VPN and Network Security

Sophie GASTELLIER-PREVOST
(Sophie.Gastellier@it-sudparis.eu)

Bureau : D101-01
Poste : 41 95

1st part

VPN ???...

- A virtual private network (VPN) is a **private data network** that makes **use of the public telecommunication infrastructure, maintaining privacy** through the use of tunneling protocols and security procedures.
- A virtual private network can be contrasted with a **system of leased lines** that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much **lower cost** by using the **shared public infrastructure** rather than a private one.

...VPN ???

- Phone companies have provided **secure shared resources for voice messages.** A virtual private network makes it possible to have the **same secure sharing of public resources for data.**
- Companies today are looking at using a virtual private network for both **extranets** and **wide-area intranets.**

Definition from Whatis.com

Summary

- Introduction to Threats
- Introduction to Technicals Mecanisms
- Technical Mechanisms: Authentication
- Technical Mechanisms: Tunneling
- Technical Mechanisms: Encryption
- Technical Mechanisms: Filtering and Firewalls

Conclusion

Introduction to threats

Chapter 1

Threats according to ITU-T Standard X.509



- Threats that an Internet connection might expose the network to:
  - Identity Interception
  - Masquerade (a person claims to be another)
  - Replay (ie. Record login procedure in order to replay it later)
  - Data Interception or Traffic Analysis
  - Manipulation (alter or take away information from a transmission)
  - Repudiation (a person denies sending or receiving information)
  - Denial of Service
  - Misrouting (manipulation of routing tables)

Internet Security

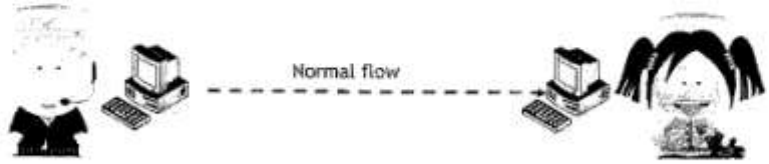
- CERT (Computer and Emergency Response Team) and FIRST (Forum of Incident Response and Security Teams)
  - Provide Internet security information, guidance and coordination for major Internet Security events
- Some statistics:
  - About 35% of the attacks are prevented by security measures like firewalls and password systems.
  - 80% comes from inside, while 20% comes from outside...
  - ...but outside attacks are 80% of costs
  - **European IT Security Market (2005) : +27%**

    Source : CANALYS / Convention de la Sécurité Juin 2005
  - **Worldwide IT market for security softwares (2005) : +14,8% (~ $7.4 billions)**

    (Source : Gartner)

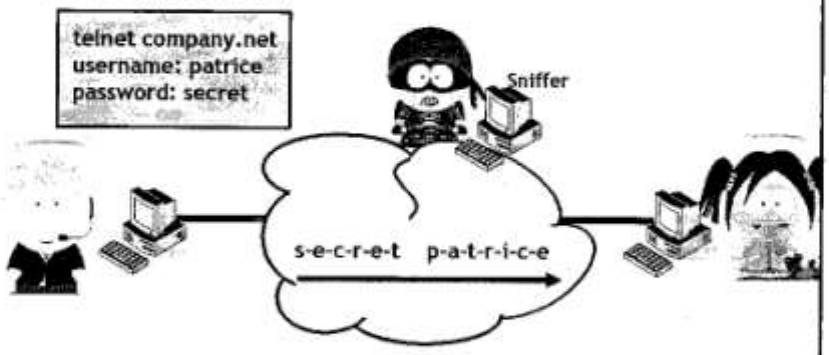
Why VPNs and Network Security ?...

- IP protocol and Internet not designed with strong security measures or guaranteed performance *("Security issues are not discussed in this document" - in many RFC documents)*
- VPNs have 4 critical functions to ensure security:



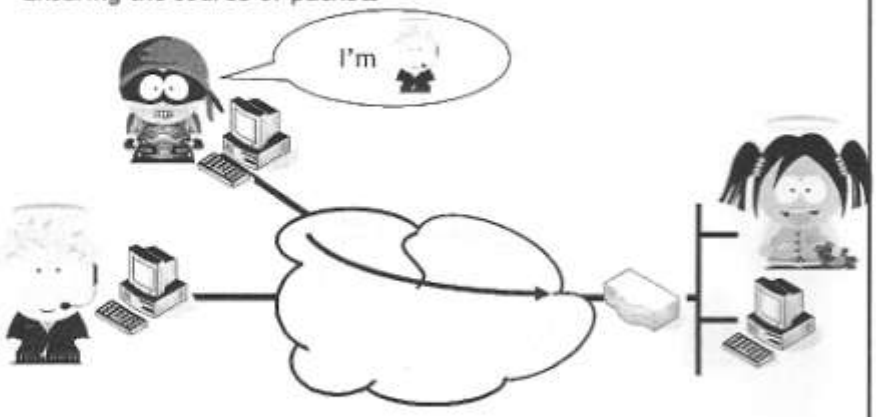
1) Authentication...

- No identity interception



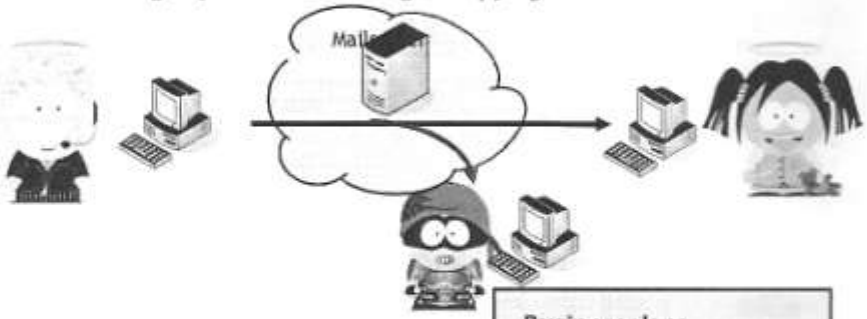
1) ...Authentication

- Ensuring the source of packets



2) Confidentiality

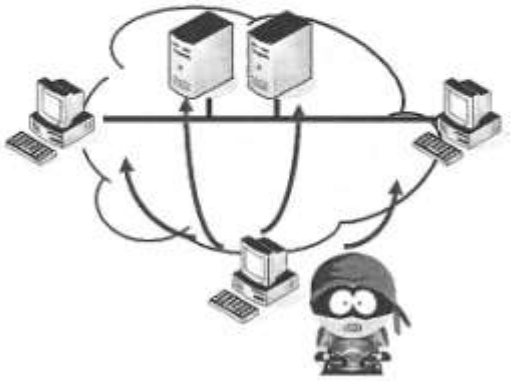
- Preventing anyone from reading or copying data



Businessplan:
- **Expand into.....**
- **Big sale beginning.....**

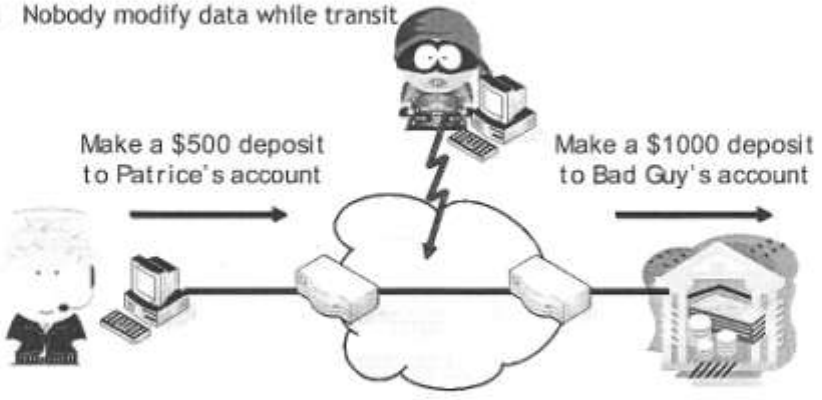
3) Access control

- No unauthorized users on the network



4) Integrity

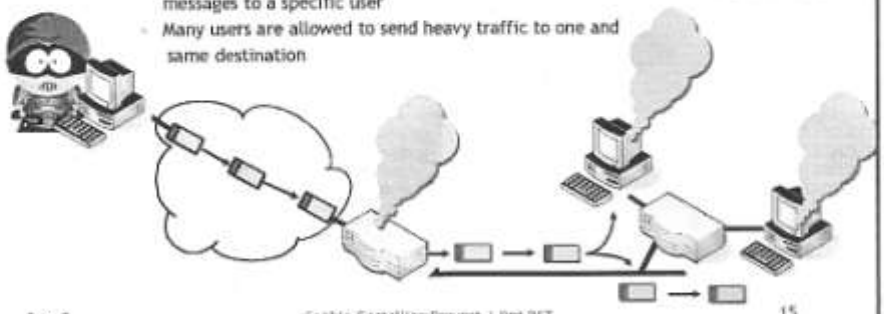
- Nobody modify data while transit



Other threats...

- Denial of Service attack
  - Making services unavailable by overloading the system with storms of messages
    - Ping commands over IP
    - Bugs in e-mail software used to send thousand of e-mail messages to a specific user
    - Many users are allowed to send heavy traffic to one and same destination

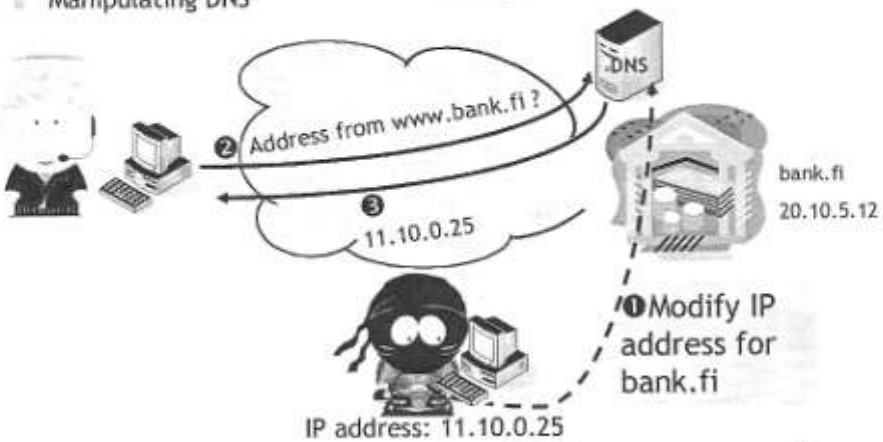




...Other threats...

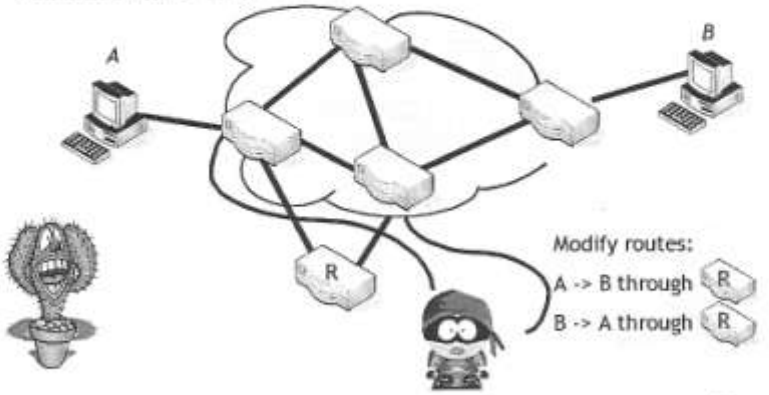


- Manipulating DNS



...Other threats...

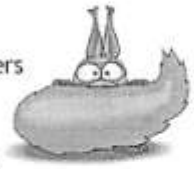
- Manipulating routing functions



...Other threats

- Bugs
  - Bugs are the most common entry point for attackers into a system.
  - All programs contain bugs.
  - The bigger the program the more bugs it contains.

    (Statistics: 4 bugs per 1000 lines of code - ie. Windows: about a few million lines of code)



⇨ Exposed computers should run as few programs as possible, and programs should be as small as possible.

Introduction to Technical mechanisms

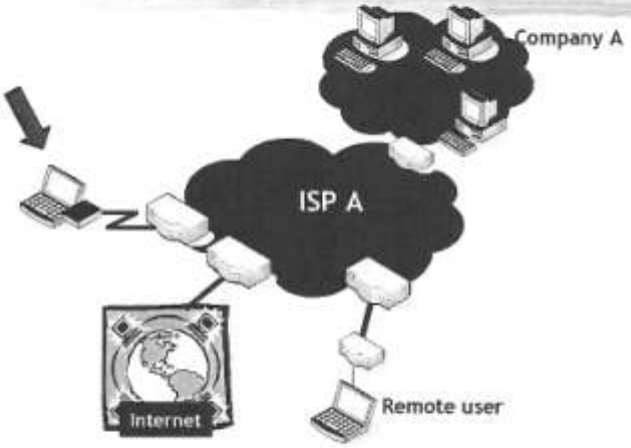
Chapter 2

Guidelines of technical mechanisms

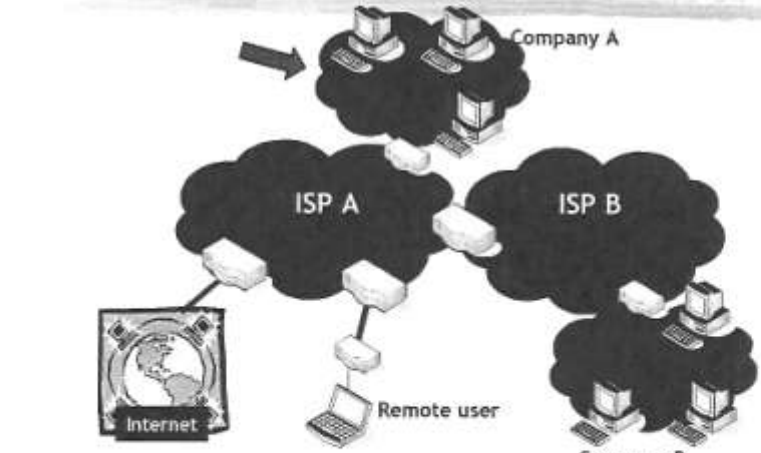


- Authentication mechanisms
  - for Authentication and Access control
- Tunneling
  - for Authentication, Access control and Confidentiality
- Encryption
  - for Authentication, Access control, Confidentiality and Integrity
- Filtering
  - for advanced Authentication and Access control
  - with routers, firewalls, integrated VPN hardware, VPN software

Case study: Which mechanisms for which access ?...



...Case study: Which mechanisms for which access ?



Technical mechanisms: **Authentication**

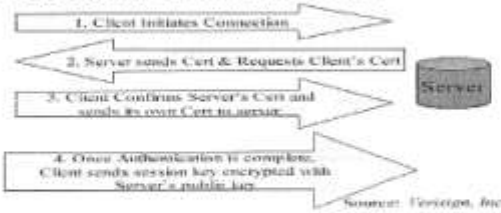
Chapter 3

For Authentication and Access Control

Authentication

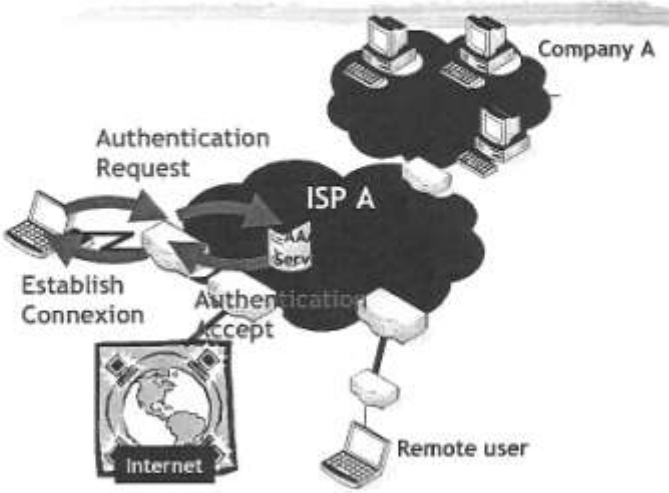
- Software-based
  - Password-based systems
  - Challenge-response systems (CHAP, PAP, RADIUS, ...)
- Hardware-based tokens (EAP - Extensible Authentication Protocol) and digital certificates

How do Digital Certificates Work?



Source: Verisign, Inc.

Case study: Authentication



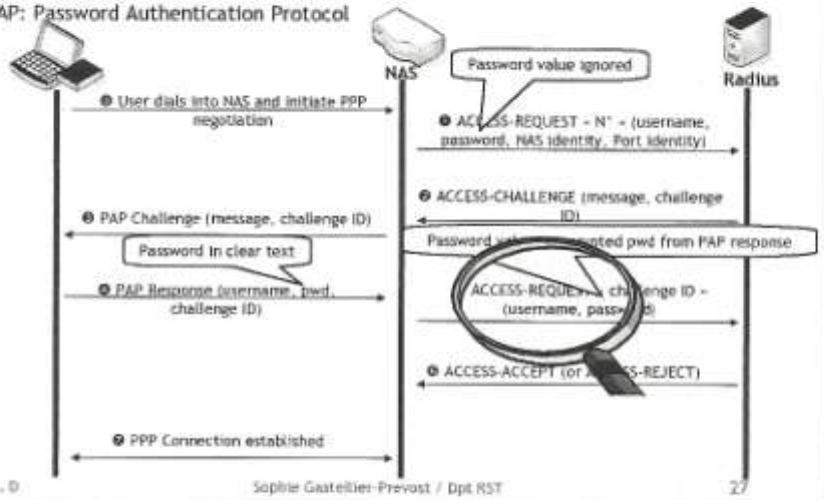
Authentication with PAP

- RADIUS: Remote Authentication Dial-In User Service
- PAP: Password Authentication Protocol

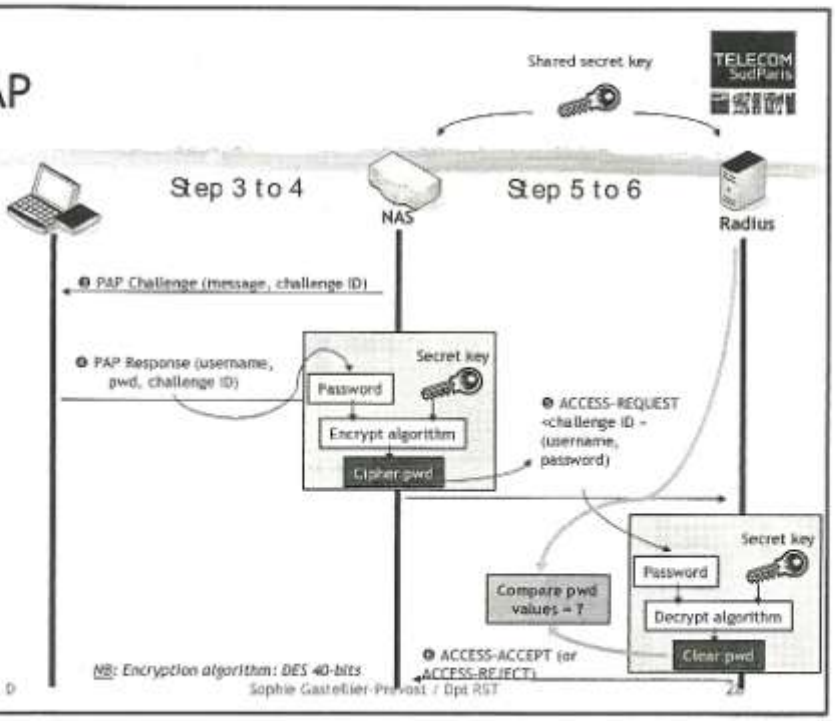


Authentication with PAP

- RADIUS: Remote Authentication Dial-In User Service
- PAP: Password Authentication Protocol

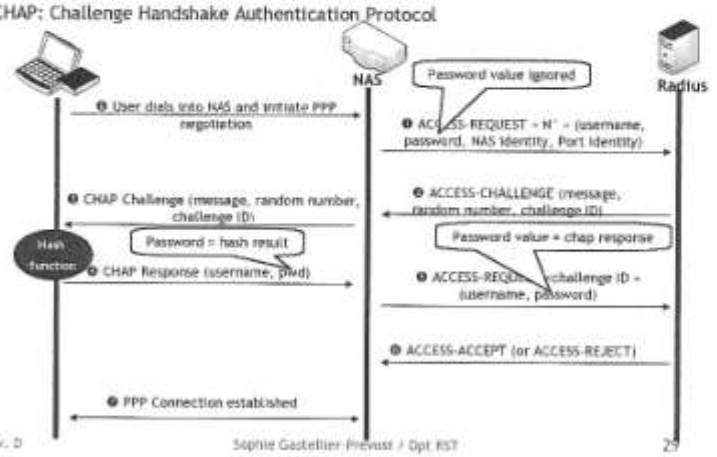


PAP



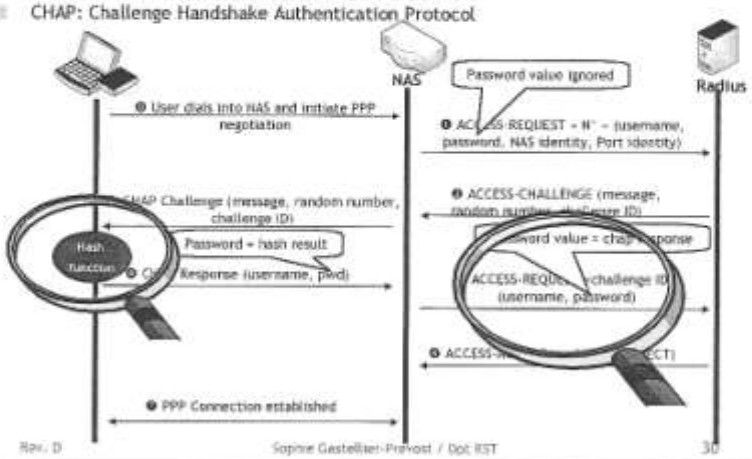
Authentication with CHAP

- RADIUS: Remote Authentication Dial-In User Service
- CHAP: Challenge Handshake Authentication Protocol

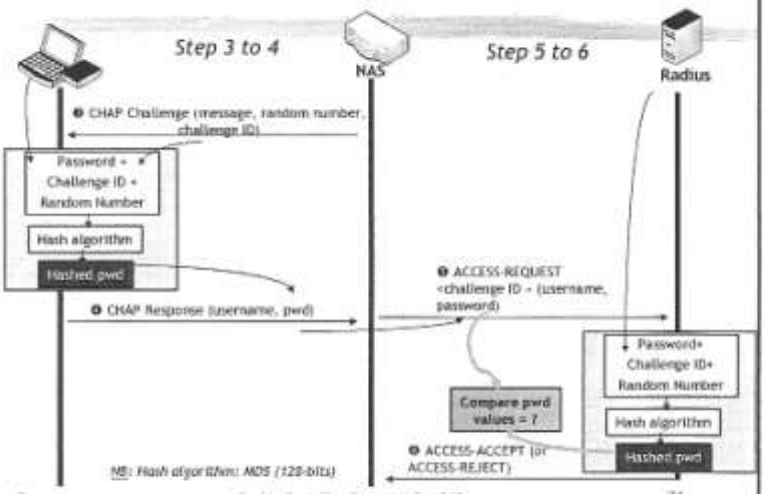


Authentication with CHAP

- RADIUS: Remote Authentication Dial-In User Service
- CHAP: Challenge Handshake Authentication Protocol



CHAP



Technical mechanisms: **Tunneling**

Chapter 4

For Authentication, Access Control and Confidentiality

Tunneling

- GRE (Generic Routing Encapsulation) — *Router-to-Router*
- PPTP (Point-to-Point Tunneling Protocol) — *Client(PC)-to-LAN*
- L2F (Layer 2 Forwarding protocol) — *LAN-to-LAN*
- L2TP (Layer 2 Tunneling Protocol) — *LAN-to-LAN*
- MPLS VPNs

...Tunneling...

- GRE (RFC 1701) - IP over IP tunneling protocol
  - Origin: IETF, 1994
  - Encapsulate every layer 3 protocols
  - Only on intermediate nodes.
  - Encryption and authentication not as elaborate as IPSec



...Tunneling...



- PPTP (RFC 2637)
  - Origin: 1996 - From Microsoft, 3Com and Ascend USR
  - *Authentication* using PPP methods (PAP, CHAP)
  - Used to tunnel PPP packets through an IP network, using a modified version of GRE protocol
  - *Data encryption* can be made with RSA RC4 algorithm (40-bits key) - not so secure
  - Mostly used by ISP/ASP for Dial-up access

✓ Requires IP (but can tunnel NetBEUI, IPX and PPP)

✓ No authentication for tunnel endpoints. Based on PPP authentication



✓ Native on Microsoft Windows NT 4.0, 2000 and 98, and Service Pack for 95

...Tunneling...

- L2F (RFC 2341)
  - Origin: 1996 - From Cisco
  - Authentication using PPP methods (PAP, CHAP) and RADIUS, TACACS protocols
  - Two levels of authentication: before setting up the tunnel, and when connection is set up at the corporate gateway

✓ No encryption method



✓Tunnels can support more than one connection
✓Not IP dependent: can work directly with ATM, FR

...Tunneling...



- L2TP (RFC 2661)
  - Designed by IETF
  - Merge of PPTP and L2F (Cisco and Microsoft, by 1998)
  - Use PPP mechanisms for connection (PAP/CHAP, RADIUS, EAP)
  - Tunnel construction based on L2F. Use of IPSec's encryption methods to strengthen VPN

...Tunneling

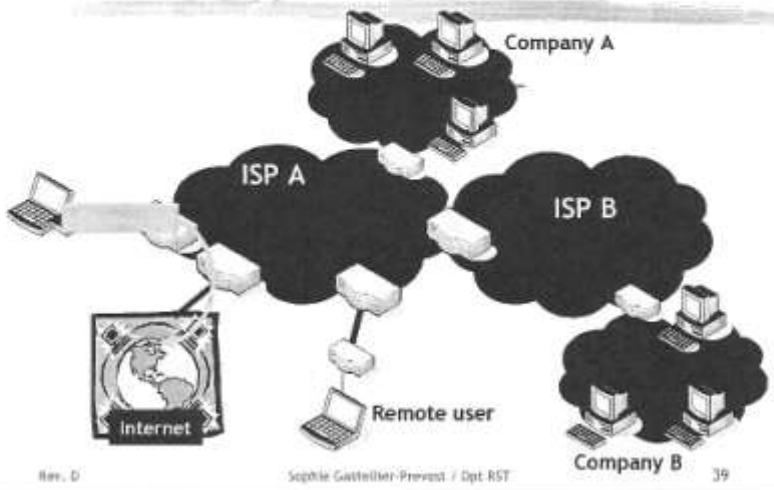
- MPLS VPNs (RFC 2547 and 2547bis)
  - Layer 2 or Layer 3-based VPNs
  - Ideally suited for Carrier-of-Carrier or Large entreprise who wants to deliver VPNs
  - LDP or RSVP protocols used to setup MPLS tunnel through provider backbone. Use of BGP to distribute VPNs information

✓ Policy-based control and management can be issues for provider with large networks

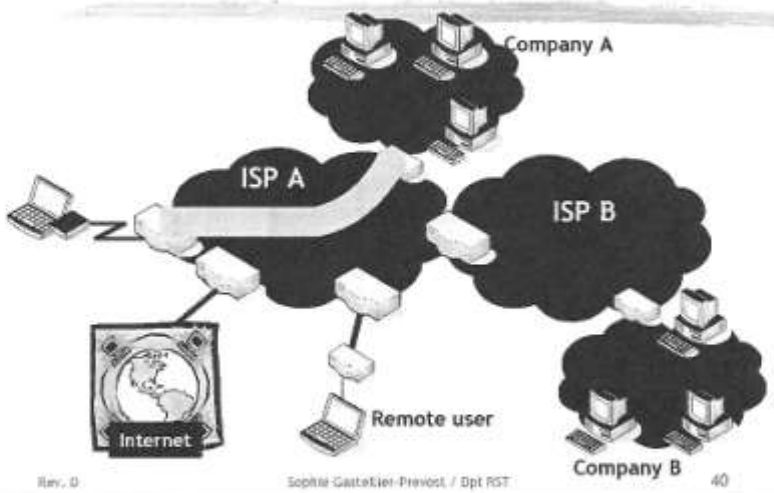


✓ Use of MPLS designed for infrastructure - scalable and flexible
✓VPN-specific information not maintained on all backbone routers
✓Offload complexity mgmt to provider

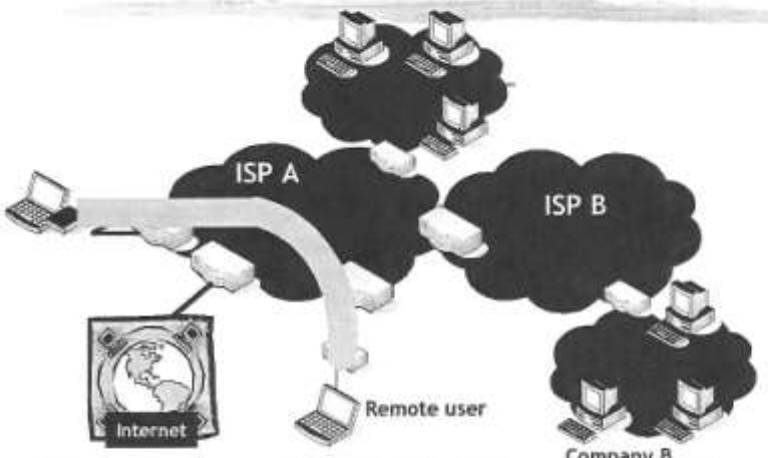
Case study: Tunneling mechanisms



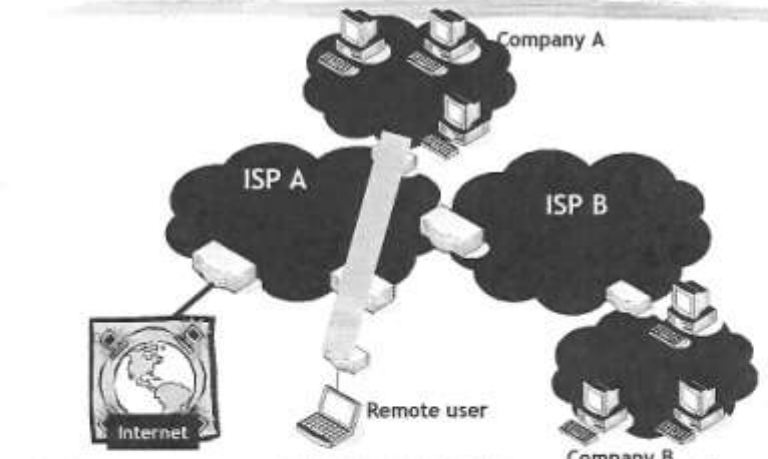
...Case study: Tunneling mechanisms...

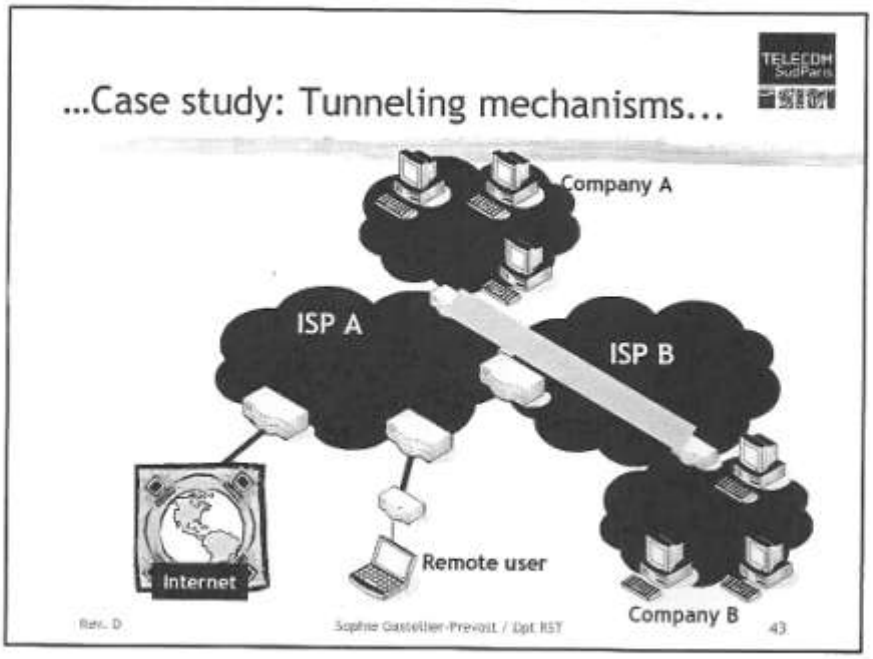


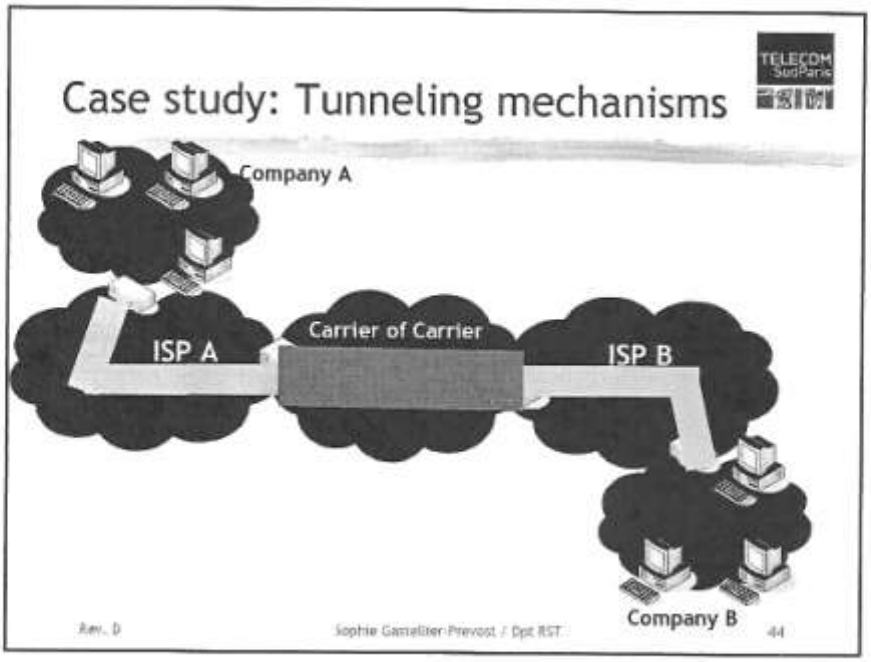
...Case study: Tunneling mechanisms...



...Case study: Tunneling mechanisms...




...Case study: Tunneling mechanisms...
Company A
ISP A
ISP B
Internet
Remote user
Company B
Rev. D
Sophie Gastellier-Prevost / Dpt RST
43


Case study: Tunneling mechanisms
Company A
ISP A
Carrier of Carrier
ISP B
Company B
Rev. D
Sophie Gastellier-Prevost / Dpt RST
44

2nd part

Summary

- Introduction to Threats
- Introduction to Technicals Mecanisms

- Technical Mechanisms: Authentication
- Technical Mechanisms: Tunneling
- Technical Mechanisms: Encryption
- Technical Mechanisms: Filtering and Firewalls

- Conclusion

Technical mechanisms: **Encryption**

Chapter 5

for Authentication, Access control, Confidentiality and Integrity

Introduction to encryption...

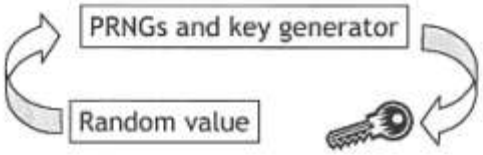
- Basic components:
  - Random values, keys, ...
  - Hashing algorithm: one-way cipher
  - Asymmetric cipher: public key systems
  - Symmetric cipher: private key systems

Random values and keys

- « The security of an algorithm rests in the key. If you 're using a cryptographically weak process to generate keys, then your whole system is weak »

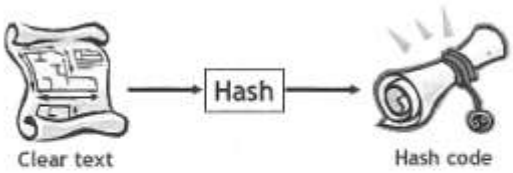
Bruce Schneier, Applied Cryptography

- PRNG: Pseudo-random key generator



Hash algorithms

- Used for integrity check (MD5, SHA-1)

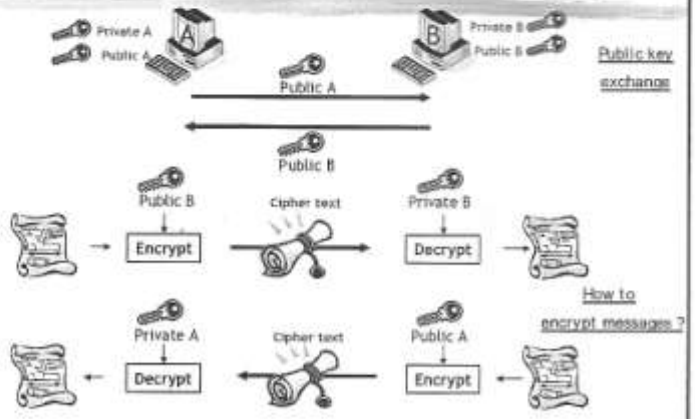


Asymmetric Cipher algorithms

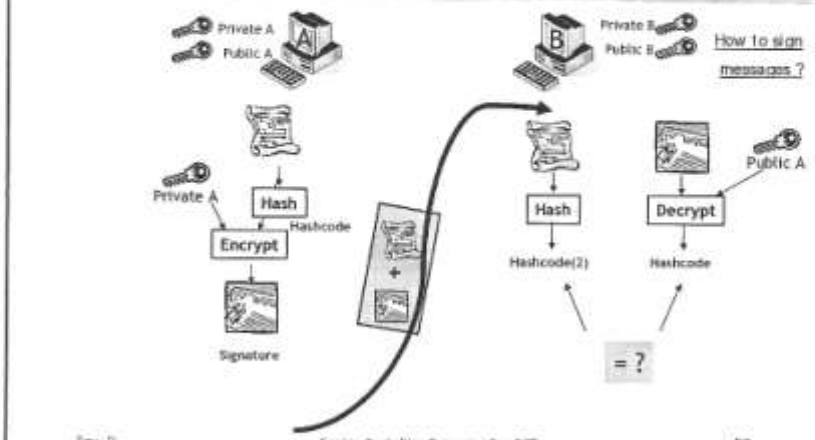
- Mostly used for signature
- 100 to 1000 times slower than private key systems
- Examples:DH (Diffie-Hellmann), RSA (Rivest, Shamir and Aldeman), PGP (Pretty Good Privacy),....



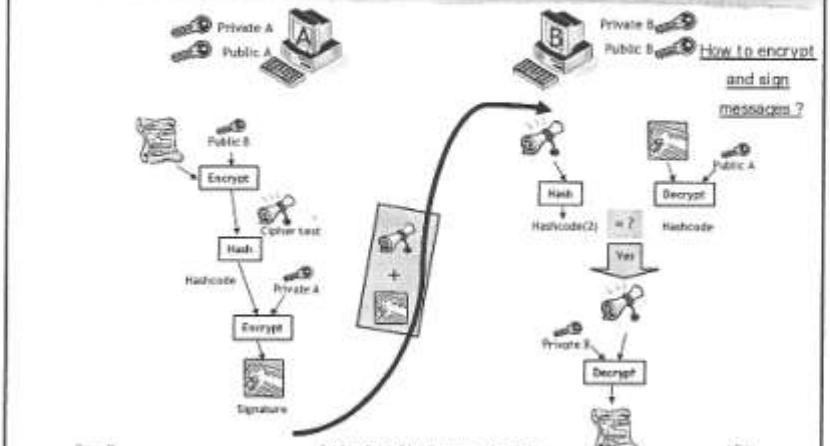
Public key exchange and Message encryption with Asymmetric Cipher algorithms



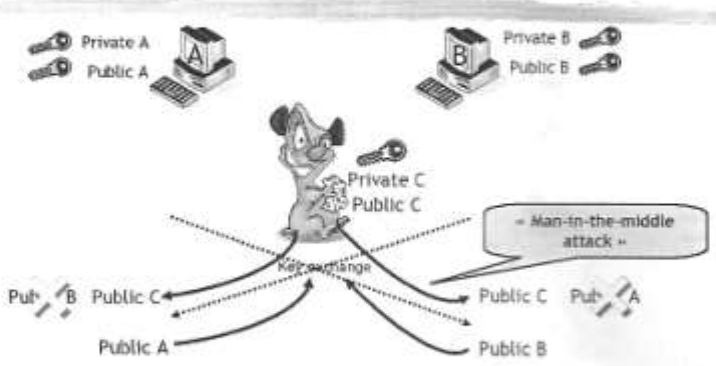
Message signature with Asymmetric Cipher algorithms



Messages encryption AND signature with Asymmetric Cipher algorithms



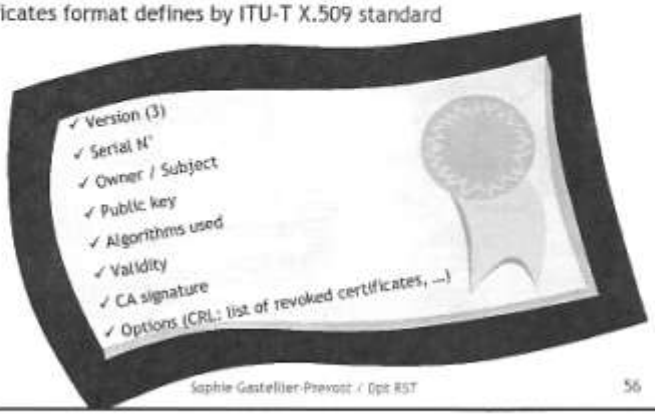
Are you sure of Public Key exchange with Asymmetric Cipher algorithms ?



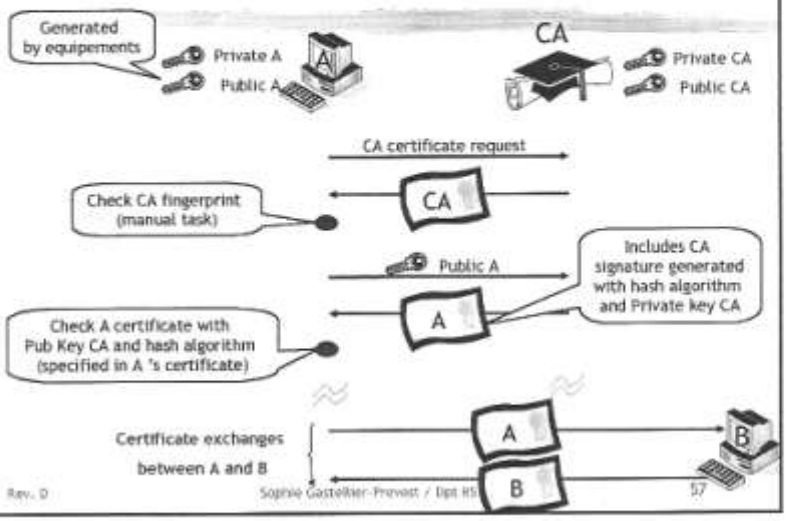
- Third party to create, exchange or revoke certificates (X.509)

Certificates

- Delivered by a third party: the Certificate Authority (CA), which guarantees the origin of public keys
- Certificates format defines by ITU-T X.509 standard

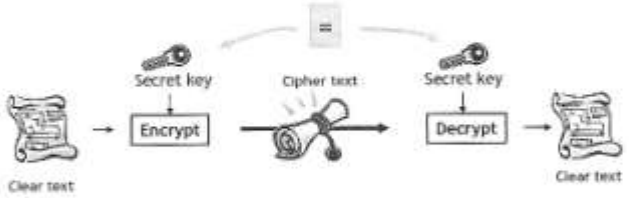


Secure Public key exchange with certificates



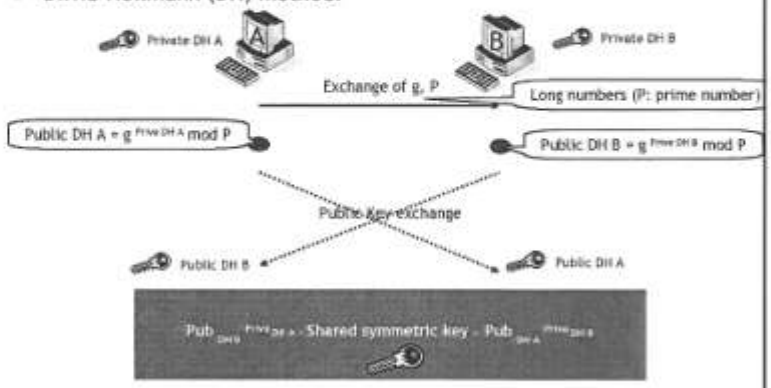
Symmetric Cipher algorithms

- Used for almost all data encryption (DES, 3DES, IDEA, AES, RC2, RC4, ...)



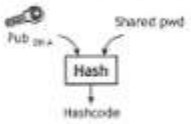
How to share the same secret key when using Symmetric algorithms ?

- Diffie-Hellmann (DH) method:

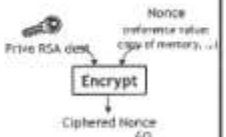


How to secure Public Key exchange with Symmetric Cipher algorithms ?

- 3 methods:



  - « Pre-Shared »
    - Exchange Public keys $_{DH}$ + Hashcode
  - « RSA-signed »
    - Generate RSA keys in addition to Public keys $_{DH}$
    - Exchange Public keys $_{DH}$ + Certificates + RSA Signature
  - « RSA-Encrypted »
    - Generate RSA keys in addition to Public keys $_{DH}$
    - Exchange Public keys $_{DH}$ + Certificates + RSA encrypted



Commonly Used Algorithms

- Study of 1999:

1996: 1430 years

2001: 15 min.

Algorithm	No. of Bits	No. of Keys	Sea… Time
DES	56	10^{16}	3.5 hours
SKIPJACK	80	10^{24}	6,655 years
3DES (2 Keys)	112	10^{33}	30,000,000,000,000 years
IDEA, RC4/128	128	10^{38}	2,000,000,000,000,000, 000 years

Source: *Internet Cryptography* by Richard E. Smith

Resume Cryptography basics

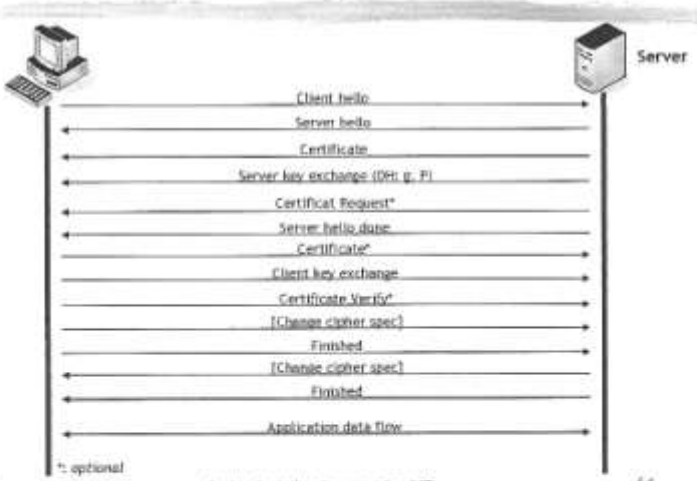


- Hash algorithms (HMAC = MD5, SHA-1) used for integrity check
- Cryptography systems used to provide data confidentiality
  - Public key cryptography sytems: RSA
  - Secret key cryptography sytems: DES, RC4, IDEA
  - *Next protocol to be used: AES (Advanced Encrytion Standard: 128 to 256 bits)*
- Certificates used to provide authentication (DH, RSA)

Encryption mechanisms

- SSL (Secure Socket Layer) and TLS (Transport Layer Security)
  - Used to secure Web transactions.
  - Two phases: server authentication and, optional client authentication
  - SSL - *Secure Socket Layer*
    - Developped by Netscape 1994, IETF released by 1996
    - Provide authentication with CA (MD5, SHA-1), encryption (RC2, RC4 128-bit, DES 40-bit, DES and 3DES) and key exchange (RSA, DH)
  - TLS - *Transport Layer Security*
    - Released by 1999
    - Provide authentication with CA (MD5, SHA-1), encryption (RC2, RC4, 40-bit DES, DES and 3DES) and key exchange (RSA, DH)
  - SSL and TLS not compatible (use different process of HMAC)

SSL and TLS messages



IPSec

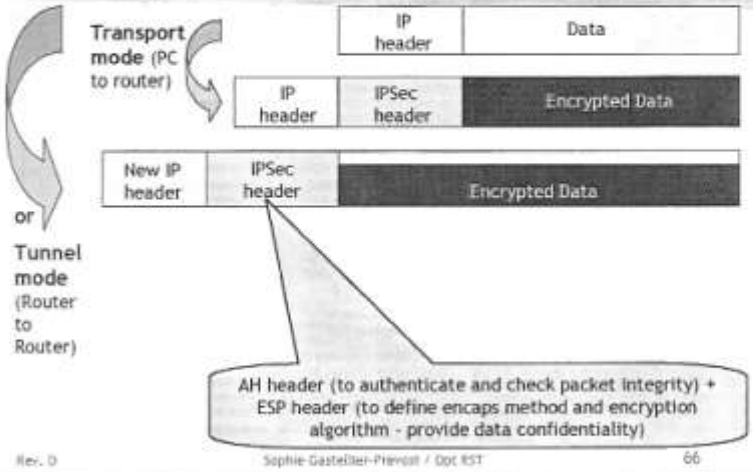
- IPSec or Secure IP, the IETF's Layer 3 Security Architecture
  - Standards begun from mid-1995. Still evolving...
  - Designed to secure IP packets as IPv6 was being developed. Can also be used with IPv4 as well.
  - Used for LAN-to-LAN solutions. Evolution to PC and mobile uses
  - Flexible suite of protocols to create a secure framework to make use of public non-trusted networks
    - User Authentication (PKI and X.509 Digital Certificates)
    - Data Integrity & Authentication (MD5, SHA-1)
    - Automated Key Management (Internet Key Exchange - IKE/ISAKMP)
    - Encryption Algorithms (3DES, DES, RC4,...)

✓ Difficult to administrate because of certificates, when extranet connections
✓ Limitation on number of simultaneous tunnels
✓ For IP Network only



✓ The IETF's Layer 3 Security Architecture
✓ Ready for PC-to-router and Rou to-router uses

How does IPSec works ?



Basic components

- SA (Security Association)
  - Unilateral connection that defines security services for the traffic (specifies encryption algorithms used, auth. method, key lifetimes, ...)
- SA is identified by a SPI (Security Paramater Index) + an IP destination address + a Security protocol identifier (AH or ESP)
- If AH or ESP: 1 incoming SA + 1 outgoing SA
- If both AH and ESP: 2 incoming SA, 2 outgoing SA
- NAT not compatible with AH
- PAT not compatible with IPSec

IPSec negociation

- IKE / ISAKMP *(Internet Key Exchange / Internet Security Association Key Management Protocol)*



Phase 1 (clear text):
Main/Agressive mode
SA for IKE
(protect Phase 2)
**: done every 24H on Cisco products (default parameter)*

- Authentication
- Algorithms negociation (hash, cipher)
- DH group negociation (=> key length)
- DH

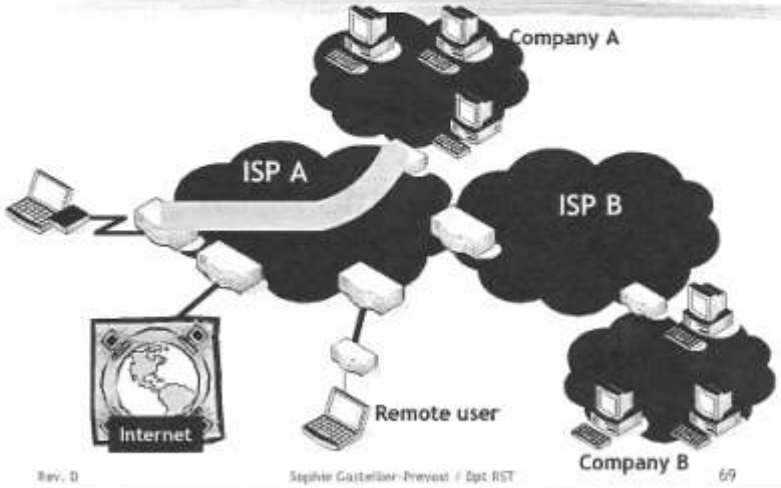
Phase 2 (ciphered):
Quick mode
SA_s for IPSec
**: done every 2H on Cisco products (default parameter)*

- Authentication
- DH group *(used if PFS activated only)*
- PFS(Perfect Forward Secrecy) - *used to generate new keys after expiration*
- Tunnel or Transport Mode
- AH and/or ESP
- Algorithms negociation for IPSec packets (hash, cipher)
- Specify which traffic to encrypt, destination, ...

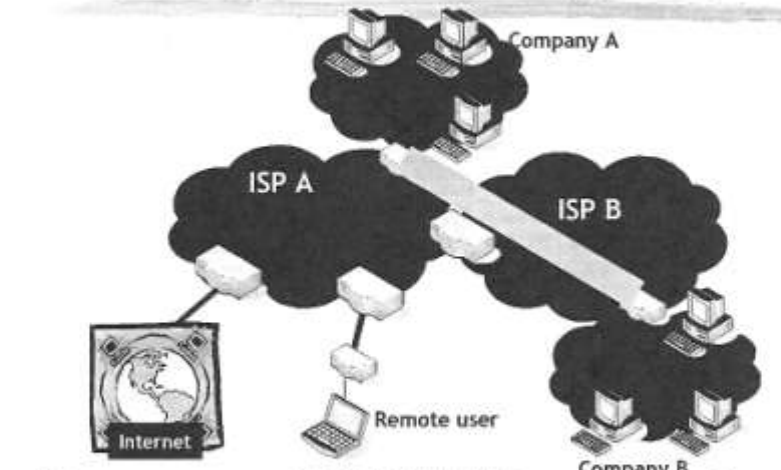
ISAKMP

IPSec

Case study: Encryption mechanisms...



...Case study: Encryption mechanisms...



Technical mechanisms: **Filtering and Firewall**

Chapter 6

for Access control and Integrity

Rev. D

Definition of Firewall

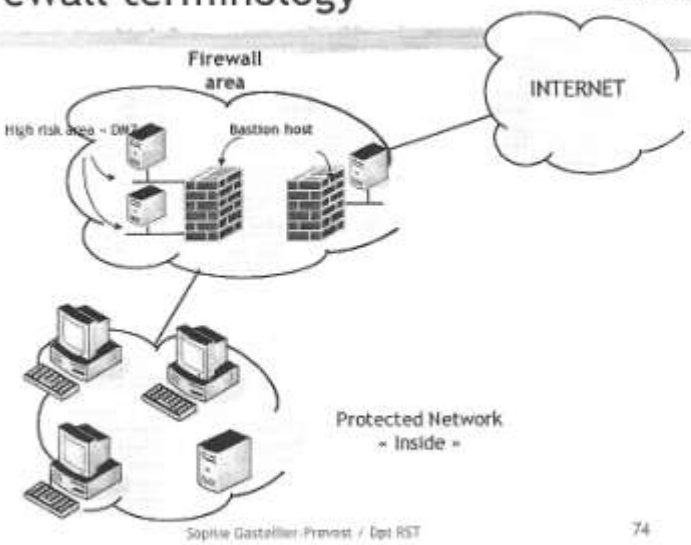
- A firewall is a set of related programs, located at a network gateway server, that **protects the resources of a private network from users from other networks.** (The term also implies the security policy that is used with the programs.)
- A firewall **examines each network packet** to determine whether to forward it toward its destination. A firewall also includes or works with a **proxy server** that makes network requests on behalf of workstation users.
- A firewall is often **installed in a specially designated computer separate from the rest of the network** so that no incoming request can get directly at private network resources.

Definition from WhatIs.com

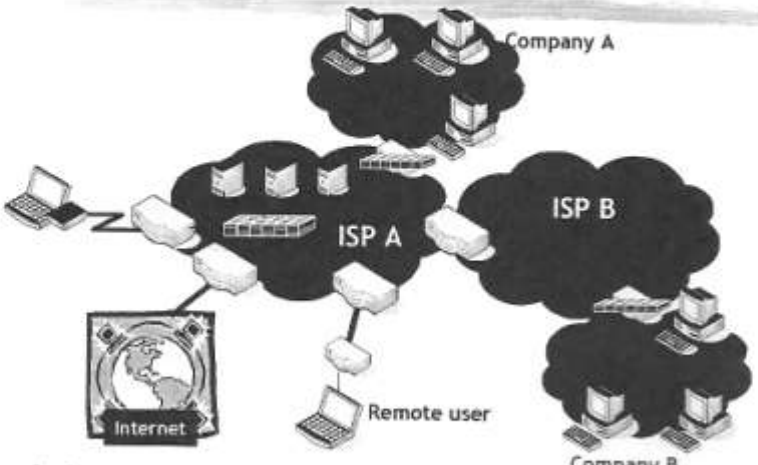
Firewall terminology...

- **Firewall area**
  - Protected area that share a common security policy. It includes DMZ and Bastion host
- **DMZ (Demilitarized Zone)**: High Risk Area
  - Part of the network that run services available to the outside => possible target of attacks
- **Bastion host** (= firewalls or routers with filtering functions)
  - Computer which is point of entry of the network to all traffic from outside to inside. (monitors, logs, continuously upgraded,...)
- **Protected Network (Inside)**

...Firewall terminology

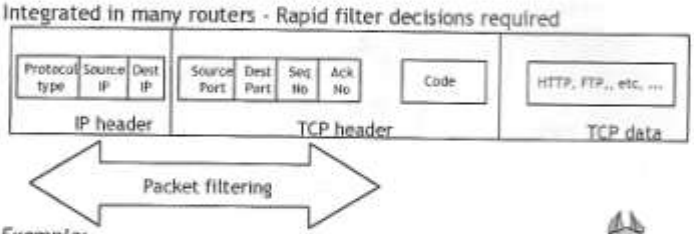


Case study: Filtering and Firewalls positioning



Types of firewalls...

- **Basic packet filtering** (or Access lists)
  - Integrated in many routers - Rapid filter decisions required

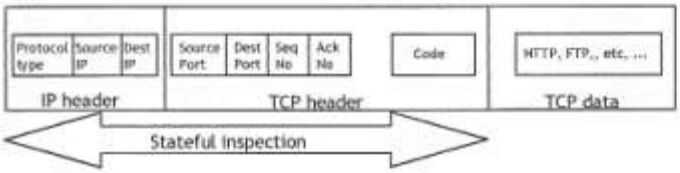


  - *Example*:
    - permit http (in/out) for any users
    - permit ftp (in/out) for 192.168.0.16 255.255.255.240
    - deny ftp (in/out) for any users



...Types of firewalls...

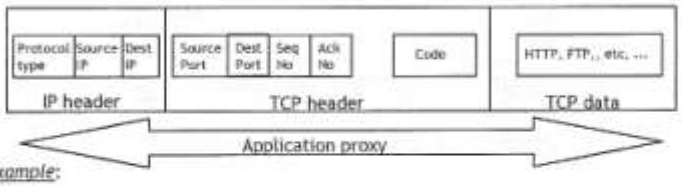
- **Stateful inspection** (also called Dynamic packet filtering, or TCP level FW)
  - Maintains table of active TCP and UDP connections (Source and Dest IP, Ports No, Current TCP seq, ...)
  - Only packets included in these sessions can pass through the firewall



  - *Example*: permit http (in/out) for any users
    - Authenticate user when session is established, or accept packet only if it belong to an existing session

...Types of firewalls

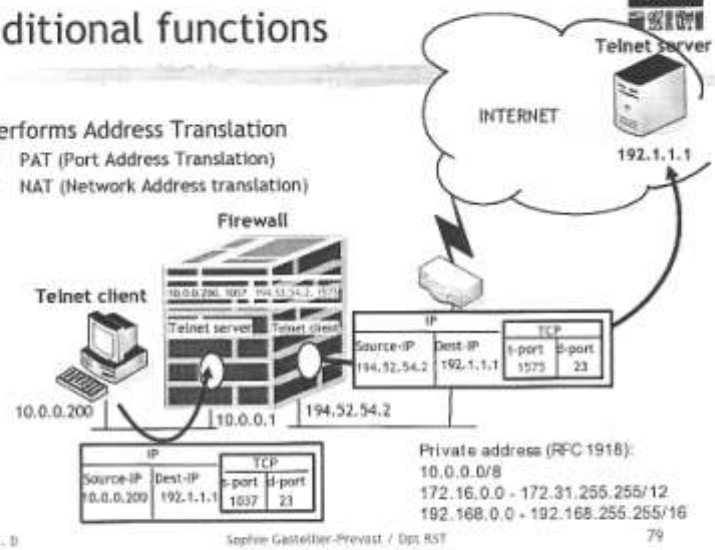
- **Application proxy**
  - More secure than packet filtering but slower than stateful inspection
  - Two TCP connections established: Packet source <-> FW and FW <-> Packet dest.
  - Applications proxies intercept arriving packets on behalf of the destination, examine payload and then relay to destination.



  - *Example*:
    - block FTP transfers involving filenames ending in « .exe »
    - block email containing « joke »

Additional functions

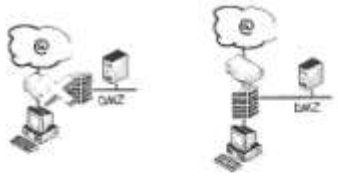
- Performs Address Translation
  - PAT (Port Address Translation)
  - NAT (Network Address translation)



Private address (RFC 1918):
10.0.0.0/8
172.16.0.0 - 172.31.255.255/12
192.168.0.0 - 192.168.255.255/16

Firewall fundamental rules...

- All ingoing flows must go through firewall





- No ingoing flow should pass through firewall without inspection (ie. « Break » the flow)



...Firewall fundamental rules

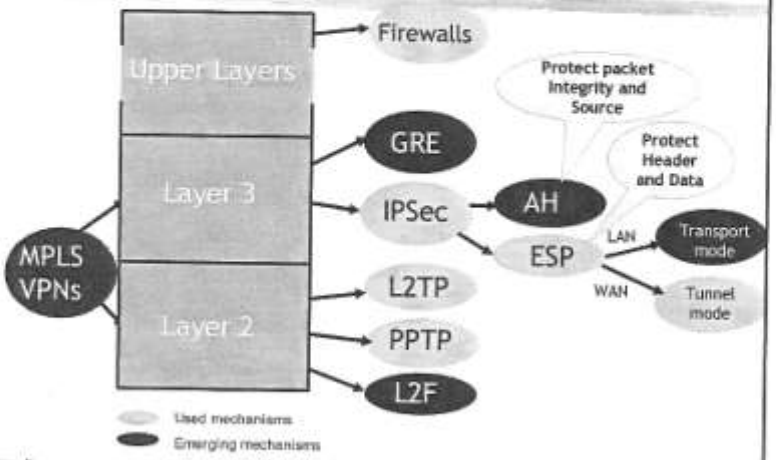
- Never be dependent of bastion platform; think about alternative solution (ie. if bastion application broken, should stay at least router with packet filtering activated)
- All traffic that is not explicitly authorized is forbidden



Conclusion

Chapter 7

Resume: Mechanisms layered model



Conclusion: One VPN mechanism Cannot fit All Subscribers !...

- Challenge: Support multiple VPN models to offer best compromise between:
  - Security requirements
  - Number of sites
  - Number of users
  - QoS requirements
  - Traffic volume
  - Willingness to outsource
  - Staff expertise



...Conclusion: Define a Policy for your Security !

- Audit
- Trust levels
- Data availability for users
- Data sensibility
- Privileged users
- Mechanisms to use *(encryption, filtering, tunneling, ...)*
- Disaster recovery plan



- Security Architecture
- Products
- Cost

Bonne lecture !