**1.**

**enable**

**configure terminal**

**hostname [tên router]**

**ip domain-name [tên miền]**

**crypto key generate rsa**

**username [tên người dùng] privilege 15 secret [mật khẩu]**

**aaa new-model**

**aaa authentication login default local**

**aaa authorization exec default local**

**line vty 0 4**

**transport input ssh**

**login local**

**exit**

**2.Giới thiệu tổng quan AAA**  
AAA là một hệ thống quản lý và bảo mật mạng, cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. AAA bao gồm các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng:

• Authentication (xác thực): cung cấp việc xác thực người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng.

• Authorization (cấp quyền): Một khi đã nhận dạng người dùng, ta có thể giới hạn thẩm quyền mà người dùng có thể làm.

• Accounting (tính cước): Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm.

Có hai giao thức bảo mật dùng trong dịch vụ AAA đó là :

1. TACACS: sử dụng giao thức hướng kết nối là TCP với port 49.

TACACS có một số ưu điểm như:

* TACACS+ hỗ trợ nhiều giao thức
* TACACS thường được dùng trong môi trường enterprise. Nó có nhiều ưu điểm và làm việc tốt đáp ứng yêu cầu quản lý mạng hàng ngày.
* TACACS+ mã hóa toàn bộ gói bằng việc sử dụng khóa bí mật chung nhưng bỏ qua header TACACS chuẩn.

2. RADIUS: Là giao thức dựa trên mô hình client-server và sử dụng giao thức UDP. Giao tiếp giữa client và RADIUS server được xác thực thông qua việc sử dụng khóa bí mật chung không được truyền qua mạng.

RADIUS có một số ưu điểm như:

* RADIUS có phần overhead ít hơn so với TACACS vì nó sử dụng UDP
* Với cách thức phân phối dạng source code, RADIUS là dạng giao thức hoàn toàn mở rộng. Người dùng có thể thay đổi nó để làm việc với bất kì hệ thống bảo mật hiện có.
* RADIUS yêu cầu chức năng tính cước (accounting) mở rộng

3.

1. Đặc điểm của Firewall:
   * Firewall là một thành phần quan trọng trong mạng để bảo vệ và kiểm soát lưu lượng mạng.
   * Nhiệm vụ chính của firewall là kiểm tra, lọc và chặn lưu lượng dựa trên các quy tắc được định nghĩa trước.
   * Firewall có thể ngăn chặn các cuộc tấn công từ bên ngoài, như tấn công từ chối dịch vụ (DoS), tấn công từ điển và tấn công thực thi mã độc.
   * Ngoài ra, firewall cũng có thể kiểm soát lưu lượng ra vào mạng bằng cách giới hạn quyền truy cập và xác thực người dùng.
2. Chức năng của Access Control List (ACL):

* ACL là một công cụ quản lý và kiểm soát lưu lượng mạng dựa trên quy tắc.
* ACL được sử dụng để xác định các quy tắc lọc gói tin cho phép hoặc từ chối truy cập vào mạng hoặc các dịch vụ.
* ACL có thể được cấu hình trên router hoặc switch để kiểm soát lưu lượng đi qua các giao diện mạng.
* Các quy tắc ACL có thể dựa trên địa chỉ IP nguồn và đích, giao thức, cổng và các thông tin khác.

4.

Mô tả cơ chế NAT:

* Cơ chế NAT (Network Address Translation) là một quy trình chuyển đổi địa chỉ IP của gói tin trong quá trình truyền thông qua một router.
* NAT cho phép nhiều thiết bị trong mạng sử dụng cùng một địa chỉ IP công cộng và cung cấp bảo mật bằng cách ẩn địa chỉ IP nội bộ.
* enable
* configure terminal
* ip nat pool NAT-POOL 209.165.200.1 209.165.200.14 netmask 255.255.255.240
* ip nat inside source list 100 pool NAT-POOL overload
* access-list 100 permit ip 192.168.1.0 0.0.0.255 any

5.

Mô tả về VPN:

* VPN (Virtual Private Network) là một công nghệ cho phép kết nối an toàn và riêng tư giữa các mạng và thiết bị từ xa thông qua mạng công cộng như Internet.
* VPN sử dụng các phương thức mã hóa và giao thức bảo mật để tạo ra một kênh kết nối an toàn giữa các địa điểm khác nhau, cho phép truyền dữ liệu một cách bảo mật và ẩn danh.

Cấu hình VPN (Site to Site)

crypto isakmp policy 1

hash sha

authentication pre-share

group 2

encryption aes 256

exit

crypto isakmp key cisco address 192.168.1.2

crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac

access-list 100 permit ip 10.0.10.0 0.0.0.255 172.16.10.0 0.0.0.255

crypto map R1-R2\_MAP 1 ipsec-isakmp

match address 100

set transform-set R1-R2

set peer 192.168.1.2

set pfs group2

exit

Cấu hình VPN (Remote access)

Truy cập vào Router B và nhập các lệnh tương tự như trên, chỉ khác biệt ở phần cấu hình của Router B.