Johnathan’s Security Lab

A Self-Hosted Virtual Test Bed Environment within a computer

Project Status: Building

Johnathan's Security Lab is a development environment and security center within the home network. Different from the normal VM environment, this server is allowed to scan both the whole home network and the private VM network. Most of the VM is protected by the virtual firewall within The VM network so that it can prevent any software testing affect the 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

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.

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

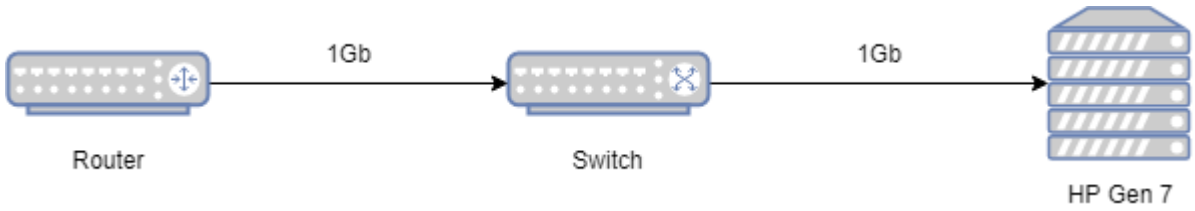
PSU	Delta DPS-400AB-12C 1U Flex 400W	1	$ 146
Adapters	SATA to 4-pins	1	$ 10
		Total	$ 3,238

Operation System

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

Network Connection

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.



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

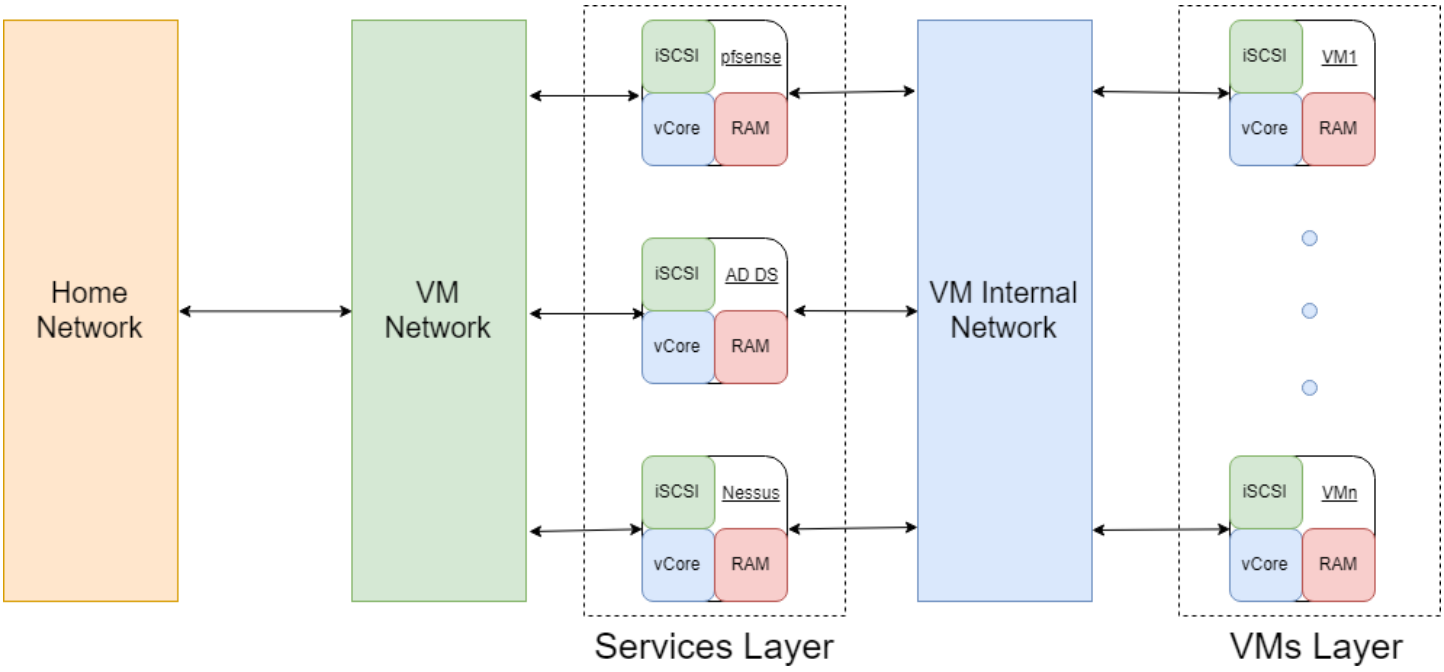
Talking about “datacenter”, there are some elements will be included:

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

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 server. It is the same as the Amazon AWS Microservice design.

Software Defined Network (SDN)

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 software. SDN in security lab can isolate the VM from the internet and intranet. Once the SDN 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.



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.