**1. Switch2**

enable

configure terminal

hostname switch1

end

copy running-config startup-config

**2. Switch2**

enable

configure terminal

hostname switch2

vlan 20

name VLAN20

exit

vlan 30

name VLAN30

exit

interface range fa0/1-12

switchport mode access

switchport access vlan 20

no shutdown

exit

interface range fa0/13-24

switchport mode access

switchport access vlan 30

no shutdown

exit

interface gig0/1

switchport mode trunk

no shutdown

exit

interface gig0/2

switchport mode trunk

no shutdown

exit

end

copy running-config startup-config

**3. SWITCH L3**

enable

configure terminal

hostname SWL3

vlan 10

name Vlan10

exit

vlan 20

name Vlan20

exit

vlan 30

name Vlan30

exit

interface vlan 10

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface vlan 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.3

no shutdown

exit

interface vlan 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.3

no shutdown

exit

interface fa0/1

no switchport

ip address 192.168.0.2 255.255.255.0

no shutdown

exit

interface gig0/1

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

interface gig0/2

switchport trunk encapsulation dot1q

switchport mode trunk

no shutdown

exit

ip routing

ip route 0.0.0.0 0.0.0.0 192.168.0.1

ip access-list extended out\_in

permit icmp any any

permit ip any any

exit

ip access-list extended dmz\_out

deny ip host 192.168.1.254 192.168.20.0 0.0.0.255

deny ip host 192.168.1.254 192.168.30.0 0.0.0.255

permit ip any any

exit

ip access-list extended vlan20\_dmz

deny ip host 192.168.20.254 host 192.168.1.2

permit ip any any

exit

interface fa0/1

ip access-group out\_in in

exit

interface vlan 10

ip access-group dmz\_out in

exit

interface vlan 20

ip access-group vlan20\_dmz in

exit

end

copy running-config startup-config

**3. Router**

enable

configure terminal

hostname R1

interface gig0/0

ip address 203.113.131.2 255.255.255.0

ip nat outside

no shutdown

exit

interface gig0/1

ip address 192.168.0.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2

no ip address

no shutdown

exit

interface gig0/2.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

ip routing

ip route 0.0.0.0 0.0.0.0 203.113.131.1

ip route 192.168.1.0 255.255.255.0 192.168.0.2

ip nat inside source list 1 interface gig0/0 overload

access-list 1 permit 192.168.0.0 0.0.0.255

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.30.0 0.0.0.255

ip access-list extended OUTSIDE\_IN

permit udp any host 192.168.1.4 eq 53

permit tcp any host 192.168.1.4 eq 53

permit tcp host 203.113.131.3 host 192.168.1.2 eq 80

permit tcp host 203.113.131.10 host 192.168.1.2 eq 80

deny tcp host 203.113.131.11 host 192.168.1.2 eq 80

permit ip any any

exit

interface gig0/0

ip access-group OUTSIDE\_IN in

end

copy running-config startup-config

**4. Firewall(ASA 5506)**

enable

Password:

configure terminal

interface GigabitEthernet1/1

no nameif

exit

interface GigabitEthernet1/2

no nameif

exit

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address 192.168.0.2 255.255.255.0

no shutdown

exit

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

configure terminal

route outside 0.0.0.0 0.0.0.0 192.168.0.1

exit

configure terminal

access-list OUTSIDE\_IN extended permit udp any host 192.168.1.3 eq 67

access-list OUTSIDE\_IN extended permit udp host 192.168.1.3 eq 68 any

access-list OUTSIDE\_IN extended permit udp any host 192.168.1.4 eq 53

access-list OUTSIDE\_IN extended permit tcp any host 192.168.1.4 eq 53

access-list OUTSIDE\_IN extended permit icmp host 203.113.131.10 host 192.168.1.2

access-list OUTSIDE\_IN extended permit tcp host 203.113.131.3 host 192.168.1.2 eq 80

access-list OUTSIDE\_IN extended permit tcp host 203.113.131.10 host 192.168.1.2 eq 80

access-list OUTSIDE\_IN extended deny icmp host 203.113.1.11 host 192.168.1.2

access-list OUTSIDE\_IN extended deny tcp host 203.113.1.11 host 192.168.1.2 eq 80

access-list OUTSIDE\_IN extended permit ip any any

access-group OUTSIDE\_IN in interface outside

access-list DMZ\_OUT extended permit icmp any any

access-group DMZ\_OUT out interface inside

policy-map global\_policy

class inspection\_default

inspect icmp

end

copy running-config startup-config

enable

configure terminal

hostname R1

*! Cấu hình interface kết nối ISP*

interface gig0/0

ip address 203.113.131.2 255.255.255.0

ip nat outside

ip access-group OUTSIDE\_IN in

no shutdown

exit

*! Interface kết nối ASA*

interface gig0/1

ip address 192.168.0.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

*! Interface trunk với Switch*

interface gig0/2

no ip address

no shutdown

exit

interface gig0/2.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

*! Bật định tuyến*

ip routing

*! Tuyến mặc định ra ISP và định tuyến đến ASA*

ip route 0.0.0.0 0.0.0.0 203.113.131.1

ip route 192.168.1.0 255.255.255.0 192.168.0.2

*! NAT Overload cho các mạng nội bộ*

access-list 1 permit 192.168.0.0 0.0.0.255

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.30.0 0.0.0.255

ip nat inside source list 1 interface gig0/0 overload

*! ACL kiểm soát truy cập từ Internet*

ip access-list extended OUTSIDE\_IN

permit tcp host 203.113.131.10 host 192.168.1.2 eq 80

deny tcp host 203.113.131.11 host 192.168.1.2 eq 80

permit udp any host 10.1.100.4 eq 53

permit ip any any

exit

*! Lưu cấu hình*

end

copy running-config startup-config

**2. Cấu hình Firewall**

enable

configure terminal

*! Đặt IP và nameif cho outside*

interface GigabitEthernet1/1

no nameif

exit

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address 192.168.0.2 255.255.255.0

no shutdown

exit

*! Đặt IP và nameif cho inside*

interface GigabitEthernet1/2

no nameif

exit

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

*! Default route ra Router*

route outside 0.0.0.0 0.0.0.0 192.168.0.1

*! ACL cho phép DHCP, ICMP, HTTP từ IP cụ thể*

access-list OUTSIDE\_IN extended permit udp any host 192.168.1.3 eq 67

access-list OUTSIDE\_IN extended permit udp host 192.168.1.3 eq 68 any

access-list OUTSIDE\_IN extended permit icmp host 203.113.131.10 host 192.168.1.2

access-list OUTSIDE\_IN extended permit tcp host 203.113.131.10 host 192.168.1.2 eq 80

access-list OUTSIDE\_IN extended deny icmp host 203.113.1.11 host 192.168.1.2

access-list OUTSIDE\_IN extended deny tcp host 203.113.1.11 host 192.168.1.2 eq 80

access-list OUTSIDE\_IN extended permit ip any any

*! Gắn ACL vào outside*

access-group OUTSIDE\_IN in interface outside

*! ACL bổ sung nếu cần cho inside*

access-list DMZ\_OUT extended permit icmp any any

access-group DMZ\_OUT out interface inside

*! Cho phép ASA kiểm tra ICMP*

policy-map global\_policy

class inspection\_default

inspect icmp

exit

*! Lưu cấu hình*

end

copy running-config startup-config

**ASA**

configure terminal

hostname ASA

int gig1/1

nameif outside

security-level 0

ip add 203.113.131.2 255.255.255.0

no shut

exit

int gig1/2

nameif inside

security-level 100

ip add 192.168.0.1 255.255.255.0

no shut

exit

route outside 0.0.0.0 0.0.0.0 203.113.131.1

route inside 192.168.1.0 255.255.255.0 192.168.0.2

object network in\_out

subnet 192.168.0.0 255.255.255.0

subnet 192.168.1.0 255.255.255.0

subnet 192.168.20.0 255.255.255.0

subnet 192.168.30.0 255.255.255.0

nat (inside,outside) dynamic interface

exit

conf t

object network router\_inside

host 192.168.1.2

nat (inside,outside) static 203.113.131.3

exit

conf t

access-list out\_in extended permit tcp any host 192.168.1.2 eq 80

access-list out\_in extended permit udp any host 192.168.1.2 eq 53

access-list out\_in extended permit tcp any host 192.168.1.2 eq 53

access-list out\_in extended permit ip any any

access-list out\_in extended permit icmp any any

access-group out\_in in interface outside

ex

configure terminal

class-map inspection\_default

match default-inspection-traffic

policy-map kiemtra

class inspection\_default

inspect icmp

inspect http

service-policy global\_policy global

end

copy running-config startup-config

**ROUTER-NAT**

ena

configure terminal

hostname R1

interface gig0/0

ip address 192.168.0.2 255.255.255.0

ip nat outside

no shutdown

ex

interface gig0/1

no ip address

no shutdown

ex

interface gig0/2

no ip address

no shutdown

exit

interface gig0/1.10

encapsulation dot1q 10

ip address 192.168.1.1 255.255.255.0

ip nat inside

no shutdown

exit

interface gig0/2.20

encapsulation dot1q 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.2

ip nat inside

no shutdown

exit

interface gig0/2.30

encapsulation dot1q 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.2

ip nat inside

no shutdown

exit

ip routing

ip route 0.0.0.0 0.0.0.0 192.168.0.1

ip nat inside source list 1 interface gig0/0 overload

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.30.0 0.0.0.255

ip access-list extended out\_in

permit ip any any

permit icmp any any

exit

interface gig0/0

ip access-group out\_in in

end

copy running-config startup-config

**ROUTER-NAT**

ena

configure terminal

hostname R1

interface gig0/0

ip address 192.168.0.2 255.255.255.0

ip nat outside

no shutdown

ex

interface gig0/1

ip address 192.168.1.1 255.255.255.0

ip nat inside

no shutdown

ex

interface gig0/2

no ip address

no shutdown

exit

interface gig0/2.20

encapsulation dot1q 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2.30

encapsulation dot1q 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

ip routing

ip route 0.0.0.0 0.0.0.0 192.168.0.1

ip nat inside source list 1 interface gig0/0 overload

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.30.0 0.0.0.255

ip access-list extended out\_in

permit ip any any

permit icmp any any

exit

interface gig0/0

ip access-group out\_in in

end

copy running-config startup-config

**3. Router**

enable

configure terminal

hostname R1

interface gig0/0

ip address 203.113.131.2 255.255.255.0

ip nat outside

no shutdown

exit

interface gig0/1

ip address 192.168.0.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2

no ip address

no shutdown

exit

interface gig0/2.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

interface gig0/2.30

encapsulation dot1Q 30

ip address 192.168.30.1 255.255.255.0

ip helper-address 192.168.1.3

ip nat inside

no shutdown

exit

ip routing

ip route 0.0.0.0 0.0.0.0 203.113.131.1

ip route 192.168.1.0 255.255.255.0 192.168.0.2

ip nat inside source list 1 interface gig0/0 overload

access-list 1 permit 192.168.0.0 0.0.0.255

access-list 1 permit 192.168.1.0 0.0.0.255

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.30.0 0.0.0.255

ip access-list extended OUTSIDE\_IN

permit udp any host 192.168.1.4 eq 53

permit tcp any host 192.168.1.4 eq 53

permit tcp host 203.113.131.3 host 192.168.1.2 eq 80

permit tcp host 203.113.131.10 host 192.168.1.2 eq 80

deny tcp host 203.113.131.11 host 192.168.1.2 eq 80

permit ip any any

exit

interface gig0/0

ip access-group OUTSIDE\_IN in

end

copy running-config startup-config