THIẾT KẾ HẠ TẦNG MẠNG LAN KHÔNG DỰ PHÒNG

LAN DESIGN WITHOUT HIGH AVAILABILITY

07th April 2015

TABLE OF CONTENTS

DOCUMENT DETAIL **3**
CHANGE RECORDS **3**
GIỚI THIỆU **4**
CÁC CHÚ Ý TRƯỚC KHI ĐỌC TÀI LIỆU **4**
CÁC QUY ƯỚC **4**
SƠ ĐỒ MẠNG (NETWORK DIAGRAM) **5**
THẢO LUẬN VỀ THIẾT BỊ MẠNG SỬ DỤNG TRONG THIẾT KẾ **12**
CẤU HÌNH MẪU (CONFIGURATION TEMPLATE) **13**
THẢO LUẬN VỀ ƯU / KHUYẾT ĐIỂM TRONG THIẾT KẾ KỂ TRÊN **30**

Document Detail

Organization:	
Document Type:	Tài Liệu Thiết Kế Mạng
Document Name:	Thiết kế hệ thống mạng LAN không dự phòng
Revision No.:	2.0
Revision Date:	07th April 2015
Prepared By:	Ha Duc Binh
Prepared Date:	04th December 2011

Change Records

Date/Time	Change description	Affected Pages	Remark
April 7, 2015	Revised network equpment		

Giới Thiệu

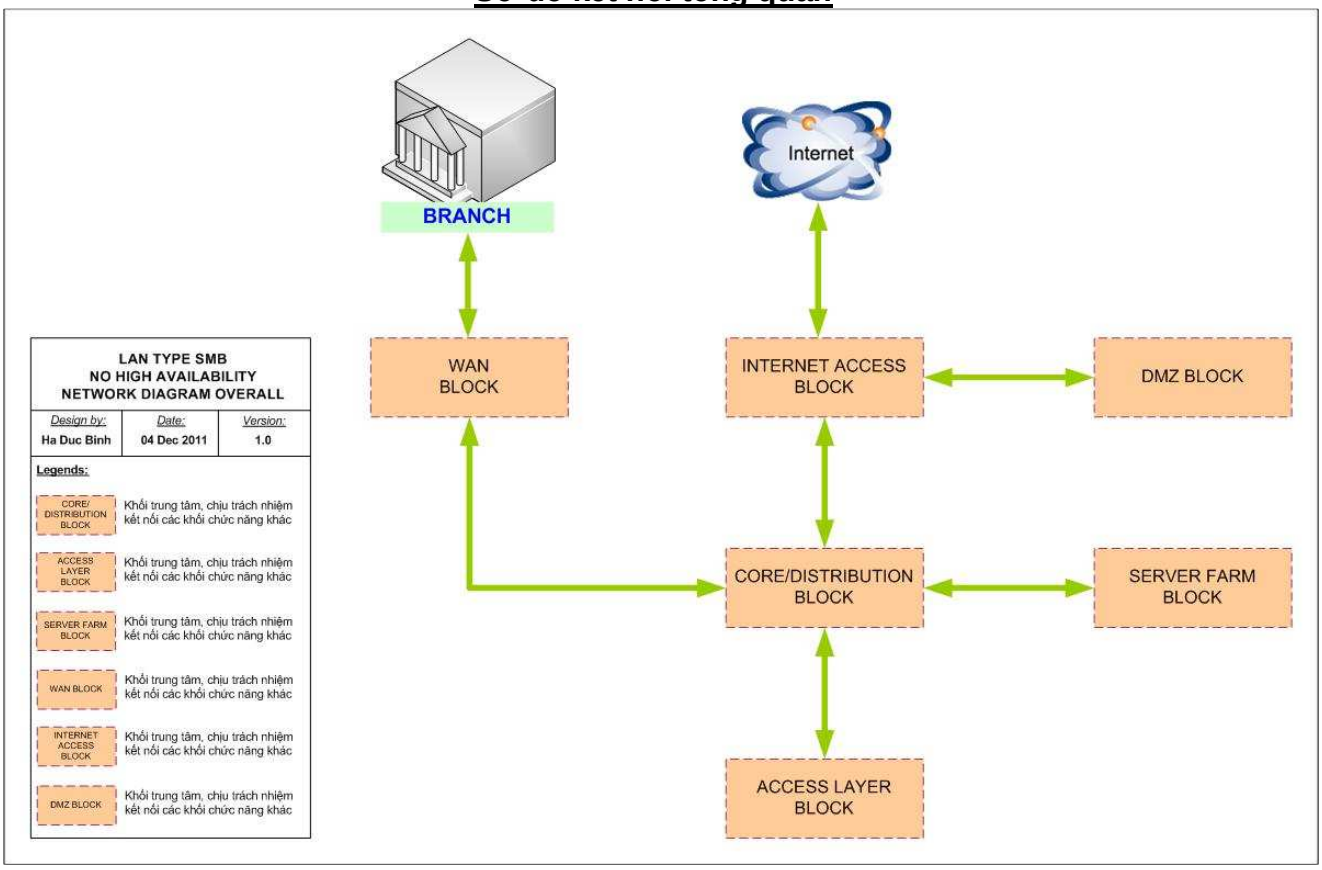
Các Chú Ý Trước Khi Đọc Tài Liệu

- Người đọc nên có chứng chỉ CCNP hoặc kiến thức tương đương CCNP.
- Thông tin được đề cập trong tài liệu này có thể được thay đổi bởi tác giả không cần thông báo trước.

Các Quy Ước

Sơ Đồ Mạng (Network Diagram)

Sơ đồ kết nối tổng quan



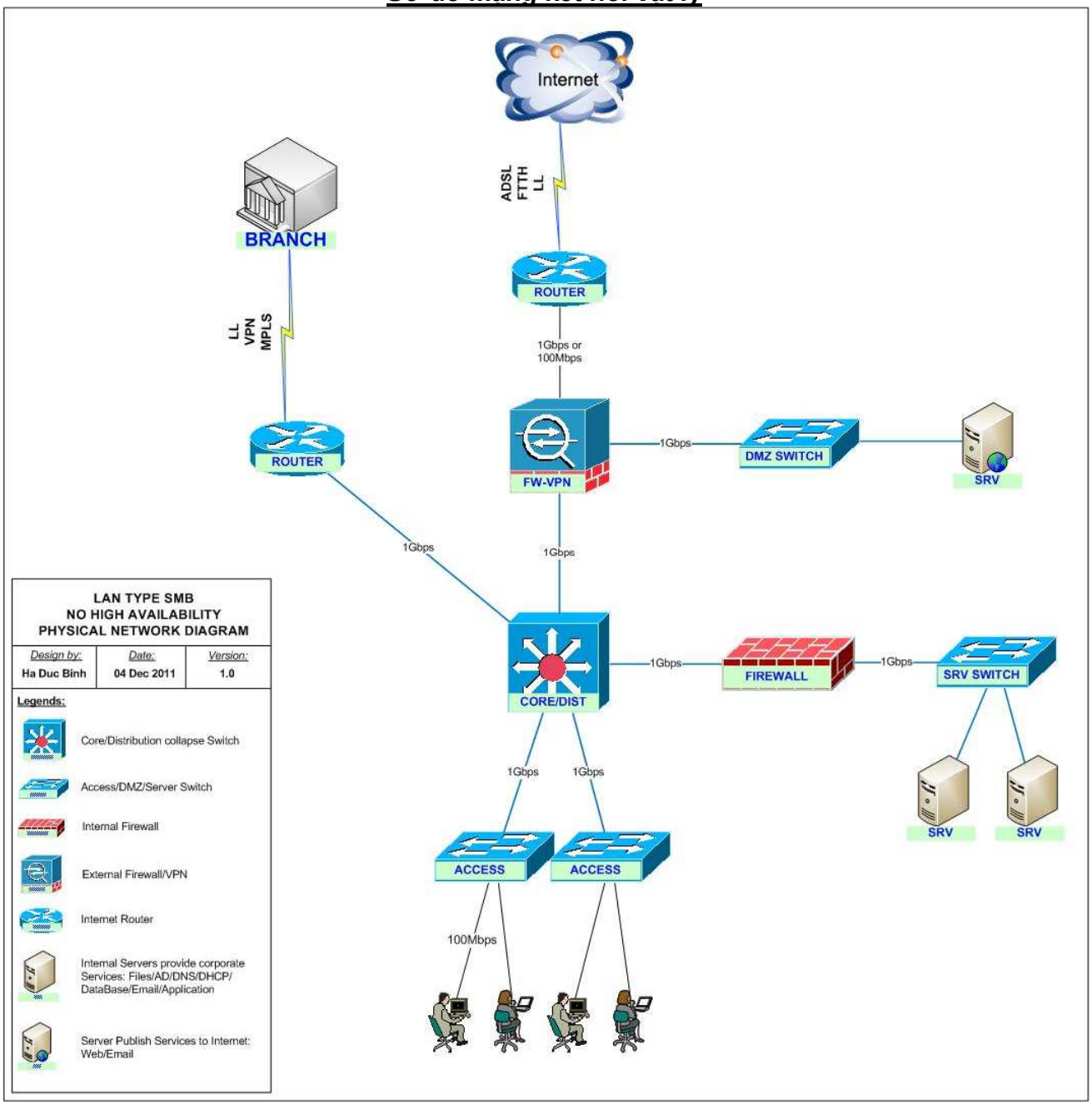
Hệ thống mạng được thiết kế dựa trên nguyên tắc module hóa các thành phần. Việc module hóa khi thiết kế có những đặc điểm nổi bật sau:

- Đơn giản, rõ ràng.
- Có thể mở rộng hệ thống mạng dễ dàng.
- Tách biệt rõ ràng chứng năng của từng module, từ đó có đầy đủ thông tin để chọn lựa đúng thiết bị mạng cho từng module:
    - Core/Distribution Block: là module trung tâm của hệ thống mạng, chịu trách nhiệm kết nối các module còn lại với nhau. Từ đây có thể thấy ưu tiên chọn thiết bị ở lớp này là “càng nhanh càng tốt”.
    - Access Layer Block: là module cung cấp kết nối cho người dùng cuối. Ưu tiên khi chọn thiết bị thuộc module này là “cung cấp nhiều cổng kết nối downlink cho người dùng, đồng thời phải có kết nối Uplink tốc độ cao để kết nối lên module Core/Distribution”, và tối ưu hóa chỉ số “giá thành / cổng downlink”. Thông thường thiết bị sử dụng tại module này chỉ cần hỗ trợ các tính năng ở lớp 2.
    - Server Farm Block: đây là module cung cấp kết nối cho các máy chủ (Servers) cung cấp dịch vụ trong mạng nội bộ, ví dụ: AD, DNS, DHCP, File, Application, Database. Thiết bị chọn ở lớp này cần có

cổng kết nối downlink tốc độ tối thiểu là 1Gbps và hoạt động ở lớp 2.

- WAN Block: là module cung cấp kết nối đến các chi nhánh khác. Thông thường, thiết bị trong module này cần hỗ trợ:
  - Các cổng giao tiếp WAN: Serial, FTTH, ADSL, …
  - Các tính năng: định tuyến động, mã hóa VPN ở phần cứng (VPN supported in hardward).
- Internet Access Block: là module nằm ở ngoài cùng của hệ thống mạng, cung cấp kết nối Internet cho người dùng nội bộ. Thông thường thiết bị được chọn ở module này cần hỗ trợ các tính năng:
  - Định tuyến.
  - NAT/PAT.
  - Firewall.
  - Remote Access VPN.
- DMZ Block: là module kết nối trực tiếp với module “Internet Access Block”. Chức năng của module này:
  - Cung cấp các dịch vụ ra ngoài Internet: Mail, Web.

Sơ đồ mạng kết nối vật lý

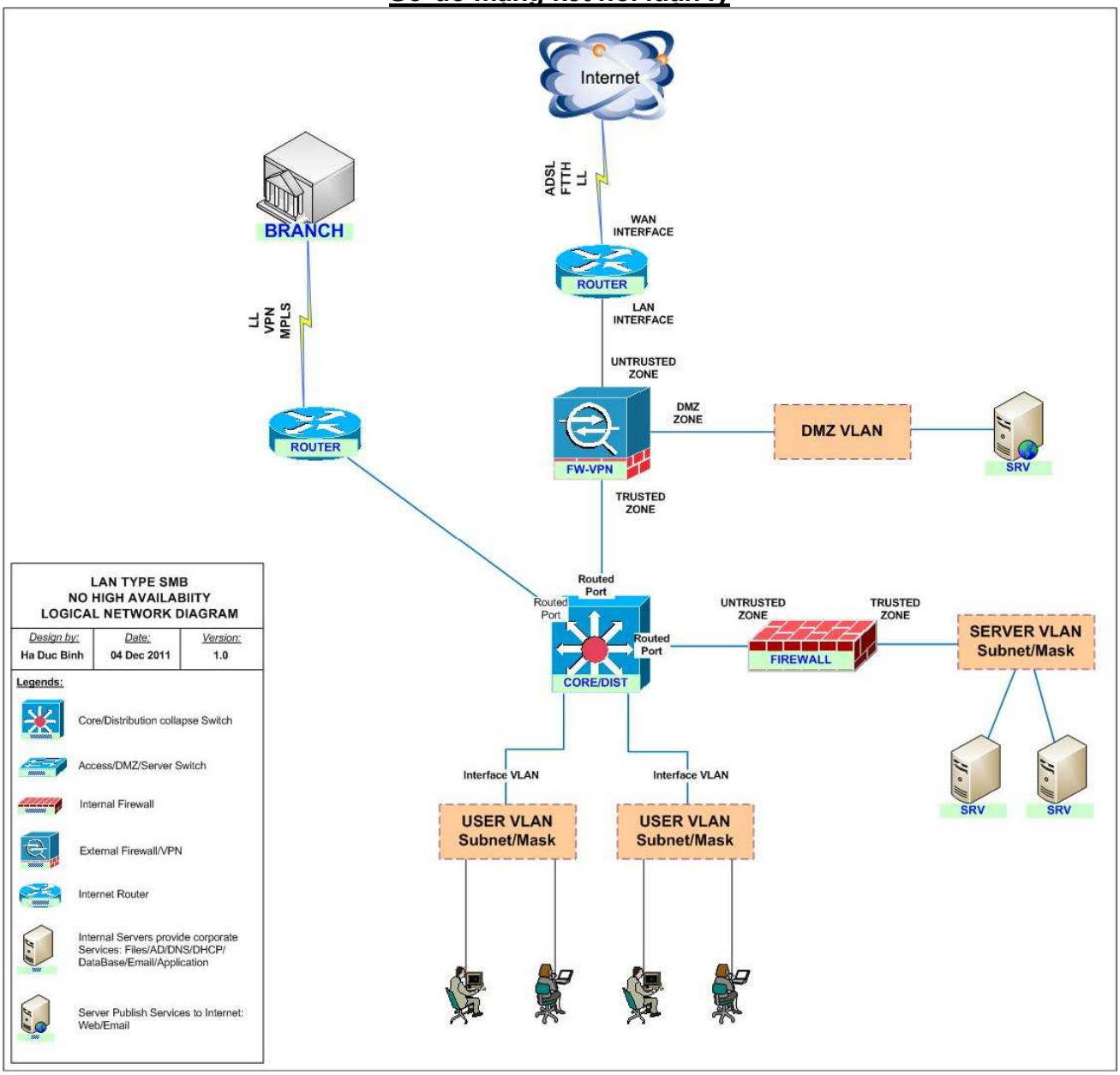


Hệ thống mạng được xây dựng dựa trên tiêu chí không hỗ trợ tính năng sẵng sang cao (HA), do đó chi tiết thiết bị đề xuất cho các module như sau:

- Core/Distribution Block: 1 x Switch có cổng kết nối tốc độ tối thiểu 1Gbps và hoạt động ở lớp 3.
- Access Layer Block: n x Switch có cổng kết nối downlink tốc độ tối thiểu 100Mbps và Uplink 1Gbps, hoạt động ở lớp 2.
- Server Farm Block:

    - 1 x Firewall: có cổng kết nối tốc độ tối thiểu 1Gbps và có Firewall Throughput tối thiểu 1Gbps.
    - 1 x Switch có cổng kết nối tốc độ tối thiểu 1Gbps và hoạt động ở lớp 2.
- WAN Block: 1 x Router có cổng kết nối LAN/WAN tương ứng.
- DMZ Block: 1 x Switch có tốc độ tối thiểu 100Mbps và hoạt động ở lớp 2.
- Internet Access Block:
    - 1 x Firewall: hỗ trợ IPSEC VPN hoặc SSL VPN (nếu yêu cầu).
    - 1 x Router (tùy chọn): có cổng kết nối LAN/WAN tương ứng.

Sơ đồ mạng kết nối luân lý

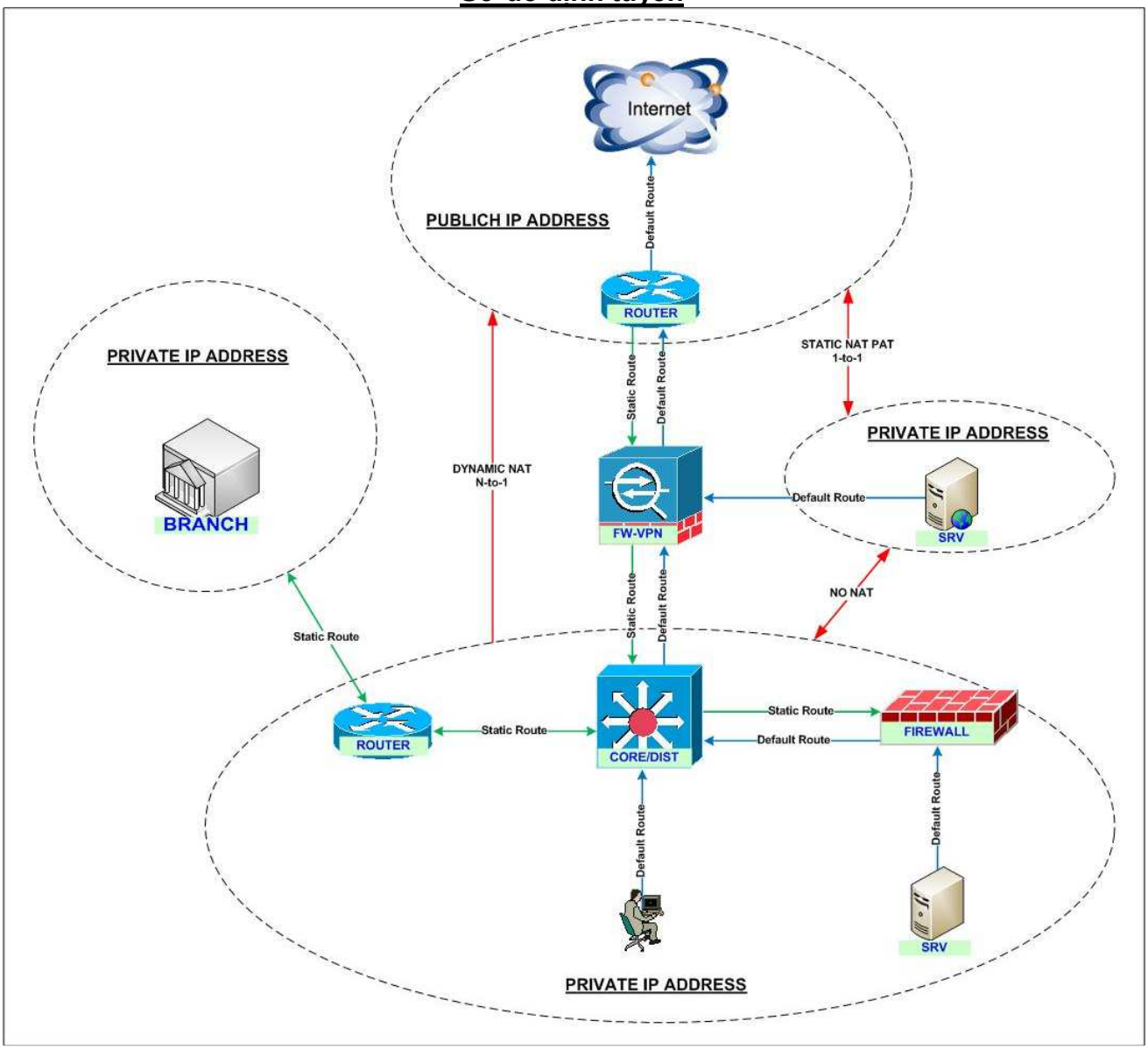


Các tính năng được sử dụng:

- Core/Distribution Switch:
  - Spanning Tree: Rapid-PVST, STP Root Bridge
  - Trunking: Dot1Q
  - Create VLAN.
  - Ether Channel.
  - VTP: Mode Transparent
  - InterVlan Routing.
  - Static Routing.
  - Device Security Hardening.

- Access Switch:
    - Spanning Tree: Rapid-PVST, Portfast
    - Create VLAN
    - Trunking: Dot1Q
    - Ether Channel.
    - VTP: Mode Transparent
    - Assign Port to VLAN
    - Device Security Hardening.
- Internal Firewall:
    - Static Routing.
    - Firewall Policy.
    - Device Security Hardening.
- Server Switch:
    - Spanning Tree: Rapid-PVST, Portfast
    - Create VLAN.
    - VTP: Mode Transparent
    - Assign Port to VLAN
    - Device Security Hardening.
- DMZ Switch:
    - Spanning Tree: Rapid-PVST, Portfast
    - Create VLAN.
    - Device Security Hardening.
- Internet Firewall:
    - Cấu hình Interface.
    - Static Routing.
    - Remote Access VPN/ SSL VPN.
    - Firewall Policy.
- Internet Router:
    - Cấu hình LAN/Internet Interface.
    - Static Routing.
- WAN Router:
    - Cấu hình LAN/WAN Interface.
    - Static Routing.

Sơ đồ định tuyến



Đối với hệ thống mạng đơn giản và không đòi hỏi tính năng sẵng sàng cao (HA), việc chọn và sử dụng định tuyến tĩnh (Static Routing) là hoàn toàn có thể chấp nhận.

- Core Switch sẽ chịu trách nhiệm định tuyến giữa các VLAN người dùng và các module khác. Chi tiết định tuyến tham khảo mô hình trên.
- External Firewall: ngoài việc định tuyến các traffic ra/vào Internet, thiết bị này còn được cấu hình thêm:
    - Firewall: lọc các packets ra/vao giữa các vùng: TRUSTED (còn gọi là INSIDE Zone), DMZ và UNTRUSTED (còn gọi là OUTSIDE Zone). Thông thường traffic từ Internet chi cho phép truy cập vào các tài nguyên được publich tại module DMZ, nghiêm cấm các kết

nối được khởi tạo từ Internet vào TRUSTED hoặc từ DMZ vào TRUSTED. Chi tiết các firewall rule này còn phụ thuộc cụ thể vào từng chính sách bảo mật của từng công ty.
    - Remote Access VPN: phục vụ cho người dùng làm việc từ xa thông qua Internet.
    - Dynamic NAT PAT: traffic từ người dùng truy cập Internet.
    - Static NAT PAT: nhằm publich dịch vụ từ DMZ ra Internet.
    - NO-NAT: không NAT các yêu cầu truy cập (nếu có) từ mạng nội bộ ra/vào DMZ.

Thảo Luận Về Thiết Bị Mạng Sử Dụng Trong Thiết Kế

- Core/Distribution Switch:
    - Cisco Catalyst 3560-X, 3650, 3750-X, 3850.
- Access Switch:
    - Cisco Catalyst 2960-Plus, 2960X.
- Internal Firewall:
    - Cisco ASA5525-X, ASA5545-X, ASA5555-X hoặc tương đương.
- Server Switch:
    - Cisco Catalyst 2960X, 3560-X, 3650, 3750-X, 3850.
- DMZ Switch:
    - Cisco Catalyst 2960-Plus, 2960X.
- Internet Firewall:
    - Cisco ASA5506-X, ASA5515-X hoặc ASA5525-X.
- Internet Router:
    - Cisco Router 1900, 2900.
- WAN Router:
    - Cisco Router 800, 1900, 2900.

References links:

- Cisco 3850 series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html

- Cisco 3750-X series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-3750-x-series-switches/index.html

- Cisco 3650 series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-3650-series-switches/index.html

- Cisco 3560-X series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-3560-x-series-switches/index.html

- Cisco 2960X series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html

- Cisco 2960-Plus series switch:
  http://www.cisco.com/c/en/us/products/switches/catalyst-2960-plus-series-switches/index.html

- Cisco ASA5500-X firewall:
  http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html

- Cisco 800 series router:
  http://www.cisco.com/c/en/us/products/routers/800-series-routers/index.html

- Cisco 1900 series router:
  http://www.cisco.com/c/en/us/products/routers/1900-series-integrated-services-routers-isr/index.html

- Cisco 2900 series router:
  http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index.html

Cấu Hình Mẫu (Configuration Template)

Core/Distribution Switch Cisco Catalyst 3650/3560-X:

!Cấu hình VLAN

Switch(config)# vlan <Vlan-ID>
Switch(config-vlan)# name <Vlan-Name>

!Cấu hình VTP mode transparent

Switch(config)# vtp mode transparent

!Cấu hình STP

!Sử dụng Rapid PVST+ hoặc MST
Switch(config)# spanning-tree mode rapid-pvst

!Cấu hình Core/Distribution là STP Root Bridge
Switch(config)# spanning-tree vlan 1-4094 priority 8192

!Tối ưu hóa các tính năng của STP
Enable BPDU Guard, BPDU Filter một các tự động trên những port được cấu hình Spanning-!Tree Portfast
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# spanning-tree portfast bpdufilter default

!Cấu hình UDLD

!Enable UDLD trên các kết nối fiber nhằm phòng tránh hiện tượng “unidirectional connection”
Switch(config)# udld aggressive

!Cấu hình Broadcast Storm

!Cấu hình Storm-Control (10%) trên các cổng Uplink (và Downlink đối với Core/Dist)
Switch(config-if)# storm-control broadcast level 10

!Cấu hình Port

!Cấu hình Trunk đối với các Port kết nối với Access Switch
Switch(config-if)# switchport mode trunk
! Nhằm phòng tránh tân công VLAN-Hopping, cấu hình native VLAN 999, là VLAN được tạo ra nhưng không sử dụng.
Switch(config-if)# switchport trunk native vlan 999

!Cấu hình Access đối với những cổng kết nối đến WAN Router, Firewall
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <Vlan-ID>
Switch(config-if)# spanning-tree portfast

!Shutdown nhung port không sử dụng hiện tại
Switch(config-if)# shutdown

!Cấu hình Ether Channel

Switch(config)# interface range Gi0/x-y
Switch(config-if)# channel-protocol lacp
Switch(config-if)# channel-group <group-number> mode active
Switch(config)# port-channel load-balance src-dst-ip

!Cấu hình InterVlan Routing and Static Routing

!Cấu hình Layer 3 Interface và InterVlan Routing
Switch(config)# Interface vlan <VLAN-ID>
Switch(config-if)# ip address x.x.x.x y.y.y.y
Switch(config-if)# no shutdown
Switch(config-if)# no ip proxy-arp
Switch(config-if)# no ip unreachables
Switch(config-if)# no ip redirects
Switch(config-if)# no ip mask-reply
Switch(config-if)# no ip directed-broadcast
!
Switch(config)# Interface loopback 0
Switch(config-if)# ip address x.x.x.x 255.255.255.255
Switch(config-if)# no ip proxy-arp
Switch(config-if)# no ip unreachables
Switch(config-if)# no ip redirects
Switch(config-if)# no ip mask-reply
Switch(config-if)# no ip directed-broadcast
!

Switch(config)# ip routing
!
Switch(config)# ip route <IP-Subnet> <IP-Subnet-Mask> <IP-Next-Hop>

!Cấu hình Device Hardening

!Cấu hình password

Switch(config)# service password-encryption
Switch(config)# no enable password
Switch(config)# enable secret <password>
Switch(config)# username <admin user> secret <password>

!Disable các dịch vụ không cần thiết

Switch(config)# no service tcp-small-servers
Switch(config)# no service udp-small-servers
Switch(config)# no ip bootp server
Switch(config)# no ip finger
Switch(config)# no service finger
Switch(config)# no service config
Switch(config)# no boot host
Switch(config)# no boot network
Switch(config)# no boot system
Switch(config)# no service pad
Switch(config-if)# no ip proxy-arp
Switch(config-if)# no ip unreachables
Switch(config-if)# no ip redirects
Switch(config-if)# no ip mask-reply
Switch(config-if)# no ip directed-broadcast
Switch(config)# no ip domain-lookup

!Disable ip source-route trong IP header

Switch(config)# no ip source-route

!Set timeout cho console laf 5 phút

Switch(config)# line console 0
Switch(config-line)# exec-time 5 0

!Chỉ cho phép truy cập vào Switch thông qua SSH

Switch(config)# access-list 11 permit x.x.x.x y.y.y.y
Switch(config)# access-list 11 deny any log
Switch(config)# line vty 0 4
Switch(config-line)# transport input ssh
Switch(config-line)# transport output none
Switch(config-line)# privilege level 1
Switch(config-line)# exec-timeout 5 0
Switch(config-line)# access-class 11 in
Switch(config-line)# login local

Switch(config)# line vty 0 15
Switch(config-line)# transport input none

!Tắt dịch vụ HTTP Server
Switch(config)# no ip http server

!Ngăn chặn tấn công vào từ chối dịch vụ vào Switch Processor làm Switch không thể xử lý các management traffic hợp lệ (STP, VTP, DTP, CDP, Routing, …)
Switch(config)# scheduler interval 500

!Cấu hình Syslog
Switch(config)# no logging console
Switch(config)# logging buffered 128000

!Cấu hình NTP
Switch(config)# ntp server <IP Address> key <Secret-key>
Switch(config)# ntp source loopback 0
Switch(config)# clock timezone GMT +7
Switch(config)# service timestamps log datetime msec localtime show-timezone
Switch(config)# service timestamps debug datetime msec localtime show-timezone

!Cấu hình CDP
!Mặc định CDP đã được tự động bật trên trên Switch.

!Cấu hình SNMP
Cấu hình SNMP Community Read-Only string để các Management Server (SolarWind, WhatsUpGold, …) có thể truy xuất vào thiết bị nhằm mục đích !monitor.
Switch(config)# snmp-server community <SNMP-String> RO 10
Switch(config)# access-list 10 remark Permit Read-Only SNMP Access from NMS only
Switch(config)# access-list 10 permit x.x.x.x y.y.y.y
Switch(config)# access-list 10 deny any log
Switch(config)# snmp-server location <Server Room A> <5th Floor>

!Cấu hình Banner
!cấu hình banner để cảnh báo mỗi khi có người truy cập vào thiết bị
Switch(config)# banner motd ^
********** NOTICE **********
This is a private network facility protected by a security system.
Access to and use of this facility requires explicit written,
current authorisation and is strictly limited to the purposes of
this organization's business.
Unauthorised or any attempt at unauthorised access, use, copying,
alteration, destruction, or damage to its data, program, or

equipment may result in criminal or civil liability or both.
****
^

Access/DMZ/Server Switch Cisco Catalyst 2960-Plus/2960X:

!Cấu hình VLAN

Switch(config)# vlan <Vlan-ID>
Switch(config-vlan)# name <Vlan-Name>

!Cấu hình VTP mode transparent

Switch(config)# vtp mode transparent

!Cấu hình STP

!Sử dụng Rapid PVST+ hoặc MST
Switch(config)# spanning-tree mode rapid-pvst

!Tối ưu hóa các tính năng của STP
Enable BPDU Guard, BPDU Filter một các tự động trên những port được cấu hình Spanning-!Tree Portfast
Switch(config)# spanning-tree portfast bpduguard default
Switch(config)# spanning-tree portfast bpdufilter default

!Cấu hình UDLD

!Enable UDLD trên các kết nối fiber nhằm phòng tránh hiện tượng “unidirectional connection”
Switch(config)# udld aggressive

!Cấu hình Broadcast Storm

!Cấu hình Storm-Control (10%) trên các cổng Uplink (và Downlink đối với Core/Dist)
Switch(config-if)# storm-control broadcast level 10

!Cấu hình Layer 2 Port

!Cấu hình Trunk đối với các Port kết nối với Access Switch
Switch(config-if)# switchport mode trunk
! Nhằm phòng tránh tân công VLAN-Hopping, cấu hình native VLAN 999, là VLAN được tạo ra nhưng không sử dụng.
Switch(config-if)# switchport trunk native vlan 999

!Cấu hình Access đối với những cổng kết nối đến WAN Router, Firewall
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <Vlan-ID>
Switch(config-if)# spanning-tree portfast

!Shutdown nhung port không sử dụng hiện tại
Switch(config-if)# shutdown

!Cấu hình Ether Channel

Switch(config)# interface range Gi0/x-y
Switch(config-if)# channel-protocol lacp
Switch(config-if)# channel-group <group-number> mode active
Switch(config)# port-channel load-balance src-dst-ip

!Cấu hình Device Hardening

!Cấu hình password

Switch(config)# service password-encryption
Switch(config)# no enable password
Switch(config)# enable secret <password>
Switch(config)# username <admin user> secret <password>

!Disable các dịch vụ không cần thiết

Switch(config)# no service tcp-small-servers
Switch(config)# no service udp-small-servers
Switch(config)# no ip bootp server
Switch(config)# no ip finger
Switch(config)# no service finger
Switch(config)# no service config
Switch(config)# no boot host
Switch(config)# no boot network
Switch(config)# no boot system
Switch(config)# no service pad
Switch(config)# no ip domain-lookup
Switch(config-if)# no ip proxy-arp
Switch(config-if)# no ip unreachables
Switch(config-if)# no ip redirects
Switch(config-if)# no ip mask-reply
Switch(config-if)# no ip directed-broadcast

!Disable ip source-route trong IP header

Switch(config)# no ip source-route

!Set timeout cho console laf 5 phút

Switch(config)# line console 0
Switch(config-line)# exec-time 5 0

!Chỉ cho phép truy cập vào Switch thông qua SSH

Switch(config)# access-list 11 permit x.x.x.x y.y.y.y
Switch(config)# access-list 11 deny any log
Switch(config)# line vty 0 4
Switch(config-line)# transport input ssh
Switch(config-line)# transport output none

Switch(config-line)# privilege level 1
Switch(config-line)# exec-timeout 5 0
Switch(config-line)# access-class 11 in
Switch(config-line)# login local
Switch(config)# line vty 0 15
Switch(config-line)# transport input none

!Tắt dịch vụ HTTP Server
Switch(config)# no ip http server

!Ngăn chặn tấn công vào từ chối dịch vụ vào Switch Processor làm Switch không thể xử lý các management traffic hợp lệ (STP, VTP, DTP, CDP, Routing, …)
Switch(config)# scheduler interval 500

!Cấu hình Management
!Cấu hình Syslog
Switch(config)# no logging console
Switch(config)# logging buffered 128000

!Cấu hình NTP
Switch(config)# ntp server <IP Address> key <Secret-key>
Switch(config)# ntp source loopback 0
Switch(config)# clock timezone GMT +7
Switch(config)# service timestamps log datetime msec localtime show-timezone
Switch(config)# service timestamps debug datetime msec localtime show-timezone

!Cấu hình CDP
!Mặc định CDP đã được tự động bật trên trên Switch.

!Cấu hình SNMP
Cấu hình SNMP Community Read-Only string để các Management Server (SolarWind, WhatsUpGold, …) có thể truy xuất vào thiết bị nhằm mục đích !monitor.
Switch(config)# snmp-server community <SNMP-String> RO 10
Switch(config)# access-list 10 remark Permit Read-Only SNMP Access from NMS only
Switch(config)# access-list 10 permit x.x.x.x y.y.y.y
Switch(config)# access-list 10 deny any log
Switch(config)# snmp-server location <Server Room A> <5th Floor>

!Cấu hình Banner
!cấu hình banner để cảnh báo mỗi khi có người truy cập vào thiết bị
Switch(config)# banner motd ^
********** NOTICE **********
This is a private network facility protected by a security system.

Access to and use of this facility requires explicit written,
current authorisation and is strictly limited to the purposes of
this organization's business.
Unauthorised or any attempt at unauthorised access, use, copying,
alteration, destruction, or damage to its data, program, or
equipment may result in criminal or civil liability or both.
****
^

WAN Router Cisco 2900 ISR2:

!Cấu hình WAN Interface

Router(config-if)# encapsulation ppp
Router(config-if)# no cdp enable
Router(config-if)# ip address x.x.x.x y.y.y.y
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
Router(config-if)# no ip directed-broadcast

!Cấu hình LAN Interface

Router(config-if)# ip address x.x.x.x y.y.y.y
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
Router(config-if)# no ip directed-broadcast

!Cấu hình Static Route

Router(config)# ip route <IP-Subnet> <IP-Subnet-Mask> <IP-Next-Hop>

!Cấu hình VTI IPSEC VPN Site-to-Site

!Cấu hình VPN Policy Phase 1 (ISAKMP)

Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encr 3des
Router(config-isakmp)# authentication pre-share
Router(config-isakmp)# group 2
Router(config)# crypto isakmp key <secret-key> address <IP-Address> <Subnet-Mask>
Router(config)# crypto isakmp keepalive 10

!Cấu hình VPN Policy Phase 2 (IPSEC)
Router(config)# crypto ipsec transform-set TRAN_TEST esp-3des esp-sha-hmac
Router(config)# crypto ipsec profile VTI
Router(config-vti)# set transform-set TRAN_TEST

!Cấu hình Interface VTI và apply IPSEC profile
Router(config)# interface tunnel 0
Router(config-if)# ip address x.x.x.x y.y.y.y
Router(config-if)# tunnel source <IP-WAN-Interface> <SubnetMask>
Router(config-if)# tunnel destination <IP-Router-Next-Hop> <SubnetMask>
Router(config-if)# tunnel protection ipsec ipv4
Router(config-if)# tunnel protection ipsec profile VTI

!Cấu hình Device Hardening
!Cấu hình password
Router(config)# service password-encryption
Router(config)# no enable password
Router(config)# enable secret <password>
Router(config)# username <admin user> secret <password>

!Disable các dịch vụ không cần thiết
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip bootp server
Router(config)# no ip finger
Router(config)# no service finger
Router(config)# no service config
Router(config)# no boot host
Router(config)# no boot network
Router(config)# no boot system
Router(config)# no service pad
Router(config)# no ip domain-lookup

!Disable ip source-route trong IP header
Router(config)# no ip source-route

!Set timeout cho console la 5 phút
Router(config)# line console 0
Router(config-line)# exec-time 5 0

!Chỉ cho phép truy cập vào Router thông qua SSH
Router(config)# access-list 11 permit x.x.x.x y.y.y.y
Router(config)# access-list 11 deny any log
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# transport output none

Router(config-line)# privilege level 1
Router(config-line)# exec-timeout 5 0
Router(config-line)# access-class 11 in
Router(config-line)# login local
Router(config)# line vty 0 15
Router(config-line)# transport input none

!Tắt dịch vụ HTTP Server
Router(config)# no ip http server

!Cấu hình Device Management
!Cấu hình Syslog
Router(config)# no logging console
Router(config)# logging buffered 128000

!Cấu hình NTP
Router(config)# ntp server <IP Address> key <Secret-key>
Router(config)# ntp source loopback 0
Router(config)# clock timezone GMT +7
Router(config)# service timestamps log datetime msec localtime show-timezone
Router(config)# service timestamps debug datetime msec localtime show-timezone

!Cấu hình CDP
!Mặc định CDP đã được tự động bật trên trên Router.

!Cấu hình SNMP
Cấu hình SNMP Community Read-Only string để các Management Server (SolarWind, WhatsUpGold, …) có thể truy xuất vào thiết bị nhằm mục đích !monitor.
Router(config)# snmp-server community <SNMP-String> RO 10
Router(config)# access-list 10 remark Permit Read-Only SNMP Access from NMS only
Router(config)# access-list 10 permit x.x.x.x y.y.y.y
Router(config)# access-list 10 deny any log
Router(config)# snmp-server location <Server Room A> <5th Floor>

!Cấu hình Banner
!cấu hình banner để cảnh báo mỗi khi có người truy cập vào thiết bị
Router(config)# banner motd ^
********** NOTICE **********
This is a private network facility protected by a security system.
Access to and use of this facility requires explicit written,
current authorisation and is strictly limited to the purposes of
this organization's business.
Unauthorised or any attempt at unauthorised access, use, copying,

alteration, destruction, or damage to its data, program, or
equipment may result in criminal or civil liability or both.
****
^

Internet Router Cisco 1900 ISR2:

!Cấu hình Internet Interface

```
Router(config# interface Gi0/1
Router(config-if)# no cdp enable
Router(config-if)# ip address 203.162.123.2 255.255.255.252
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
Router(config-if)# no ip directed-broadcast
```

!Cấu hình LAN Interface

```
Router(config)# interface Gi0/0
Router(config-if)# ip address 203.162.100.1 255.255.255.240
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
Router(config-if)# no ip directed-broadcast
```

!Cấu hình Static Route

```
Router(config)# ip route 0.0.0.0 0.0.0.0 203.162.123.1
```

!Cấu hình Device Hardening

!Cấu hình password

```
Router(config)# service password-encryption
Router(config)# no enable password
Router(config)# enable secret <password>
Router(config)# username <admin user> secret <password>
```

!Disable các dịch vụ không cần thiết

```
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip bootp server
Router(config)# no ip finger
Router(config)# no service finger
Router(config)# no service config
```

Router(config)# no boot host
Router(config)# no boot network
Router(config)# no boot system
Router(config)# no service pad
Router(config)# no ip domain-lookup

!Disable ip source-route trong IP header
Router(config)# no ip source-route

!Set timeout cho console la 5 phút
Router(config)# line console 0
Router(config-line)# exec-time 5 0

!Chỉ cho phép truy cập vào Router thông qua SSH
Router(config)# access-list 11 permit x.x.x.x y.y.y.y
Router(config)# access-list 11 deny any log
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# transport output none
Router(config-line)# privilege level 1
Router(config-line)# exec-timeout 5 0
Router(config-line)# access-class 11 in
Router(config-line)# login local
Router(config)# line vty 0 15
Router(config-line)# transport input none

!Tắt dịch vụ HTTP Server
Router(config)# no ip http server

!Cấu hình Device Management
!Cấu hình Syslog
Router(config)# no logging console
Router(config)# logging buffered 128000

!Cấu hình NTP
Router(config)# ntp server <IP Address> key <Secret-key>
Router(config)# ntp source loopback 0
Router(config)# clock timezone GMT +7
Router(config)# service timestamps log datetime msec localtime show-timezone
Router(config)# service timestamps debug datetime msec localtime show-timezone

!Cấu hình CDP
!Mặc định CDP đã được tự động bật trên trên Router.

!Cấu hình SNMP

Cấu hình SNMP Community Read-Only string để các Management Server (SolarWind, WhatsUpGold, …) có thể truy xuất vào thiết bị nhằm mục đích !monitor.

```
Router(config)# snmp-server community <SNMP-String> RO 10
Router(config)# access-list 10 remark Permit Read-Only SNMP Access from NMS only
Router(config)# access-list 10 permit x.x.x.x y.y.y.y
Router(config)# access-list 10 deny any log
Router(config)# snmp-server location <Server Room A> <5th Floor>
```

!Cấu hình Banner

```
!cấu hình banner để cảnh báo mỗi khi có người truy cập vào thiết bị
Router(config)# banner motd ^
**************************** NOTICE *******************************
This is a private network facility protected by a security system.
Access to and use of this facility requires explicit written,
current authorisation and is strictly limited to the purposes of
this organization's business.
Unauthorised or any attempt at unauthorised access, use, copying,
alteration, destruction, or damage to its data, program, or
equipment may result in criminal or civil liability or both.
***********************************************************************
^
```

Internet Firewall ASA5515-X:

!Cấu hình Interface

```
ASA5510(config)# interface Gi0/0
ASA5510(config-if)# nameif TRUSTED
ASA5510(config-if)# ip address 192.168.10.1 255.255.255.0
ASA5510(config-if)# security-level 100
!
ASA5510(config)# interface Gi0/1
ASA5510(config-if)# nameif DMZ
ASA5510(config-if)# ip address 192.168.20.1 255.255.255.0
ASA5510(config-if)# security-level 50
!
ASA5510(config)# interface Gi0/2
ASA5510(config-if)# nameif UNTRUSTED
ASA5510(config-if)# ip address 203.162.100.2 255.255.255.240
ASA5510(config-if)# security-level 0
```

!Cấu hình Static Route

```
ASA5510(config)# route UNTRUSTED 0.0.0.0 0.0.0.0 203.162.100.1
ASA5510(config)# route TRUSTED 192.168.0.0 255.255.0.0 192.168.10.2
```

!Cấu hình Remote Access VPN

!Cấu hình VPN policy phase 1 (ISAKMP)

```
ASA5510(config)# crypto isakmp policy 1
ASA5510(config-isakmp)# authentication pre-share
ASA5510(config-isakmp)# encryption 3des
ASA5510(config-isakmp)# group 2
```

!Cấu hình VPN policy phase 2 (IPSEC)

```
ASA5510(config)# crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-
hmac
ASA5510(config)# crypto dynamic-map DYMAP 1 set transform-set 3DES-SHA
ASA5510(config)# crypto dynamic-map DYMAP 1 set reserve-route
ASA5510(config)# crypto map CRYPMAP ipsec-isakmp dynamic DYMAP
```

!Apply VPN policy phase 1 và phase 2 vào Interface UNTRUSTED

```
ASA5510(config)# crypto isakmp enable UNTRUSTED
ASA5510(config)# crypto map interface UNTRUSTED
```

!Cấu hình VPN Group Policy cho Group IT Admin

```
ASA5510(config)# access-list ACL_SPLIT_TUNNEL standard permit 192.168.0.0
255.255.0.0
ASA5510(config)# access-list ACL_VPN_IT extended permit ip any 192.168.0.0
255.255.0.0
ASA5510(config)# ip local pool VPN_IPPOOL_IT 192.168.50.21-192.168.50.254
mask 255.255.255.0
ASA5510(config)# group-policy VPN_IT internal
ASA5510(config)# group-policy VPN_IT attributes
ASA5510(config-vpn-att)# dns-server value 192.168.11.11 192.168.11.12
ASA5510(config-vpn-att)# vpn-filter value ACL_VPN_IT
ASA5510(config-vpn-att)# ip-comp enable
ASA5510(config-vpn-att)# split-tunnel-policy tunnelspecified
ASA5510(config-vpn-att)# split-tunnel-network-list value ACL_SPLIT_TUNNEL
ASA5510(config-vpn-att)# address-pools value VPN_IPPOOL_IT
```

!Cấu hình VPN tunnel-group

```
ASA5510(config)# tunnel-group TG_IT type remote-access
ASA5510(config)# tunnel-group TG_IT general-attributes
ASA5510(config-vpn-tunnel-ge)#  address-pool VPN_IPPOOL_IT
ASA5510(config-vpn-tunnel-ge)# default-group-policy VPN_IT
ASA5510(config)# tunnel-group TG_IT ipsec-attributes
ASA5510(config-vpn-tunnel-att)# pre-shared-key 123456
```

!Tạo VPN user

```
ASA5510(config)# Username vpn-user1 password <password>
ASA5510(config)# Username vpn-user1 attributes
ASA5510(config-user-att)# vpn-group-policy TG_IT
```

ASA5510(config-user-att)# service-type remote-access

!Cấu hình NAT Publich Web (TCP:80) va Mail (POP3) ra ngoài Internet
ASA5510(config)# static (DMZ,UNTRUSTED) tcp interface 80 192.168.20.20 80 netmask 255.255.255.255
ASA5510(config)# static (DMZ,UNTRUSTED) tcp interface 110 192.168.20.20 110 netmask 255.255.255.255

!Cấu hình NAT n-1 cho phép người dùng có thể truy cập Internet
ASA5510(config)# global (UNTRUSTED) 1 interface

!Cấu hình NAT Exempt traffic tu DMZ->TRUSTED, DMZ->VPN, TRUSTED->DMZ, TRUSTED->VPN
ASA5510(config)# access-list DMZ_nat0 remark NO NAT Traffic DMZ->VPN, DMZ->TRUSTED
ASA5510(config)# access-list DMZ_nat0 extended permit ip 192.168.20.0 192.168.10.0 255.255.255.0
ASA5510(config)# access-list DMZ_nat0 extended permit ip 192.168.20.0 192.168.50.0 255.255.255.0
!
ASA5510(config)# access-list TRUSTED_nat0 remark NO NAT Traffic TRUSTED->DMZ, TRUSTED->VPN
ASA5510(config)# access-list TRUSTED_nat0 extended permit ip 192.168.10.0 192.168.20.0 255.255.255.0
ASA5510(config)# access-list TRUSTED_nat0 extended permit ip 192.168.10.0 192.168.50.0 255.255.255.0

ASA5510(config)# nat (DMZ) 0 access-list DMZ_nat0
ASA5510(config)# nat (TRUSTED) 0 access-list TRUSTED_nat0

!Cấu hình Firewall Policy
!Cấu hình ACL
ASA5510(config)# access-list TRUSTED_IN remark Permit traffic from Internal Network access Internet
ASA5510(config)# access-list TRUSTED_IN extended permit ip any any
!
ASA5510(config)# access-list DMZ_IN remark Permit Servers from DMZ zone to access Internet and Internal IP Address 192.168.11.11
ASA5510(config)# access-list DMZ_IN extended permit ip any host 192.168.11.11
ASA5510(config)# access-list DMZ_IN extended deny ip any 192.168.0.0 255.255.0.0 log
ASA5510(config)# access-list DMZ_IN extended permit ip any any
!
ASA5510(config)# access-list UNTRUSTED_IN remark Permit Some traffic (mail,web) access to DMZ Zone from Internet

ASA5510(config)# access-list DMZ_IN extended permit tcp any host 203.162.100.2 eq 80
ASA5510(config)# access-list DMZ_IN extended permit tcp any host 203.162.100.2 eq 110

!Apply ACL to Interface
ASA5510(config)# access-group TRUSTED_IN in interface TRUSTED
ASA5510(config)# access-group DMZ_IN interface DMZ
ASA5510(config)# access-group UNTRUSTED_IN interface UNTRUSTED

!Cấu hình Management
!Cho phép ping đến TRUSTED interface để troubleshoot
ASA5510(config)# icmp permit any TRUSTED

!Cấu hình PC có IP 192.168.44.44 được phép telnet vào ASA
ASA5510(config)# telnet 192.168.44.44 255.255.255.255 TRUSTED

!Cấu hình cho phép PC có IP 192.168.44.44 quản lý ASA thông qua ASDM (TCP port 4443)
ASA5510(config)# http server enable 4443
ASA5510(config)# http 192.168.44.44 255.255.255.255 TRUSTED

Internal Firewall ASA5555-X:

!Cấu hình Interface
ASA5550(config)# interface Gi0/0
ASA5550(config-if)# nameif TRUSTED
ASA5550(config-if)# ip address 192.168.100.1 255.255.255.0
ASA5550(config-if)# security-level 100
!
ASA5550(config)# interface Gi0/1
ASA5550(config-if)# nameif UNTRUSTED
ASA5550(config-if)# ip address 192.168.101.1 255.255.255.0
ASA5550(config-if)# security-level 0

!Cấu hình Static Route
ASA5550(config)# route UNTRUSTED 0.0.0.0 0.0.0.0 192.168.101.2

!Cấu hình no NAT-Control
ASA5550(config)# no nat-control

!Cấu hình Firewall Policy
ASA5550(config)# access-list TRUSTED_IN remark Permit traffic from Server Farrm access outside network
ASA5550(config)# access-list TRUSTED_IN extended permit ip any any

!
ASA5550(config)# access-list UNTRUSTED_IN remark Permit traffic access from outside to some Servers in Server Farm
ASA5550(config)# access-list UNTRUSTED_IN extended permit tcp any host 192.168.100.10 eq 443
ASA5550(config)# access-list UNTRUSTED_IN extended permit tcp any host 192.168.100.10 eq 445
ASA5550(config)# access-list UNTRUSTED_IN extended deny ip any any

!Apply ACL to Interface
ASA5550(config)# access-group TRUSTED_IN in interface TRUSTED
ASA5550(config)# access-group UNTRUSTED_IN in interface UNTRUSTED

!Cấu hình Management
!Cho phép ping đến TRUSTED interface để troubleshoot
ASA5550(config)# icmp permit any TRUSTED

!Cấu hình PC có IP 192.168.44.44 được phép telnet vào ASA
ASA5550(config)# telnet 192.168.44.44 255.255.255.255 TRUSTED

!Cấu hình cho phép PC có IP 192.168.44.44 quản lý ASA thông qua ASDM (TCP port 4443)
ASA5550(config)# http server enable 4443
ASA5550(config)# http 192.168.44.44 255.255.255.255 TRUSTED

Thảo Luận Về Ưu / Khuyết Điểm Trong Thiết Kế Kể Trên

Ưu Điểm:

- Chi phí đầu tư thấp nhất.
- Triển khai đơn giản, nhanh chóng.
- Thiết kế dạng module, có thể mở rộng hệ thống mạng khi cần thiết.

Khuyết Điểm:

- Không có tính dự phòng, hệ thống mạng dễ bị tổn thương khi có sự cố.