International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 1 [ISSN : 2250-3757]
Publication Date : 30 April, 2015

UTM Virtual LAB Design

Dhari Kh Abedula

***Abstract*— In this paper , I will examine the Security design parts of the University Technology Malaysia UTM Virtual LAB environment , beginning with the security areas and requirements that guided the creation and evolution of the LAB project . In addition, design Guides provide an overview of the Security solutions architecture and Scenarios. with Security traffic across the Security server through the internet , with Active Directory server to provide the Authentication methodology, and data protection provide backups with checkpoint and rollback mechanisms .**

***Index Terms*— VMware, Virtual LAB .**

I. Introduction

The UTM Virtual LAB environment was created to provide a safe, lab environment for use in the Advance Information School (AIS) Master program at UTM University. The AIS program covers a variety of topics, such as hacking techniques and advanced network concepts, that would require root access to the provided systems, raising a large number of issues regarding the security of the systems themselves, and the privacy of the students using them. Prior to the UTM Virtual LAB project , the only option available for laboratory assignments was a physical lab , dedicated to special courses, with all of the resources shared by the students.

However, this meant any crashes or system problems that was the result of one students work, could prevent the entire class from accessing the lab systems until the systems could be rebooted or restored. In addition, students were not given root privilege to these machines, and were limited in the type of activities they could perform.

A. Security Areas

The goal of the UTM Virtual LAB environment is to provide a safe environment where students can configure systems from inside or through internet , explore networks, and conduct attacks without any risk to other student systems, or the campus network. In addition, because many vulnerabilities are system or service specially , the environment had to accurately real-world systems. UTM Virtual LAB deal with three area in order to provide the security issues .

II. Design Overview

- The design enables you to address the following issues for the inside / outside shored desktops :
- Security design access from outside through VMware View Security Server and Active Directory .
- Security design access from inside , through Active Directory .
- Management Data backup and recovery using vSphere Data Protection (VDP) .

A. VMware View Security Server

When the View Secure Gateway Server sees an incoming RDP connection through the HTTPS connection , it forwards this connection to the appropriate virtual desktop. To ensure that all virtual desktops are only accessed through View Connection Server, firewall rules can be applied to each virtual desktop so that all RDP connections originate from a View Connection Server . This way , direct access to virtual desktops bypassing View Connection Server is not possible because View Connection Server acts as gatekeeper for all virtual desktop access . With VDM 2.1 and newer , the View Agent can be configured so that direct incoming RDP connections to virtual desktops are not allowed. This ensures that all remote access to virtual desktops must pass through a View Connection Server and ensure all remote access under secure encryption tunnel . ESX Server isolation and virtual networking features to configure a secure environment is the creation of a network demilitarized zone (DMZ) on a single ESXi host , When creating a DMZ within a single ESX Server, you can use fairly lightweight firewalls.

While a virtual machine in this configuration cannot exert direct control over another virtual machine or access its memory, all the virtual machines are still connected through a virtual network, and this network could be leveraged for virus propagation or targeted for other types of attacks . You can consider the virtual machines in the DMZ neither more nor less secure than separate physical machines connected to the same network .

B. vSphere Data Protection (VDP)

vSphere Data Protection (VDP) is a robust, simple-to-deploy, disk-based backup and recovery solution. vSphere Data Protection fully integrated with VMware vCenter Server and enables centralized and efficient management of backup jobs while storing backups in duplicated destination storage is

Provides fast and efficient data protection for all of your virtual machines, even those powered off or moved between physical hosts.
Significantly reduces disk space consumed by backup data using smart duplication across all backups.
Reduces the cost of backing up virtual machines and minimizes the backup window using change block tracking and VMware virtual machine snapshots.
Allows for easy backups without the need for third- party agents installed in each virtual machine.

- Uses a simple straight-forward installation as an integrated component within vSphere, that can be managed by a web portal.
- Direct access to vSphere Data Protection configuration integrated into the standard vSphere Web Client.
- Protects backups with checkpoint and rollback
- mechanisms.
- Provides simplified recovery of Windows and Linux files with end-user initiated file level recoveries from a web-based interface.

C. Specifying the Backup Schedule

On the Schedule page of the Create a new backup job wizard, you can specify the time intervals to back up the virtual machines in your backup job. Backups occur as near to the startup of the backup window as possible. The available time intervals are:

- Daily
- Weekly (on a specified day)
- Monthly (on a specified day of the month)

III. Flow of Information and Data Communication

Figure 1 1illustrates a typical local area network (LAN) design, and the public or the Internet - facing network services were placed in the DMZ Security Server Through VMware View Security server , and Protection part ,which is represent the automatically backup mechanism .Three scenarios were used to describe the flow of information in the network.

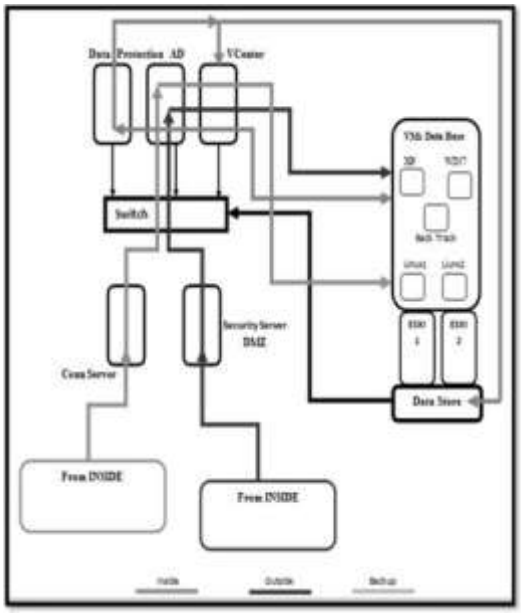

Figure 1: UTM Virtual LAB simulation architecture

A. Scenario 1 – Internal user requesting for UTM Virtual Lab

In this scenario, a (Access From Inside Group) is trying to access UTM Virtual Lab , hosted on two ESXI hosts , will be through AD. UTM .Local Server , in order to do Authentication in Active directory , and Authorization from Active Directory Group police . The following steps explain the data flow necessary to reach the UTM Virtual Lab , From inside group .

1.From inside (internal users machine) requests for "www.UTM.Local" through VMware View Client software ,The request is forwarded to the VMware View Connection Server to select which Lab and Class .
2.VMware Connection Server Forwarded the request to the Active directory with user credential . to make sure the user available in the authentication database
3.Active directory check the user credential , and give him the specific policy if any , from group policy list .
4. Active directory forwarded the request to the Vcenter server to allow user access to virtual mechanic .
5.vCenter server , deliver the virtual machine to the VMware connection server , in order to access from the user .

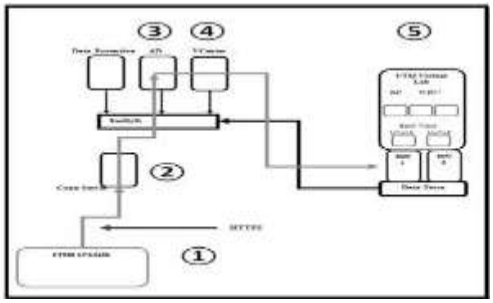

Figure 2: Scenario 1 Access from Inside

B. Scenario 2 – External Internet user requesting for UTM Virtual Lab

In this scenario an external internet users is trying to access UTM Virtual Lab , through the VMware View Security Server , which is provide security getaway for the UTM Virtual Lab . The following steps explain the data flow necessary to reach the UTM Virtual Lab , From Outside Group .

1. From outside (Internet users machine) requests for "www.UTM.Local " from the web browsing, or VMware View client . the request it will be go to the VMware View Security Server , which is represent security getaway . the Security server it will be start to encrypting the traffic , monitoring at the same time , and send the request to the VMware view Connection Server .
2. VMware Connection Server Forwarded the request to the Active directory with user credential . to make sure the user available in the authentication database
3. Active directory check the user credential , and give him the specific policy if any , from group policy list .
4. Active directory forwarded the request to the vCenter server to allow user access to virtual mechanic .
5. vCenter server , deliver the virtual machine to the VMware connection server , in order to access from the user .

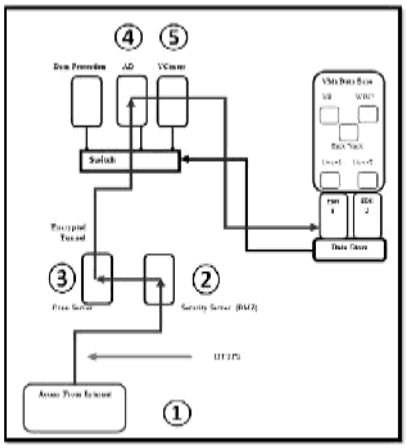

Figure 3: Scenario 2 Access from Outside

C. Scenario 3 – vSphere Data Protection (VDP) for UTM Virtual Lab

The following steps explain the data protection back up process used vSphere Data Protection (VDP) Server , integrated with vCenter Server , in order to save on the storage area .

1.On VCP Client page provides list of scheduled backup jobs as well as details about each backup job.
2. Make sure all the Backup Virtual PC available on vCenter server with Authorize access .
3. The Virtual PC star to send the Backup to the VCP Server From the Backup agent .
4. VCP Server deliver all the Backup image to the Storage area.

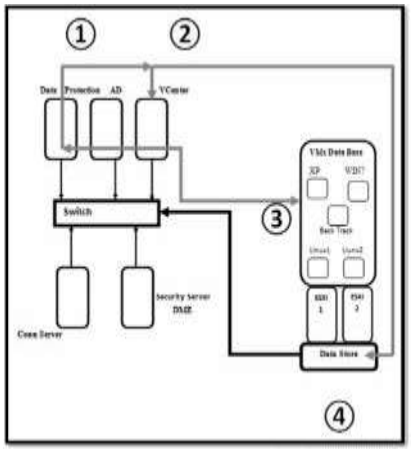

Figure 4: Scenario 3 Data Protection Process

IV. Summary

This secure virtual lab design infrastructure is constructed with a large number and variety of systems, applications, and features in order to provide the targeted level of security, capacity, performance, functionality, and flexibility. In addition, it utilizes an extensive set of administrative and management services, such as Active Directory, vCenter Server, View Security , and View Manager, to simplify the administrative tasks and thus enhance the sustainability of this infrastructure.

The design, implementation, and operation of this infrastructure design a variety of knowledge and skills and are quite complex in nature. Thus, they provide good learning and research opportunities for students as well.

REFERENCES

[1] Chao, L. (2010). Virtualized Computer Lab. In Society for Information Technology & Teacher Education International Conference, pp. 2679–2681.

[2] Faircloth, J. (2011). Building penetration test labs. In Penetration Tester's Open Source Toolkit, (Elsevier), pp. 371–401.

[3] Lowe, S. (2011). Mastering Vmware Vsphere 4. (Sybex Inc).

[4] Sands, R., Hsieh, G., Hendricks, W., and Williams, A. (2011). Building a Secure Virtual Lab Infrastructure for IT Education.

[5] Sands, Reginald A. (2011). Building a Secure Virtual Lab Environment using VMware Virtualization Infrastructure. M.S. Project. Department of Computer Science, Norfolk State University.

About Author :

Dhari KH Abedula, is an IT Security enthusiast and a researcher in Universiti Teknologi Malaysia (UTM). And security specialist in the American International Group (AIG). He has a more than ten years experience in the IT industry and a wide range of certifications.