The Chinese University of Hong Kong
Department of Information Engineering

IERG 4841 Networking Laboratory II
Advance computer network design and setup
(Student Manual)

Lab 2: Servers Deployment and Management

In the first part of this lab, you need to configure your ASA5505 to manage one more vlan segment for hosting the management interface of VM Hypervisor. In addition, the VPN dialup service is needed to provide the remote access for off-site staff and access management to the management zone for IT staff from anywhere.

In the second part, you need to deploy the management severs for two hypervisors and setup the clutter zone to provide the High-Availability (HA) environment for the servers running on them.

In the last part, you need to deploy the linux firewall and 2 application servers to the cluster. Configure DNS and web service on them and setup the suitable firewall policy at the Linux firewall to protect the application servers.

***In the manual, we only cover the IP subnetting method to implement the DMZ. We also accept any method which can secure the DMZ.*

Part #1: Setup the Server Management Zone

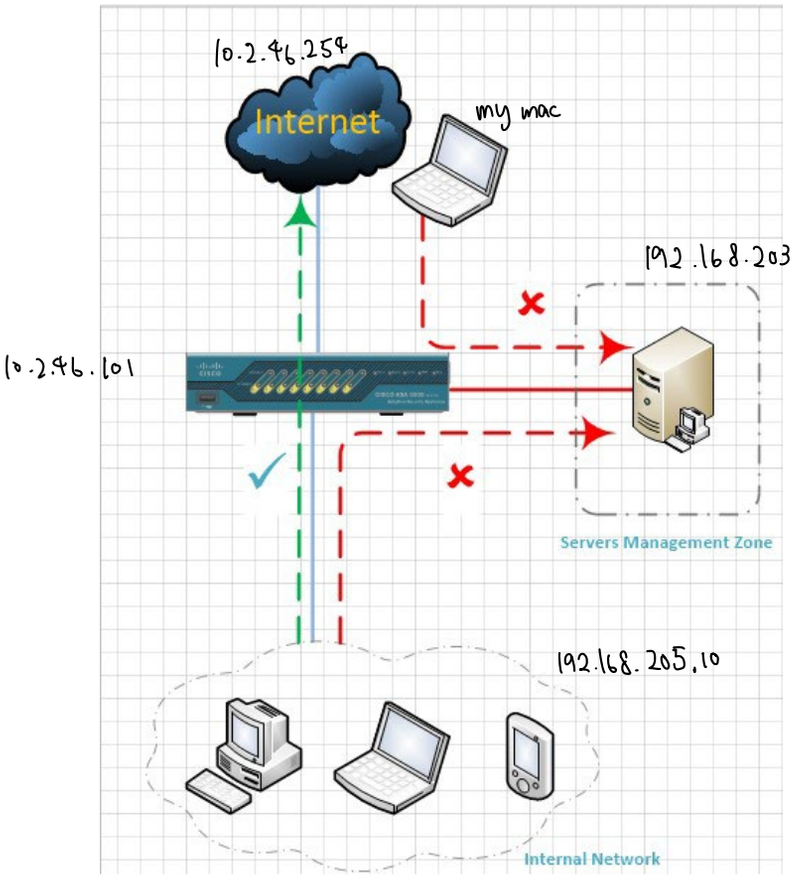

Figure 1

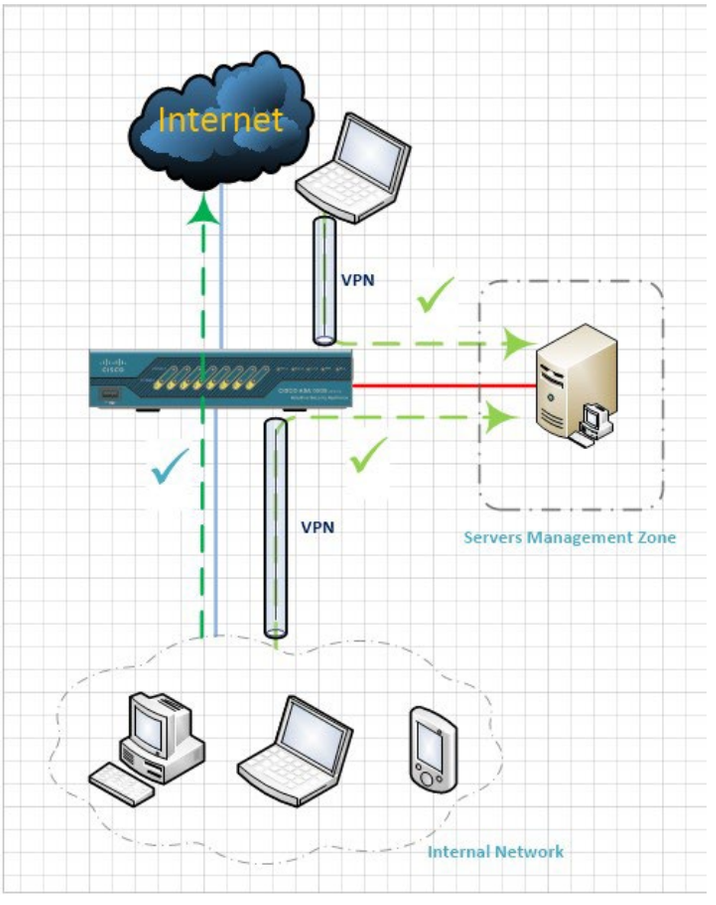

Figure 2

- Create new vlan interface at ASA5505:
  - As the ASA5505 running under the base license, please check the limitation at appendix D.
  - Assign vlan 11 to the server management zone
  - Make sure no traffic can route from internal and Internet to server management zone.
  - Make sure you have configured your switch as well.
- Setup VPN dialup service:
  - L2TP over IPsec VPN
  - MS-CHAP/MS-CHAP-v2 authentication
  - Staff from Internet or Internal network should able to access the service.
  - Only authenticated users can access the server management zone.

Hints

- *NAT-T which is necessary for L2TP/IPSec tunnel pass through the NAT enabled network*
- *You will need to connect "nlab vpn" before connecting to your VPN service if the vpn client is outside network lab. Please refer the appendix C for more detail of nlab vpn.*
- *You can focus on windows 10 client as XP/Vista/linux/mac will not be checked.* (/25)

ip local pool VPNPOOL 192.168.199.129-192.168.199.254 255.255.255.128

ikev1 pre-shared-key 1234

Vpnuser

1234

Part #2: Setup the virtualization environment

- Managing the local VM Hypervisor
  - Access the main console of your ESXi hypervisor.
  - Enter the configuration page by pressing [F2] key.

    Username: root

    Password: AsD24!!0
  - Configure your ESXi hypervisor management network.
    - Assign vlan ID to your management interface. It should be the same as server management zone (ie. vlan11).
    - Select the network interface which the link status is connected.
    - Assign IP address / subnet mask / gateway IP / hostname…...
    - Please change the default password.
  - Configure the switch port 7 & port 8 to trunk mode.
  - Make sure the vlan access table contain vlan ID 11- 16.
  - Access the vSphere web Client at your PC:

    URL: https://192.168.203.102/

    Username: root

    Password: <Enter the new password you have assigned at above step>
  - The hypervisor license should be expired. Go to “Manage” tab at left plane, and then click “Licensing” → “Assign license”.
    - Enter Key: ***[Please check the KEY at blackboard]***
  - Configure the network connection of the hypervisor
    - At the left panel, select “Networking”
    - At Port groups tab,
      - Click “Add port group”
        - Choose “Virtual Machine” as connection types
        - Choose “vSwitch0” for Virtual switch
        - Fill in:
          - Name: LAN1
          - VLAN ID: 11
        - Click “next” and then “Add”
      - Repeat the above steps to create port-group for vlan 12 to 16

- Managing the remote VM Hypervisor
  - The SME firm also subscript the IaaS service from the Data Center (DC). They have run a hypervisor at data center and logically connected the layer2 network between office and DC via the link at switch port 8.
  - Access the vSphere web Client at your PC:
  - URL: https://192.168.203.101/
    Username: root
    Password: AsD24!!0
  - The hypervisor license should be expired. Go to "Manage" tab at left plane, and then click "Licensing" → "Assign license".
    - Enter Key: ***[Please check the KEY at blackboard]***
  - Configure the network connection of the hypervisor
    - At the left panel, select "Networking"
  - At Virtual Switches tab
    - Select Add standard virtual switch
    - Create vswitch1 to vswitch5 (total 5 virtual switches)
    - Select vmnic1 to vmnic5 for vswtich1 to vswitch5's uplink accordingly.
  - Create LAN1 port group to vswitch0, LAN2 to vswitch1 …. LAN6 to vswitch5.
- Deploy the Management Server
  - Download the management server at:
    - http://www.ine.cuhk.edu.hk/ierg4841/files/VMware-VCSA-all-6.7.0-13643870.iso
    - Windows 10 can mount the iso file natively. Follow the user manual and deploy the vCenter to the DC's hypervisor.
    - Choose "Thin Provision" at Disk Format
  - Assign IP: 192.168.203.1/24 to the vCenter.
  - Once the installation completed, you can access the vSphere web client at
    - https://192.168.203.1/
  - Create the additional admin user and use that user for management.
  - The vCenter license should be expired. Right click the vCenter server and choose Assign License". At "NEW LICENSE" tab, input keys:
    [Please check the KEY at blackboard]
  - At "EXISTING LICENSES", assign the newly added key to the current vCenter server.
  - Create one Datacenter and create one cluster group under it.
  - Create one resource pool under the cluster group
  - Add two hypervisors to the cluster group.

vlan 103 → LAN2
vlan 121 → LAN6

Part #3: Deploy the application servers

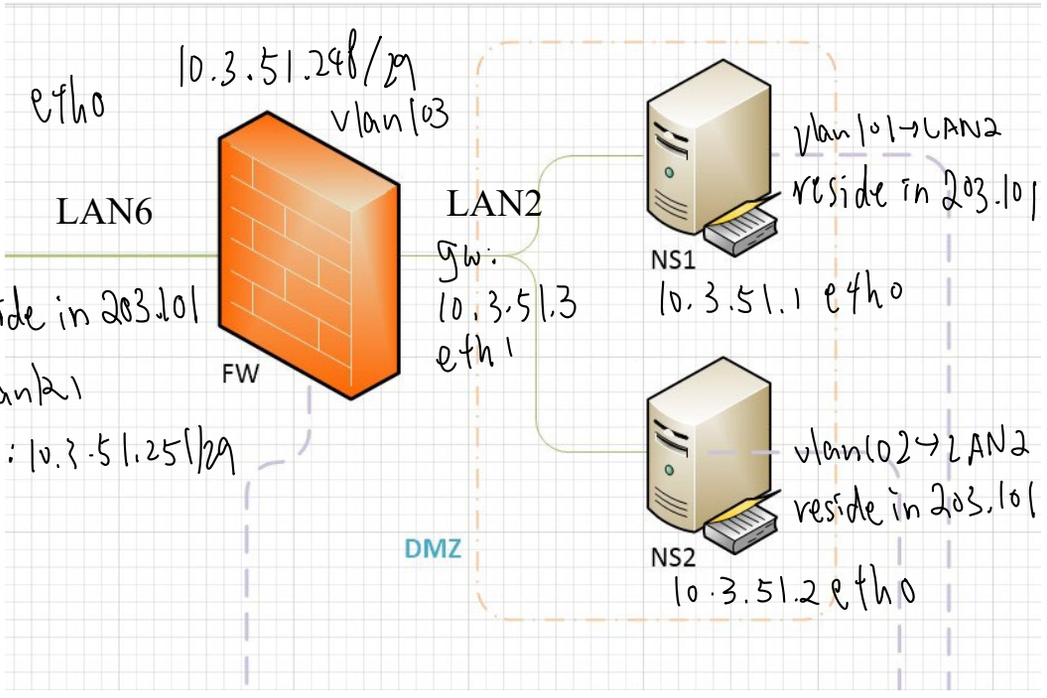

Figure 3

- Import the firewall template to hypervisor
  - At vSphere web client, right click the resource pool and select "Deploy OVF Template"
  - Choose "Local file" and click "Choose Files". Browse and select all files under "C:\VMWare\VMX-Temp\VMX-3\"
  - Choose "Thin Provision" at Disk Format
- Import the application servers template to hypervisor
  - Repeat the above steps but choose the template stored at VMX-1 and VMX-2
- IP subnetting root abc123
  - Refer to Appendix A, please figure out the block of public IP you have been assigned.
  - Please base on the following to subnet your /24 public IP.
    - ✧ 10.3.x.0/25 will be assigned to DMZ → 10.3.51.0/25
    - ✧ 10.3.x.248/29 will be assigned to firewall ext. interface 10.3.51.248/29

    ** 10.3.x.251 - 10.3.x.254 have been used by ISP router.
    10.3.51.251 – 10.3.51.254 249 / 250

    service network restart

- You need to setup your own DNS server to host your company domain name.

  **Please refer to appendix A to figure out which domain name has been assigned to your group.

  - Use yum update to update the outdated bind package.
  - NS1 should be used for the web server and DNS server with ip address 10.3.X.1 10.3.51.1
  - It also acts as a forwarder for your internal host to resolve name.

    **You can use 137.189.87.1 & 137.189.87.2 as your forwarder host
  - NS2 should be used for the secondary DNS server with ip address 10.3.X.2
- Setup the testing web site at 10.3.x.1
- Setup firewall rule(s) at firewall VM such that
  - All traffic with destination to firewall will be blocked except
    - The echo request/reply messages
  - All traffic from outside which target to DMZ's servers will be blocked except
    - The DNS query to your DNS server (10.3.x.1 and 10.3.x.2)
    - The HTTP access to 10.3.x.1
    - The echo request/reply messages

References

- Linux man page of iptables
  (*http://linux.die.net/man/8/iptables*)
- Linux man page of ip6tables
  (*http://linux.die.net/man/8/ip6tables*)
- Configure the dial up service on Cisco ASA device
  (*http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_l2tp_ipsec.html*)
- Troubleshooting for IPsec related problem
  (*http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html*)
- The VMware document
  (*https://docs.vmware.com/en/VMware-vSphere/index.html*)
- Linux IPv6 How-to
  (*http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/*)
- Windows IPv6 technology note
  (*http://technet.microsoft.com/en-us/network/bb530961.aspx*)
- Cisco IPv6 How-to
  (*http://docwiki.cisco.com/wiki/Cisco_IOS_IPv6_Feature_Mapping*)
- Cisco ASA-5505 feature license and specifications
  (*https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/specs.pdf*)

Appendix A

Information for Group 1:

IP address assigned to Main Office: 10.2.46.101/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp01.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp01.nlab2.ine.cuhk.edu.hk (10.3.51.1)

ns2. gp01.nlab2.ine.cuhk.edu.hk (10.3.51.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data Center for public access: 10.3.51.0/24

IP address for Data Center router: 10.3.51.254

IP address reserved by Data Center: 10.3.51.251 – 10.3.51.254

Information for Group 2:

IP address assigned to Main Office: 10.2.46.102/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp02.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp02.nlab2.ine.cuhk.edu.hk (10.3.52.1)

ns2. gp02.nlab2.ine.cuhk.edu.hk (10.3.52.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.52.0/24

IP address for Data Center router: 10.3.52.254

IP address reserved by Data Center: 10.3.52.251 – 10.3.52.254

Information for Group 3:

IP address assigned to Main Office: 10.2.46.103/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp03.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp03.nlab2.ine.cuhk.edu.hk (10.3.53.1)

ns2. gp03.nlab2.ine.cuhk.edu.hk (10.3.53.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.53.0/24

IP address for Data Center router: 10.3.53.254

IP address reserved by Data Center: 10.3.53.251 – 10.3.53.254

Information for Group 4:

IP address assigned to Main Office: 10.2.46.104/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp04.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp04.nlab2.ine.cuhk.edu.hk (10.3.54.1)

ns2. gp04.nlab2.ine.cuhk.edu.hk (10.3.54.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.54.0/24

IP address for Data Center router: 10.3.54.254

IP address reserved by Data Center: 10.3.54.251 – 10.3.54.254

Information for Group 5:

IP address assigned to Main Office: 10.2.46.105/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp05.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp05.nlab2.ine.cuhk.edu.hk (10.3.55.1)

ns2. gp05.nlab2.ine.cuhk.edu.hk (10.3.55.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.55.0/24

IP address for Data Center router: 10.3.55.254

IP address reserved by Data Center: 10.3.55.251 – 10.3.51.254

Information for Group 6:

IP address assigned to Main Office: 10.2.46.106/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp06.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp06.nlab2.ine.cuhk.edu.hk (10.3.56.1)

ns2. gp06.nlab2.ine.cuhk.edu.hk (10.3.56.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.56.0/24

IP address for Data Center router: 10.3.56.254

IP address reserved by Data Center: 10.3.56.251 – 10.3.56.254

Information for Group 7:

IP address assigned to Main Office: 10.2.46.107/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp07.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp07.nlab2.ine.cuhk.edu.hk (10.3.57.1)
ns2. gp07.nlab2.ine.cuhk.edu.hk (10.3.57.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.57.0/24

IP address for Data Center router: 10.3.57.254

IP address reserved by Data Center: 10.3.57.251 – 10.3.57.254

Information for Group 8:

IP address assigned to Main Office: 10.2.46.108/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp08.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp08.nlab2.ine.cuhk.edu.hk (10.3.58.1)
ns2. gp08.nlab2.ine.cuhk.edu.hk (10.3.58.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.58.0/24

IP address for Data Center router: 10.3.58.254

IP address reserved by Data Center: 10.3.58.251 – 10.3.58.254

Information for Group 9:

IP address assigned to Main Office: 10.2.46.109/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp09.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp09.nlab2.ine.cuhk.edu.hk (10.3.59.1)
ns2. gp09.nlab2.ine.cuhk.edu.hk (10.3.59.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.59.0/24

IP address for Data Center router: 10.3.59.254

IP address reserved by Data Center: 10.3.59.251 – 10.3.59.254

Information for Group 10:

IP address assigned to Main Office: 10.2.46.110/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp10.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp10.nlab2.ine.cuhk.edu.hk (10.3.60.1)

ns2. gp10.nlab2.ine.cuhk.edu.hk (10.3.60.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.60.0/24

IP address for Data Center router: 10.3.60.254

IP address reserved by Data Center: 10.3.60.251 – 10.3.60.254

Information for Group 11:

IP address assigned to Main Office: 10.2.46.111/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp11.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp11.nlab2.ine.cuhk.edu.hk (10.3.61.1)

ns2. gp11.nlab2.ine.cuhk.edu.hk (10.3.61.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.61.0/24

IP address for Data Center router: 10.3.61.254

IP address reserved by Data Center: 10.3.61.251 – 10.3.61.254

Information for Group 12:

IP address assigned to Main Office: 10.2.46.112/24

IP address for Main Office ISP's router: 10.2.46.254

IP address for the ESXi server located at main office: 192.168.203.102/24

Domain name managed by your group: gp12.nlab2.ine.cuhk.edu.hk

Name servers for your domain: ns1. gp12.nlab2.ine.cuhk.edu.hk (10.3.62.1)

ns2. gp12.nlab2.ine.cuhk.edu.hk (10.3.62.2)

IP address for the ESXi server located at Data Center: 192.168.203.101/24

IP address range at Data center for public access: 10.3.62.0/24

IP address for Data Center router: 10.3.62.254

IP address reserved by Data Center: 10.3.62.251 – 10.3.62.254

Appendix B

IPv6 address assignment for:

Group 1: 2405:3000:3:F602::/63

DC router: FE80::7:B4FF:FE00:0B00

Group 1 router: FD96:730D:4F8D:1001::21

Group 2: 2405:3000:3:F604::/63

DC router: FE80::7:B4FF:FE00:0C00

Group 2 router: FD96:730D:4F8D:1002::21

Group 3: 2405:3000:3:F606::/63

DC router: FE80::7:B4FF:FE00:0D00

Group 3 router: FD96:730D:4F8D:1003::21

Group 4: 2405:3000:3:F608::/63

DC router: FE80::7:B4FF:FE00:0E00

Group 4 router: FD96:730D:4F8D:1004::21

Group 5: 2405:3000:3:F60A::/63

DC router: FE80::7:B4FF:FE00:0F00

Group 5 router: FD96:730D:4F8D:1005::21

Group 6: 2405:3000:3:F60C::/63

DC router: FE80::7:B4FF:FE00:1000

Group 6 router: FD96:730D:4F8D:1006::21

Group 7: 2405:3000:3:F60E::/63

DC router: FE80::7:B4FF:FE00:1100

Group 7 router: FD96:730D:4F8D:1007::21

Group 8: 2405:3000:3:F610::/63

DC router: FE80::7:B4FF:FE00:1200

Group 8 router: FD96:730D:4F8D:1008::21

Group 9: 2405:3000:3:F612::/63

DC router: FE80::7:B4FF:FE00:1300

Group 9 router: FD96:730D:4F8D:1009::21

Group 10: 2405:3000:3:F614::/63

DC router: FE80::7:B4FF:FE00:1400

Group 10 router: FD96:730D:4F8D:100A::21

Group 11: 2405:3000:3:F616::/63

DC router: FE80::7:B4FF:FE00:1500

Group 11 router: FD96:730D:4F8D:100B::21

Group 12: 2405:3000:3:F618::/63

DC router: FE80::7:B4FF:FE00:1600

Group 12 router: FD96:730D:4F8D:100C::21

Appendix C: Setup and Connect to VPN Service

- If you are using IE Computing lab's PC, the VPN connection already setup for you.
  - For Windows 7 user, left click the network icon at notification area and select nlab vpn >> connect.
- If you are outside IE network, please follow the procedure below to create the VPN connection:
  - The setup procedures of the IPSEC VPN is similar to the [CUHK VPN server] (http://www.cuhk.edu.hk/itsc/network/vpn/vpn.html), except:
    - Replace the hostname to vpn.ine.cuhk.edu.hk
    - Do not select unencrypted password (PAP) at encryption protocol.
    - Use your Windows Login-name with realm and password for authentication (ie. IEPCLAN\Username)
    - The Max connection time is 4 hours

Appendix D: Cisco ASA-5505 features

Table A-1 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Users, concurrent[1]	10	*Optional Licenses: 50 / Unlimited*	10	*Optional Licenses: 50 / Unlimited*
Security Contexts	No support		No support	
VPN Sessions[2]	10 combined IPSec and WebVPN		25 combined IPSec and WebVPN	
Max. IPSec Sessions	10		25	
Max. WebVPN Sessions	2	*Optional License: 10*	2	*Optional License: 10*
VPN Load Balancing	No support		No support	
Failover	None		Active/Standby (no Stateful Failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns[3]	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*	Base (DES)	*Optional license: Strong (3DES/AES)*
Minimum RAM	128 MB		128 MB	

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit when they communicate with the outside (Internet VLAN), including when the inside initiates a connection to the outside as well as when the outside initiates a connection to the inside. Note that even when the outside initiates a connection to the inside, outside hosts are *not* counted towards the limit; only the inside hosts count. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the outside Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host** command to view host limits.
2. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.