Giao thức kerberos

Ưu điểm:

+ độ ăn toàn cao

+ single sign-on rất tiện

Nhược điểm:

+ phức tạp,tốn chi phí

+ kdc dễ bị quá tải

+ đồng bộ thời gia giữa các server là rất chặt chẽ

Giao thức eap, radius và 802.1x

1 giao thứ eap

- EAP = Extensible Authentication Protocol

- eap +ko dây(wlan -wifi)

+ có dây(datalink)

-Có thể đổi thuộc hệ thống

- eap có 4 message:

1 request

2 response

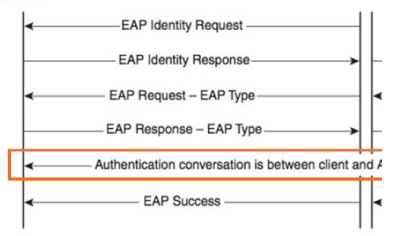
1. success
2. Failure

- hỗ trợ 40 phương thức xác thực

- default = eap- md5(giống chap)

- authenticator +có dây NAS

+ko dây AP



2 chuẩn 802.1x

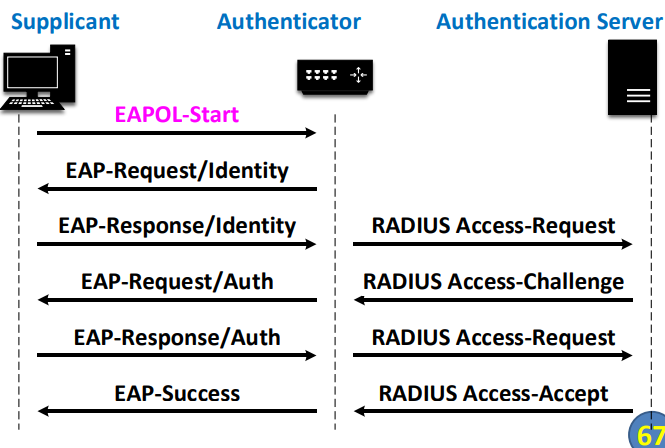
- chuẩn dành cho mạng lan quy định cách sử dụng giao thức eap/lan

=> EAP ol= EAP over LAN

3 giao thức RADIOS

- RADIUS = Remote Authentication Dial-In User Service

- hoạt động theo chuẩn 3A



Chương 3

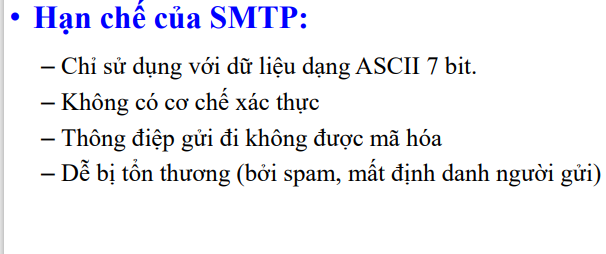
Giao thức http

Cổng 80

Code 220 ready

Code 250 accept

Code 354 start



Mục đích mime hỗ trợ smtp

Trong việc truyênd được nhiều định dạng, format khác nhau

-mime là 1 chuẩn ko phải giao thức

Base64-encoding

Xác thực pop3:apop

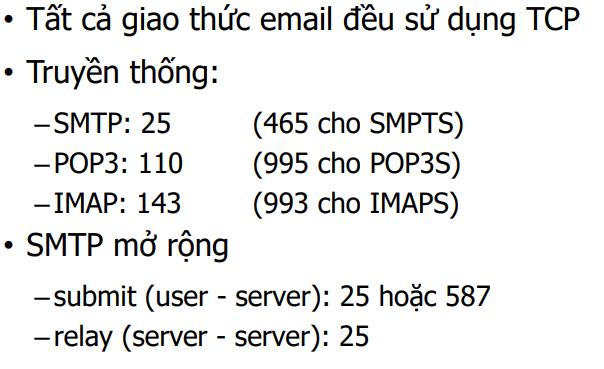
SPF(Sender Policy Framework giải pháp chống mạo danh người gửi)

Giao thức an toàn tông tin điện tử

Chống can thiệp nội dung

S/mine:mã hóa nọi dung bức thư

PGP: kí số bức thư

1

Esmtp,SPF

Imaps, smtps, pop3s

s/mine, PGP

Đăng nhạp từ xa(telnet,SSH)

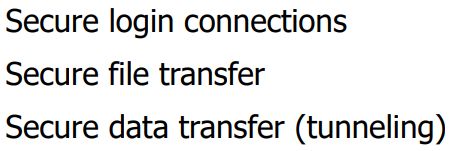
Ssh

Secure shell

3 nhiệm vụ

Đăng nhập từ xa

Truyền file tù xa

Tạo đường hầm để truyền thông tin 

-xác thực

+ xác thực server : xác thực bằng public key

+ xác thưc bằng client: xác thực bằng password hoặc bằng public key

- xác thực thông điệp: hmac(md5, sha1)

-mã hóa dữ liệu: symmetric ciphers

-nén dữ liệu :GZIP

- có ba giao thức con

1giao thức ssh trans

Xác thực server

Trao đổi khóa

Mã hóa dl toàn vẹn

Nén dl

2 giao thức ssh auth

Xác thực clie nt

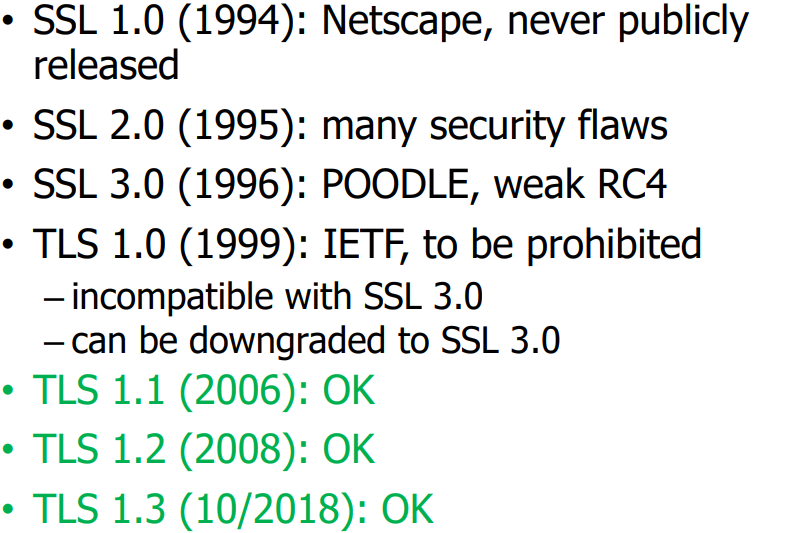
3 giao thức ssh conn

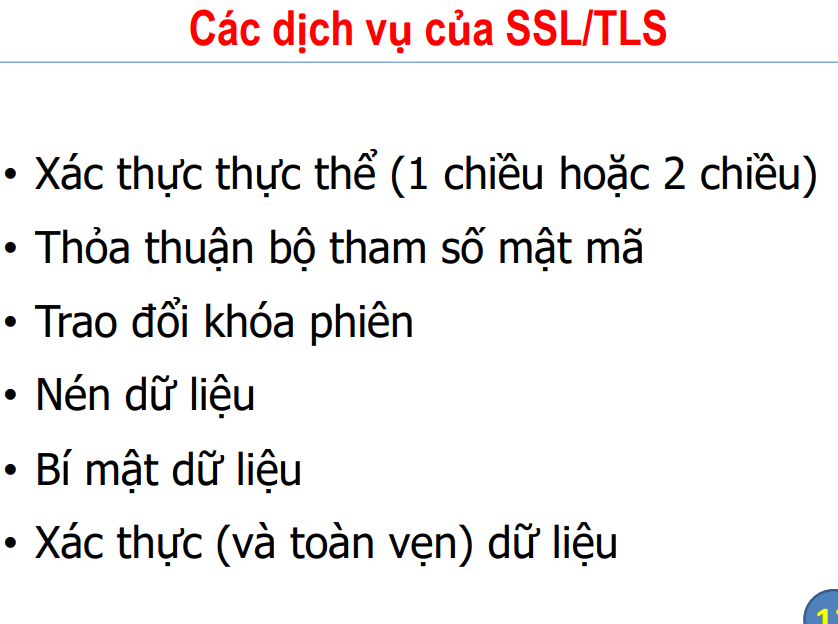
Cho phép client kết nối đến server

Dc sử dụng các dịch vụ của ssh

Bộ gia thức ssl/tls

Tổng quan







Giao thức record

Giao thức SSH

3 giao thức con của SSH

Ssh trans

- xác thực server -> xác thực bằng public key(server)

-trao đổi khóa

- trao đổi các tham số mật mã

-mã hóa dữ liệu

Ssh auth :xác thực client

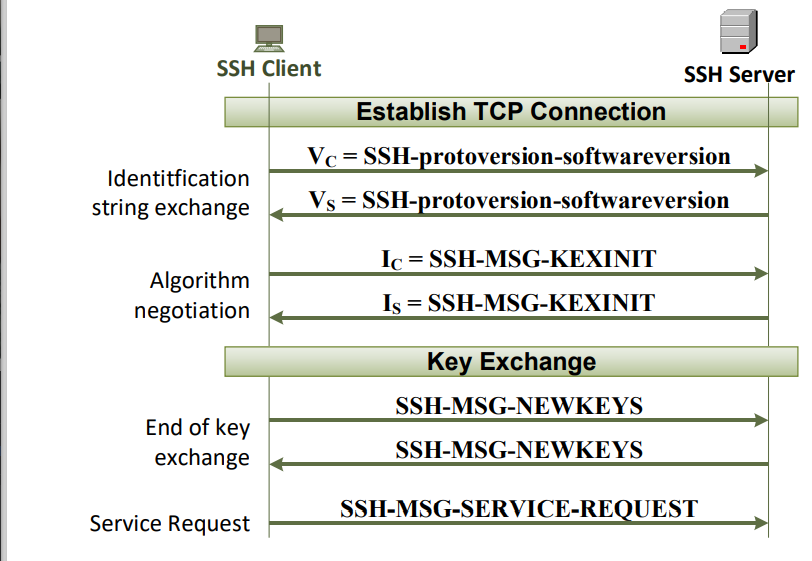
-2 cách xác thực:password hoặc public key

Ssh conn: cho phép client kết nối đến server

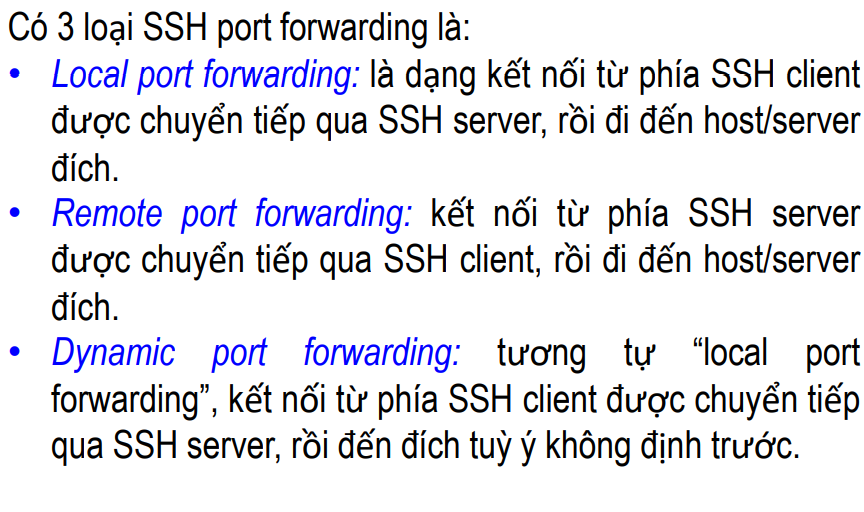
Sftp = ssh+ftp

Ftps = ftp+ssl

\*)ssh Trans



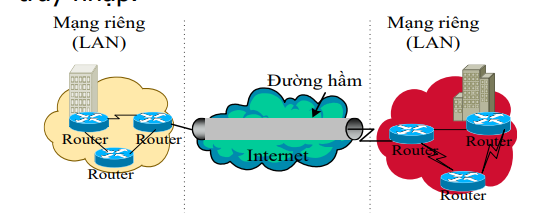
Port forwarding



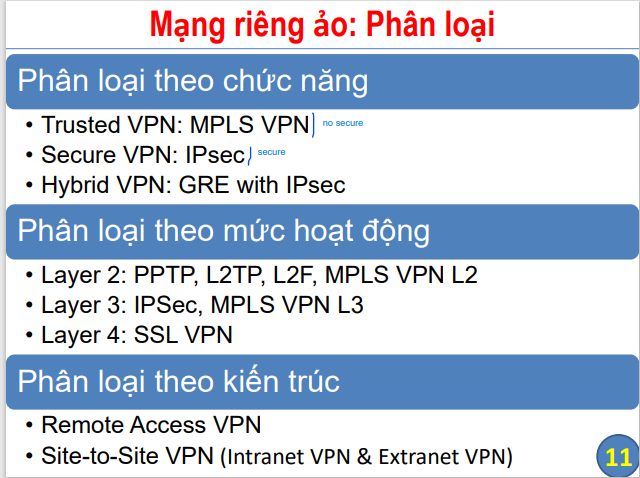
VPN

1 tống quan về VPN

\*)mạng riêng(private network)



\*)phân loại vpn



Remove access VPN single VPN

Trong site to site VPN + internet VPN

+ extranet VPN

Dịch vụ an toàn có thể cung cấp

• Đảm bảo tính bí mật

• Đảm bảo tính toàn vẹn

• Đảm bảo tính xác thực

• Chống tấn công phát lại

2 giới thiệu IPSEC

IPSec = Internet Protocol Security

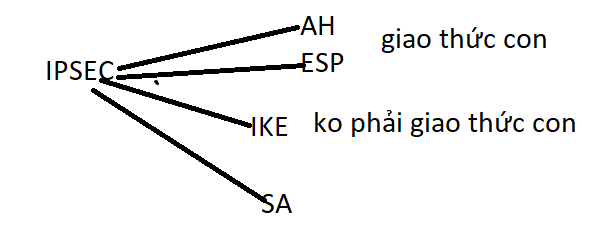
Cung cấp các khả năng:

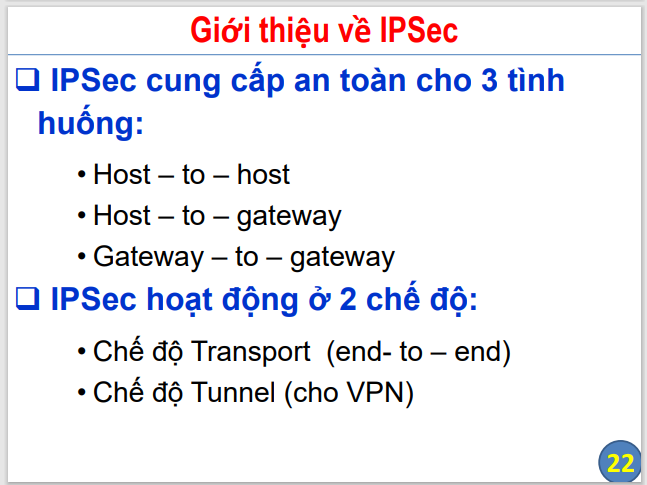
• Xác thực nguồn gốc thông tin

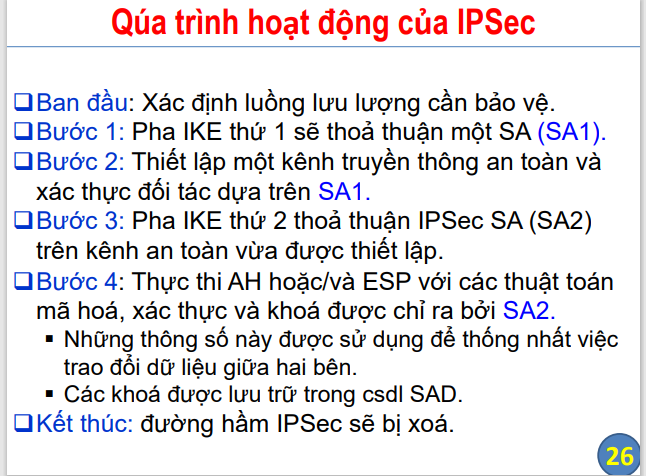
• Kiểm tra tính toàn vẹn thông tin

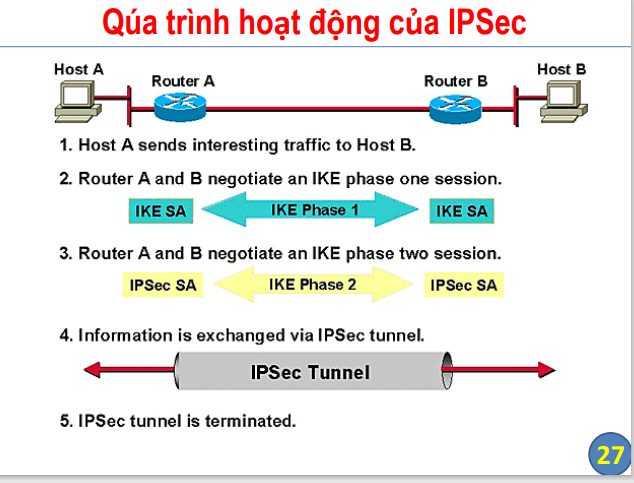
• Đảm bảo bí mật nội dung thông tin

• Cung cấp khả năng tạo và tự động làm tươi khoá mật mã một cách an toàn









3 Tổ hợp an toàn (SA)

Tổ hợp at= 1 danh sách các thông số

-1 kết nối logic theo 1 hướng duy nhất

\*)Có hai kiểu SA:

• ISAKMP SA (hay IKE SA)

• IPSec SA

\*)Một SA gồm 3 phần:

+ chỉ số tha số an toàn

+ địa chỉ đích

+giao thức an toàn(AH,ESP)

\*)Nội dung của 1 SA

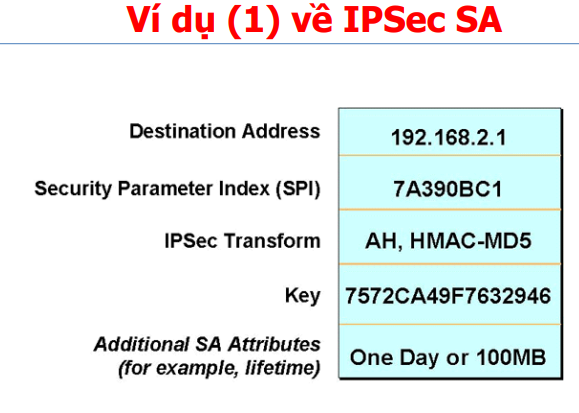
• Giao thức an toàn: AH, ESP

• Thuật toán, khóa mật mã: DES, 3DES

• Phương pháp, khóa xác thực cho AH | ESP: Hàm băm (HMAC, MD5, SHA1), chữ ký số (RSA), chứng thư số, Diffie-Hellman…

• Thông tin liên quan đến khoá: khoảng thời gian thay đổi, khoảng thời gian làm tươi.

• Thông tin liên quan đến chính SA: địa chỉ nguồn SA, khoảng thời gian làm tươi.

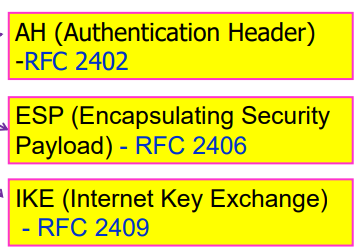


\*)Một SA sử dụng hai cơ sở dữ liệu:

▪ Cơ sở dữ liệu tổ hợp an toàn (SAD - Security Association Database)

▪ Cơ sở dữ liệu chính sách an toàn (SPD- Security Policy Database)

Trong SAD thì có trường SPI còn SPD ko có



Khi chúng ta bảo vệ 1 gói tin bằng

AH vậy trường protocol là 51 (xác thực, toàn vẹn)

ESP vậy trường protocol là 50(xác thực , toàn vẹn, bí mật)

-xác thực người gửi, toàn vẹn dữ liệu, chống chối bỏ

Giao thức AH

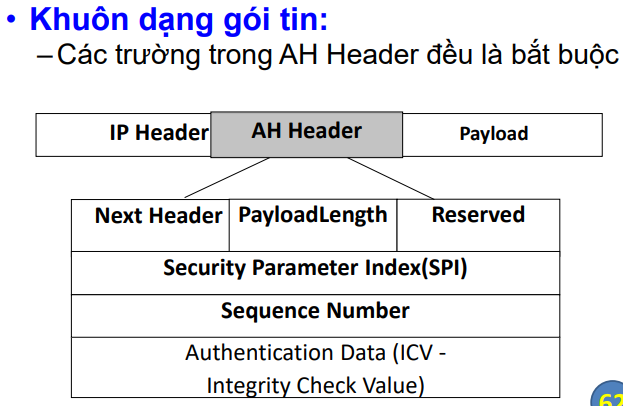
+transport(vận tải)

+tunnel(đường hầm)

- AH ưu điểm :Bảo vệ được toàn bộ gói tin

- AH nhược điểm :ko mã hóa

Chế độ tunnel:



Trường ICP có 96 bit

ICP = Hash(IP Header+Payload+key)

Giao thức ESP

Nhược điểm ko mã hóa , ko xác thực ip header nên dễ bị giả mạo

Ưu điểm có được mã hóa dữ liệu