Johnathan’s Security Lab

A Self-Hosted Virtual Testbed Environment

Project Status: Building

Johnathan's Security Lab is a set of configurations for network, VPN and testing environment within my home network. Different from the normal home network and VM environment, this setup is designed for providing service in a more secure environment. Different level of security are applied in this project. Including vLAN isolation, secure VPN setup and VM sandbox isolation. Most services are provided by the VMs. Service VMs will be directly attached at the core network so that it can easily serve the whole network client including the Testing VMs. Most of the Testing VMs are protected by the virtual firewall within The VM network so that it can prevent any software testing affect the real home network. Due to all machine is built from VM within the virtualized network, it can be easy deploy and protected by a firewall or easy to shift between Home network and VM private network and form an easy deployment security lab.

Project Background

This project provides a secure network configuration for a home environment. By using network isolation, AP isolation and VPN separation, the network is secured to provide services and prevent the attack. Three layers level security is set to secure the network: 1. Internet Connection, 2. Core Network, 3. DMZ. Firewall rules are set to deny all the connection to the Core Network while Core Network can make any connection within the network. Network isolation is provided by vLAN technology which is a layer 2 protection. All request connection the near vLAN are needed to pass through the Cisco router. Firewall rules are set to block the packet before routing. Three VPN are set as the service* and the intranet access gateway. All VPN channels are planned and secured by firewall rules so that even provided the VPN services for the outsider, the core network is also protected.

Cloud Computing is one of the hot topics in these few years. Hardware performance improvement, network bandwidth increases, and hardware standard are forming the global standard. No more specific devices are required for a single purpose. Over time, people try to use the x86 platform or ARM platform to simulate most of the workload. Although the performance is limited in virtualization, this solution still has easy to deploy, easy to maintain, easy to upgrade advantages. This project aims at using the virtualization technology to build a virtual network, virtual machine to simulate a datacenter and build some virtual machine for testing, sandbox and some IT audit software. Combining to the physical network, it can provide a flexible network setup environment including the protection between the physical network and the virtual network. Some of the trusted services VMs can also provide services to the physical network and the virtual network at the same time.

*VPN service is only for home office use, home resources accessing and network security use.

** Every VPN connection will have log and send to my mailbox through SMTP

Designed by Johnathan Leung

Specification

Hardware

[DIY] HP Gen 7 MicroServer			
Items	Name of items	Number of	Price (HKD)
Possessor	Intel® Core™ i5-4440 Processor 6M Cache, up to 3.30 GHz	1	$ 500
Motherboard	Asus H87I-Plus ITX	1	$ 300
RAM	Kingston 1600MHz 8GB DDR3 RAM	1	$ 200
Storage [1]	ADATA 128GB SSD	1	$ 500
Storage [2]	WD Blue 1TB 7200rpm HDD	3	$ 900
Storage [3]	Toshiba 500GB 7200rpm HDD	1	$ 300
Case	HP Gen 7 MicroServer Modified Ver.	1	$ 382
PSU	Delta DPS-400AB-12C 1U Flex 400W	1	$ 146
Adapters	SATA to 4-pins	1	$ 10
		Total	$ 3,238

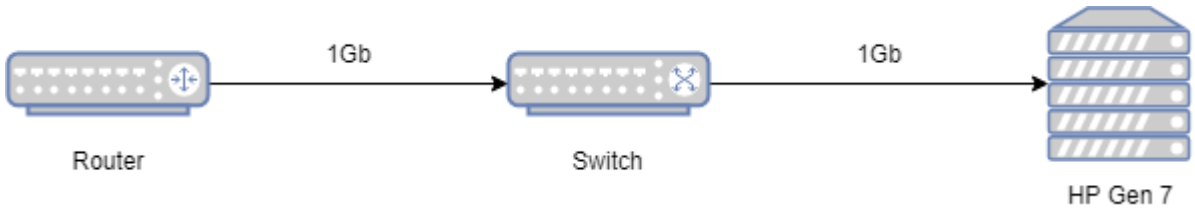
Network Equipment

Cisco RV320 VPN Router	1	$ 350
TP-link C7 AC1750	1	$ 550

Operation System

ESXi-6.5.0	
Version	6.5.0 (Build 5310538)
Image	ESXi-6.5.0-20170404001-standard (VMware, Inc.)

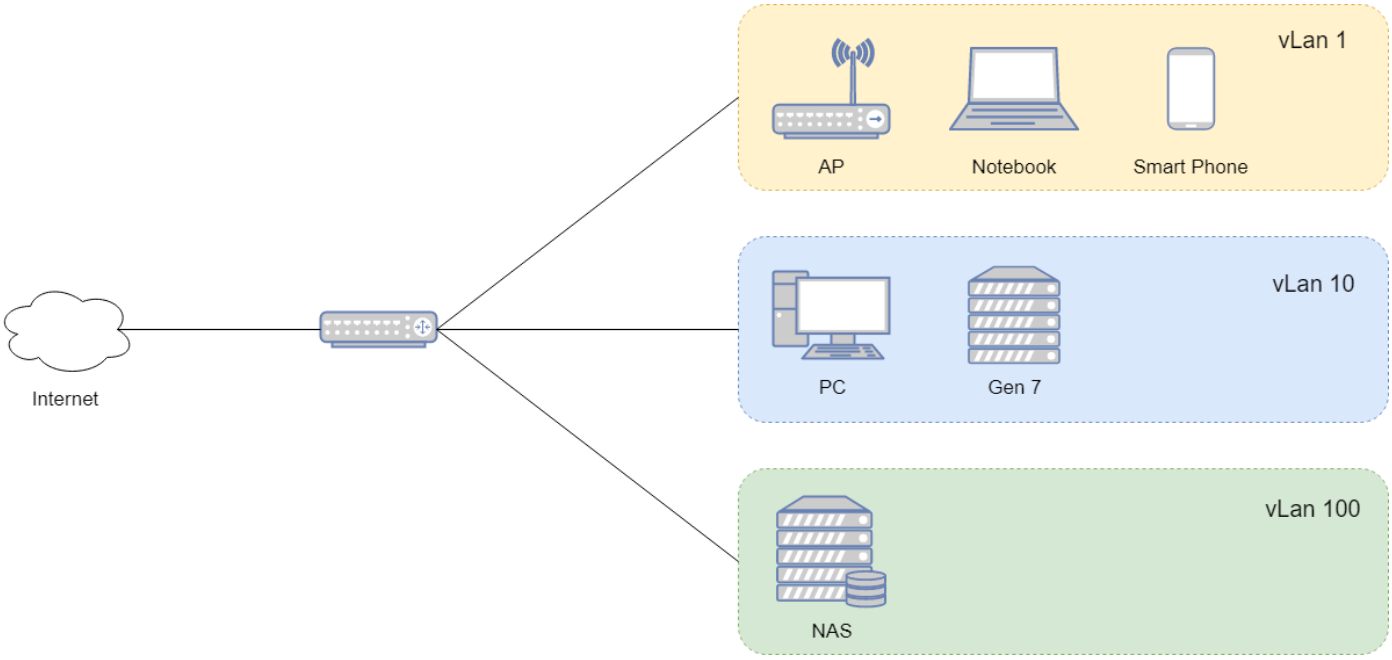
There is only 1 Giga Ethernet cable connected to the Gen 7 MicroServer which is allowed to access internet and home intranet. All the VM shared the bandwidth for both internet and intranet. Due to it is designed as a security lab, the interconnection between VM is more important. This design also can limit the damage to the home network from the VM inside the security lab. Internal Network using the VMXNET 3 as the Network Adapter to provide the 10Gb/s network connection between the VMs.



vLAN Setup

vLAN (Virtual Local Area Network) is a layer 2 logical grouping to sperate the LAN traffic packet. vLAN setup can isolate different types of device broadcasting packets to increase the level of security. The tagged packet also can reduce the need to have routers deployed on a network to contain broadcast traffic. Flooding of a packet is limited to the switch ports that belong to a vLAN. It reduces the impact of the DHCP starvation attack especially the Wireless network environment.

ID	IP range	Target Users
vLan 1	192.168.2.0/24	Wi-Fi and Guest Users
vLan 10	10.0.0.0/24	Core Network
vLan 100	10.0.1.0/24	DMZ – Local Resources



Designed by Johnathan Leung

Firewall Rule

Access Right

	192.168.2.0/24	10.0.0.0/24	10.0.1.0/24
192.168.2.0/24	X	Deny	Allow
10.0.0.0/24	Allow	X	Allow
10.0.1.0/24	X	X	X

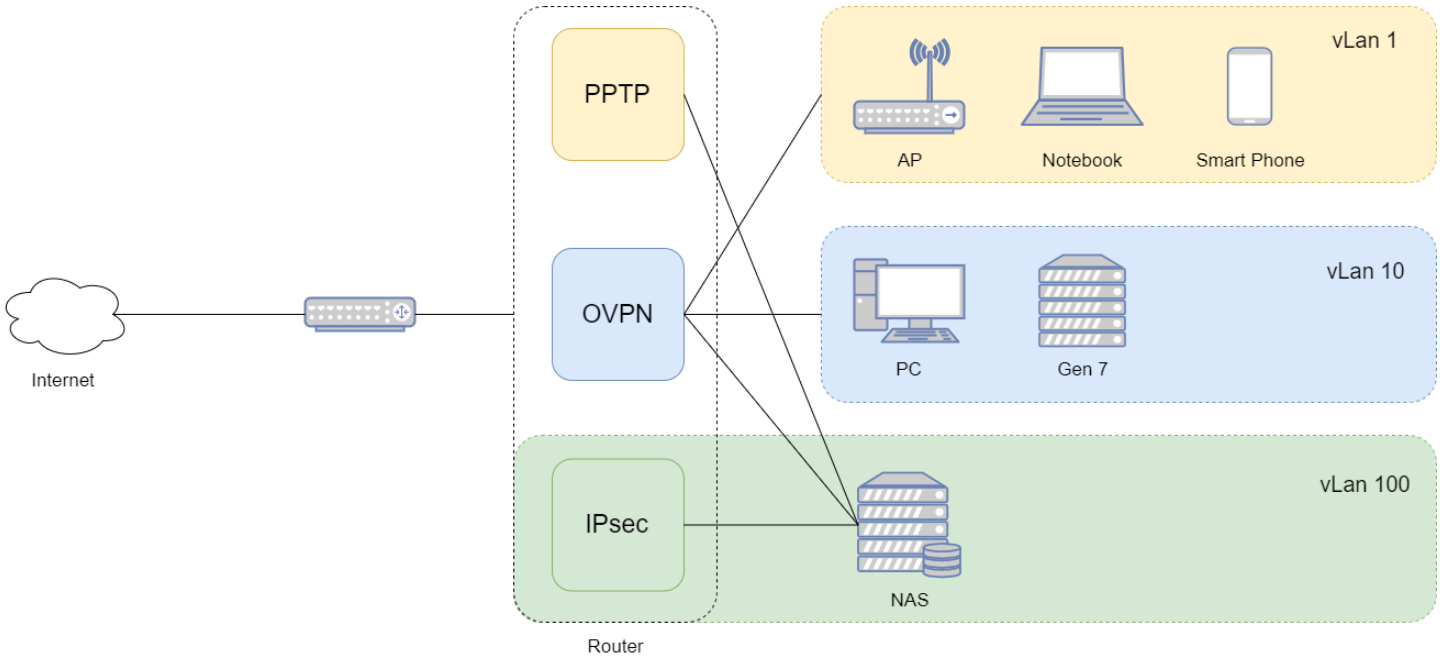
Rules

	Protocol	Source IP	Destination IP
Deny	SSH	WAN	ANY
Allow	*	10.0.0.0/24	192.168.2.0/24
Allow	*	LAN	10.0.1.110
Deny	*	10.0.1.0/24	192.168.2.0/24
Deny	*	*	10.0.0.0/24

Secure VPN Setup

VPN Server is set as the service and access gateway.

PPTP	Internet Connect Level + NAS	10.0.1.10 – 10.0.1.19
IPsec with Pre-shared key	Internet Connect Level + NAS (secured)	10.2.0.0
OpenVPN (OVPN)	Master VPN Level (Access All)	172.31.0.0/24



Designed by Johnathan Leung

Virtual Infrastructure

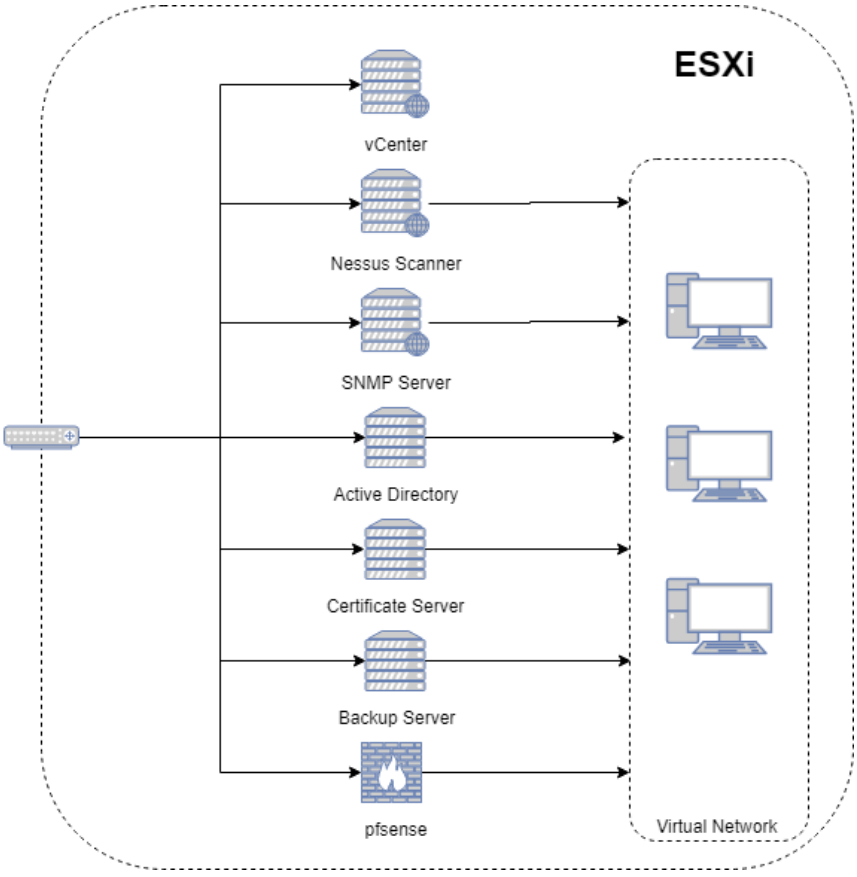
Due to the limited resources at Home and it is just a testing environment but not the datacenter for production, the resources used should be minimized to finish the whole virtual architecture so that more resources can be released for other valuable operation. One single platform also can be easy to deploy and manage. Reduce the workload on building a new platform for development.

Virtual Datacenter

Talking about “Datacenter”, there are some elements will be included:

- Network Switch
- Firewall
- Microsoft Active Directory
- Exchange Server
- Storage
- Backup Server

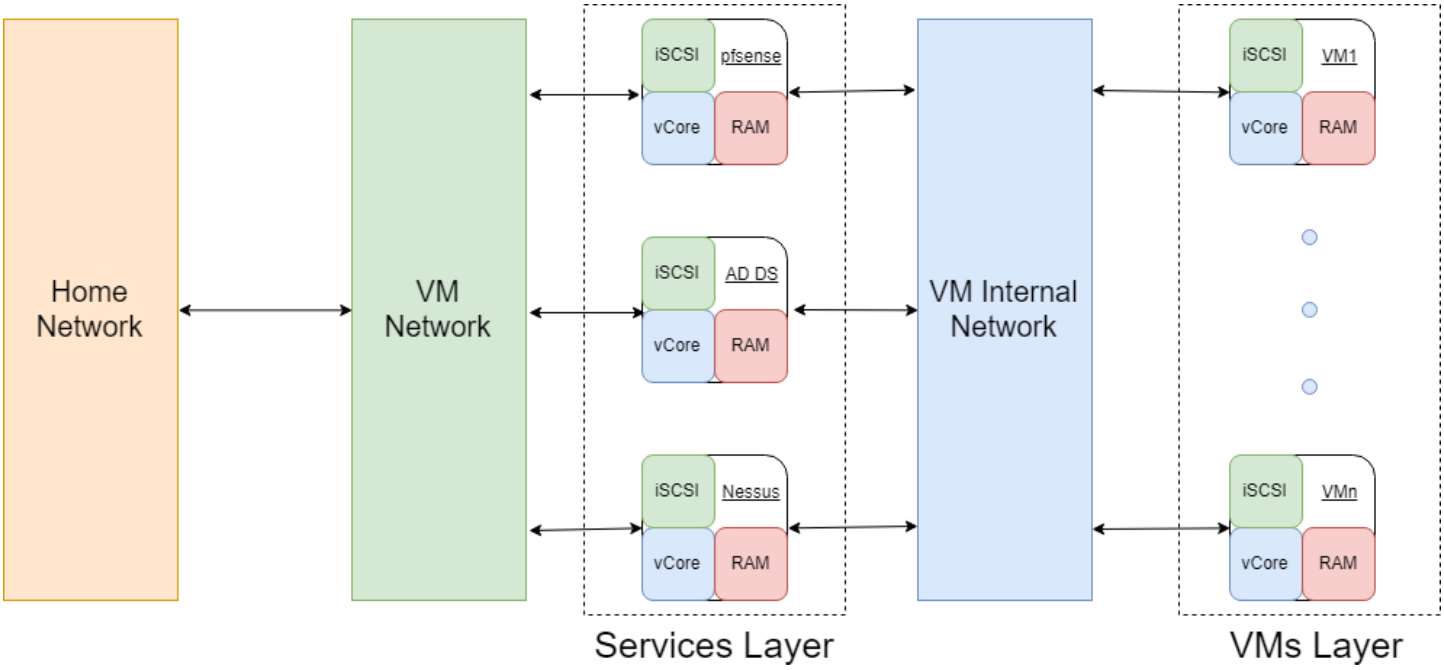
In the past, each of the elements is specific equipment in the datacenter which is expensive and occupy the storage space. With the advantage of virtualization. Now most of them can be done within a VM. For easy manage and isolation, one VM will only provide one service and make it as tiny as possible. It is the same as the Amazon AWS Microservice design.



Designed by Johnathan Leung

VM-based Network

For different reasons, a traditional datacenter always needs to expand the equipment whatever it is network equipment or computational unit. However, it is required man-power for setup and most of the equipment is expensive. Thanks for virtualization technology, now we can define the network with VM. VM-based Network in security lab can isolate the VM from the internet and intranet. Once the VM-based Network is well-defined, no more setup is needed when a new VM is going to deploy. This design can increase productivity and reduce the time for development environment setup. While the internal network using VMware provided solution VMXNET-3, providing a high speed (10Gb/s) internal network communication. This technology causes a speed improvement between internal VMs communication and it is a free and simple solution for scaling up the network.



Isolated Security Testing Lab

To ensure the device security, IT audit elements are set to review the whole network security but sometimes that software also has a risk of damaging to the network. Therefore, isolated testing is required before deploying on the real network. For those security-related tools, it will first deploy on the Internal network or even without network. After well-prepared, their tools can attach to the VM network which is directly attached to the home network to provide the services. All software firewall will also be one of the bridges between the VM network and VM Internal Network to provide services but will not start up at the same time. This design is allowed the user to design which VM can be internal device accessible and which VM is internet access. Those complex operations can be done in a second with software control.