Contents

[2.Stage 2: Firewall (sub-interface, failover, gatewave cho vlans) 7](#_Toc131148102)

[2.2 Failover 7](#_Toc131148103)

[2.3 IP interface FW 7](#_Toc131148104)

[2.4 IP interface RGW + inspect icmp 8](#_Toc131148105)

[2.5 Test NAT + để PC trong Lan ra outside, cần NAT và icmp inspect 8](#_Toc131148106)

[2.6 Test\_ping FW 🡪 RGW-20 8](#_Toc131148107)

[2.7 ACL outside ping inside 9](#_Toc131148108)

[2.8 Chuyển đổi vlan 60 80 + after instruction 9](#_Toc131148109)

[2.9 VRRP trên 2 RGW-20, 21 10](#_Toc131148110)

[2.10 DHCP sub-inter vlan trên firewall 10](#_Toc131148111)

[2.11 Port-security 10](#_Toc131148112)

[2.12 SSH 11](#_Toc131148113)

[2.13 iBGP 12](#_Toc131148114)

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **103.95.197.144/28** | |
| **Vlan 40: VanPhong** | | **103.95.196.0/24** | |
| **Vlan 50: KyThuat** | | **103.95.197.0/26** | |
| **VLan60: LanhDao** | | **103.95.197.160/28** | |
|  |  | | |
| ***SW-Core-1***  en  conf t  hostname SW-CORE-1  inter range e1/0 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  inter range e1/2-3  channel-group 1 mode on  exit  inter port-channel 1  sw tr en dot  sw mod tru  do wr  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  vlan 80  name DMZ  vlan 2  name ssh\_telnet  inter vlan 30  ip add 103.95.197.147 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.3 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.3 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.163 255.255.255.240  no sh  ##########Them vlan 80  inter vlan 80  ip add 103.95.197.241 255.255.255.240  no sh  spanning-tree mode rapid  spanning-tree vlan 30 root primary  spanning-tree vlan 40 root primary  spanning-tree vlan 50 root primary  spanning-tree vlan 60 root primary  ***DSW-12***  en  conf t  hostname DSW-12  inter range e1/0 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  vlan 80  name DMZ  vlan 2  name ssh\_telnet  inter vlan 30  ip add 103.95.197.149 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.5 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.5 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.165 255.255.255.240  no sh  do wr  do ping 103.95.197.147  do ping 103.95.197.148  spanning-tree mode rapid  spanning-tree vlan 30 root primary  spanning-tree vlan 40 root primary  spanning-tree vlan 50 root primary  ##### doi root vlan 60, 80  spanning-tree vlan 60 root primary  ##### | | | ***SW-Core-2***  en  conf t  hostname SW-CORE-2  inter range e1/0 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  inter range e1/2-3  channel-group 1 mode on  exit  inter port-channel 1  sw tr en dot  sw mod tru  do wr  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  vlan 80  name DMZ  vlan 2  name ssh\_telnet  inter vlan 30  ip add 103.95.197.148 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.4 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.4 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.164 255.255.255.240  no sh  inter vlan 80  ip add 103.95.197.242 255.255.255.240  no sh  spanning-tree mode rapid  spanning-tree vlan 60 root primary  spanning-tree vlan 80 root primary  ***DSW-11***  en  conf t  hostname DSW-11  inter range e1/0 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  vlan 80  name DMZ  vlan 2  name ssh\_telnet  inter vlan 30  ip add 103.95.197.150 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.6 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.6 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.166 255.255.255.240  no sh  do wr  do ping 103.95.197.147  do ping 103.95.197.148  spanning-tree mode rapid  spanning-tree vlan 60 root primary |
| ***ASW-01***  en  conf t  hostname ASW-01  inter range e1/2 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  inter vlan 30  ip add 103.95.197.151 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.7 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.7 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.167 255.255.255.240  no sh  inter e0/0  sw mode acc  sw ac vlan 30  no sh  inter e0/1  sw mode acc  sw ac vla 40  no sh | | | ***ASW-02***  en  conf t  hostname ASW-02  inter range e1/2 - 3  sw trunk enc dot  sw mode trunk  sw trunk allow vlan all  exit  vlan 30  name Ketoan  vlan 40  name VanPhong  vlan 50  name KyThuat  vlan 60  name LanhDao  inter vlan 30  ip add 103.95.197.152 255.255.255.240  no sh  inter vlan 40  ip add 103.95.196.8 255.255.255.0  no sh  inter vlan 50  ip add 103.95.197.8 255.255.255.192  no sh  inter vlan 60  ip add 103.95.197.168 255.255.255.240  no sh  inter e0/0  sw mode acc  sw ac vlan 50  no sh  inter e0/1  sw mode acc  sw ac vla 60  no sh |

2. Firewall

Note:

Nhớ bật interface vật lý để sub-interface hoạt động  
- Khi 1 switch két nối với một Firewall, cổng của switch phải được cấu hình trunk + allow vlan,,  
- Trên firewall 🡪 tag vlans id cho interface sau hi nameif   
- Các pc khi để gatewave la ip vlan trên switch , ko ping đc 2.2.2.2  
 + Khi đổi gatewave thành ip trên sub-interface , ping được 2.2.2.2  
 + inside sec = 0 không thể ping outside sec= 0 (bắt buộc sec inside phải cao)  
- Để outside ping được vào inside   
 - cấu hình access-list và access-group

Firewall

interface GigabitEthernet0/0

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/0.10

vlan 10

nameif inside\_vlan\_10

security-level 50

ip address 10.0.10.1 255.255.255.0

!

interface GigabitEthernet0/0.40

vlan 40

nameif inside\_vlan\_40

security-level 50

ip address 10.0.40.1 255.255.255.0

!

interface GigabitEthernet0/1

nameif outside

security-level 0

ip address 4.4.4.1 255.255.255.0

!

access-list outside\_access\_in extended permit icmp any any

access-group outside\_access\_in in interface outside

route outside 2.2.2.0 255.255.255.0 4.4.4.2 1

route inside\_vlan\_10 10.0.10.0 255.255.255.0 10.0.10.4 1

route inside\_vlan\_40 10.0.40.0 255.255.255.0 10.0.40.4 1

2.Stage 2: Firewall (sub-interface, failover, gatewave cho vlans)  
 2.1 Sub-interface  
 + Tạo vlan 30,40,50 trên g0/1.30, 40, 50 của G0/1 của firewall  
 + Tạo vlan 60,80 trên g0/2.60, 80 của G0/2 của firewall

|  |  |  |
| --- | --- | --- |
| *G0/1.30 G0/1.40 G0/1.50* | | |
| inter g0/1.30  vlan 30  nameif inside\_01\_30  sec 80  ip add 103.95.197.151 255.255.255.240  no sh | inter g0/1.40  vlan 40  sec 80  nameif inside\_01\_40  ip add 103.95.196.7 255.255.255.0  no sh | inter g0/1.50  vlan 50  sec 80  nameif inside\_01\_50  ip add 103.95.197.7 255.255.255.192  no sh |
| *G0/2.60 G0/2.80* | | |

2.2 Failover

|  |  |
| --- | --- |
| FW-01 | FW-02 |
| failover lan unit primary  failover lan interface interface\_g0/7 g0/7  failover interface ip interface\_g0/7 103.95.198.33 255.255.255.240 standby 103.95.198.34  failover  inter g0/7  no sh | failover lan unit secondary  failover lan interface interface\_g0/7 g0/7  failover interface ip interface\_g0/7 103.95.198.33 255.255.255.240 standby 103.95.198.34  failover  inter g0/7  no sh |
|  |  |

2.3 IP interface FW

|  |  |
| --- | --- |
|  |  |
| FW-1  inter g0/0  nameif outside  ip add 103.95.198.3 255.255.255.240  no sh | FW-2  inter g0/0  nameif outside  ip add 103.95.198.4 255.255.255.240  no sh |
| ## Đang ở chế độ standby nên chưa conf được ip firewall 2 | |

2.4 IP interface RGW + inspect icmp

|  |  |
| --- | --- |
| RGW-20  inter e0/1  ip add 103.95.198.13 255.255.255.240  no sh | RGW-21  inter e0/2  ip add 103.95.198.14 255.255.255.240  no sh |
| Fixup protocol icmp |  |
| *#Ping\_test: FW đã ping được đến RGW-21,21* | |

2.5 Test NAT  
+ để PC trong Lan ra outside, cần NAT và icmp inspect

|  |  |
| --- | --- |
| object network inside\_vlan\_30  subnet 103.95.197.144 255.255.255.240  nat (inside\_01\_30,outside) dynamic interface  object network inside\_vlan\_40  subnet 103.95.196.0 255.255.255.0  nat (inside\_01\_40,outside) dynamic interface  object network inside\_vlan\_50  subnet 103.95.197.0 255.255.255.192  nat (inside\_01\_50,outside) dynamic interface  object network inside\_vlan\_60  subnet 103.95.197.160 255.255.255.240  nat (inside\_01\_60,outside) dynamic interface | Note: 1 inside 1 nat  ## Test1:  object network inside  subnet 103.95.0.0 255.255.0.0  nat (inside\_01\_30,outside) dynamic interface  --> Conclusion: Khong the nat vi cau lenh nat(inside\_.. chi dc 1 vlan,..) |
| *#Ping\_test: RGW-20 không thể ping mạng LAN* |  |

2.6 Test\_ping FW 🡪 RGW-20

|  |  |
| --- | --- |
| ip route 0.0.0.0 0.0.0.0 103.95.198.3 | --tao default root va 1 loo 0 : 8.8.8.8/24 tren router-20 |
| route outside 8.8.8.0 255.255.255.0 103.95.198.13 | --Tao outsdie route cho firewall |
| *#test\_ping : FW-ASA-1 da ping duoc 8.8.8.8 inter RGW-20* | |

2.7 ACL outside ping inside

|  |  |
| --- | --- |
| access-list outside\_access\_in extended permit icmp any any  access-group outside\_access\_in in interface outside | -Tao access-list de outside ping inside |
| *#note: Khi vào lab hoàn chỉnh , chỉnh sửa lại acl để bảo đảm an toàn inside network* | |

2.8 Chuyển đổi vlan 60 80 + after instruction

+ Tạo vlan 80 , chuyển đổi vlan 60, 80 qua sub-interface g0/2. Của FW-02  
+ Tạo vlan sw-1,2, spanning-tree root qua sw-2 để có thể nhận gatewave đến cổng G0/2. Của FW-01

|  |  |
| --- | --- |
| vlan 80  name DMZ  inter vlan 80  ip add 103.95.197.243 255.255.255.240  no sh | vlan 80  name DMZ  inter vlan 80  ip add 103.95.197.244 255.255.255.240  no sh  inter e0/2  sw tr en dot  sw mod tru  no sh |
| 30,40,50 root sw-1  60,80 root sw-2 | --- Cấu hình spanningtree để nhận root 60,80 qua SW-2, (root ở SW-1 sẻ không thấy gatewave trên g0/2. ) |
| *#note: allow vlan trên port chan 1 để vlan 80 có thể ping nhau, trunk đường lên gatewave FW* | |
| inter g0/2.80  vlan 80  sec 80  nameif inside\_02\_80  ip add 103.95.197.241 255.255.255.240  no sh  inter g0/2.60  vlan 60  sec 80  nameif inside\_02\_60  ip add 103.95.197.169 255.255.255.240  no sh | --- ---Tren FW-ASA-1  ## sub-interface cho vlan 60,80 o port g0/2 |
| *--- test\_ping: pc vlan 80 pingable to gatewave asa-active* | |
| -Bo NAT, dung static tro de VRRP ip 2 RGW-20vsRGW-21  -Bo NAT  -show nat  -show run nat  - no object network inside\_01\_30 | |
|  |  |

2.9 VRRP trên 2 RGW-20, 21

-VRRP 1

- doi ip /28 thanh /27 de de lam viec ###

- vrrp 1 ip 103.95.198.20

- tu firewall , route den .20 qua .13

route outside 103.95.198.20 255.255.255.255 103.95.198.13

|  |  |
| --- | --- |
|  |  |
| *NOTE: Done*  -Khi vrrp , VIP sẻ ở trên router master, -> pc chỉ có thể ping looback của RGW-20 ( là ROuter Master, VIP chọn )  -Khi cấu hình firewall, nếu mạng inside chỉ có gatewave là interface của firewall (mạng con kết nối thẳng tới firewall) , thì ko cần route inside  -Các mạng ngoài cần khai báo route vào mạng LAN (inside) thông qua cổng nexthop là interface của Firewall.  -Có 5 vlans , nên từ router ở ngoài phải có 5 static route vào 5vlans, để có thể trả echo reply khi pc LAN ping tới | |

2.10 DHCP sub-inter vlan trên firewall

|  |  |
| --- | --- |
| Vlan 30  dhcpd address 103.95.196.50-103.95.196.100 inside\_01\_40  dhcpd enable insdide\_01\_40  dhcpd options 3 ip 103.95.196.7 ## khai gatewave tại FW-01  Vlan 40  dhcpd address 103.95.197.10-103.95.197.14 inside\_01\_50  dhcpd enable inside\_01\_405 | ## kích hoạt dhcp trên vpc  dhcp |
|  |  |
|  |  |

2.11 Port-security

|  |  |  |
| --- | --- | --- |
| ASW-01 | E0/0 | switch port-security (bat mode port-security)  switch port-security maximum 1 (so lan MAC duoc thay doi la 1)  switch port-security mac-address gom 2 option:  - add MAC manual: switch port-security mac-address 00:50:79:66:68:0d  - add auto: switch port-security mac-address sticky  (sticky: SW tu dong update dia chi MAC dau tien duoc gan) |
| E0/1 | switch port-security (bat mode port-security)  switch port-security maximum 1 (so lan MAC duoc thay doi la 1)  switch port-security mac-address gom 2 option:  - add MAC manual: switch port-security mac-address 00:50:79:66:68:0e  - add auto: switch port-security mac-address sticky  (sticky: SW tu dong update dia chi MAC dau tien duoc gan) |
| ASW-02 | E0/0 | switch port-security (bat mode port-security)  switch port-security maximum 1 (so lan MAC duoc thay doi la 1)  switch port-security mac-address gom 2 option:  - add MAC manual: switch port-security mac-address 00:50:79:66:68:0f  - add auto: switch port-security mac-address  sticky (sticky: SW tu dong update dia chi MAC dau tien duoc gan) |
| E0/1 | switch port-security (bat mode port-security)  switch port-security maximum 1 (so lan MAC duoc thay doi la 1)  switch port-security mac-address gom 2 option:  - add MAC manual: switch port-security mac-address 00:50:79:66:68:10  - add auto: switch port-security mac-address sticky  (sticky: SW tu dong update dia chi MAC dau tien duoc gan) |

2.12 SSH

|  |  |
| --- | --- |
| --------------------SW-CORE-1  ip domain-name minhchinhchien.com  username minh pass minh  crypto key gene rsa modu 1024  vlan 2  no sh  inter vlan 2  ip add 103.95.198.66 255.255.255.240  no sh  inter vlan 1  shutdown  no ip add  inter range e0/1,e1/0  sw tr all vlan add 2  no sh  inter port-chann 1  sw tr all vlan add 2  ip domain-name minhchinhchien.com  username minh pass minh  crypto key gene rsa modu 1024  line vty 0 4  login local  transport input ssh  exec-timeout 3 | --------------------SW-CORE-2  ip domain-name minhchinhchien.com  username minh pass minh  crypto key gene rsa modu 1024  vlan 2  no sh  inter vlan 2  ip add 103.95.198.70 255.255.255.240  no sh  inter vlan 1  shutdown  no ip add  inter range e0/1,e1/0  sw tr all vlan add 2  no sh  inter port-cha 1  sw tr all vlan add 2  ip domain-name minhchinhchien.com  username minh pass minh  crypto key gene rsa modu 1024  line vty 0 4  login local  transport input ssh  exec-timeout 3 |
|  |  |

2.13 iBGP

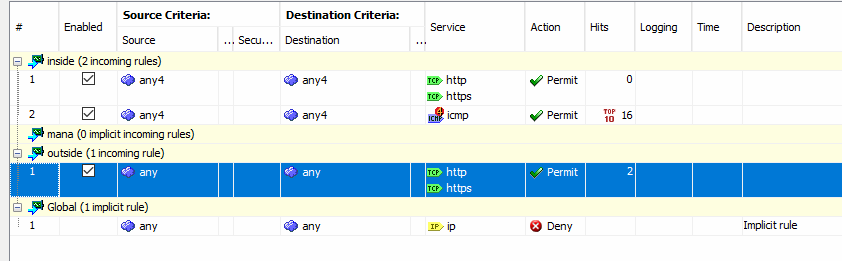
|  |  |
| --- | --- |
| **Router 20**  inter e0/3  no sh  ip add 103.95.198.17 255.255.255.240  router bgp 65001  neighbor 103.95.198.18 remote-as 65001  neighbor 103.95.198.18 update-source e0/3 | **Router 21**  inter e0/3  no sh  ip add 103.95.198.18 255.255.255.240  router bgp 65001  neighbor 103.95.198.17 remote-as 65001  neighbor 103.95.198.17 update-source e0/3 |
|  |  |

|  |  |
| --- | --- |
| enable  configure terminal  interface Ethernet0/0  ip address 103.95.198.1 255.255.255.240  no shutdown  exit  router bgp 65000  bgp log-neighbor-changes  neighbor 192.0.2.2 remote-as 65001  neighbor 192.0.2.2 update-source Ethernet0/1  access-list 1 permit 0.0.0.0 255.255.255.255  access-list 2 permit 103.95.198.0 0.0.0.15  ip prefix-list in-country seq 10 permit 117.117.1.0/22  route-map in-country permit 10  match ip address prefix-list in-country  set local-preference 200  neighbor 192.0.2.2 route-map in-country in  exit  ip route 0.0.0.0 0.0.0.0 192.0.2.1 | enable  configure terminal  interface Ethernet0/0  ip address 192.0.2.1 255.255.255.0  no shutdown  exit  router bgp 65001  bgp log-neighbor-changes  neighbor 192.0.2.2 remote-as 65000  neighbor 192.0.2.2 update-source Ethernet0/0  access-list 1 permit 0.0.0.0 255.255.255.255  ip prefix-list out-country seq 10 permit 12.0.0.0/16  route-map out-country permit 10  match ip address prefix-list out-country  set local-preference 200  neighbor 192.0.2.2 route-map out-country out  exit  ip route 0.0.0.0 0.0.0.0 192.0.2.1 |
|  |  |

2.14 ASDM conf Firewall

-Copy file asdm tu boot:/ 🡪 falsh:/  
- Inter

|  |  |
| --- | --- |
| int mana 0/0  nameif mana  sec 30  ip add 192.168.78.78 255.255.255.0  no sh  http server enable  http 192.168.78.0 255.255.255.0 mana  aaa authentication http console LOCAL | # have in network segment with Vmnet8 (192.168.78.0)  # When ssh, use username and password is stored locally on this device (in that case is Firewall) |

2.14 Giải thích ASDM để open port cho web  


Inside: duyệt các rules khi huưướng đến khu vực mạng “inside”  
 -vd: xét gói tin khi có huưướng đến inside network  
 **## be normalize >.<**

