|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bảng địa mạng cho các VLAN/Router trong các KTX A** | | | | | | | |
| **VLAN Id** | **VLAN Name** | **Number**  **(118 host)** | **Network** | **Subnet** | **Usable Range** | **Broadcast** | **Wildcard** |
| VLAN 10 | SinhVien | 72 | 192.168.100.0 | 255.255.255.128  (/25) | 192.168.100.1 - 192.168.100.126 | 192.168.100.127 | 0.0.0.127 |
| 192.168.101.0 | 255.255.255.128  (/25) | 192.168.101.1 - 192.168.101.126 | 192.168.101.127 | 0.0.0.127 |
| VLAN 20 | GiangVien | 30 | 192.168.100.128 | 255.255.255.224  (/27) | 192.168.100.129 - 192.168.100.158 | 192.168.100.159 | 0.0.0.31 |
| 192.168.101.128 | 255.255.255.224  (/27) | 192.168.101.129 - 192.168.101.158 | 192.168.101.159 | 0.0.0.31 |
| VLAN 30 | QuanLy | 8 | 192.168.100.176 | 255.255.255.240  (/28) | 192.168.100.177 - 192.168.100.190 | 192.168.100.191 | 0.0.0.15 |
| 192.168.101.176 | 255.255.255.240  (/28) | 192.168.101.177 - 192.168.101.190 | 192.168.101.191 | 0.0.0.15 |
| VLAN 99 | Native | 10 | 192.168.100.160 | 255.255.255.240  (/28) | 192.168.100.161 - 192.168.100.174 | 192.168.100.175 | 0.0.0.15 |
| 192.168.101.160 | 255.255.255.240  (/28) | 192.168.101.161 - 192.168.101.174 | 192.168.101.175 | 0.0.0.15 |
| Router | Router | 2 | 192.168.100.192 | 255.255.255.252  (/30) | 192.168.100.193 - 192.168.100.194 | 192.168.100.195 | 0.0.0.3 |
| 192.168.101.192 | 255.255.255.252  (/30) | 192.168.101.193 - 192.168.101.194 | 192.168.101.195 | 0.0.0.3 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bảng địa mạng cho các VLAN/Router trong các KTX B** | | | | | | | |
| **VLAN Id** | **VLAN Name** | **Number**  **(118 host)** | **Network** | **Subnet** | **Usable Range** | **Broadcast** | **Wildcard** |
| VLAN 10 | SinhVien | 72 | 192.168.200.0 | 255.255.255.128  (/25) | 192.168.200.1 - 192.168.200.126 | 192.168.200.127 | 0.0.0.127 |
| 192.168.201.0 | 255.255.255.128  (/25) | 192.168.201.1 - 192.168.201.126 | 192.168.201.127 | 0.0.0.127 |
| VLAN 20 | GiangVien | 30 | 192.168.200.128 | 255.255.255.224  (/27) | 192.168.200.129 - 192.168.200.158 | 192.168.200.159 | 0.0.0.31 |
| 192.168.201.128 | 255.255.255.224  (/27) | 192.168.201.129 - 192.168.201.158 | 192.168.201.159 | 0.0.0.31 |
| VLAN 30 | QuanLy | 8 | 192.168.200.176 | 255.255.255.240  (/28) | 192.168.200.177 - 192.168.200.190 | 192.168.200.191 | 0.0.0.15 |
| 192.168.201.176 | 255.255.255.240  (/28) | 192.168.201.177 - 192.168.201.190 | 192.168.201.191 | 0.0.0.15 |
| VLAN 99 | Native | 10 | 192.168.200.160 | 255.255.255.240  (/28) | 192.168.200.161 - 192.168.200.174 | 192.168.200.175 | 0.0.0.15 |
| 192.168.201.160 | 255.255.255.240  (/28) | 192.168.201.161 - 192.168.201.174 | 192.168.201.175 | 0.0.0.15 |
| Router | Router | 2 | 192.168.200.192 | 255.255.255.252  (/30) | 192.168.200.193 - 192.168.200.194 | 192.168.200.195 | 0.0.0.3 |
| 192.168.201.192 | 255.255.255.252  (/30) | 192.168.201.193 - 192.168.201.194 | 192.168.201.195 | 0.0.0.3 |

**Tiến độ công việc:**

1/ Bảng địa chỉ IP:

|  |  |  |  |
| --- | --- | --- | --- |
| **Servers** | **Port** | **Ipv4/Subnet Mask** | **Ipv6** |
| DNS | Fa0 | 192.168.99.2 /24 | 2001:C0A8:99::2 |
| WEB | Fa0 | 192.168.99.3 /24 | 2001:C0A8:99::3 |
| MAIL | Fa0 | 192.168.99.4 /24 | 2001:C0A8:99::4 |
| FTP | Fa0 | 192.168.99.5 /24 | 2001:C0A8:99::5 |
| DHCP | Fa0 | 192.168.99.6 /24 | 2001:C0A8:99::6 |
| SYSLOG | Fa0 | 192.168.99.7 /24 | 2001:C0A8:99::7 |
| NTP | Fa0 | 192.168.99.8 /24 | 2001:C0A8:99::8 |
| Radius Server A | Fa0 | 192.168.99.9 /24 | 2001:C0A8:99::9 |
| Radius Server B | Fa0 | 192.168.99.10 /24 | 2001:C0A8:99::10 |
| Radius Server C | Fa0 | 192.168.99.11 /24 | 2001:C0A8:99::11 |
| **Router** | **Port** | **Ipv4/Subnet Mask** | **Ipv6** |
| Site A | G0/0 | 10.10.2.2 /30 | 2001:C0A8:2::2  FE80::2 |
| G0/1 | 192.168.100.193 /30 | 2001:C0A8:100::1  FE80::2 |
| G0/1.10 | 192.168.100.1 /25 | 2001:C0A8:110::1  FE80::2 |
| G0/1.20 | 192.168.100.129 /27 | 2001:C0A8:120::1  FE80::2 |
| G0/1.30 | 192.168.100.177 /28 | 2001:C0A8:130::1  FE80::2 |
| G0/2 | 192.168.101.193 /30 | 2001:C0A8:101::1  FE80::2 |
| G0/2.10 | 192.168.101.1 /25 | 2001:C0A8:111::1  FE80::2 |
| G0/2.20 | 192.168.101.129 /27 | 2001:C0A8:121::1  FE80::2 |
| G0/2.30 | 192.168.101.177 /28 | 2001:C0A8:131::1  FE80::2 |
| Se0/3/0 | 10.10.4.1 | 2001:C0A8:4::2  FE80::2 |
| Se0/3/1 | 10.10.4.2 | N/A |
| Site A\_BackUp | G0/0 | 10.10.3.2 /30 | 2001:C0A8:3::2  FE80::3 |
| G0/1 | 192.168.100.193 /30 | 2001:C0A8:100::1  FE80::3 |
| G0/1.10 | 192.168.100.1 /25 | 2001:C0A8:110::1  FE80::3 |
| G0/1.20 | 192.168.100.129 /27 | 2001:C0A8:120::1  FE80::3 |
| G0/1.30 | 192.168.100.177 /28 | 2001:C0A8:130::1  FE80::3 |
| G0/2 | 192.168.101.193 /30 | 2001:C0A8:101::1  FE80::3 |
| G0/2.10 | 192.168.101.1 /25 | 2001:C0A8:111::1  FE80::3 |
| G0/2.20 | 192.168.101.129 /27 | 2001:C0A8:121::1  FE80::3 |
| G0/2.30 | 192.168.101.177 /28 | 2001:C0A8:131::1  FE80::3 |
| Se0/3/0 | 10.10.5.1 | 2001:C0A8:5::2  FE80::2 |
| Se0/3/1 | N/A | N/A |
| Site B | G0/0 | 192.168.200.193 /30 | 2001:C0A8:200::1  FE80::4 |
| G0/1 | 192.168.201.193 /30 | 2001:C0A8:201::1  FE80::4 |
| G0/0.10 | 192.168.200.1 /25 | 2001:C0A8:210::1  FE80::4 |
| G0/0.20 | 192.168.200.129 /27 | 2001:C0A8:220::1  FE80::4 |
| G0/0.30 | 192.168.200.177 /28 | 2001:C0A8:230::1  FE80::4 |
| G0/2 | N/A | N/A |
| G0/1.10 | 192.168.201.1 /25 | 2001:C0A8:211::1  FE80::4 |
| G0/1.20 | 192.168.201.129 /27 | 2001:C0A8:221::1  FE80::4 |
| G0/1.30 | 192.168.201.177 /28 | 2001:C0A8:231::1  FE80::4 |
| Se0/3/0 | 10.10.4.2 | 2001:C0A8:4::1  FE80::4 |
| Se0/3/1 | 10.10.5.2 | 2001:C0A8:5::1  FE80::4 |
| Server | Gig0/0/0 | 10.10.1.2 /30 | 2001:C0A8:1::2  FE80::1 |
| Gig0/0/1 | 192.168.99.1 /24 | 2001:C0A8:99::1  FE80::1 |
| ASA 5506-X | Gig1/1 | 10.10.2.1 /30 | 2001:C0A8:2::1  FE80::8 |
| Gig1/2 | 10.10.3.1 /30 | 2001:C0A8:3::1  FE80::9 |
| Gig1/3 | 10.10.1.1 /30 | 2001:C0A8:1::1  FE80::7 |
| Gig1/4 |  |  |

2/ Bảng Mode VLAN của các Switch:

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | **Port** | **Mode** | **VLAN** |
| Core\_A\_1  Core\_B\_1 | Fa0/1-4 | Trunking Native Vlan 99 | N/A |
| G1/0/5-7 | Etherchannel group 1 PAgP  Trunking Native Vlan 99 | N/A |
| Core\_A\_2  Core\_B\_2 | Fa0/1-4 | Trunking Native Vlan 99 | N/A |
| G1/0/5-7 | Etherchannel group 1 PAgP  Trunking Native Vlan 99 | N/A |
| Distribution\_A\_1  Distribution\_B\_1 | Fa0/1-6 | Trunking Native Vlan 99 | N/A |
| Distribution\_A\_2  Distribution\_B\_2 | Fa0/1-6 | Trunking Native Vlan 99 | N/A |
| SW\_A\_1  SW\_B\_1 | Fa0/3 | Access | 10 |
| Fa0/4 | Access | 30 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_2  SW\_B\_2 | Fa0/3-4 | Access | 10 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_3  SW\_B\_3 | Fa0/3-4 | Access | 10 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |
| SW\_A\_4  SW\_B\_4 | Fa0/3-4 | Access | 20 |
| Fa0/1-2 | Trunking Native Vlan 99 | N/A |

3/ Địa chỉ IP và VLAN của các thiết bị:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Devices** | **Mode Connection** | **Ipv4** | **Ipv6** | **VLAN** |
| SV1-20 | Wireless | DHCP | DHCP | 10 |
| QL1-4 | Wireless | DHCP | DHCP | 30 |
| GV1-8 | Wireless | DHCP | DHCP | 20 |

4/ Thiết lập:

* OSPF giữa các router:
  + Show ip protocols
  + *Router Site A:*
    - Router-id: 2.2.2.2
    - ospf 1
    - network 192.168.100.0 0.0.0.255 area 0
    - network 192.168.101.0 0.0.0.255 area 0
    - network 10.10.2.0 0.0.0.3 area 0
    - network 10.10.4.0 0.0.0.3 area 0
  + *Router Site A\_BackUp:*
    - Router-id: 3.3.3.3
    - ospf 1
    - network 192.168.100.0 0.0.0.255 area 0
    - network 192.168.101.0 0.0.0.255 area 0
    - network 10.10.3.0 0.0.0.3 area 0
    - network 10.10.5.0 0.0.0.3 area 0
  + *Router Site B:*
    - Router-id: 4.4.4.4
    - ospf 1
    - network 192.168.200.0 0.0.0.255 area 0
    - network 192.168.201.0 0.0.0.255 area 0
    - network 10.10.4.0 0.0.0.3 area 0
    - network 10.10.5.0 0.0.0.3 area 0
  + *Router Servers:*
    - Router-id: 1.1.1.1
    - ospf 1
    - network 192.168.99.0 0.0.0.255 area 0
    - network 10.10.1.0 0.0.0.3 area 0
  + *Router Site A\_BackUp:*
    - Router-id: 3.3.3.3
    - ospf 1
    - network 10.10.3.0 0.0.0.3 area 0
  + *ASA 5506-X:*
    - Router-id: 7.7.7.7
    - ospf 1
    - network 10.10.1.0 255.255.255.252 area 0
    - network 10.10.2.0 255.255.255.252 area 0
    - network 10.10.3.0 255.255.255.252 area 0
    - network 10.10.7.0 255.255.255.252 area 0
    - network 10.10.8.0 255.255.255.252 area 0
* Cấu hình ip trên ASA 5506-X:
  + *Gig 1/3:*
    - namif inside\_Servers
    - security-level 100
    - ip address 10.10.1.1 255.255.255.252
    - no shutdown
  + *Gig 1/1:*
    - namif inside\_SiteA
    - security-level 100
    - ip address 10.10.2.1 255.255.255.252
    - no shutdown
  + *Gig 1/2:*
    - namif inside\_SiteABackUp
    - security-level 100
    - ip address 10.10.3.1 255.255.255.252
    - no shutdown
* Thiết lập trên Mail server:
  + domain name: tdtu.edu.vn
    - User: student1
      * Password: 123
    - User: student2
      * Password: 123
* Thiết lập trên FTP server:
  + User: student1
    - Password: 123
  + User: student2
    - Password: 123
* Thiết lập trên các Access Point:
  + *Floor1\_A\_1*
    - SSID: Floor1\_A\_1
    - Password: 12345678
  + *Floor2\_A\_1*
    - SSID: Floor2\_A\_1
    - Password: 12345678
  + *Floor3\_A\_1*
    - SSID: Floor3\_A\_1
    - Password: 12345678
  + *Floor4\_A\_1*
    - SSID: Floor4\_A\_1
    - Password: 12345678
  + *Floor1\_A\_2*
    - SSID: Floor1\_A\_2
    - Password: 12345678
  + *Floor2\_A\_2*
    - SSID: Floor2\_A\_2
    - Password: 12345678
  + *Floor3\_A\_2*
    - SSID: Floor3\_A\_2
    - Password: 12345678
  + *Floor4\_A\_2*
    - SSID: Floor4\_A\_2
    - Password: 12345678
* Sub-interface cho VLAN 10 trên Router Site A:
  + interface g0/1.10
  + encapsulation dot1q 10
  + ip address 192.168.100.1 255.255.255.128
  + no shutdown
  + Làm tương tự cho các VLAN khác tương ứng với các interface .20, .30 cùng với địa chỉ VLAN tương ứng đã chia ở trên.
* Lấy địa chỉ ip từ DHCP Server trên các cổng sub-interface trên Router Site A:
  + interface g0/1.10
  + ip helper-address 192.168.99.6
  + Làm tương tự các sub-interface còn lại
* Thiết lập spanning-tree vlan 1, 10, 20, 30, 99 root primary trên Core\_A\_1 và Core\_B\_1
* Thiết lập port-security trên switch nối các server.
  + show port-security
* Thiết lập dhcp snooping với các cổng từ các switch nối các thiết bị host, switch và router. (limit rate là 20: giới hạn các packet truyền nhận mỗi giây để ngăn server quá tải).
  + show ip dhcp snooping
* ACL Extended 100
  + Chặn các SV trong ktx xài ftp
  + Đặt lên các subinterface của SV theo chiều in.
* Tạo dhcpv6 pool cho Router Site\_A:
  + ipv6 dhcp pool vlan\_10:
    - address prefix 2001:C0A8:110::/64
    - dns-server 2001:C0A8:99::3
  + Trên cổng interface gig 0/1.10:
    - ipv6 address FE80::2 link-local
    - ipv6 nd managed-config-flag
    - ipv6 dhcp server vlan\_10
  + Làm tương tự cho các vlan và các cổng còn lại.
* Thiết lập ntp server trên toàn bộ thiết bị trừ các host.
  + ntp server 192.168.99.8
* Thiết lập syslog server trên router servers.
  + logging 192.168.99.7
* Xây dựng ipsec giữa site B và site C
  + show crypto ipsec sa
  + Xây dựng site C với địa chỉ ipv4 là 192.168.250.0 /24
    - Router G0/0: 192.168.250.1 /24
    - PC: 192.168.250.2 /24
    - Router Serial 0/3/0: 10.10.6.2 /30
    - Router Site A Serial 0/3/1: 10.10.6.1 /30
    - Định tuyến ospf 1 với area 0 với router id là 5.5.5.5 bao gồm các mạng 192.168.250.0 và 10.10.6.0
    - Bên Router Site A cũng định tuyến ospf 1 với area 0 với ip 10.10.6.0
  + Trên router site B:
    - license boot module c1900 technology-package securityk9
    - save config và reload lại router
    - Tạo access-list 110 cho phép toàn bộ SV, GV và QL qua bên mạng của site C
    - crypto isakmp policy 10
    - encryption aes 256
    - authentication pre-share
    - group 5
    - exit
    - crypto isakmp key vpnpa55 address 10.10.6.2
    - crypto map VPN-MAP 10 ipsec-isakmp
    - description VPN connection to site C
    - set peer 10.10.6.2
    - set transform-set VPN-SET
    - match address 110
    - exit
    - interface s0/3/0
    - crypto map VPN-MAP
  + Trên router site C:
    - license boot module c1900 technology-package securityk9
    - save config và reload lại router
    - Tạo access-list 110 cho phép mạng từ site C qua các mạng SV, GV, QL
    - crypto isakmp policy 10
    - encryption aes 256
    - authentication pre-share
    - group 5
    - exit
    - crypto isakmp key vpnpa55 address 10.10.4.2
    - crypto map VPN-MAP 10 ipsec-isakmp
    - description VPN connection to site C
    - set peer 10.10.4.2
    - set transform-set VPN-SET
    - match address 110
    - exit
    - interface s0/3/0
    - crypto map VPN-MAP
* Thiết lập portfast và bpguard trên các cổng của switch nối với các host.
* Thiết lập Etherchannel cho các Switch Core với phạm vi là 3 port.
  + interface range gig1/0/5-7
    - channel-protocol pagp (giao thức của cisco)
    - channel-group 1 mode desirable (để gửi lời yêu cầu thiết lập ethernet channel với thiết bị còn lại)
    - exit
  + interface port-channel 1
    - switchport mode trunk
    - switchport trunk native vlan 99
  + Làm tương tự các bước trên với thiết bị còn lại nhưng thiết lập channel-group 1 với mode auto (không cần phải khởi tạo yêu cầu nữa).
  + show etherchannel summary
* Thiết lập cân bằng tải cho các Etherchannel:
  + port-channel load-balance src-dst-mac
  + show etherchannel load-balance
* Cấu hình cho các Radius Server tương ứng:
  + Mục AAA On:
    - Client Name:
      * RouterSiteA – 10.10.2.2 – SiteA
      * RouterSiteBackUp – 10.10.3.2 – SiteABackUp
    - Username: AdminSiteA – Password: AdminSiteA123
  + Làm tương tự cho các Radius Server B và C, sửa lại các địa chỉ IP và username với password cho phù hợp.
* Áp Radius Server vào các Router:
  + Router Site A:
    - aaa new-model
    - username AdminA secret AdminA123
    - aaa authentication login default group radius local
    - aaa authentication enable default group radius local
    - aaa authorization exec default group radius local
    - radius-server host 192.168.99.9 key SiteA
    - ip domain-name SiteA.com
    - ip ssh version 2
    - crypto key generate rsa
    - 1024
    - line vty 0 4
    - transport input ssh
    - login authentication default
    - line console 0
    - login authentication default
  + Làm tương tự cho các Router còn lại với user, pass và radius server phù hợp. (AdminB – AdminB123 | AdminC – AdminC123)
* Cấu hình PAT trên các Router:
  + show ip nat translations
  + Router Site A:
    - interface gigabitEthernet 0/1.10
    - ip nat inside
    - interface gigabitEthernet 0/1.20
    - ip nat inside
    - interface gigabitEthernet 0/1.30
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/2.10
    - ip nat inside
    - interface gigabitEthernet 0/0
    - ip nat outside
    - access-list 102 permit ip 192.168.100.1 0.0.0.127 any
    - access-list 102 permit ip 192.168.101.1 0.0.0.127 any
    - access-list 102 permit ip 192.168.100.129 0.0.0.31 any
    - access-list 102 permit ip 192.168.101.129 0.0.0.31 any
    - access-list 102 permit ip 192.168.100.177 0.0.0.15 any
    - access-list 102 permit ip 192.168.101.177 0.0.0.15 any
    - ip nat inside source list 102 interface gigabitEthernet 0/0 overload
* Cấu hình zone-pair trên router Servers.
  + **Tạo zone security**
    - Zone security Server
    - Zone security Outside
  + **Tạo class-map**
    - Class-map type inspect FTP
    - Match access-group 100
  + **Tạo policy-map và gắn class-map tương ứng**
    - Policy-map type inspect Server-To-Outside
    - Class type inspect 100
    - Inspect
    - Policy-map type inspect Outside-To-Server
    - Class type inspect 100
    - Inspect
  + **Tạo zone-pair và gắn policy-map tương ứng**
    - Zone-pair security Server-To-Outside source Server destination Outside
    - Service-policy type inspect Server-To-Outside
    - Zone-pair security Outside-To-Server source Outside destination Server
    - Service-policy type inspect Outside-To-Server
  + **Gán zone cho port cổng (interface) tương ứng**
    - Interface g0/0/1
    - Zone-member security Server
    - Interface g0/0/0
    - Zone-member security Outside
  + show policy-map type inspect zone-pair sessions
* ssh tới Router Site A:
  + ssh -l AdminSiteA 192.168.100.193
  + AdminSiteA123
* Thiết lập lại policy-map global-policy trên ASA 5506-X để cho phép các máy ICMP tới Internet.
  + no policy-map global-policy
  + no class-map inspection\_default
  + class-map inspection\_default
  + match default-inspection-traffic
  + exit
  + policy-map global\_policy
  + class inspection\_default
  + inspect icmp
  + inspect dns preset\_dns\_map
  + inspect ftp
  + inspect tftp
  + exit
  + no service-policy global\_policy global
  + service-policy global\_policy global
  + exit
  + write memory
* PAT/NAT từ router site A ra tường lửa:
  + Trên cổng inside\_SiteA ra cổng outside\_ISP1:
    - object network inside\_SiteA\_outside\_ISP1
    - subnet 10.10.2.0 255.255.255.252
    - nat (inside\_SiteA,outside\_ISP1) dynamic interface