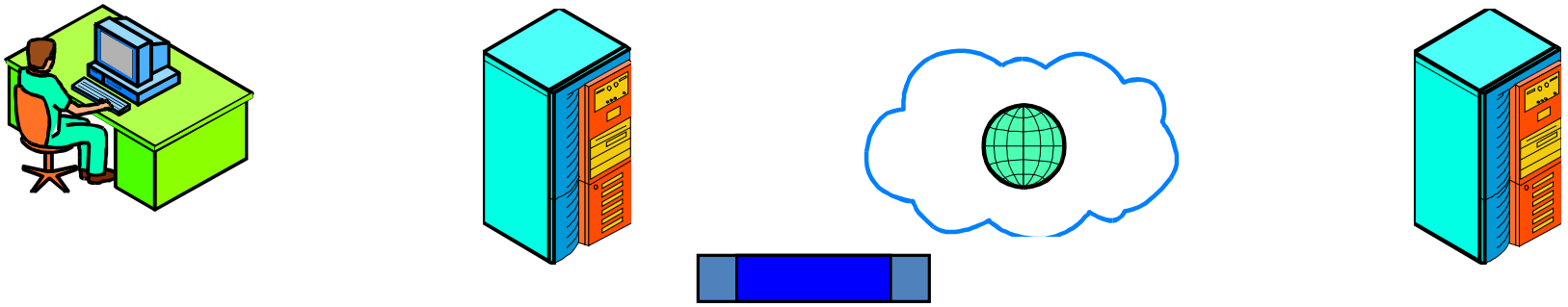





PPTP

- PPTP Operation
  - User dials into local PPTP *access concentrator* host
  - User sends the access concentrator a PPP frame within an IP packet

PPTP

- PPTP Operation
  - Access concentrator places incoming IP packet within another IP packet
  - Sends packet to the distant *RAS*

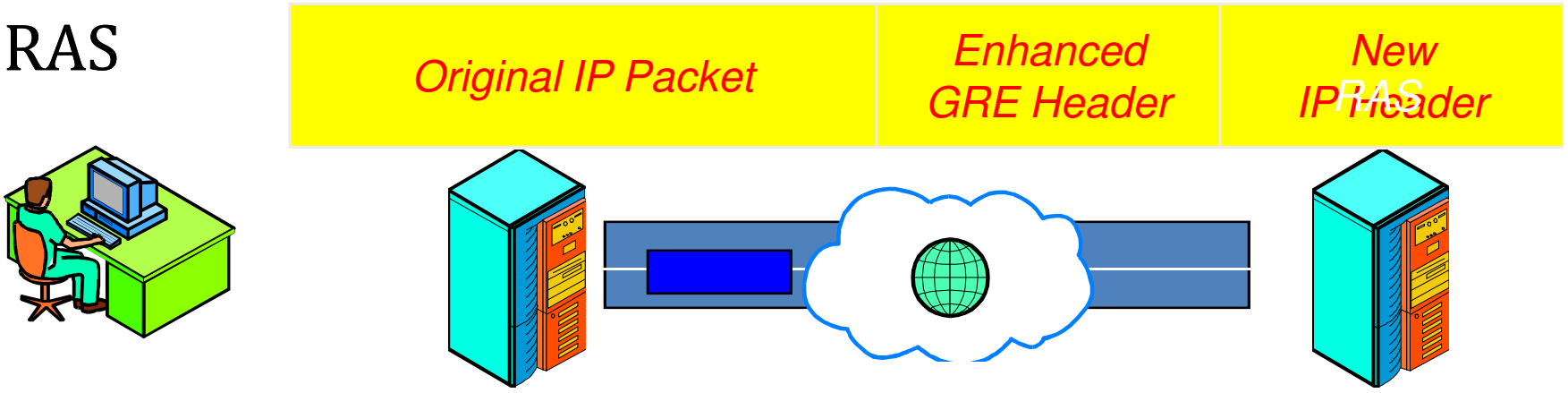


PPTP

- PPTP Operation
  - Distant RAS removes the original packet
  - Deals with the PPP frame within the packet

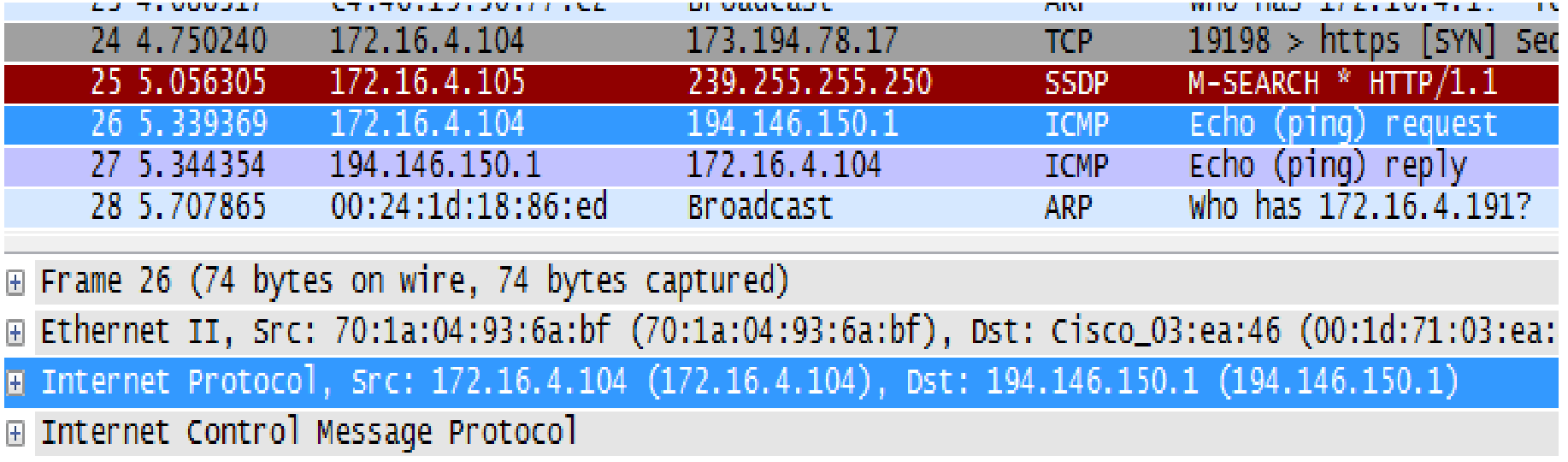
PPTP

- PPTP Encapsulation
  - Access concentrator receives the original IP packet, which has the IP address of the access concentrator
  - Adds an *enhanced general routing encapsulation (GRE)* header for security
  - Adds a new IP header with the IP address of the RAS



```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.4.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.4.1
```



```
PPP adapter VPN Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.17.37.203
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.4.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.4.1
```

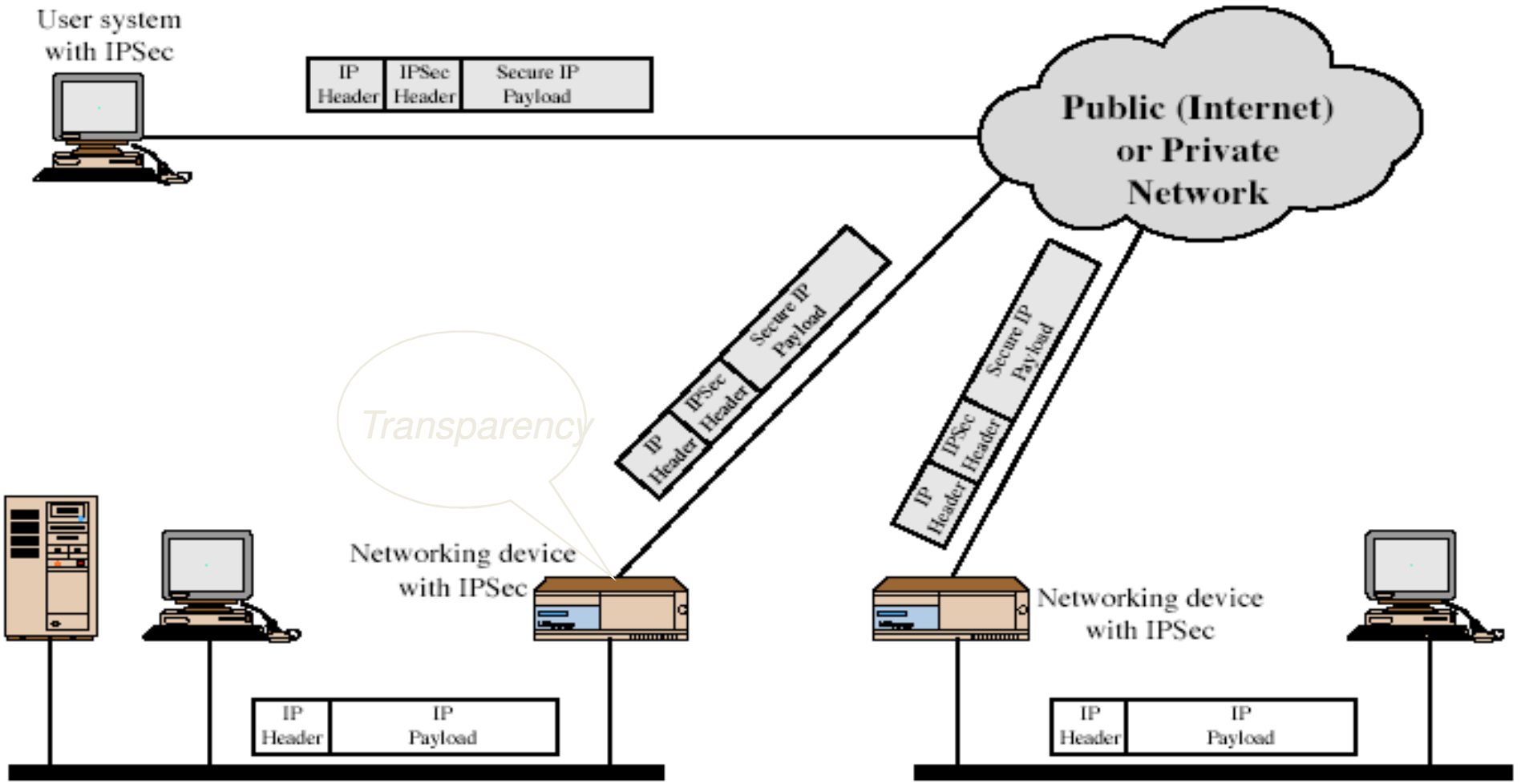
12 1.454983	172.17.37.203	194.146.150.1	ICMP	Echo (ping) request
13 1.459960	194.146.150.1	172.17.37.203	ICMP	Echo (ping) reply
14 1.503097	172.16.4.53	172.16.4.255	NBNS	Name query NB WPAD.
15 1.559756	172.16.4.104	1.1.1.1	GRE	Encapsulated PPP
16 1.820381	172.16.4.93	172.16.4.255	NBNS	Name query NB ISATA
17 1.917758	172.17.2.121	255.255.255.255	NBNS	Name query NB ISATA
18 2.017780	172.16.4.104	1.1.1.1	GRE	Encapsulated PPP
19 2.254888	00:24:1d:75:2d:fb	Broadcast	ARP	Who has 172.16.4.2?
20 2.308586	00:24:1d:18:86:ed	Broadcast	ARP	Who has 172.16.4.19

- Frame 12 (107 bytes on wire, 107 bytes captured)
- Ethernet II, Src: 70:1a:04:93:6a:bf (70:1a:04:93:6a:bf), Dst: Cisco_03:ea:46 (00:1d:71:03:
- Internet Protocol, Src: 172.16.4.104 (172.16.4.104), Dst: 1.1.1.1 (1.1.1.1)
- Generic Routing Encapsulation (PPP)
- Point-to-Point Protocol
- Internet Protocol, Src: 172.17.37.203 (172.17.37.203), Dst: 194.146.150.1 (194.146.150.1)
- Internet Control Message Protocol

IPSec

- General IP Security mechanisms
- Provides
  - authentication
  - confidentiality
  - key management
- Applicable to use over LANs, across public & private WANs, & for the Internet

IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
Transparency
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

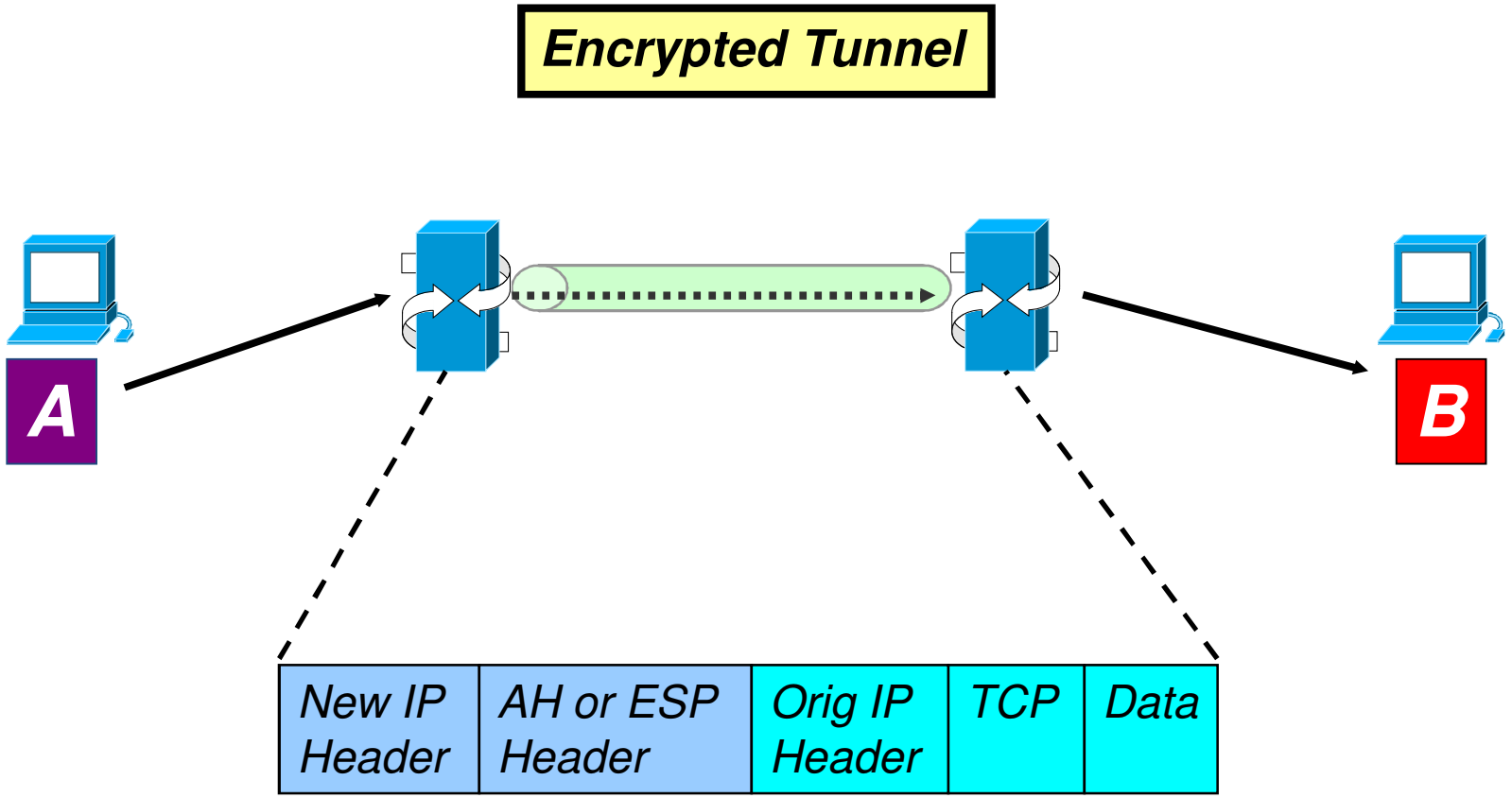
- Is below transport layer, hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users

Architecture & Concepts

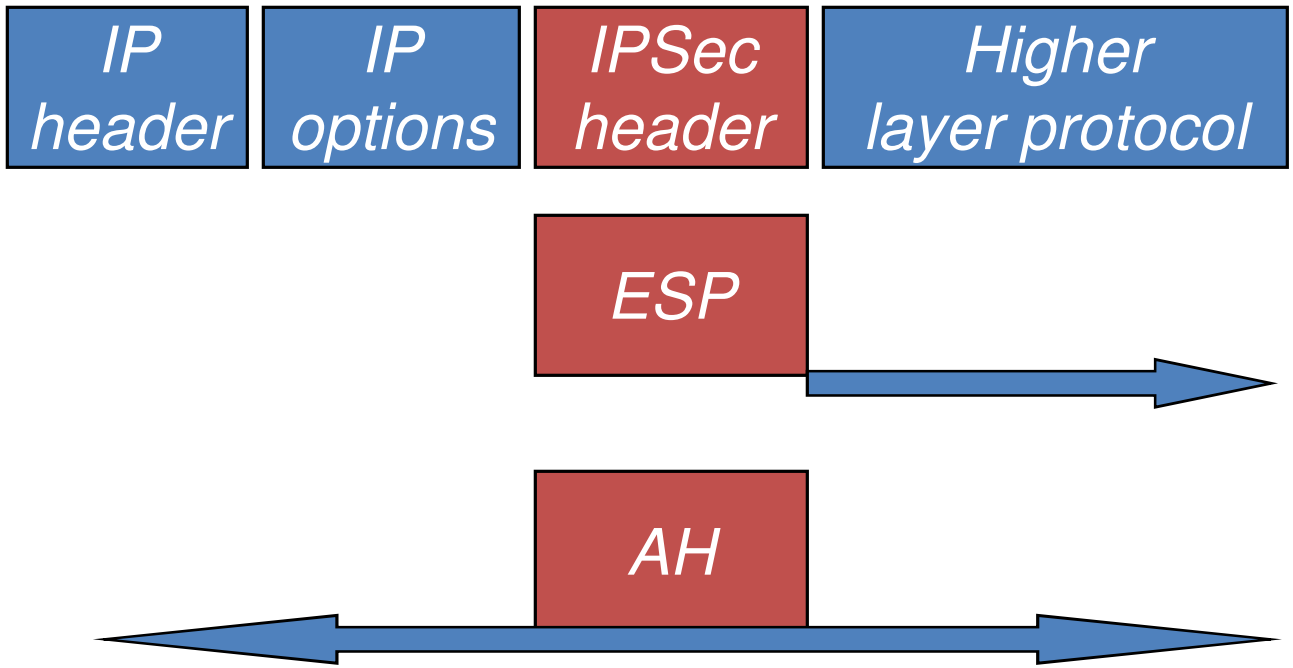
- Tunnel vs. Transport mode
- Security association (SA)
  - Security parameter index (SPI)
  - Security policy database (SPD)
  - SA database (SAD)
- Authentication header (AH) Protocol
- Encapsulating security payload (ESP) Protocol

Transport Mode vs. Tunnel Mode

- *Transport mode: host -> host*
- *Tunnel mode: host->gateway or gateway->gateway*

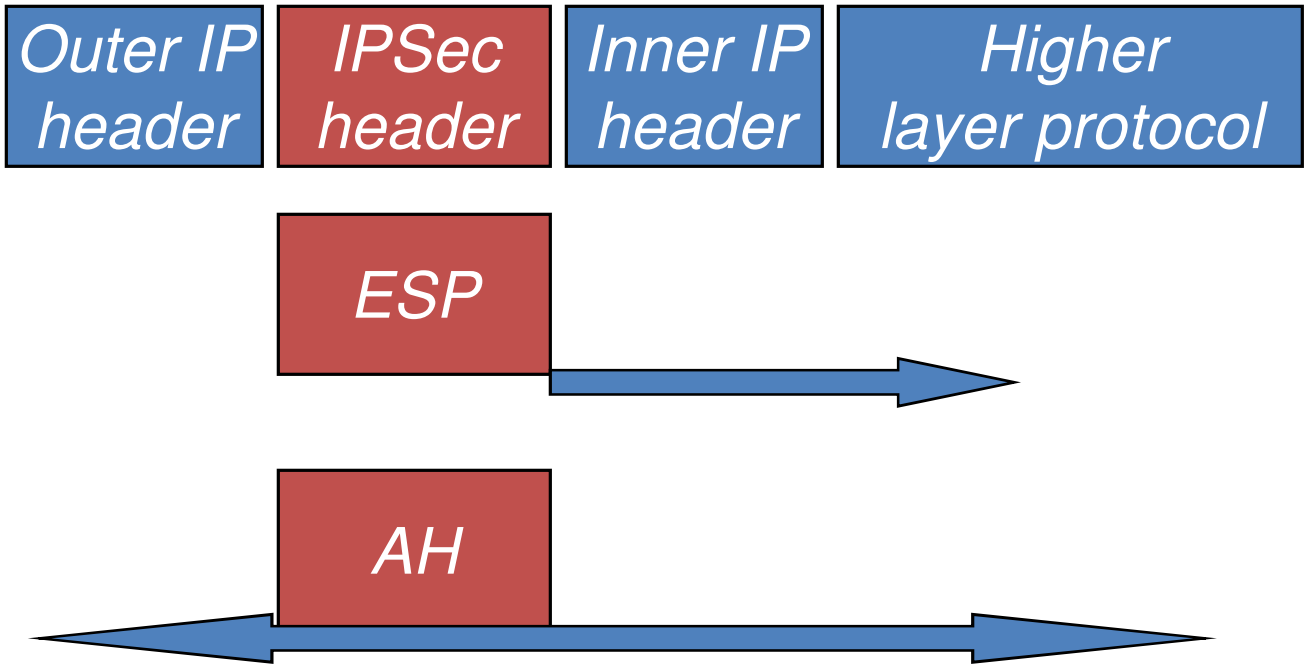


Transport Mode



- ESP protects higher layer payload only
- AH can protect IP headers as well as higher layer payload

Tunnel Mode



- ESP applies only to the tunneled packet
- AH can be applied to portions of the outer header

Security Association (SA)

- حاوی
  - الگوریتم ها
  - کلیدهای مورد نیاز
  - پروتکل AH یا ESP
  - زمان انقضاء کلید
  - پنجره جلوگیری از حمله تکرار
  - شماره آخرین بسته سالم دریافت شده
  - SPI
  - مشخصات ترافیکی که SA برای آن تولید شده است شامل:
    - آدرس مبدا و مقصد بسته
    - پروتکل لایه بالاتر
    - پورت های پروتکل لایه بالاتر

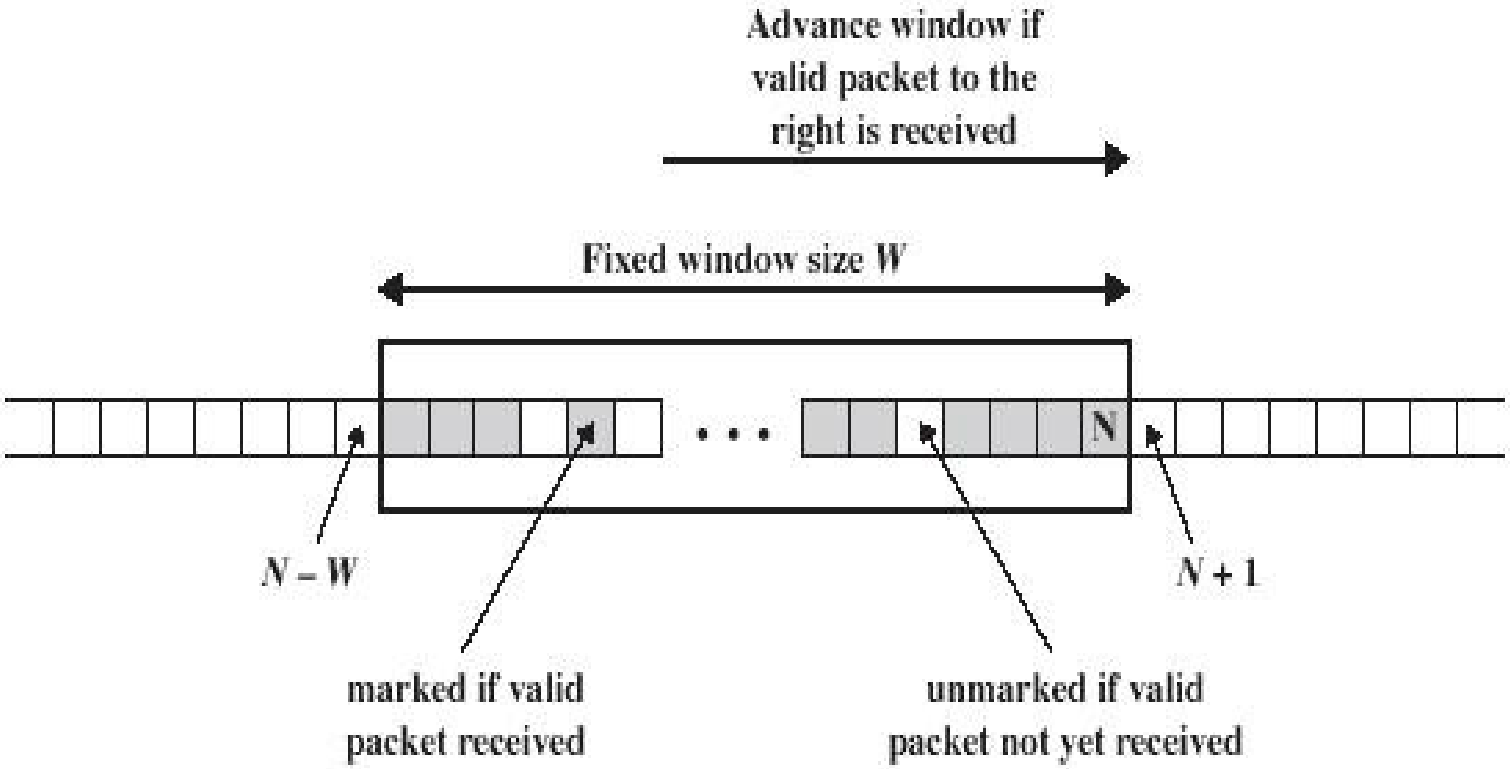
Security Association (SA)

- در یک جدول به نام SAD نگاه داری می گردد
- اندیس SA در جدول فوق توسط SPI مشخص می شود
- اتصال یک طرفه از فرستنده به گیرنده
  - برای ارتباط دو طرفه، دو SA مورد نیاز است
- کلیدها بایستی به نحوی مذاکره شود
  - Pre-shared key
  - IKE

جلوگیری از حمله تکرار

اختصاص یک شمارنده با مقدار صفر به هر ***SA***

افزایش شمارنده به ازای هر بسته جدید که با این ***SA*** فرستاده می شود



پروتکل مبادله کلید اینترنت (IKE)

- برای برقراری ارتباط بین دو طرف لازم است که یک *SA* بین طرفین ایجاد شود.
- برقراری و تجدید این *SA* ها می تواند بصورت دستی یا خودکار انجام گردد.
- پروتکلی که این وظیفه را (بصورت خودکار) در اینترنت به عهده دارد *IKE* می باشد

پروتکل مبادله کلید اینترنت (IKE)

- معرفی *IKE*
  - پروتکل اصلی برای ایجاد و ابقاء *IPSec SA*
  - پیش فرض *IPSec* برای مبادله امن کلید
  - فراهم کردن یک ارتباط امن بین طرفین باتوافق بر روی کلیدهای جلسه
  - متکی به مکانیزمهای رمز کلید عمومی و توابع درهم کلیددار

روشهای احراز اصالت

- روشهای احراز اصالت در *IKE*

۱- روش کلید از پیش مشترک (*Preshared Key*)

۲- روش امضای کلید عمومی (*Public Key Signature*)

۳- روش رمزکلید عمومی (*Public Key Encryption*)

٤- روش رمزکلید عمومی اصلاح شده (*Public Key Encryption Revised*)

پایگاه سیاست های امنیتی (SPD)

- SPD در یک جدول که توسط راهبر سیستم تعریف شده است قرار دارد.
- رکوردهای آن برای هر بسته وارد شده و در حال خروج سیاست امنیتی را مشخص می کند:
  - حفاظت (Apply)
  - عبور بدون حفاظت (Bypass)
  - دور انداختن (Reject)

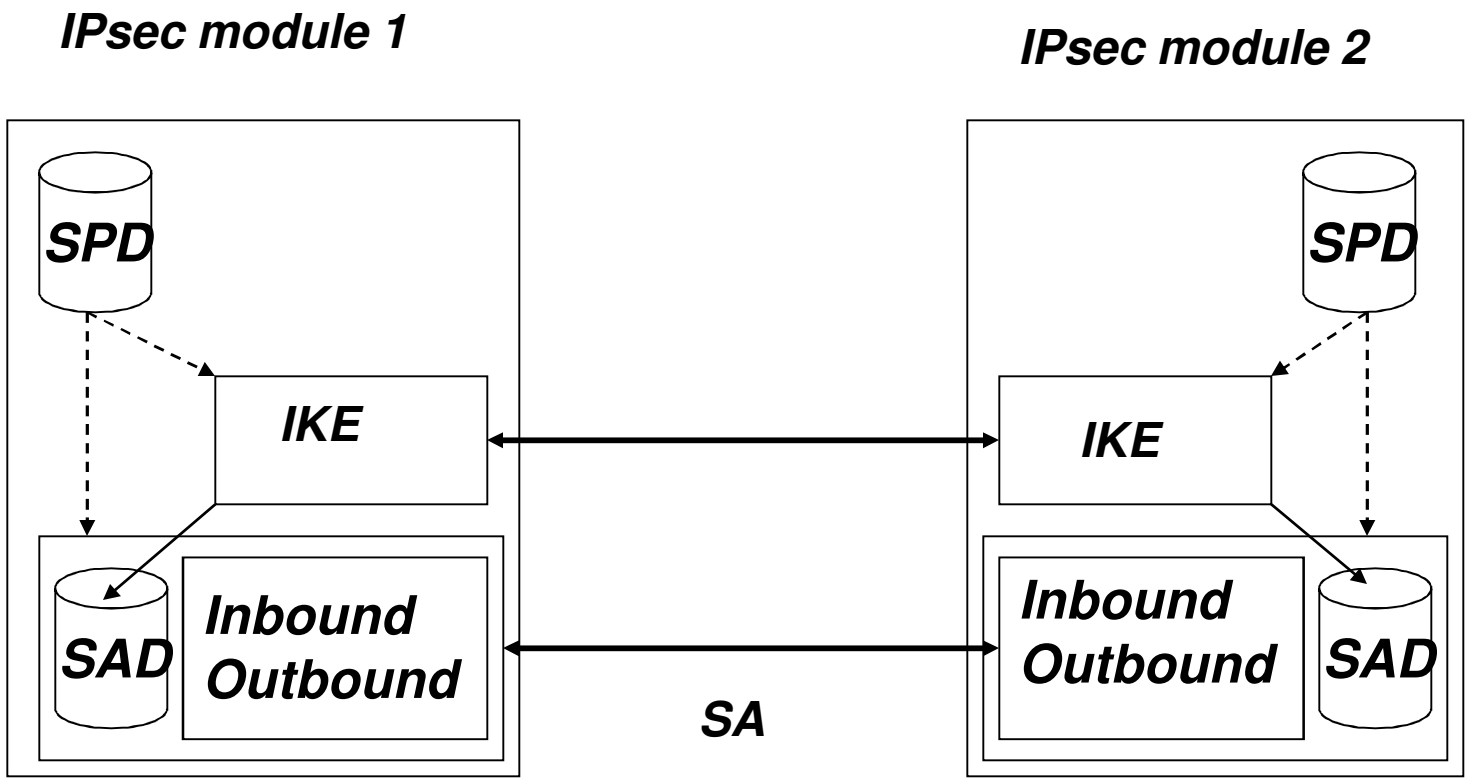
پایگاه سیاست های امنیتی (SPD)

- هر رکورد حاوی
  - مشخصات بسته هایی است که باید سیاست خاصی در مورد آنها اعمال شود. پارامترهای انتخاب سیاست عبارتند از:
    - مشخصات آدرس مبدا و مقصد بسته
      - Range
      - Subnet
    - مشخصات پروتکل لایه بالاتر
      - TCP,UDP,..
    - در صورت TCP یا UDP بودن، مشخصات پورتها

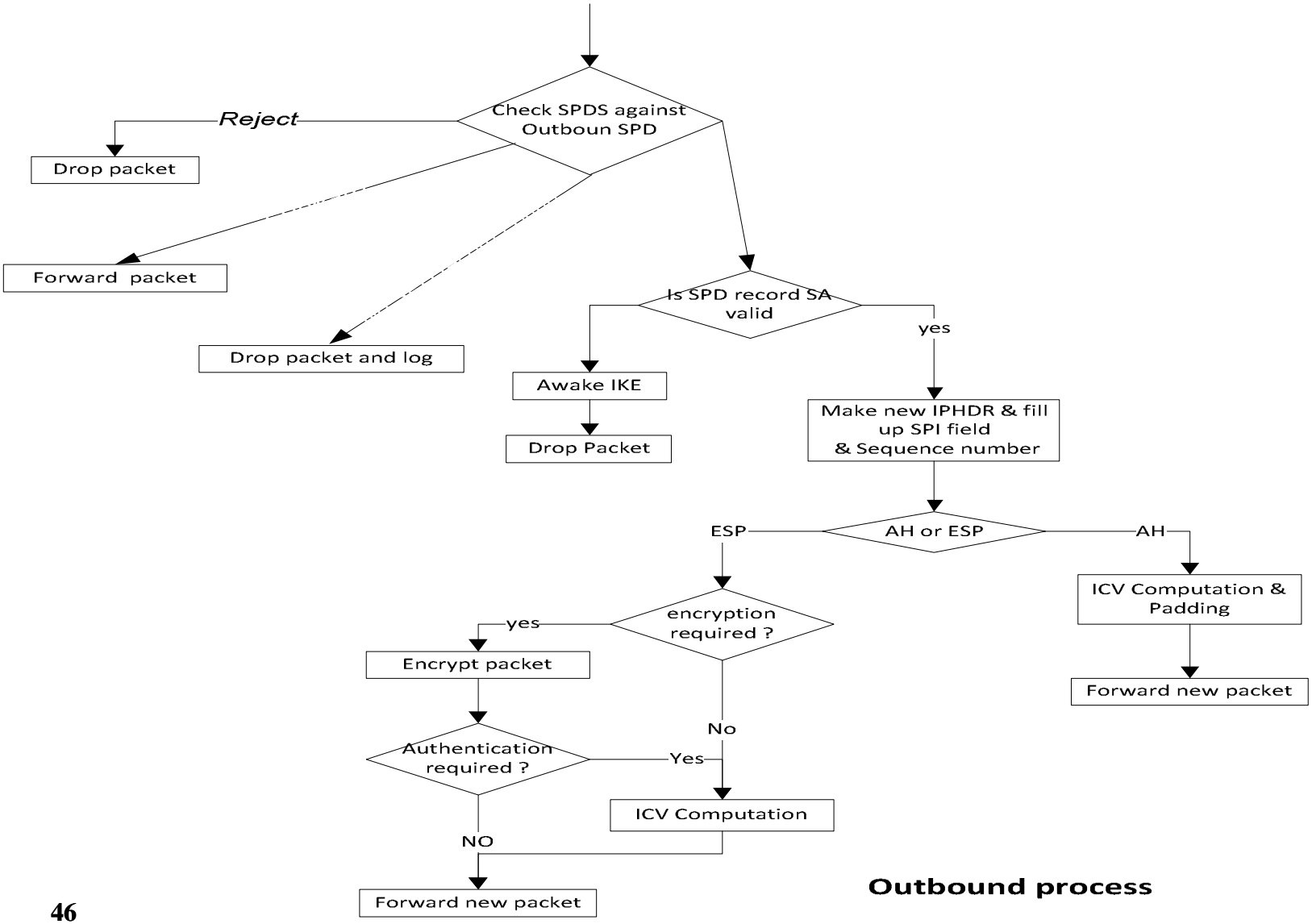
پایگاه سیاست های امنیتی (SPD)

- هر رکورد حاوی
  - سیاست امنیتی
    - Apply
    - Reject
    - Bypass
  - و در صورت Apply مشتمل بر:
    - طرف مقابل در برقراری ارتباط
    - پروتکل AH یا ESP یا هردو
    - الگوریتم های قابل قبول برای احراز اصالت و رمزنگاری
    - طول مدت قابل قبول برای SA (SA Life Time)

معماری IPSec



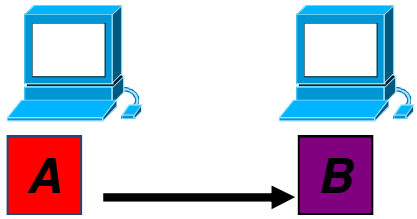
Outbound Process



Outbound process

Outbound Processing

Outbound packet (on A)

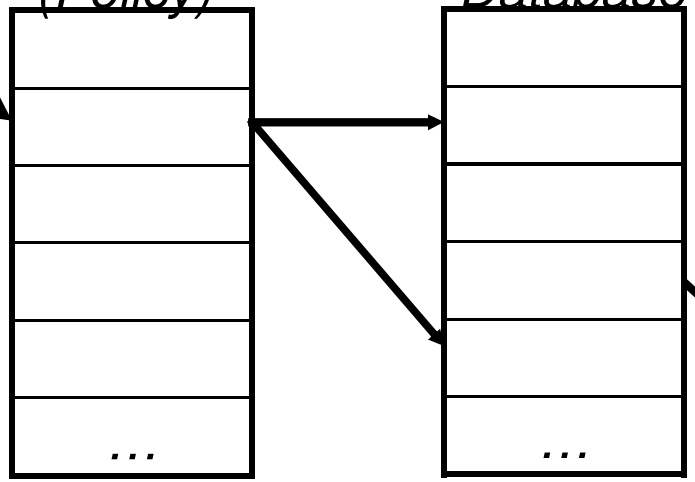


IP Packet

Is it for IPSec?
If so, which policy entry to select?

SPD (Policy)

SA Database



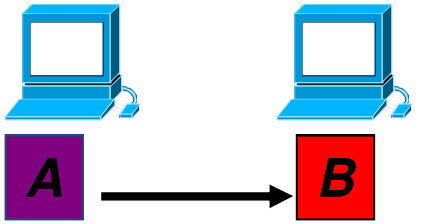
Determine the SA and its SPI

IPSec processing

SPI & IPSec Packet

Send to B

Inbound Processing



Inbound packet (on B)

From A

SPI & Packet

SA Database

Use SPI to index the SAD

…

SPD (Policy)

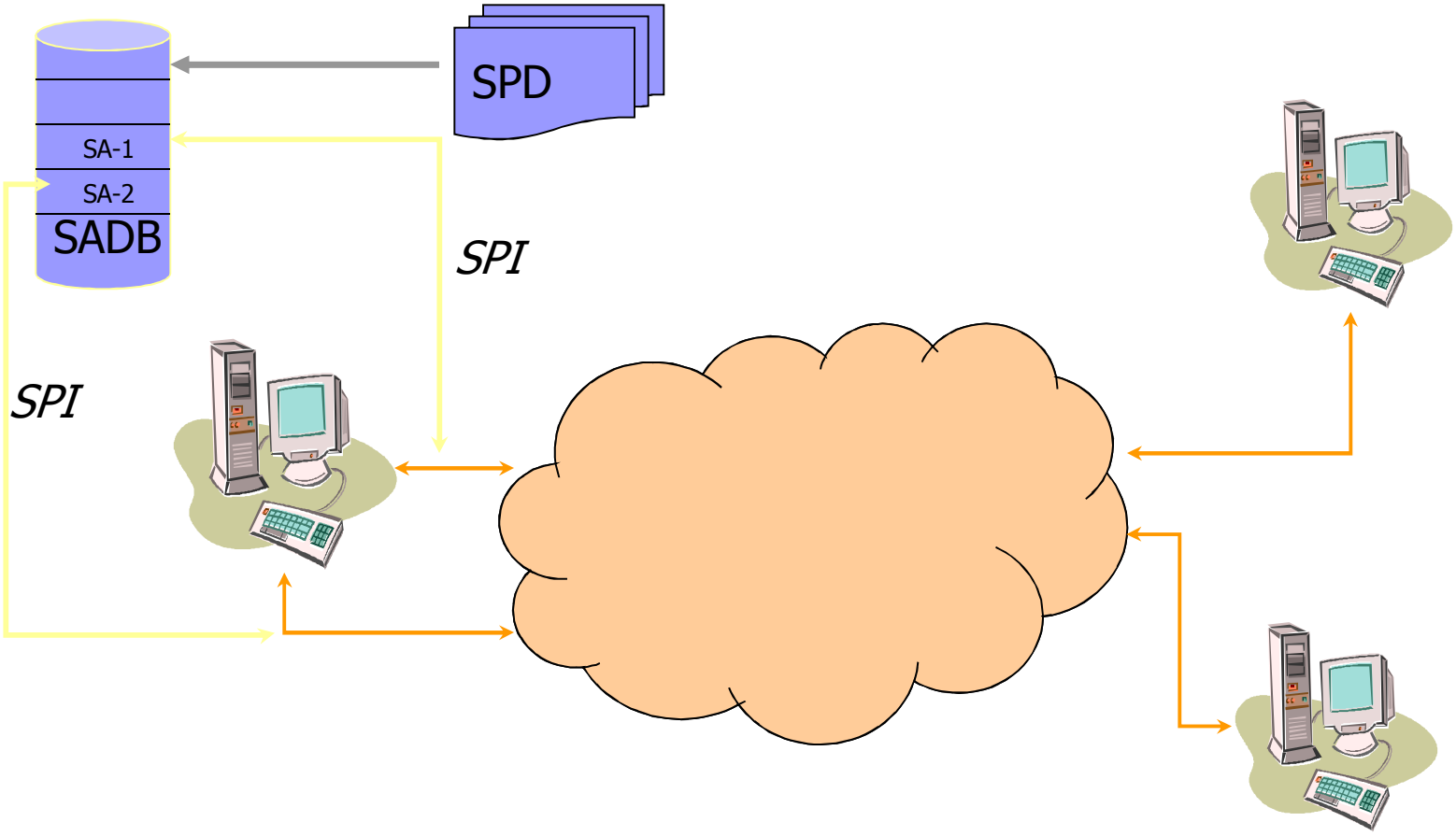
Was packet properly secured?

Original IP Packet

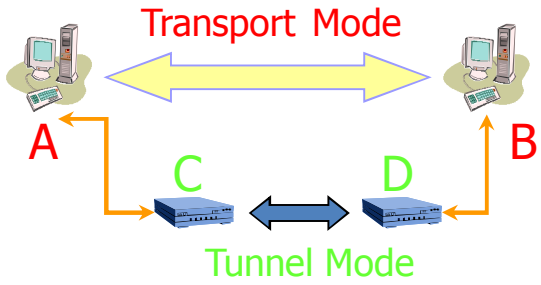
"un-process"

…

How They Fit Together



SPD and SADB Example



A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

A's SADB

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

From	To	Protocol	Port	Policy	Tunnel Dest
A_{sub}	B_{sub}	Any	Any	ESP[3DES]	D

C's SPD

From	To	Protocol	SPI	SA Record
A_{sub}	B_{sub}	ESP	14	3DES key

C's SADB

پروتکل مبادله کلید اینترنت (IKE)

- برای برقراری ارتباط بین دو طرف لازم است که یک SA بین طرفین ایجاد شود.
- برقراری و تجدید این SA ها می تواند بصورت دستی یا خودکار انجام گردد.
- پروتکلی که این وظیفه را (بصورت خودکار) در اینترنت به عهده دارد IKE می باشد

پروتکل مبادله کلید اینترنت (IKE)

- معرفی IKE

  - پروتکل اصلی برای ایجاد و ابقاء IPSec SA
  - پیش فرض IPSec برای مبادله امن کلید
  - فراهم کردن یک ارتباط امن بین طرفین باتوافق بر روی کلیدهای جلسه
  - متکی به مکانیزمهای رمز کلید عمومی و توابع درهم کلیددار
  - چارچوب IKE بر اساس پروتکل ISAKMP (Internet SA Key Management Protocol)

IKEفازهای

- IKE دارای دو فاز می باشد :
  - فاز I : برپایی ISAKMP SA (IKE SA)

    برپایی یک کانال امن احراز اصالت شده بین دو طرف
  - فاز II : برپایی IPSec SA

    استفاده از کانال امن ایجاد شده در فاز ۱ برای ارائه سرویسهای امنیتی IPSec
- فاز I : می تواند به دو روش انجام شود:
  - مبادله مود اصلی (Main mode)
  - مبادله مود اعلان شناسه ها (Aggressive mode)
- فاز II : به روش زیر انجام می شود:
  - مبادله مود سریع (Quick mode)

روشهای احراز اصالت

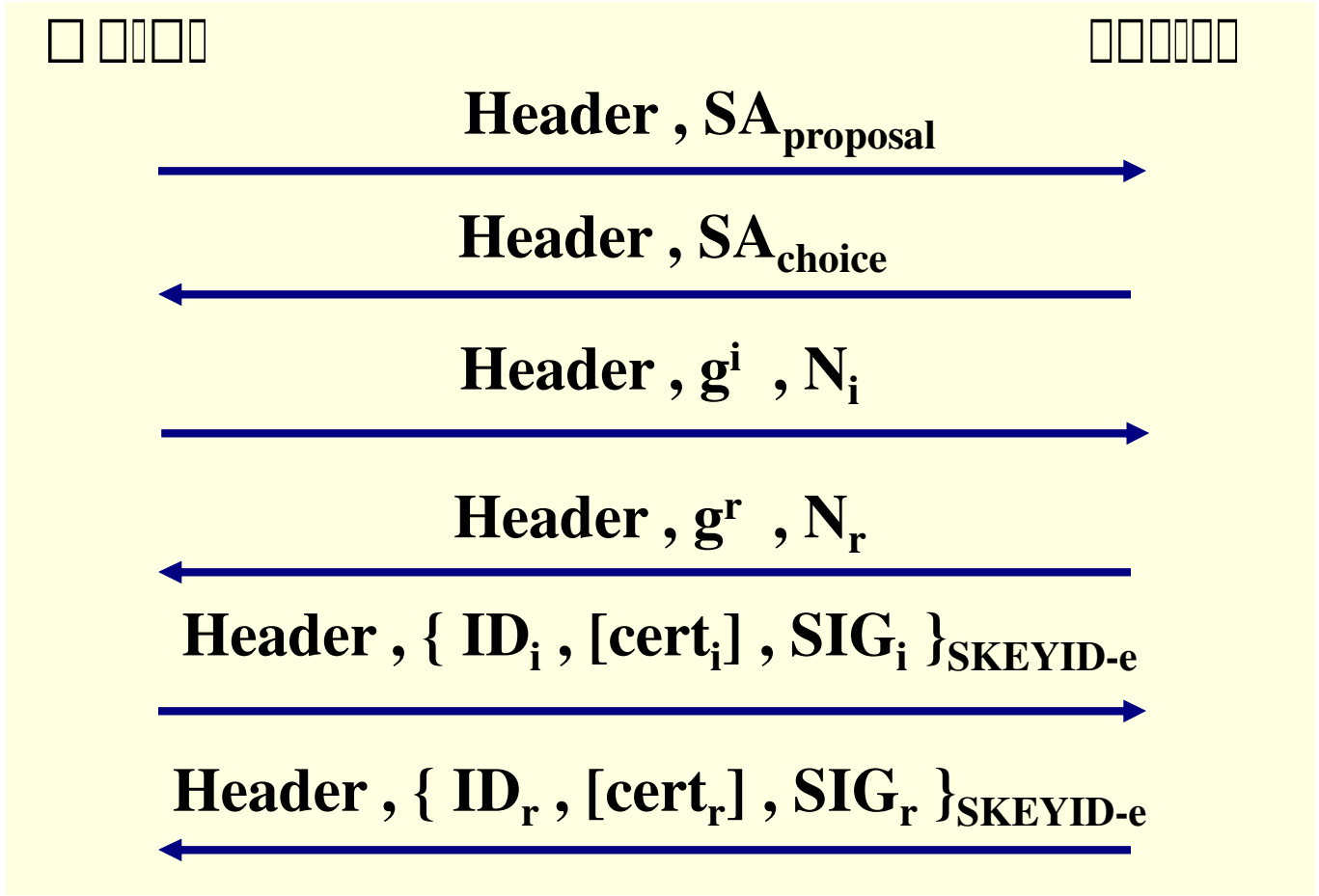
- روشهای احراز اصالت در مبادلات فاز I
:

۱- روش کلید از پیش مشترک (Preshared Key)

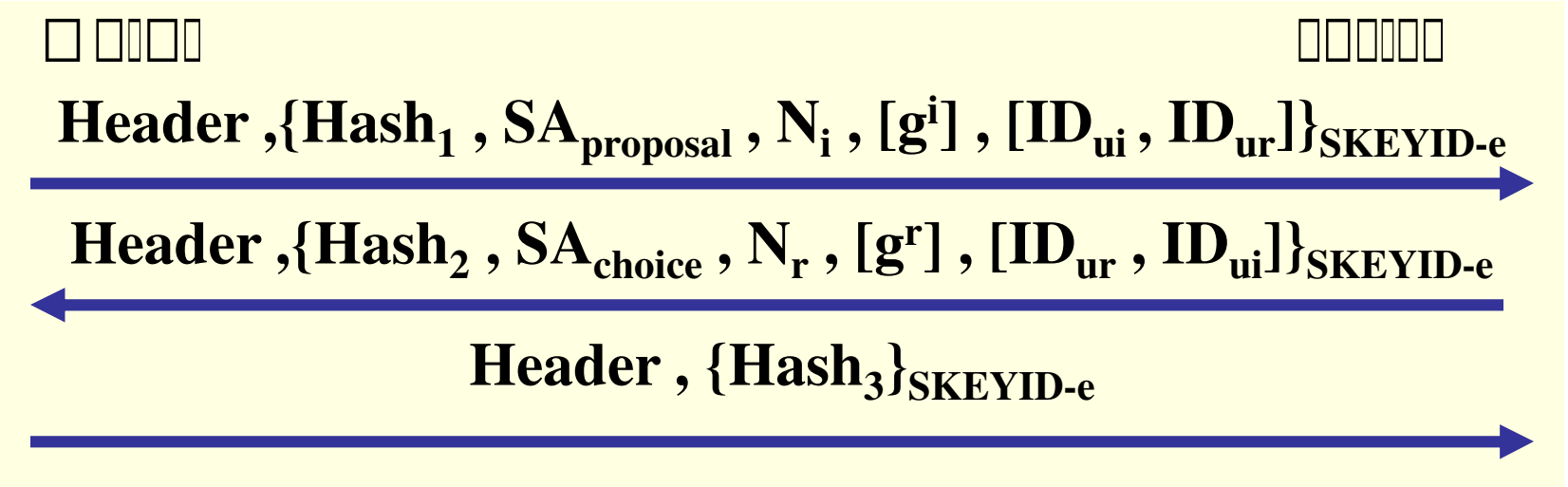
۲- روش امضای کلید عمومی (Public Key Signature)

۳- روش رمزکلید عمومی (Public Key Encryption)

٤- روش رمزکلید عمومی اصلاح شده (Revised Public Key Encryption)


Header , $SA_{proposal}$
Header , SA_{choice}
Header , g^i , N_i
Header , g^r , N_r
Header , { ID_i , [$cert_i$] , SIG_i }$_{SKEYID-e}$
Header , { ID_r , [$cert_r$] , SIG_r }$_{SKEYID-e}$

پروتکل IKE در فاز ۲ (مود سریع)



$Hash_1 = prf\ (SKEYID\text{-}a\ ,\ Message\ ID \mid SA \mid Ni \mid [g^i] \mid [ID_{ui} \mid ID_{ur}])$

$Hash_2 = prf\ (SKEYID\text{-}a\ ,\ Message\ ID \mid Ni \mid SA \mid N_r \mid [g^i] \mid [ID_{ui} \mid ID_{ur}])$

$Hash_3 = prf\ (SKEYID\text{-}a\ ,\ Message\ ID \mid Ni \mid N_r)$

$KEYMAT = prf\ (\ SKEYID\text{-}d\ ,\ [\ g^i\ ] \mid protocol \mid SPI \mid N_i \mid N_r\ )$

وجود نقاط ضعف در IKE

- در پروتکل معرفی شدهٔ IKE نقاط ضعفی به چشم می خورد:
  - تعداد زیاد پیام
  - پیچیدگی مشخصات
  - عملکرد ضعیف در برابر حملات DoS

پروتکلهای جایگزین

پروتکلهای جایگزین IKE

- ✓ معرفی پروتکل IKEv2 (۲۰۰۱)

JFKr

- معرفی پروتکل JFK (۲۰۰۲)

JFKi

Full-SIGMA

- معرفی پروتکل SIGMA (۲۰۰۲)

SIGMA-0