

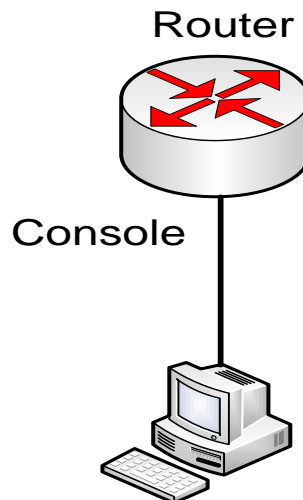


92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Bài: Recovery IOS bằng Xmodem và TFTPDLND

Khi ta cần nâng cấp hoặc phục hồi hệ điều hành cho Router, mà hiện tại không còn có một IOS nào còn tồn tại trong Router thì hai phương pháp có thể thực hiện là Xmodem và TFTPDLND. Ta sẽ làm những mô hình lab dưới đây.

I. Xmodem



Xmodem thường được sử dụng trong trường hợp phục hồi hệ điều hành cho một con Router mà nó không còn hệ điều hành. Router chỉ có boot vào rommon. Ngoài ra ta có thể dùng phương thức này trong trường hợp không có một TFTP Server hoặc không có một kết nối đến một network nào cả. Trong trường hợp này ta chỉ



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

có duy nhất một kết nối từ PC đến Router thông qua cổng console. Tuy nhiên phương thức truyền này khá tốn thời gian.

Mặc định khi ta dùng chương trình hyperterminal của Window hoặc các chương trình khác kết nối đến Router thông qua cổng console thì ta để tốc độ truyền file là 9600 bps. Tuy nhiên nếu ta để tốc độ truyền như vậy thì quá trình này khá lâu. Vì vậy lúc này ta chuyển tốc độ truyền dữ liệu vào Router lên 115200 bps. Ta sẽ vào chế độ rommon của Router bằng tổ hợp phím Ctrl + Break và chuyển tốc độ giao tiếp giữa Router và PC lên 115200 bps.

```
rommon 1 >confreg  
Configuration Summary  
enabled are:  
break/abort has effect  
console baud: 9600  
boot: the ROM Monitor
```

```
do you wish to change the configuration? y/n [n]: y  
enable "diagnostic mode"? y/n [n]:  
enable "use net in IP bcast address"? y/n [n]:  
enable "load rom after netboot fails"? y/n [n]:  
enable "use all zero broadcast"? y/n [n]:  
disable "break/abort has effect"? y/n [n]:  
enable "ignore system config info"? y/n [n]:  
change console baud rate? y/n [n]: y  
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7  
change the boot characteristics? y/n [n]:
```

```
Configuration Summary  
enabled are:  
break/abort has effect  
console baud: 115200
```



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
boot: the ROM Monitor
```

```
do you wish to change the configuration? y/n [n]:
```

```
You must reset or power cycle for new config to  
take effect.
```

```
rommon 2 >reset
```

Quá trình trên ta có thể làm nhanh hơn bằng cách chuyển số config register từ số hoạt động bình thường là 0x2102 thành số 0x3822 bằng câu lệnh

```
rommon 1 > confreg 0x3822
```

Sau khi làm đến đây ta sẽ thấy rằng chương trình hyperterminal của ta lúc này không còn giao tiếp được với Router nữa bởi vì mặc định hyperterminal hoạt động ở 9600 bps còn Router lúc này hoạt động ở 115200 bps.

Ta mở lại chương trình hyperterminal và chỉnh tốc độ hoạt động của nó lên 115200 bps. Lúc này ta sẽ bắt đầu quá trình nạp hệ điều hành cho Router bằng giao thức xmodem

```
rommon 1 >  
rommon 1 >xmodem -?  
xmodem: illegal option -- ?  
usage: xmodem [-cyrx] <destination filename>  
-c CRC-16  
-y ymodem-batch protocol  
-r copy image to dram for launch  
-x do not launch on download completion  
rommon 2 >  
rommon 2 >  
rommon 2 > xmodem -c c1600-is-mz.122-10a.bin
```

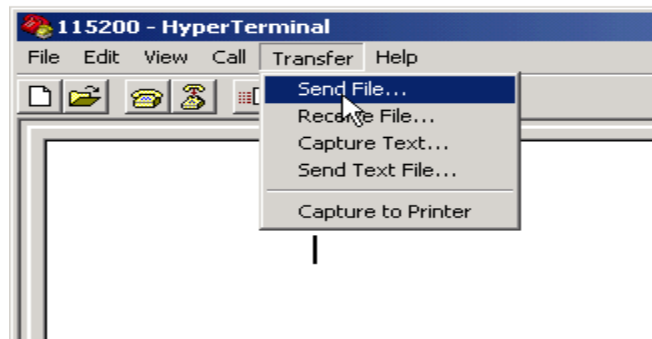


92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Do not start the sending program yet...

File size	Checksum	File name
9939820 bytes (0x97ab6c)	0x4991	c2600-is-mz.122-7a.bin

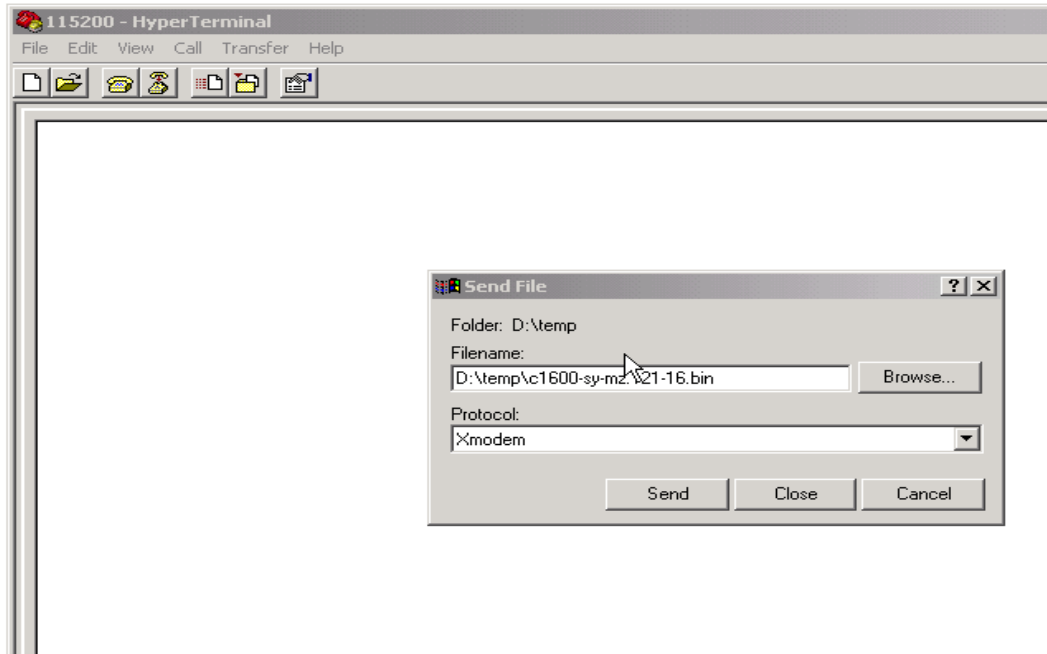
Ta bắt đầu quá trình gửi IOS bằng cách vào Transfer / Send File. Chọn IOS mình cần nạp và phương thức truyền là Xmodem. Tuy nhiên ta nên chú ý xem rằng IOS mình nạp vào có thích hợp với dung lượng flash của router và loại router. Xem hình 1; 2; 3 bên dưới



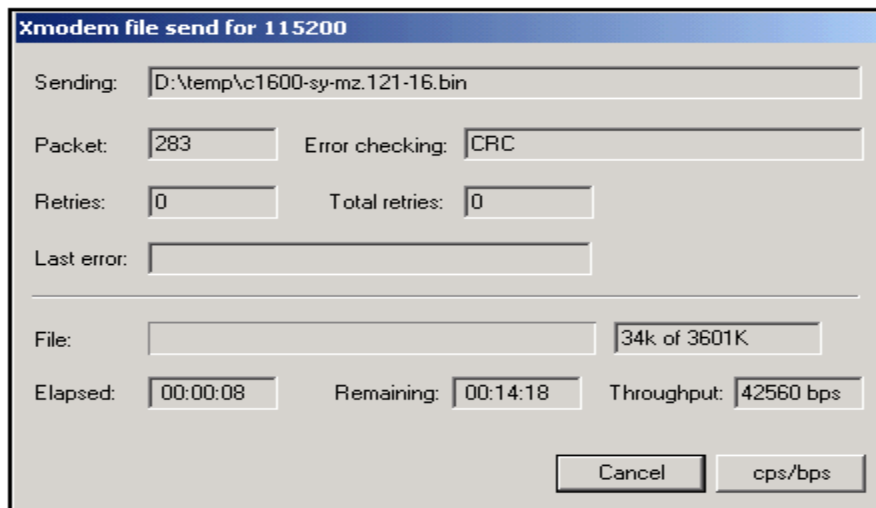
Hình 1.



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đình Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Hình 2.





92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Hình 3.

Sau khi quá trình ta truyền IOS thành công ta nên kiểm tra lại flash của Router và chuyển số config register lại thành 0x2102

```
rommon 9 >dir flash:  
File size Checksum File name  
3686656 bytes (0x384100) 0x1a5e c1600-sy-mz.121-  
16.bin  
rommon 10 >confreg 0x2102
```

You must reset or power cycle for new config to take effect.

```
rommon 11 >reset  
System Bootstrap, Version 12.0(19981130:173850)  
[rameshs-120t_lava 114],  
DEVELOPMENT SOFTWARE Copyright (c) 1994-1998 by  
cisco Systems, Inc.  
Simm with parity detected, ignoring onboard DRAM  
C1600 platform with 16384 Kbytes of main memory  
program load complete, entry point: 0x4020060,  
size: 0x15568c  
%SYS-6-BOOT_MESSAGES: Messages above this line are  
from the boot loader.  
program load complete, entry point: 0x2005000,  
size: 0x3840e0
```

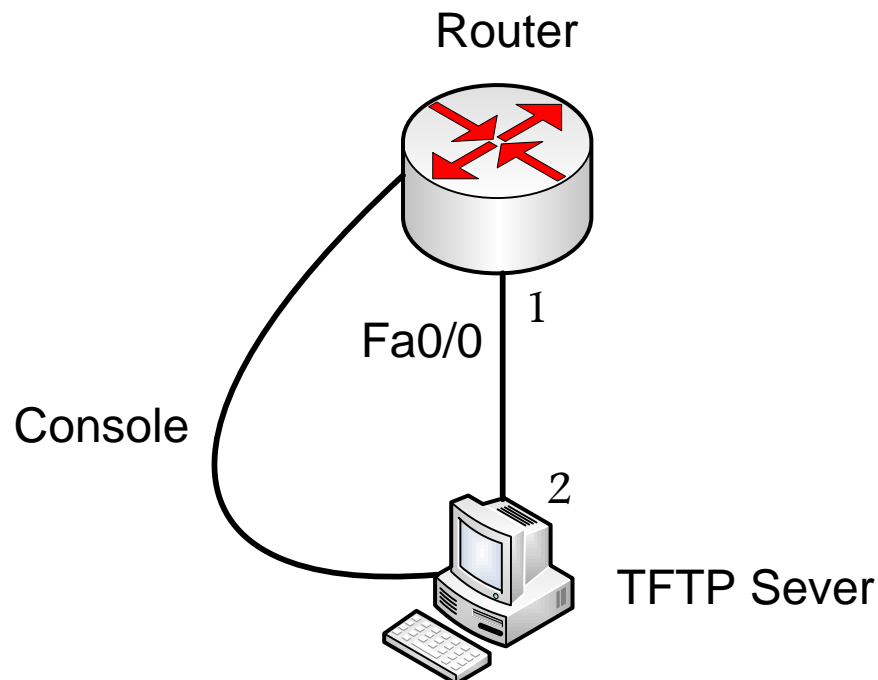
```
Self decompressing the image :  
#####  
#####
```



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

II. TFTPDLND

- Trong điều kiện có network thì ta nên recovery IOS bằng phương pháp TFTPDLND vì tốc độ truyền file của giao thức này hơn hẳn Xmodem.
- Lúc này ta cần có một PC với vai trò là TFTP Server.
- Sơ đồ kết nối như bên dưới và nhập những lệnh bên dưới nhằm thiết lập những thông số kết nối để Router có thể kết nối đến PC.



rommon 17 > ?



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đình Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
rommon 18 > set
```

```
rommon 19 > IP_ADDRESS=192.168.1.1
```

```
rommon 20 > IP_SUBNET_MASK=255.255.255.0
```

```
rommon 21 > DEFAULT_GATEWAY=192.168.1.2
```

```
rommon 22 > TFTP_SERVER=192.168.1.2
```

```
rommon 23 > TFTP_FILE=c2600-advsecurityk9-mz.124-8d.bin
```

```
rommon 24 > tftpdnld
```

```
IP_ADDRESS: 192.168.1.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.1.2
TFTP_SERVER: 192.168.1.2
TFTP_FILE: c2600-is-mz.113-2.0.3.Q
```

```
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on
flash will be lost!
```

```
Do you wish to continue? y/n: [n]: y
```

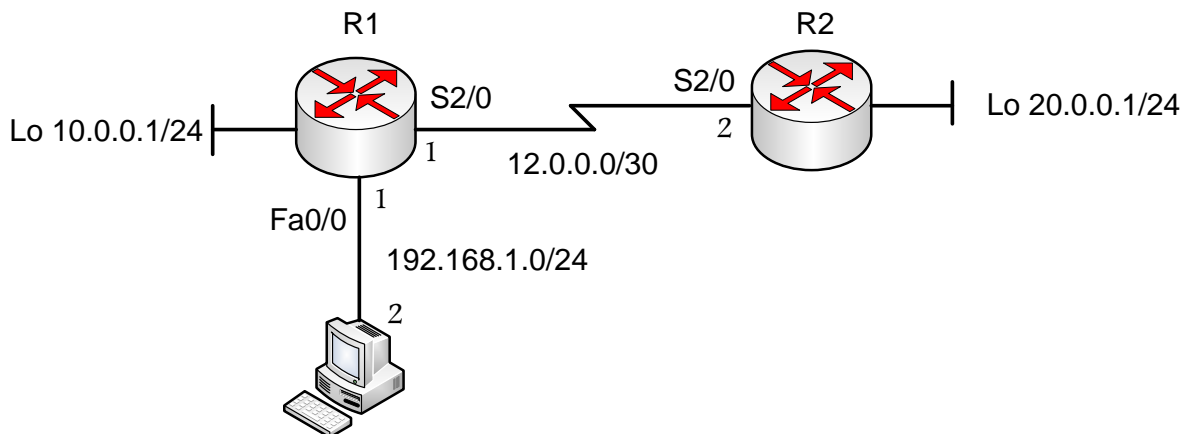
Ta mở chương trình TFTP Sever trên PC và quan sát quá trình hoạt động

```
Receiving c2600-is-mz.113-2.0.3.Q from
171.69.1.129 !!!!!!!
File reception completed.
Copying file c2600-is-mz.113-2.0.3.Q to flash.
Erasing flash at 0x607c0000
program flash location 0x60440000
rommon 22 >
```




92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Bài: Lab SSH



Trong bài lab trước ta đã biết cấu hình router từ xa thông qua giao thức telnet tuy nhiên telnet là một giao thức không có tính bảo mật. Thông tin được gửi đi dưới dạng cleartext. Như vậy để nâng cao tính bảo mật ta sẽ dùng giao thức SSH thay thế cho telnet.



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Các bước cần phải làm cho bài lab như sau

- Cấu hình địa chỉ IP vào các interface của router . Cấu hình static route trên Router 1 và Router 2
- Ping kiểm tra từng segment trong mô hình.
- Cấu hình SSH trên Router 1 và Router 2.
- Capture lại thông tin được trao đổi trên đường truyền.

1. Cấu hình địa chỉ IP và định tuyến cho mô hình bằng static route

a. Router 1

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#interface serial 2/0
```

```
Router(config-if)#ip address 12.0.0.1 255.255.255.252
```

```
Router(config-if)#no shutdown
```

```
Router(config)#exit
```

```
Router(config)#interface serial fa0/0
```

```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config)#exit
```

```
Router(config)#interface loopback 0
```

```
Router(config)#ip address 10.0.0.1 255.255.255.0
```



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
Router(config)#exit
```

```
Router(config)#ip route 0.0.0.0 0.0.0.0 12.0.0.2
```

b. Router 2

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config)#interface serial 2/0
```

```
Router(config-if)#ip address 12.0.0.2 255.255.255.252
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#clock rate 64000
```

```
Router(config)#exit
```

```
Router(config)#interface loopback 0
```

```
Router(config)#ip address 20.0.0.1 255.255.255.0
```

```
Router(config)#exit
```

```
Router(config)#ip route 192.168.1.0 255.255.255.0 12.0.0.1
```

```
Router(config)#ip route 10.0.0.0 255.255.255.0 12.0.0.1
```

2. Quá trình kiểm tra

- Từ Router 1 ping đến các IP của Router 2
- Ở PC ta dùng lệnh ipconfig và ping từ PC đến các interface của Router 1 và Router 2



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter Local Area Connection 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3579:5ac7:1d13:44fz16
    IPv4 Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 6:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\nhanld>
```

3. Cấu hình SSH trên Router 1 và Router 2

Để cấu hình SSH ta cần phải cấu hình một số phần như sau:

- Cấu hình hostname
- Cấu hình domain name
- Tạo ra key từ hostname và domain name ở trên
- Tạo ra một username và password cho user đăng nhập vào Router.
- Cấu hình một số tính năng cho giao thức SSH trên router.
- Cấu hình cho giao thức SSH vào đường vty.

Trên Router 1 ta nhập vào những lệnh sau:

```
Router(config)#hostname R1
```

```
R1(config)#ip domain name abc.com
```

```
R1(config)#crypto key generate rsa general-keys modulus 1024
```



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
The name for the keys will be: R1.abc.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*June 24 19:25:30.035: %SSH-5-ENABLED: SSH 1.99 has been
enabled
```

```
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ip ssh version 2
R1(config)# username cisco password cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Tương tự ta cấu hình cho Router 2
Router(config)#hostname R2

```
R2(config)#ip domain name bcd.com
```

```
R2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R2.bcd.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*June 24 19:25:30.035: %SSH-5-ENABLED: SSH 1.99 has been
enabled
```

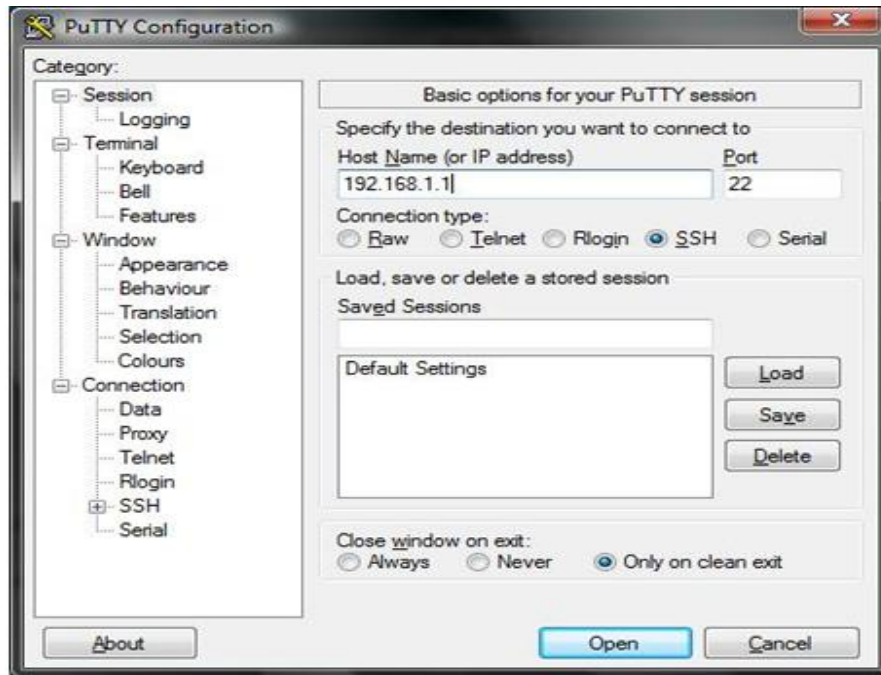
```
R2(config)# ip ssh time-out 60
R2(config)# ip ssh authentication-retries 2
R2(config)# ip ssh version 2
R2(config)# username cisco123 password cisco123
R2(config)# line vty 0 4
R2(config-line)# login local
R2(config-line)# transport input ssh
R2(config-line)# exit
```

Ở PC ta tạo kết nối SSH đến Router 1 thông qua chương trình Putty

Giảng Viên: Lê Đình Nhân – Email: nhanld@athenvn.com



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Lúc này ta phải chấp nhận key được tạo thông qua thuật toán RSA để tạo kết nối SSH.

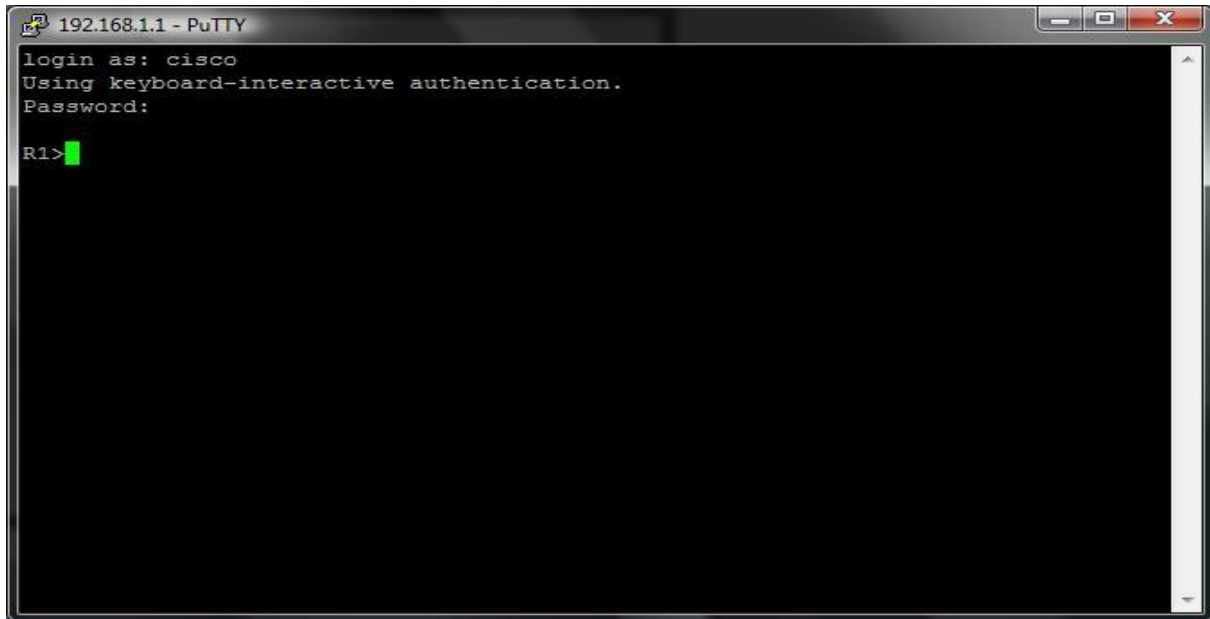


Giảng Viên: Lê Đình Nhân – Email: nhanld@athenvn.com



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Ta nhập vào username và password tương ứng mà ta đã tạo trên Router 1 để đăng nhập vào Router 1



Đứng ở giao diện dòng lệnh của Router 1, để tạo kết nối SSH đến Router 2 ta cần phải nhập câu lệnh sau:

```
R1#ssh -v 2 -l cisco123 -p 22 12.0.0.2
```




92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
192.168.1.1 - PuTTY
login as: cisco
Using keyboard-interactive authentication.
Password:

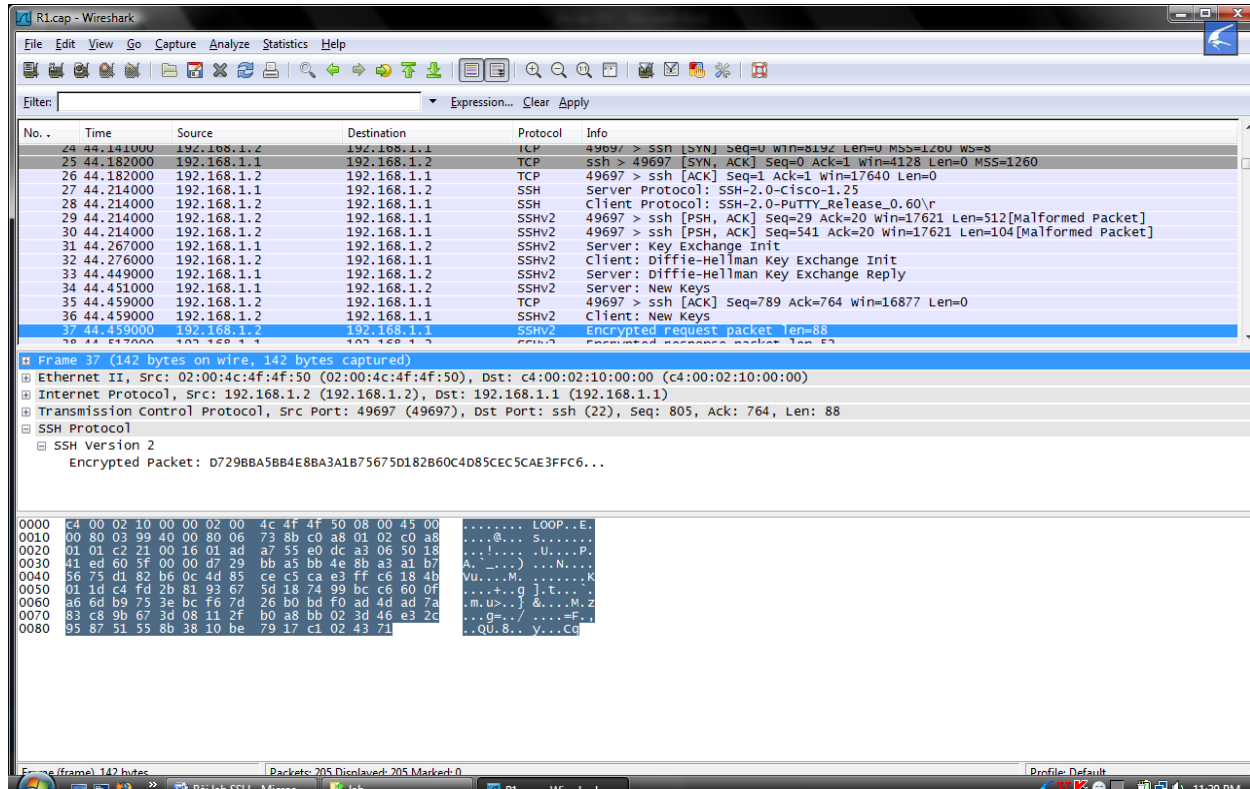
R1>enable
Password:
R1#ssh -v 2 -l cisco123 -p 22 12.0.0.2

Password:
R2>enable
```

Nhằm mục đích kiểm tra tính năng bảo mật của giao thức SSH ta thực hiện quá trình capture các luồng traffic trao đổi trên router . Hình đầu tiên là ta capture traffic từ PC đến Router1.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn





92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Bài: Truy cập vào Router thông qua SDM

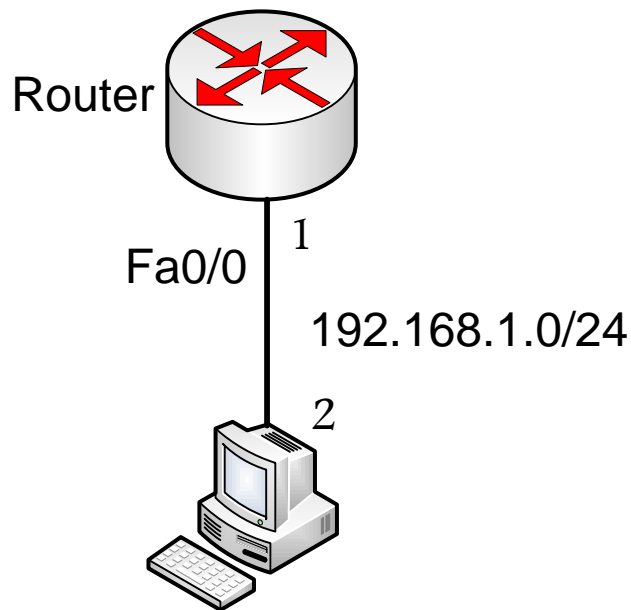
Ta có thường cấu hình các thiết bị của Cisco thông qua giao diện CLI tuy nhiên Cisco cũng hỗ trợ cấu hình thiết bị thông qua giao diện đồ họa. Một sản phẩm GUI được Cisco hỗ trợ để cấu hình router được gọi là Security Device Manager.

SDM là một ứng dụng Web-base hoạt động trên nền Java. SDM được cài đặt sẵn trong flash một số dòng sản phẩm router và admin có thể cấu hình router bằng trình duyệt Web kết hợp với SSL và Java. Trong quá trình cấu hình SDM dùng SSL để admin cấu hình và dùng SSH để tương tác ngược trở lại với giao diện web của admin.

SDM không được hỗ trợ tất cả dòng router. Ta có thể vào www.cisco.com/go/sdm để kiểm tra xem router của mình có được hỗ trợ hay không. Nếu như một router chưa có được cài đặt SDM thì ta có thể install nó vào router. IOS tối thiểu để có thể install SDM là version 12.2 và flash của router phải có sẵn từ 5 – 8 MB. Ta sẽ thực hiện bài lab theo sơ đồ như sau:



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Các bước ta cần làm trong bài lab như sau:

- Cấu hình căn bản
- Cấu hình SDM cho router
- Install SDM vào PC
- Kết nối từ PC đến Router

1. Cấu hình căn bản

Trước khi cấu hình để đăng nhập vào router thông qua giao diện SDM thì ta cũng phải cấu hình căn bản cho router như sau

```
Router> enable
```

```
Router# configure terminal
```



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

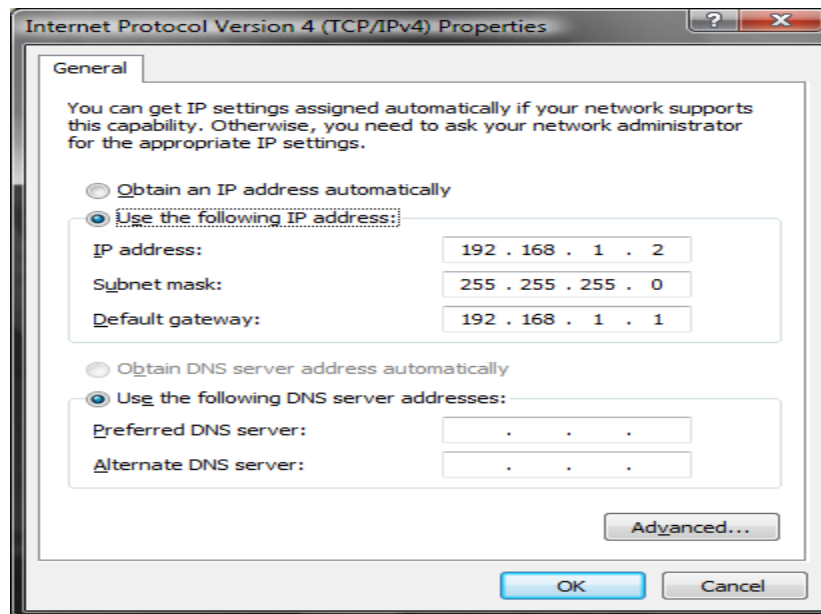
```
Router(config)# interface fastethernet 0/0
```

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
Router(config-if)# no shutdown
```

```
Router(config-if)#exit
```

Cấu hình địa chỉ IP vào PC.





92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
Administrator: C:\Windows\system32\cmd.exe

Ethernet adapter Local Area Connection 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3579:5ac7:1d13:44f%16
    IPv4 Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 6:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 12:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\nhanld>
```

Tiếp theo ta kiểm tra xem địa chỉ IP đã được cấu hình và ping kiểm tra từ PC đến router.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\nhanld>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=115ms TTL=255
Reply from 192.168.1.1: bytes=32 time=31ms TTL=255
Reply from 192.168.1.1: bytes=32 time=16ms TTL=255
Reply from 192.168.1.1: bytes=32 time=31ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 115ms, Average = 48ms

C:\Users\nhanld>
```



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

2. Cấu hình SDM cho Router

Ta sẽ nhập vào những lệnh theo cấu trúc như bên dưới

```
Router(config) # hostname router_name
Router(config) # ip domain-name domain_name
Router(config) # ip http server
Router(config) # ip http secure-server
Router(config) # ip http authentication local
Router(config) # username username privilege 15 secret 0
password
Router(config) # ip http timeout-policy idle seconds life seconds
requests number
Router(config) # line vty 0 15
Router(config-line) # privilege level 15
Router(config-line) # login local
Router(config-line) # transport input ssh
Router(config-line) # exit
```

SDM sử dụng SSL để send quá trình cấu hình và dùng SSH để trả lại giao diện của người đang cấu hình. Tuy nhiên cả hai giao thức SSL và SSH đều yêu cầu phải có cặp key theo thuật toán RSA. Để tạo ra được key ta cần phải có hostname và ip domain name. Tuy nhiên trong quá trình này ta không cần phải tạo key một cách manual bởi vì lần đầu tiên ta đăng nhập vào router thông qua giao diện SDM thì router sẽ tự động tạo ra key. Và cặp key sẽ được dùng trong quá trình SSL và SSH. Bởi vì SDM được hoạt động trên giao diện Web-base nên hai câu lệnh ip http server và ip http secure-server được dùng để kích hoạt Web Server, tính năng SSL trên Router.

Câu lệnh ip http authentication xác nhận dùng local database.

Username account để đăng nhập vào router phải là privilege 15.

Câu lệnh ip http timeout – policy chỉ là một câu lệnh option. Tuy nhiên ta nên dùng nó để xác nhận thời gian mà kết nối SDM được duy trì.



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

- Biến idle xác nhận số giây mà một kết nối web được duy trì trong trường hợp là không có data được gửi hay nhận. Mặc định là 180 giây.
- Biến life xác nhận số giây mà kết nối web được lưu trữ trong web server từ khi kết nối này được tạo. Mặc định là 180 giây nhưng ta có thể điều chỉnh tăng lên 86400 giây.
- Biến requests giới hạn số kết nối đồng thời vào router. Mặc định là 1
- Phần cuối là ta sẽ cấu hình VTY apply vào trong SSH. Quá trình này được dùng để tương tác với router. Để có thể cấu hình bằng SDM thì username đăng nhập phải là privilege 15 và trong quá trình cấu hình ở trên thì ta đang chứng thực bằng local database nên ta nhập câu lệnh login local.

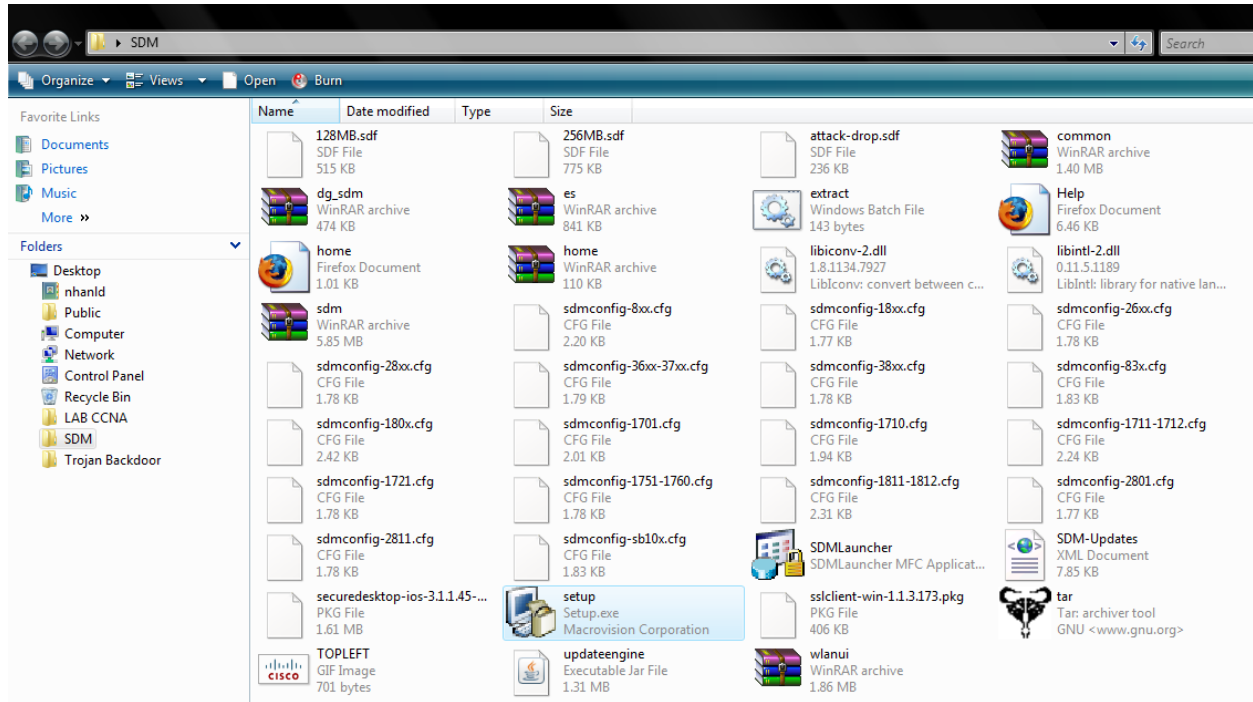
```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#ip domain name abc.com
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# username cisco privilege 15 password cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
```

3. Truy cập vào Router thông qua giao diện SDM

Ta có thể truy cập vào router thông qua giao thức http hoặc là https. Ta sẽ thực hiện quá trình cài đặt SDM vào trong PC hoặc vào trong Router. Ở đây ta chỉ thực hiện quá trình cài đặt vào trong PC. Ta chọn vào setup.exe trong SDM.zip



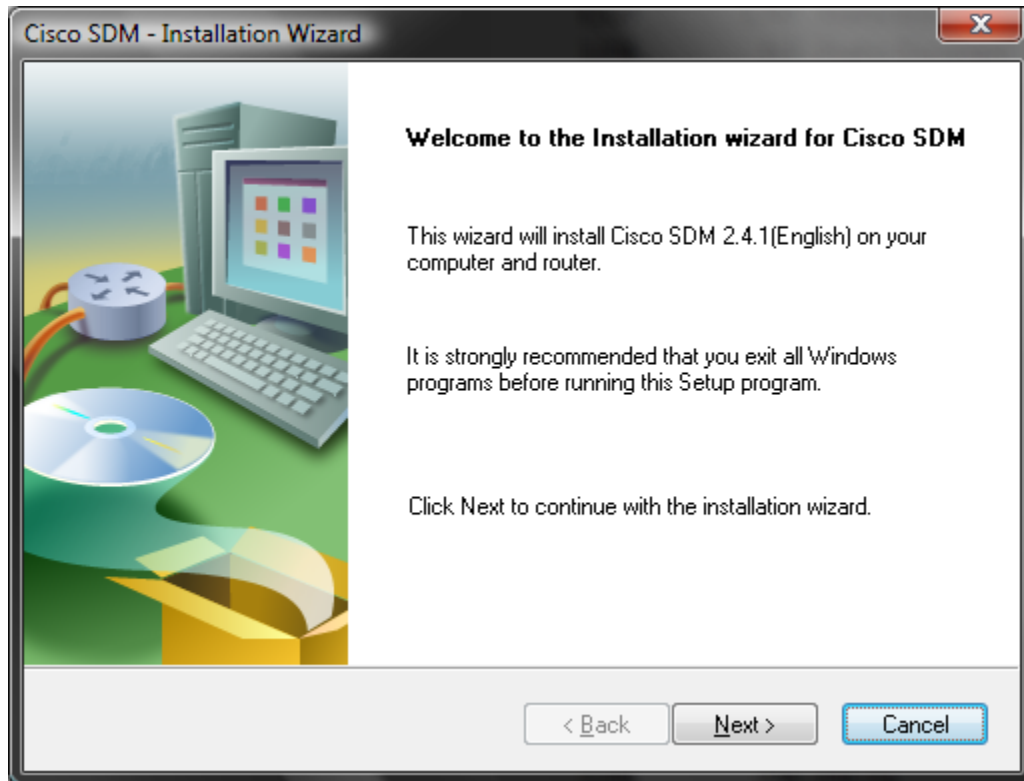
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Ta Click Next để làm tiếp

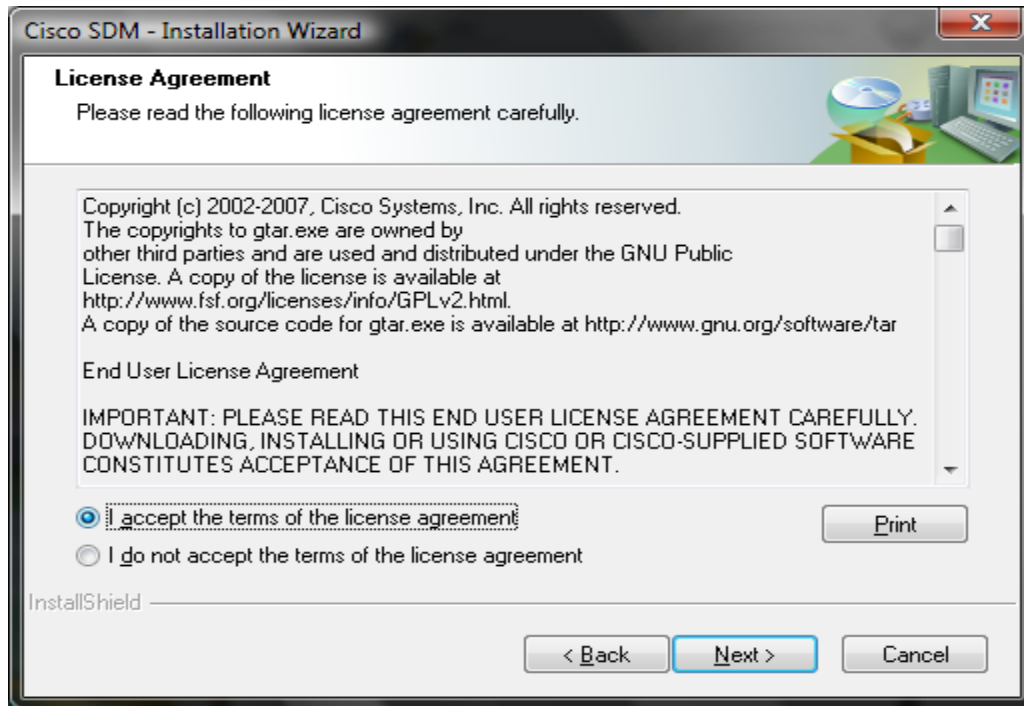


92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đình Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

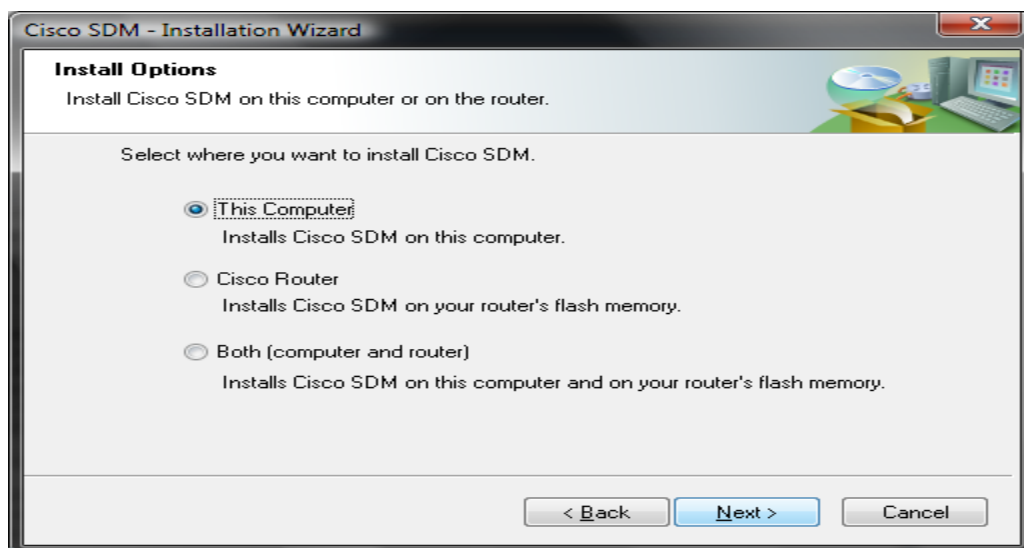




92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Ta chọn vào button “ I accept terms of the license agreement ”. Chọn Next

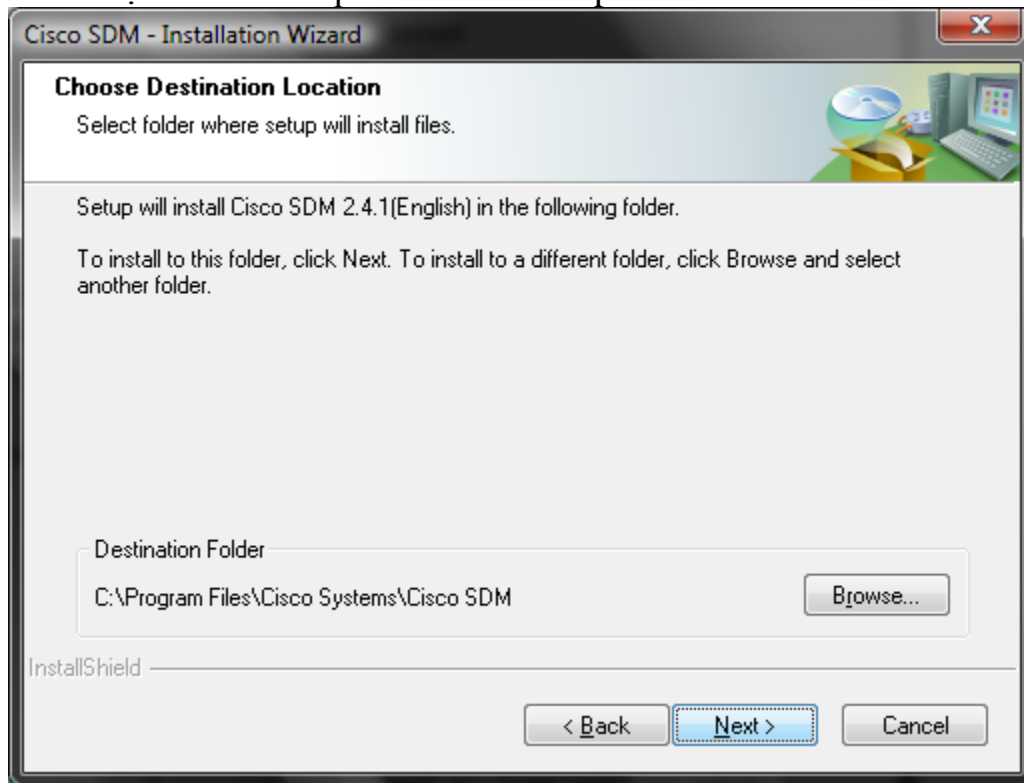


Giảng Viên: Lê Đình Nhân – Email: nhanld@athenvn.com



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

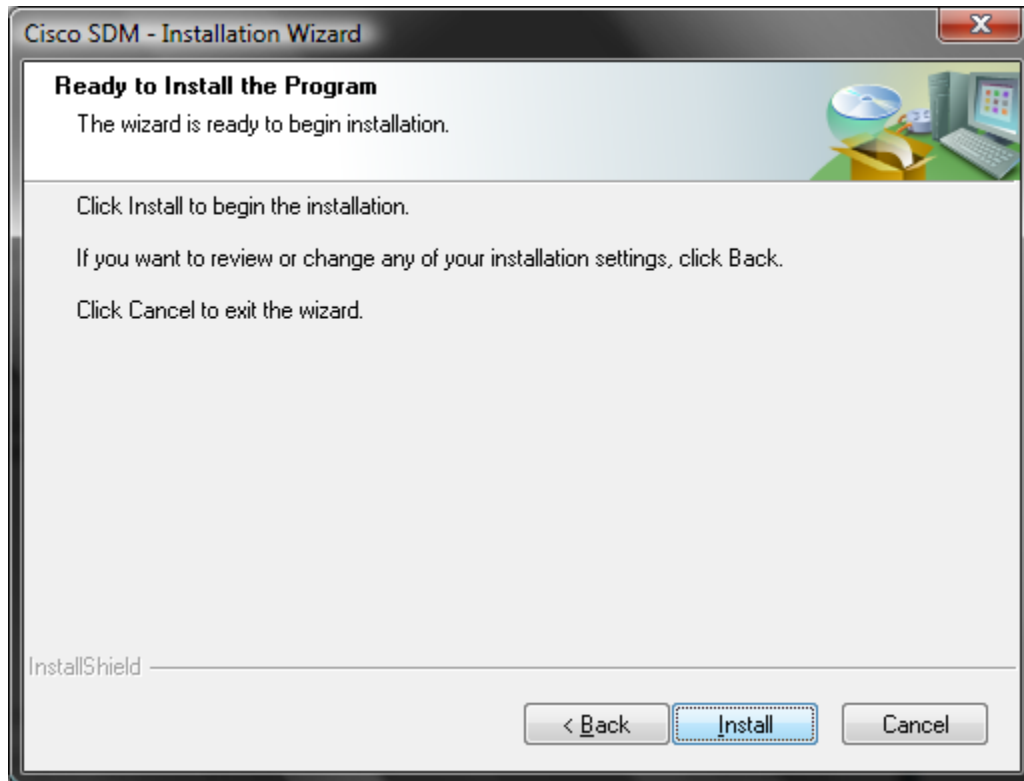
Ở đây ta có nhiều lựa chọn “ This computer ” chỉ install SDM trên một máy tính nào đó, “ Cisco Router ” install vào trong Router trong trường hợp này thì router phải có từ 5 – 8 MB free trên flash của router. Mục cuối cùng ta install trên cả hai. Ở đây ta chỉ chọn “ This computer ” và làm tiếp theo wizard của nó.



Ta có thể chọn nơi lưu trữ hoặc chọn đường dẫn mặc định và Next tiếp tục.



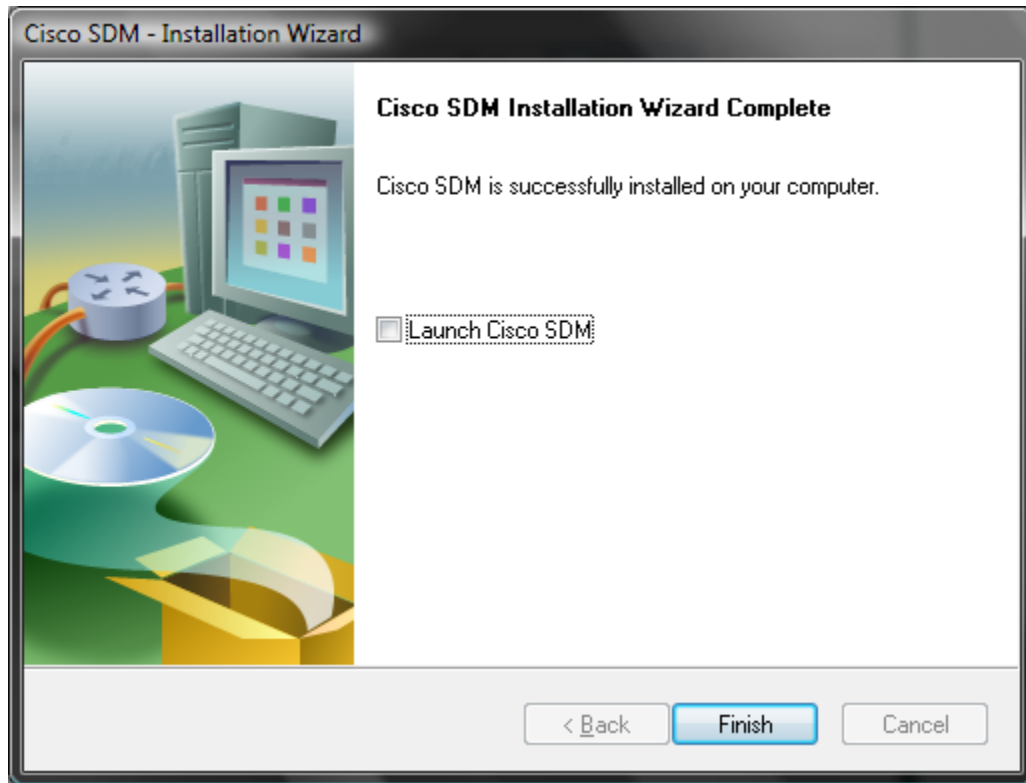
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Ta chọn install để bắt đầu quá trình cài đặt và Finish.



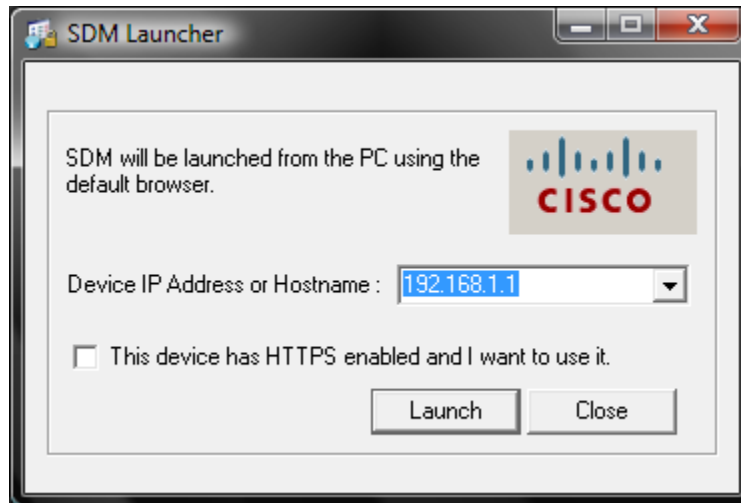
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Sau khi cài đặt xong, ngoài desktop xuất hiện thêm một icon “ Cisco SDM ” bên ngoài desktop. Ta thực hiện quá trình connect vào router thông qua giao diện SDM dựa trên giao thức http như sau

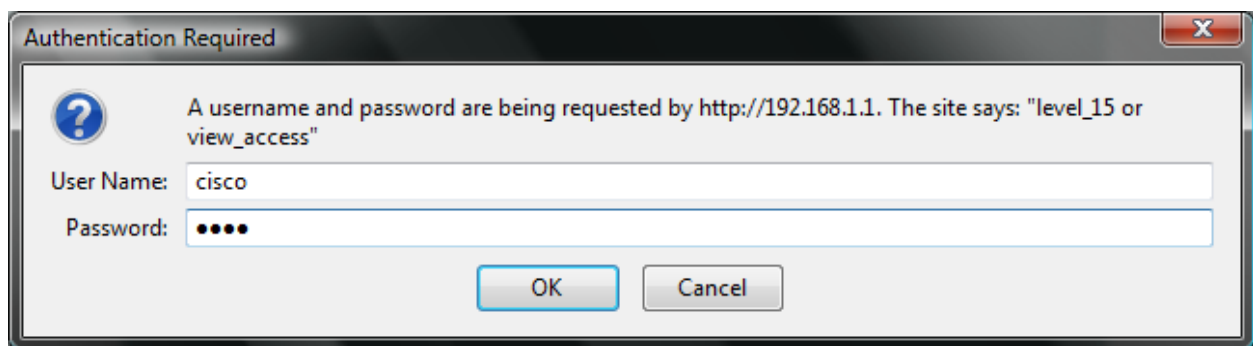


92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



a. SDM-HTTP

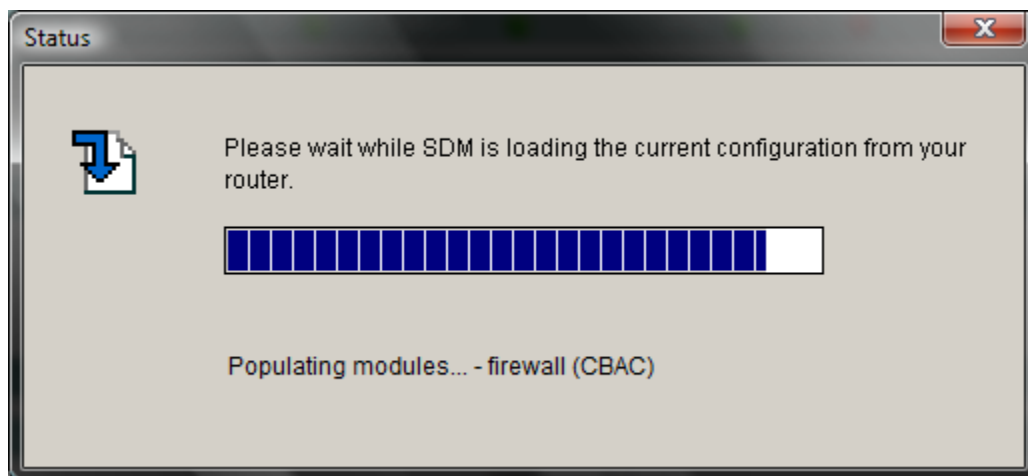
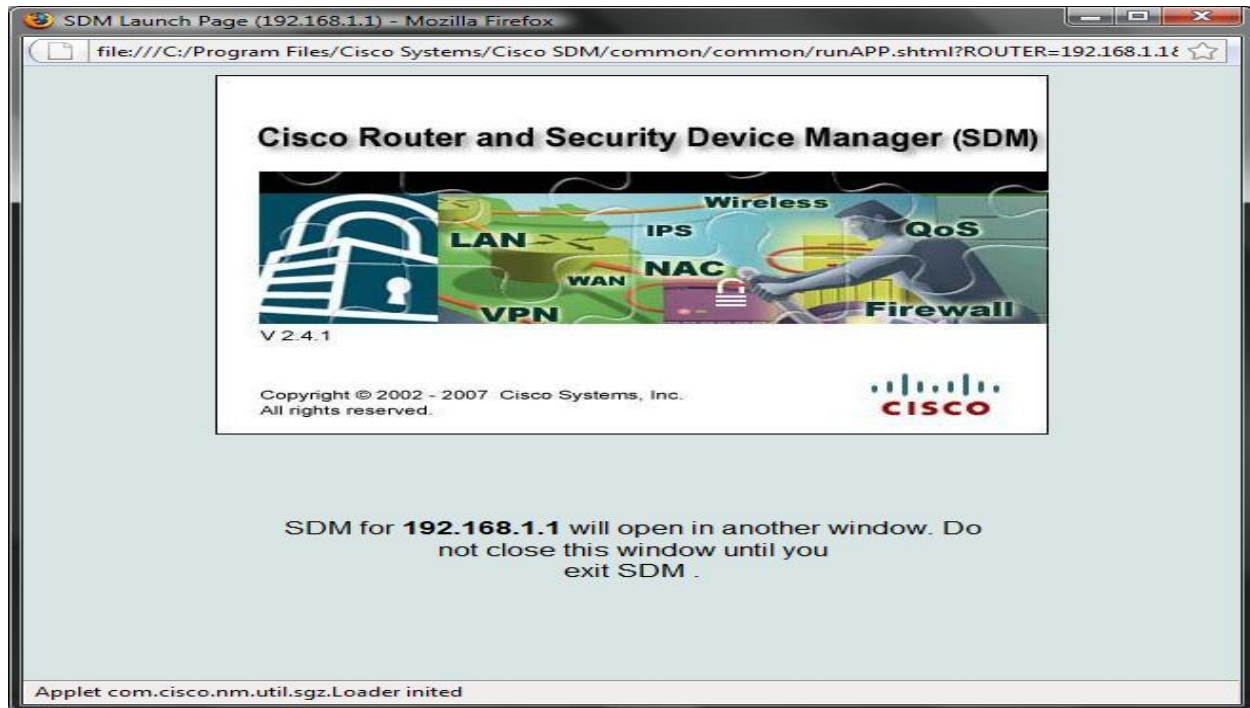
Vào Cisco SDM nhập vào địa chỉ IP của Router. Tuy nhiên ta phải tắt đi chức năng “ Block pop-up Window “ ở trình duyệt Web. Lúc này sẽ xuất hiện một forum login để ta đăng nhập. Ta nhập vào username và password với privilege 15.



Trình duyệt Web sẽ trả về cho ta màn hình “ Cisco Router and Security Device Manager “



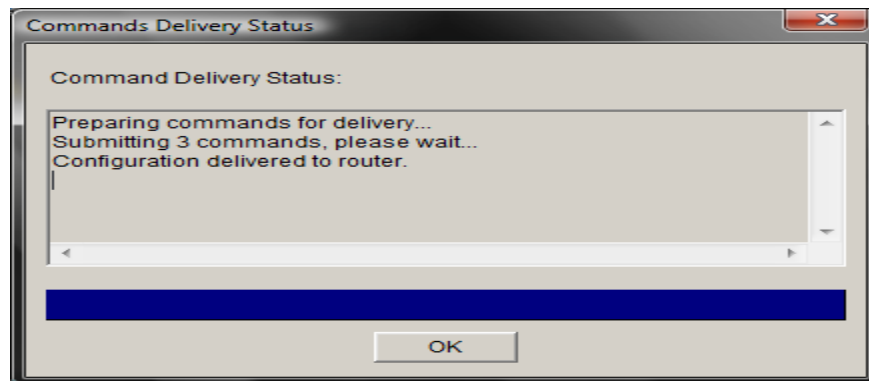
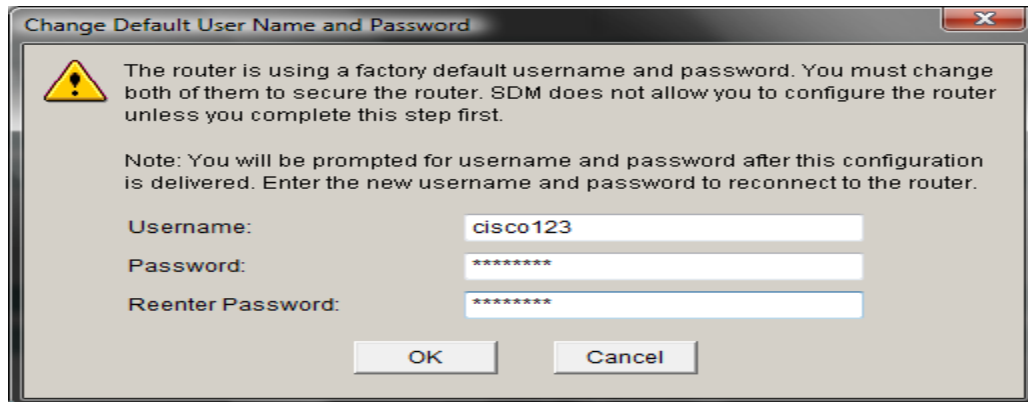
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Lúc này, Router sẽ yêu cầu ta tạo mới một username và password để thay thế cho username và password ta đã nhập vào router từ giao diện console của nó.



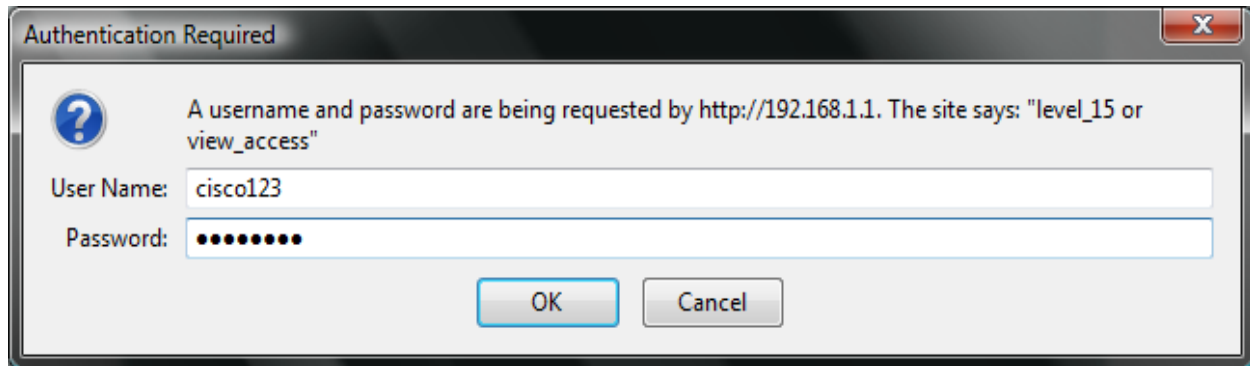
92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



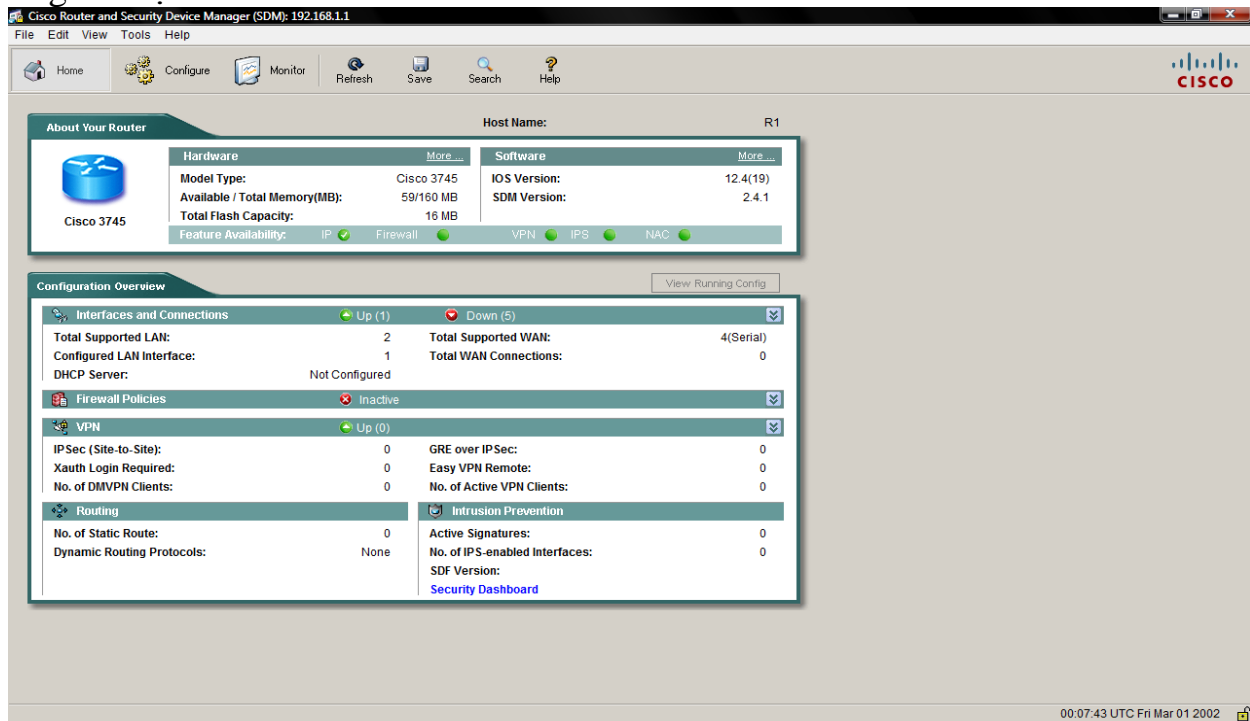
Ta Click OK và reconnect lại router từ PC thông qua “ Cisco SDM ”. Đến đây ta thực hiện lại quá trình login bằng username và password mới.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



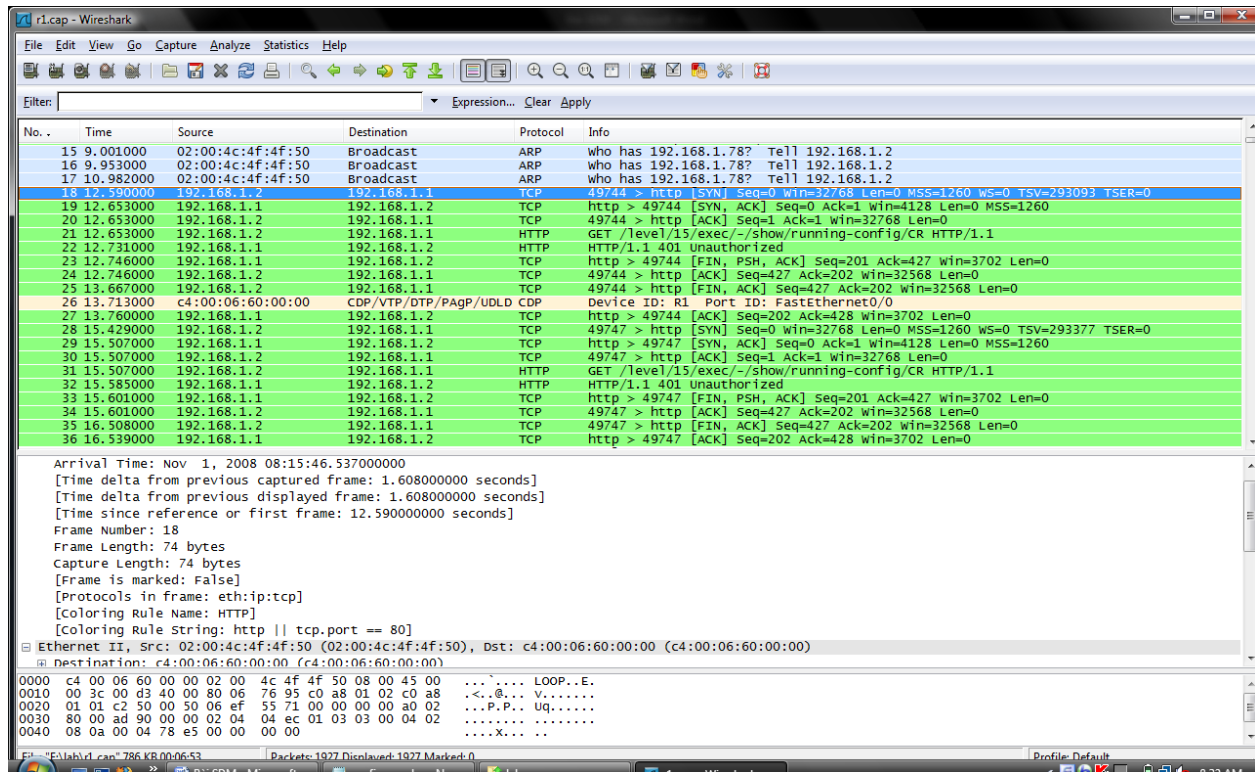
Đến đây ta đã thực hiện xong quá trình đăng nhập vào Router thông qua SDM. Ta có giao diện để cấu hình router như bên dưới.



Ta thực hiện quá trình capture kết nối trên ta nhận xét rằng nó đang hoạt động dựa trên giao thức http port 80. Tuy nhiên làm như vậy thì không có tính bảo mật cho việc router.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

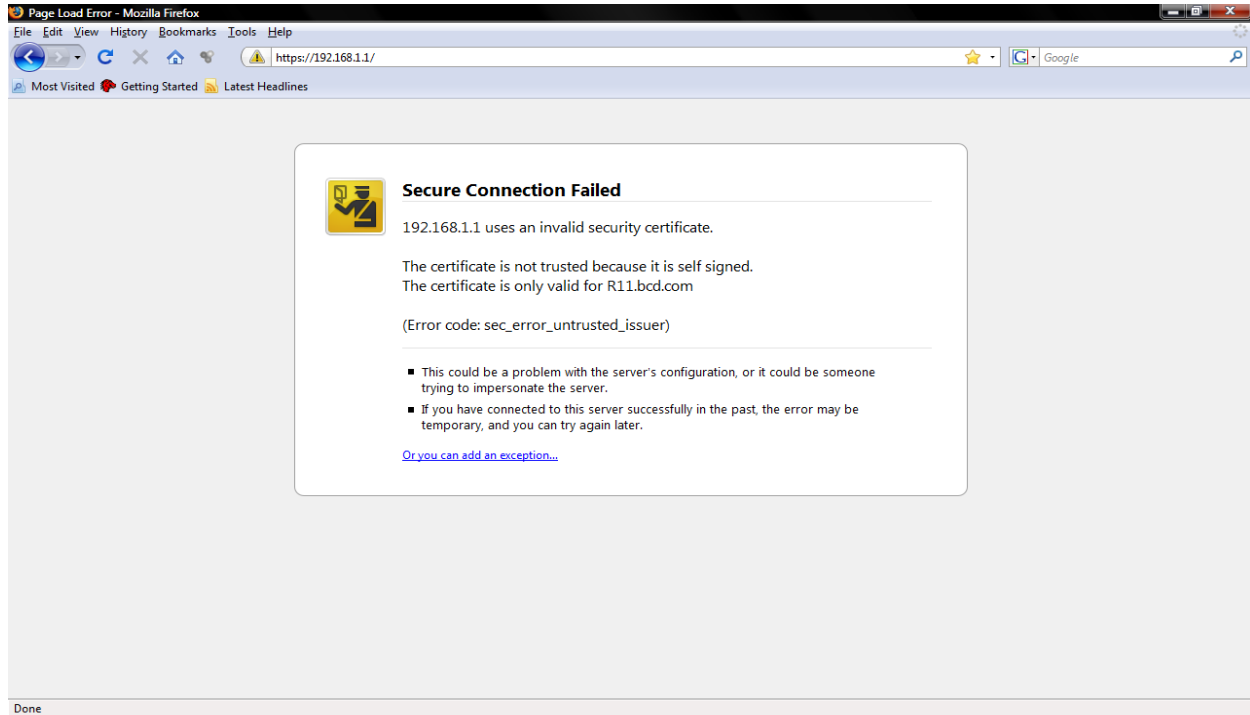


b. SDM-HTTPS

Nếu ta cấu hình router thông qua http thì quá trình ta làm sẽ bị dễ dàng sniffer. Lúc này ta sẽ chuyển sang dùng SSL kết hợp với SDM để cấu hình Router. Để có thể hoạt động được trên SSL trước tiên ta phải thấy được certificate do IOS của router tạo ra. Ở trình duyệt web nhập <https://192.168.1.1>, trình duyệt web sẽ báo rằng certificate này có vấn đề. Tuy nhiên để kết nối vào router ta phải chấp nhận certificate này. Và chứng chỉ này không có thực trong môi trường internet nên trình duyệt web cảnh báo cho người dùng.



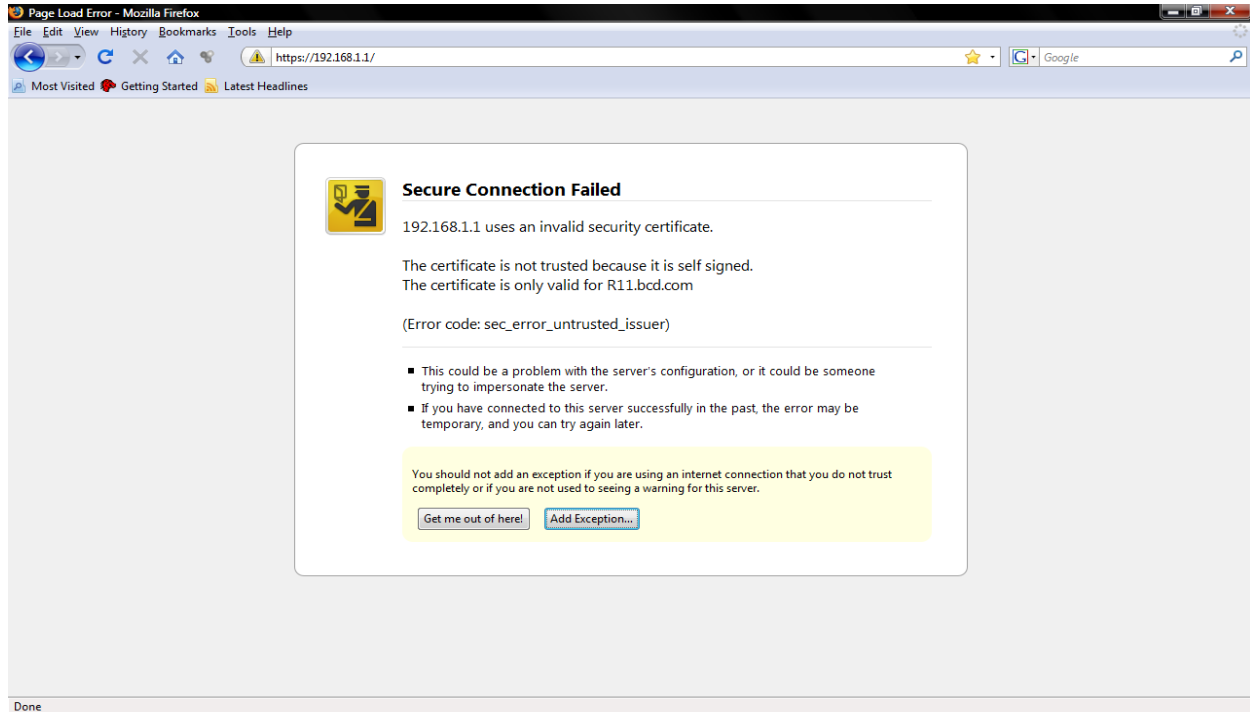
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Đến đây ta phải chấp nhận certificate này để có thể tạo được kết nối SSL. Ta click vào “ Or you can add an exception ”. Và click vào “ Add exception ” để lưu trữ certificate vào trong trình duyệt Web. Ta có thể kiểm tra certificate là do IOS của router tự sinh ra.



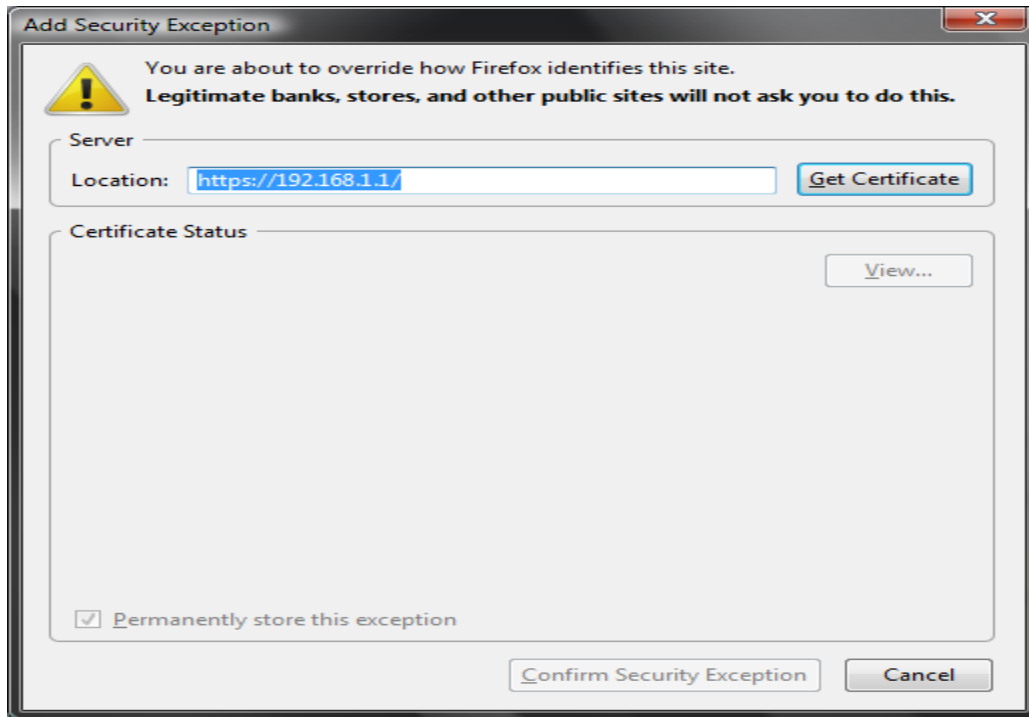
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Click vào “ Get Certificate “

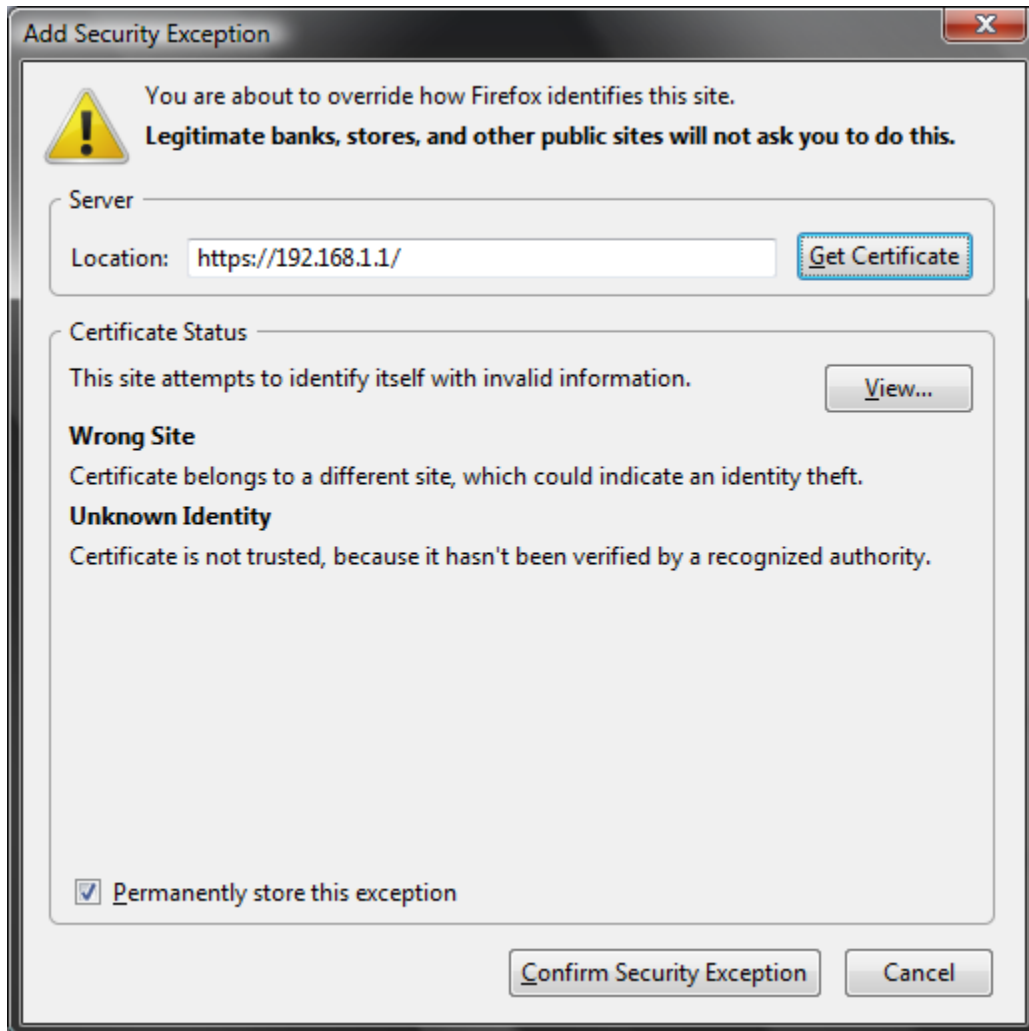


92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn





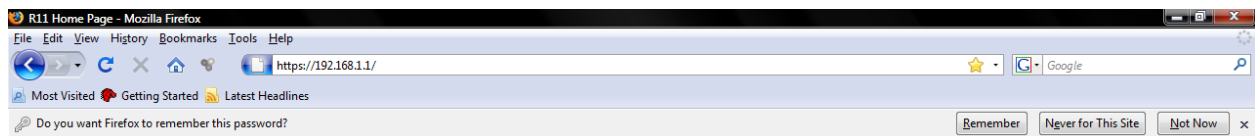
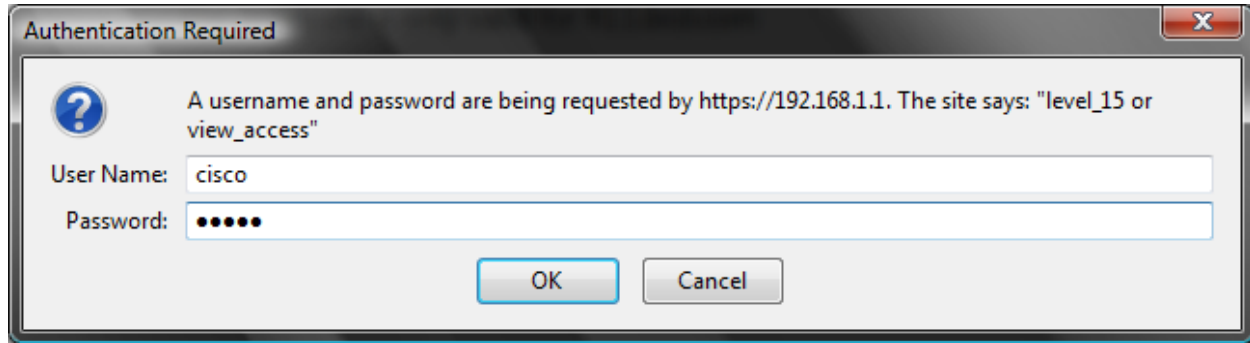
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Click vào Confirm Security Exception. Router sẽ trả lại cho ta màn hình login. Ta nhập vào username và password đã được cấu hình.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Cisco Systems

Accessing Cisco 3745 "R11"

- [Show diagnostic log](#) - display the diagnostic log.
- [Monitor the router](#) - HTML access to the command line interface at level [0](#), [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [12](#), [13](#), [14](#), [15](#)
- [Show tech-support](#) - display information commonly needed by tech support.
- [Extended Ping](#) - Send extended ping commands.
- [QoS Device Manager](#) - Configure and monitor QoS through the web interface.

Help resources

1. [CCO at www.cisco.com](http://www.cisco.com) - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.



Lúc này ta có thể kết nối đến router bằng SDM và chạy trên protocol SSL. Ta cho vào “ The device has https enabled and want to use it ”



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn




Okay, ta chấp nhận certificate này. Ta làm lại quá trình đăng nhập như SDM, tạo một username password mới như hình bên dưới.



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Change Default User Name and Password

 The router is using a factory default username and password. You must change both of them to secure the router. SDM does not allow you to configure the router unless you complete this step first.

Note: You will be prompted for username and password after this configuration is delivered. Enter the new username and password to reconnect to the router.

Username:

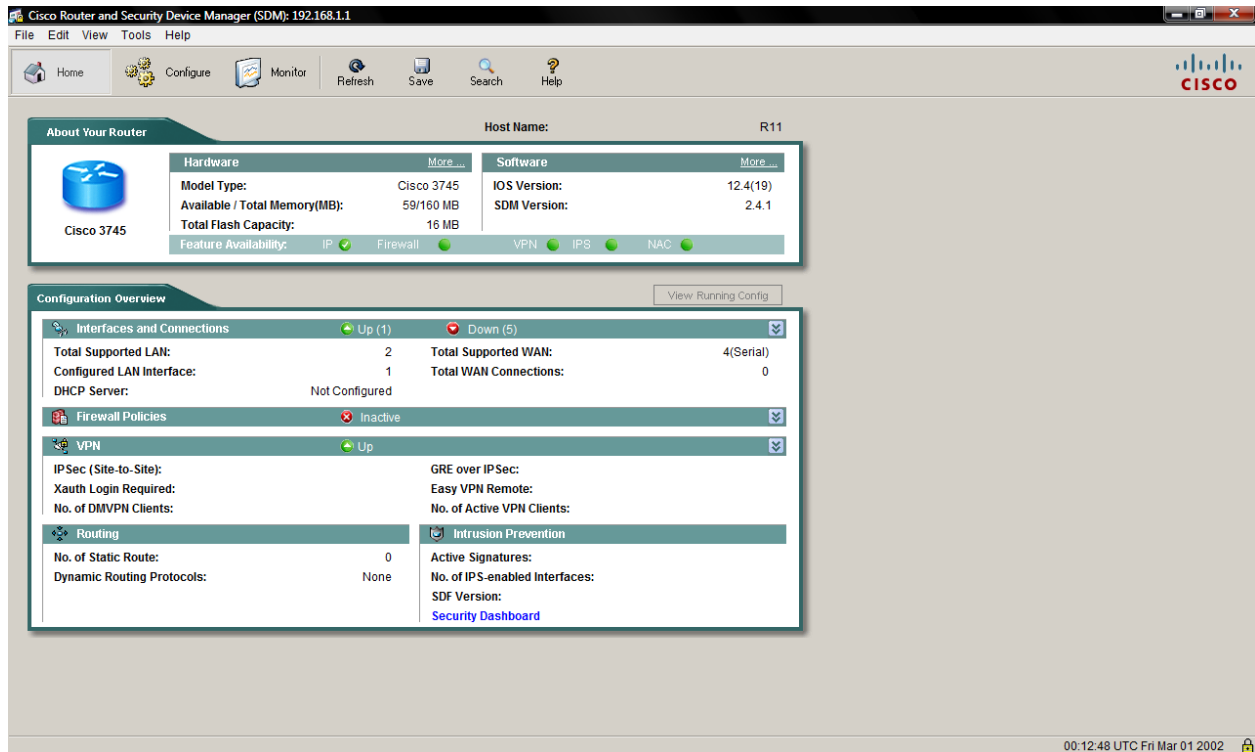
Password:

Reenter Password:

Ta logon vào Router bằng username và password mới.



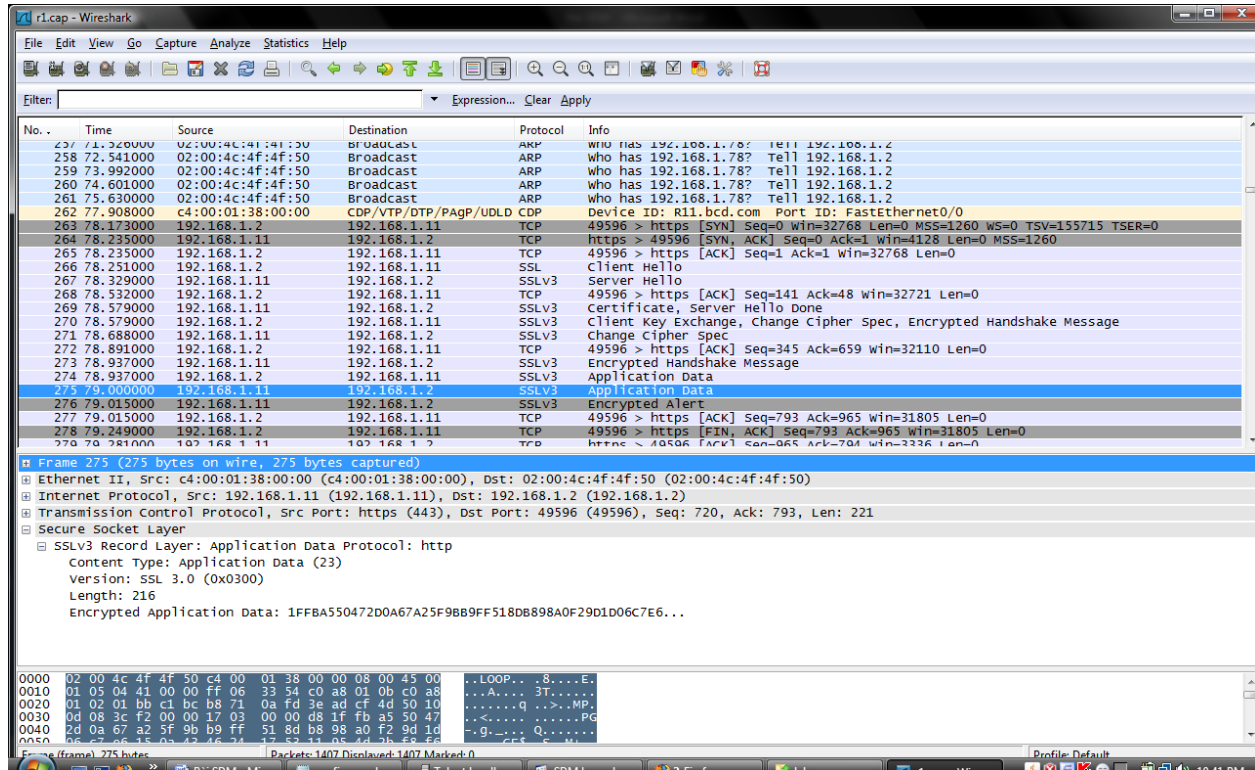
92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Ta capture luồng traffic từ Router đến PC ta thấy giao thức đang hoạt động ở đây là SSL.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Bài: VPN IPSEC SITE TO SITE

Giảng Viên: Lê Đình Nhân – Email: nhanld@athenvn.com



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

PRE-SHARED KEY

Cấu hình Pre-shared key cho site to site VPN ta cần phải làm một số bước như sau:

1. Những việc cần chuẩn bị cho việc cấu hình IPSec và Preshared key.
2. Cấu hình IKE (Internet Key Exchange).
3. Cấu hình IPSec.
4. Kiểm tra quá trình cấu hình.

I. Một số công việc ta cần kiểm tra trước

- Kiểm tra các kết nối đã được cấu hình thông chưa.
- Kiểm tra xem Access-list có cho phép dùng IPSec hay không.
- Kiểm tra xem router cho phép quá trình crypto hay không.
- Xác nhận xem interface nào sẽ được apply quá trình crypto.
- Chính sách crypto nào sẽ được apply.

II. Cấu hình IKE

Trong mode IKE cho phép đồng bộ hóa IPSec policy đến remote user. Sau khi làm xong quá trình này cho phép các client kết nối đến router download một ip address và các cấu hình network thông qua DHCP. Địa chỉ IP này được dùng như là một địa chỉ bên trong được dùng trong quá trình đóng gói tin dưới nền IPSec và nó cũng được dùng xem nó có tương ứng với IPSec policy hay không.

Quá trình cấu hình IKE với pre-shared bao gồm 4 bước:



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

- enable isakmp
- Tạo policy cho IKE
- Cấu hình tính đồng bộ cho IKE và pre-shared key
- Kiểm tra quá trình hoạt động của IKE.

a. Enable isakmp

Dùng câu lệnh **crypto isakmp enable** trong global mode.

b. Tạo chính sách cho IKE

Sau khi đã enable isakmp trên router kể đến ta cần xác định xem policy nào sẽ được apply. Một số công việc ta cần phải xác định như sau:

- Số priority nào sẽ được gán vào policy. Trong quá trình này thì số priority càng nhỏ thì độ ưu tiên của nó càng cao. Điều này rất cần thiết khi ta cấu hình nhiều IKE policy.
- Phương thức mã hóa thông tin sẽ được dùng là gì ? Mặc định router dùng DES tuy nhiên ta có thể chuyển sang dùng 3DES
- Phương thức hash được dùng. Mặc định router dùng SHA ta có thể chuyển sang dùng MD5
- Phương thức chứng thực được dùng. Ở đây ta sẽ cấu hình dùng pre-shared key.
- Kể đến là Diffie – Hellman group nào sẽ được dùng. Mặc định là group 1 768 bit Diffie – Hellman được dùng và ta cũng có thể chuyển sang dùng group 2 1024 bit Diffie – Hellman.
- Lifetime được gán vào cho Internet Key Exchange security associate.

Các câu lệnh ta sẽ dùng tương ứng với những mục ở trên như sau:

- Đầu tiên là ta tạo ra một policy bằng câu lệnh sau **crypto isakmp policy priority** được gán trong global mode.
- Xác định phương thức mã hóa với câu lệnh **encryption {des|3des}**



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

- Xác định phương thức hash bằng câu lệnh **hash {sha|md5}**
- Xác định phương thức chứng thực bằng câu lệnh **authentication {rsa-sig|rsa-encr|pre-share}**
- Xác định Diffie-Hellman group được dùng **group {1|2}**
- Xác định thời gian sống **lifetime seconds**

3. Cấu hình tính đồng bộ cho IKE và Pre-share key

Sau khi ta đã cấu hình IKE policy cho các thiết bị thì bước kế tiếp ta làm ở đây sẽ là thiết lập tính đồng bộ (identity) cho IKE và pre-share key cho các thiết bị. Mặc định thì router dùng IP address cho quá trình đồng bộ giữa các thiết bị. Tuy nhiên ta có thể chuyển sang dùng hostname cho quá trình đồng bộ. Mặc định thì router dùng IP address cho quá trình này. Câu lệnh dùng để chuyển như sau:

crypto isakmp identity {address | hostname}

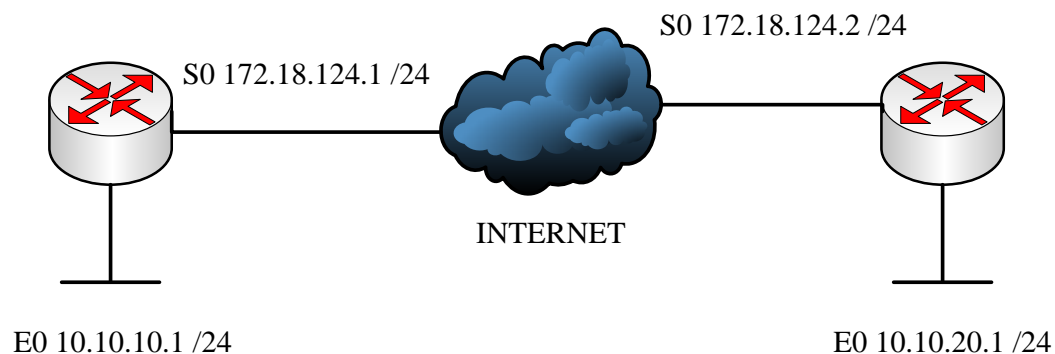
Cấu hình pre-share key là quá trình mà ta phải làm. Bạn phải xác định preshare-key nào sẽ được dùng cho các thiết bị trong mạng của mình. Preshare key phải được cấu hình giống nhau trên các peer. Bởi vì các peer của ika chứng thực với nhau bằng tạo và gửi những key đã được hash mà nó bao gồm preshare key trong đó. Và ở peer nhận sẽ tạo lại key bằng cách dùng chung thuật toán hash và preshare key. Câu lệnh cấu hình như sau:

**crypto isakmp key keystring {address peer-address | hostname peer –
hostname}**

Ta có sơ đồ bài lab như sau:



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn



Trước khi cấu hình Internet Key Exchange trên router ta cấu hình địa chỉ vào các interface của nó như sau:

```
R1#configure terminal
R1(config)#int s 1/0
R1(config-if)#ip add 172.18.214.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 64000
R1(config-if)#exit
R1(config-if)#int fastethernet 0/0
R1(config-if)#ip add 10.10.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#no keepalive
```



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
R1(config-if)#exit
```

```
R2#configure terminal
```

```
R2(config)#int s 1/0
```

```
R2(config-if)#ip add 172.18.214.2 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#clock rate 64000
```

```
R2(config-if)#exit
```

```
R2(config-if)#int fastethernet 0/0
```

```
R2(config-if)#ip add 10.10.20.1 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#no keepalive
```

```
R2(config-if)#exit
```

Ta cấu hình Internet Key Exchange trên Router 1 và Router 2 như sau

```
R1#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

R1(config)#**crypto isakmp enable**

R1(config)#**crypto isakmp policy 2**

R1(config-isakmp)#**encryption 3des**

R1(config-isakmp)#**hash md5**

R1(config-isakmp)#**authentication pre-share**

R1(config-isakmp)#**exit**

R1(config)#**crypto isakmp key cisco address 172.18.124.2**

R1(config)#**^Z**

R1#

R2#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#**crypto isakmp enable**

R2(config)#**crypto isakmp policy 2**

R2(config-isakmp)#**encryption 3des**

R2(config-isakmp)#**hash md5**

R2(config-isakmp)#**authentication pre-share**

R2(config-isakmp)#**exit**



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

R2(config)#**crypto isakmp key cisco address 172.18.124.1**

R2(config)#^Z

R2#

Lúc này thì ta đã cấu hình isakmp policy. Để xem lại ta kiểm tra lại ta có cấu hình như thế nào thì ta dùng lệnh show crypto isakmp xem lại các thông số của isakmp policy.

R1#**show crypto isakmp policy**

Protection suite of priority 2

encryption algorithm: 3DES--Triple Data Encryption Standard (168 bit keys)

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite

encryption algorithm: DES--Data Encryption Standard

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature (56 bit keys)

Diffie-Hellman group: #1 (768 bit)



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

lifetime: 86400 seconds, no volume limit

R1#

R2#show crypto isakmp policy

Protection suite of priority 2

encryption algorithm: 3DES--Triple Data Encryption Standard

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite

encryption algorithm: DES--Data Encryption Standard

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

R2#

Quá trình chứng thực bằng IKE hỗ trợ chứng thực cho các thiết bị, chưa hỗ trợ chứng thực cho user. Tuy nhiên nếu ta dùng chứng thực bằng Extended Authentication (XAuth) thì nó cho phép ta làm điều này. XAuth sẽ kết hợp với AAA



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

để chứng thực cho user sau khi đã ta chứng thực cho các thiết bị. Ta cấu hình như sau:

R1(config)#crypto isakmp key cisco address 172.18.124.2 no-xauth

III. Cấu hình IPSec

Giống như cấu hình pre-share key, ta nên xác định ta cần phải làm là bao nhiêu bước. Quá trình này bao gồm 5 bước như sau:

- Tạo ra transform set.
- Thiết lập lifetime cho IPSec SA.
- Tạo ra access-list và nó được dùng để xác định cụ thể traffic nào được mã hóa.
- Tạo crypto map.
- Apply crypto map này vào một interface cụ thể.

1. Tạo ra Transform set

- Transform set là công cụ nhằm mục đích bảo vệ luồng thông tin. Và nó sẽ được tạo khi ta cấu hình payload authentication, payload encryption và IPSec. Giống như cấu hình chứng thực việc cấu hình transform set phải được giống nhau trên các thiết bị. Ví dụ ta phải cấu hình tên cho quá trình transform set phải giống nhau. Để cấu hình transform set ta dùng câu lệnh như sau



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

**crypto ipsec transform-set *transform-set-name* {[*transform1*] [*transform2*]
[*transform3*]}**

Ở mục này ta có một số chọn lựa như sau

transform-set-name tên của quá trình

transform1 có thể chọn là ah-md5-hmac hoặc ah-sha-hmac.

transform2 có thể esp-des esp-3des hoặc esp-null.

transform3 có thể esp-md5-hmac hoặc esp-sha-hmac.

- Mặc định IPsec mode đang ở dạng tunnel. Ta có thể chuyển sang dùng dạng transport bằng câu lệnh:

mode {*tunnel* | *transport*}

2. Lifetime cho IPsec SA

Ta xét thời gian lifetime cho IPsec nhằm mục đích xác nhận xem IPsec SA sẽ có hiệu lực trong khoảng thời gian là bao lâu cho đến khi nó cần được thương lượng lại để xin lại. Ở đây bạn có thể cấu hình bằng hai cách: một là trong global mode và hai là trong crypto map.

Khi cấu hình lifetime thì ta xác định hai thông số đó là: second và kilobytes. Thông số second dùng để xác định thời gian sống cho IPsec SA trước khi nó bị hết hạn. Mặc định thời gian sống là 3600 second. Thông số kilobyte xác định kích thước gói tin. Mặc định kích thước gói tin 4608000 kilobyte. Hai câu lệnh như sau.



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

crypto ipsec security-association lifetime seconds *seconds*

crypto ipsec security-association lifetime kilobytes *kilobytes*

3. Tạo Access list

Sau khi xét cấu hình transform set và lifetime. Việc kế tiếp ta cần phải làm là cấu hình access list để nó bảo vệ data flow của IPSec. Để cấu hình extended access list cho IPSec ta cần phải xác định một số việc như sau:

- Chọn outbound traffic để bảo vệ
- Xử lý inbound traffic cho việc chọn lựa traffic IPSec.
- Xử lý inbound traffic cho mục đích filter những traffic cần được protect.

Ngoài ra khi ta đàm phán cho quá trình xử lý IKE, thì access list xác định khi nào chấp nhận những yêu cầu IPSec SA.

4. Tạo Crypto map

IPSec SA được thiết lập chỉ thông qua câu lệnh crypto map. Lệnh crypto map dùng để kết nối một hay nhiều trình tự lại với nhau. Một trình tự được đại diện bởi một IPSec SA. Mỗi trình tự crypto map xác định một số việc cụ thể như sau:

- Traffic nào cần được bảo vệ
- Luồng thông tin đến remote peer nào cần được protect
- Transform nào được dùng để bảo vệ traffic
- IPSec SA sẽ được thiết lập thông qua thông IKE hay là manual
- Ngoài ra còn có các biến khác để dùng cho việc mô tả xác định life time cho crypto map



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Tất cả mọi trình tự trong crypto map được kết nối chặt chẽ với nhau thông qua name of crypto map. Mỗi một trình tự chỉ có thể là một trong những dạng sau:

- Cisco: trong trình tự này thì Cisco Encryption Technology được dùng thay thế cho IPsec.
- IPsec-manual: trong trình tự này thì IKE không được dùng để thiết lập IPsec – SA.
- IPsec – isakmp: dùng IKE để thiết lập IPsec SA.

Ở đây ta chỉ bàn về cách dùng IKE để thiết lập IPsec. Ta dùng câu lệnh như sau:

crypto map map-name seq-num ipsec-isakmp

map – name: là tên dùng trong quá trình crypto map

seq – num: số thứ tự trong quá trình crypto map (1 – 65535) với số nhỏ có độ ưu tiên cao hơn.

Sau khi ta đã dùng câu lệnh ở trên thì ta sẽ đăng nhập vào mode của crypto map mode. Ở đây ta xác định một số biến như sau:

- **match address {access-list-number | name}**: câu lệnh này phải có để xác định access list nào được apply.
- **set peer {peer - address | hostname - peer }**: xác định IPsec peer.
- **set transform-set transform-setname [transform-set-name2 transformset-name6]**: xác định transform set được dùng trong quá trình IPsec.

5. Applied Crypto map

Sau khi bạn đã tạo ra IPsec tunnel thì bước kế tiếp là bạn phải apply nó vào một interface cụ thể. Để apply ta phải vào interface mode và dùng câu lệnh:

crypto map map-name



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

Vì mục đích redundancy, bạn có thể apply một crypto map vào một interface. Mặc định thì nó như sau:

- Mỗi một interface có một SA database.
- IP address của local interface được dùng như là local address được dùng cho IPsec traffic.

Nếu như muốn dùng crypto map trên nhiều interface bạn cần phải xác định interface đó. Ta có thể làm như sau:

Mỗi interface sẽ tương ứng với một IPsec SA database được thiết lập vào một thời điểm. Còn các traffic nào được chia sẻ trên tất cả interface thì nó dùng chung một crypto map.

IP address của interface được định nghĩa thường được dùng trong trường hợp này là local ip address và nó được dùng IPsec traffic tại điểm xuất phát ban đầu và đích cần đến có chia sẻ dùng chung một crypto map set.

crypto map *map-name* *local-address* *local-id*

Để định nghĩa một interface ta dùng câu lệnh như trên ở global mode với map-name là tên của crypto map và local-id là IP address của interface đang được định nghĩa.

Cấu hình Crypto IPsec với tên là test và Crypto map với tên là test1 như sau

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#crypto ipsec transform-set test esp-des



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

R1(cfg-crypto-trans)#exit

R1(config)#access-list 100 permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255

R1(config)#crypto map test1 100 ipsec-isakmp

R1(config-crypto-map)#match address 100

R1(config-crypto-map)#set transform-set test

R1(config-crypto-map)#set peer 172.18.124.2

R1(config-crypto-map)#exit

R1(config)#interface s0/0

R1(config-if)#crypto map test1

R1(config-if)#^Z

R1#

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#crypto ipsec transform-set test esp-des

R2(cfg-crypto-trans)#exit

R2(config)#access-list 100 permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255

R2(config)#crypto map test1 100 ipsec-isakmp



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

```
R2(config-crypto-map)#match address 100  
R2(config-crypto-map)#set transform-set test  
R2(config-crypto-map)#set peer 172.18.124.1  
R2(config-crypto-map)#exit  
R2(config)#interface s1/0  
R2(config-if)#crypto map test1  
R2(config-if)#^Z  
R2#
```

Ngoài ra nếu ta muốn thực hiện quá trình chứng thực cho user bằng XAuth thì phải xác nhận user và group nào có thẩm quyền. Lúc này ta cần dùng AAA để thực hiện quá trình này và dùng **crypto map** để apply AAA ta đã tạo ra.

IV. Kiểm tra và thẩm định quá trình hoạt động của IPSec

- Dùng lệnh show crypto isakmp sa cho ta biết các tất cả active SA đang có trên thiết bị.

```
R1#show crypto isakmp sa
```

dst	src state	conn-id	slot
172.18.124.2	172.18.124.1	QM_IDLE	82 0

- Muốn xem cấu hình transform set thì dùng câu lệnh show crypto ipsec transform-set



92 Nguyễn Đình Chiểu, DaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

R1#show crypto ipsec transform-set

Transform set test: { esp-des }

will negotiate = { Tunnel, }

- Kiểm tra xem một IPSec SA đang hoạt động thì dùng lệnh show crypto ipsec sa

R1#show crypto ipsec sa

interface: Serial0/0

Crypto map tag: test1, local addr. 10.1.1.1

local ident (addr/mask/prot/port):

(10.1.1.1/255.255.255.255/0/0)

remote ident (addr/mask/prot/port):

(10.1.1.2/255.255.255.255/0/0)

current_peer: 10.1.1.2

PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10

#send errors 10, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.2

path mtu 1500, media mtu 1500



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

current outbound spi: 20890A6F

inbound esp sas:

spi: 0x257A1039(628756537)

transform: esp-des ,

in use settings ={Tunnel, }

slot: 0, conn id: 26, crypto map: test1

sa timing: remaining key lifetime (k/sec): (4607999/90)

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

outbound esp sas:

spi: 0x20890A6F(545852015)

transform: esp-des ,

in use settings ={Tunnel, }

slot: 0, conn id: 27, crypto map: test1

sa timing: remaining key lifetime (k/sec): (4607999/90)

IV size: 8 bytes

replay detection support: Y



92 Nguyễn Đình Chiểu, ĐaKao, Quận 1, Tp HCM
2 Bis Đinh Tiên Hoàng P.Đa Kao Quận 1 TPHCM Hotline: 090 78 79 477
Website: www.athena.edu.vn

outbound ah sas: