Cấu hình Cisco ASA 5505

# Note: Câu lệnh câu hình trước khi đổi password asa, password asa mới là 123, password mặc định khi cấu hình (trước khi đổi là blank \_ rỗng)

**Bước 1**: Kích hoạt Key Security License:

- Phải sử dụng bản Security License để có thể sử dụng Trunk trên cổng vlan và có tại được nhiều hơn 3 vlans trên cisco asa 5505 cũng như một số tính năng quan trọng khác.

en (với password đăng nhập cisco ASA 5505 mặc định là blank \_ rỗng)

activation-key 0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D

reload (khởi động lại để kích hoạt key)

**Bước 2**: Cấu hình các vlans

- Thiết lập các vlan với security-level dựa trên mức độ mật (quan trọng) của vlan đó.

En

Conf t

Interface vlan 1

Nameif inside (đặt tên cho vlan)

Ip address 192.168.1.1 255.255.255.0 (đặt địa chỉ ip cho cổng vlan)

security-level 100 (đặt mức độc bảo mật)

no shut (bật cổng vlan)

ex

int vlan 2

nameif outside

ip address 209.165.200.226 255.255.255.0

security-level 0

no shut

ex

Tương tự với vlan 3 security-level 50, vlan 4 – vlan 9 có security-level là 70 , vlan 10 có security-level là 90

**Bước 3**: Định tuyến cho các gói tin ra ngoài:

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

209.165.200.225 255.255.255.0 là IP của cổng router nối với ASA.

**Bước 4**: Cấu hình Class-map và Policy-map cho phép các gói tin đi qua

conf t

class-map testMap

match any

ex

policy-map testPolicy

class testMap

inspect icmp

ex

service-policy testPolicy global

ex

telnet timeout 5

ssh timeout 5

**Bước 5**: Cấu hình cổng cho vlan:

conf t

int Ethernet 0/1 (cổng nối vào mạng nội bộ)

switchport mode trunk

switchport trunk allowed vlan 1,4-10

ex

conf t

int Ethernet 0/0 (cổng nối ra outside, mạng bên ngoài)

switchport mode access

switchport access vlan 2

ex

conf t

int Ethernet 0/2 (cổng nối ra dmz)

switchport mode access

switchport access vlan 3

ex

conf t

int Ethernet 0/3 (cổng nối ra BackupServer)

switchport mode access

switchport access vlan 10

ex

**Bước 6**: Thiết lập các đối tượng mạng (object network)

object network inside-subnet (tương ứng với vlan inside (vlan 1))

subnet 192.168.1.0 255.255.255.0 (dải địa chỉ của object)

nat (inside,outside) dynamic interface

- Sử dụng nat động tại cổng ra outside, gói tin khi đi qua cổng outside từ trong ra ngoài sẽ được chuyển đổi địa chỉ nguồn tin (với giá trị địa chỉ trong dải 192.168.1.0 255.255.255.0) sang địa chỉ cổng (209.165.200.226) và ngược lại khi đi từ ngoài vào sẽ được chuyển đổi địa chỉ đích tin (lúc này là địa chỉ cổng) sang địa chỉ đích thực trong mạng nội bộ

- Tương tự với các object network tương ứng với các vlan nội bộ khác trừ dmz được cấu hình nat tĩnh

object network dmzServer (webserver)

hot 192.168.3.3

nat (dmz,outside) static 209.165.200.227

object network dnsServer

host 192.168.3.10

nat (dmz,outside) static 209.165.200.229

object network emailServer

host 192.168.3.4

nat (dmz,outside) static 209.165.200.228

**Bước 7**: Cấu hình access-list:

+ Xử lý trên cổng vlan outside :

- Vì mặc định outside có sevurity-level 0, thấp nhất nên không thể truy cập dmz (security-level 50) và mạng nội bộ (security-level 70,100) nên muốn cho outside truy cập web công ty cần dùng access-list

- Cho phép mạng bên ngoài truy cập vào website public của công ty (thuộc dmz) với địa chỉ ip được ISP cấp là 209.165.200.226 và tên miền congtynhkd.com

access-list outside extended permit tcp any host 192.168.3.3

access-list outside extended permit tcp any host 192.168.3.3 eq www

access-list outside extended permit icmp any host 192.168.3.3

- Cho phép các gói tin phản hồi từ outside đi vào để ping thành công từ trong ra ngoài outside

access-list outside extended permit icmp any object KyThuat-obj echo-reply

access-list outside extended permit icmp any object KinhDoanh-obj echo-reply

access-list outside extended permit icmp any object PhanTich-obj echo-reply

access-list outside extended permit icmp any object ThietKe-obj echo-reply

access-list outside extended permit icmp any object LapTrinh-obj echo-reply

access-list outside extended permit icmp any object NhanSu-obj echo-reply

access-list outside extended permit icmp any object inside-subnet echo-reply

access-group outside in interface outside (áp dụng với gói tin đi vào cổng outside)

+ Xử lý trên cổng vlan dmz:

- Cho phép các gói tin phản hồi về mạng nội bộ (vì sử dụng access-list, mặc định sẽ có câu lệnh deny any any ở cuối cùng nên cần phải cấp phép các gói tin cần thiết)

access-list dmz extended permit icmp any object KinhDoanh-obj echo-reply

access-list dmz extended permit icmp any object PhanTich-obj echo-reply

access-list dmz extended permit icmp any object ThietKe-obj echo-reply

access-list dmz extended permit icmp any object LapTrinh-obj echo-reply

access-list dmz extended permit icmp any object NhanSu-obj echo-reply

access-list dmz extended permit icmp any object KyThuat-obj echo-reply

access-list dmz extended permit icmp any object inside-subnet echo-reply

- Cho phép các gói tin domain (gói tin yêu cầu phần giải địa chỉ miền) vào (cổng 53)

access-list dmz extended permit udp any eq domain any

- Cho phép các gói tin email đi vào (cổng 25)

access-list dmz extended permit tcp any any eq smtp

access-list dmz extended permit tcp host 192.168.3.4 any

access-group dmz in interface dmz (Áp dụng với các gói tin đi vào cổng dmz)

+ Xử lý trên cổng vlan KinhDoanh (Các cổng nội bộ khác tương tự)

- Cho phép truy cập web và gói tin tcp đi đến vlan KinhDoanh để vlan KinhDoanh vào được web của công ty

access-list kd extended permit tcp object dmzServer object KinhDoanh-obj

access-list kd extended permit tcp object dmzServer object KinhDoanh-obj eq www

access-list kd extended permit icmp object KinhDoanh-obj object dmzServer

- Cho phép gói tin dns đi qua cổng domain từ vlan KinhDoanh (trong dải 192.168.4.0 255.255.255.0) đi đến object network dnsServer (máy chủ DNS) qua cổng domain

access-list kd extended permit udp 192.168.4.0 255.255.255.0 object dnsServer eq domain

- Chặn không cho vlan KinhDoanh ping sang các vlan khác

access-list kd extended deny icmp object KinhDoanh-obj object LapTrinh-obj

access-list kd extended deny icmp object KinhDoanh-obj object PhanTich-obj

access-list kd extended deny icmp object KinhDoanh-obj object ThietKe-obj

access-list kd extended deny icmp object KinhDoanh-obj object NhanSu-obj

access-list kd extended deny icmp object KinhDoanh-obj object KyThuat-obj

- Cho phép vlan KinhDoanh ping ra các mạng khác (trừ các vlan đã chặn ở trên)

access-list kd extended permit icmp object KinhDoanh-obj any

- Cho phép email đi qua

access-list kd extended permit tcp any any eq smtp

- Áp dụng cho các gói tin đi vào cổng vlan KinhDoanh

access-group kd in interface KinhDoanh

**Bước 8:** Cấu hình telnet và ssh: (cấu hình mẫu cho máy giám đốc, các máy quản lý khác tương tự)

conf t

- Thiết lập tài khoản và mật khẩu cho Telnet

username admin password admin

- Cho phép Telnet từ địa chỉ máy giám đốc vào từ cổng inside

telnet 192.168.1.10 255.255.255.255 inside

telnet timeout 50

- Kích hoạt xác thực telnet

aaa authentication telnet console LOCAL

enable password 123

! config ssh

- Tạo ra cặp khóa RSA. Giá trị 1024 là số bit được dùng trong tính toán modulus.

crypto key generate rsa modulus 1024

- Thiết lập tài khoản cho ssh

username cisco password cisco

- Cho phép SSH từ địa chỉ máy giám đốc vào từ cổng inside

ssh 192.168.1.10 255.255.255.255 inside

ssh timeout 20

- Kích hoạt xác thực SSH

aaa authentication ssh console LOCAL

# Note: Trên máy tính giám đốc, để sử dụng telnet và SSH, ta dùng câu lệnh sau:

- Telnet:

telnet 192.168.1.1 (cổng vlan 1 (inside) trên cisco ASA)

Nhập tài khoản => Nhập mật khẩu

- SSH:

ssh -l cisco 192.168.1.1

Nhập mật khẩu

