HumanityLink 2.0 aka HLDeuce

vDM Challenge 2: EatBrains Virus

vCenterNerd
nigelhickey.com

Nigel Hickey; VCIX6-DTM

@vCenterNerd

TABLE OF CONTENTS

1 DOCUMENT CONTROL

Preparation

Action	Name	Date
Technical Content	Nigel Hickey	7/8/2017
Formatting	Nigel Hickey	7/10/2017

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
1.0	7/8/2017	Internal	All	Initial Draft
1.1	7/11/2017	VDM Release	All	VDM Release

Distribution

Name	Organization	Role	E-mail
Eric Wright	vDM	Head Canadian, Eh!	eric@discoposse.com
Angelo Luciani	vDM	Chief Ginger Officer	Aluciani@gmail.com
Melissa Palmer	vDM	Dr. Evil's Sister	vmiss33@gmail.com
Byron Schaller	vDM	Judge	byron.schaller@gmail.com
Rebecca Fitzhugh	vDM	Judge	rmfitzhugh@gmail.com
Lior Kamrat	vDM	Judge	https://twitter.com/LiorKamrat
Nigel Hickey	vCenterNerd Consulting	Architect / Engineer	Nigel.Hickey@gmail..com

2 PROJECT OVERVIEW

2.1 INTRODUCTION & SCOPE

Briefing from vDM HQ:

"You thought everything was running smoothly after you implemented the HumanityLink 2.0 software across the earth. It was, for a little while at least. Something has gone horribly wrong in the brand new infrastructure you have just implemented. The first site of your design from Challenge 1 has become infected with the EatBrains virus and ransomware which is now running rampant across your infrastructure. The EatBrains virus infects files and maps to SMB shares in order to spread itself further. There is also a variant that has the potential to store itself in memory on network devices and to emulate routers within the environment. EatBrains also has a phone home feature that allows for remote execution using the infected devices in the environment."

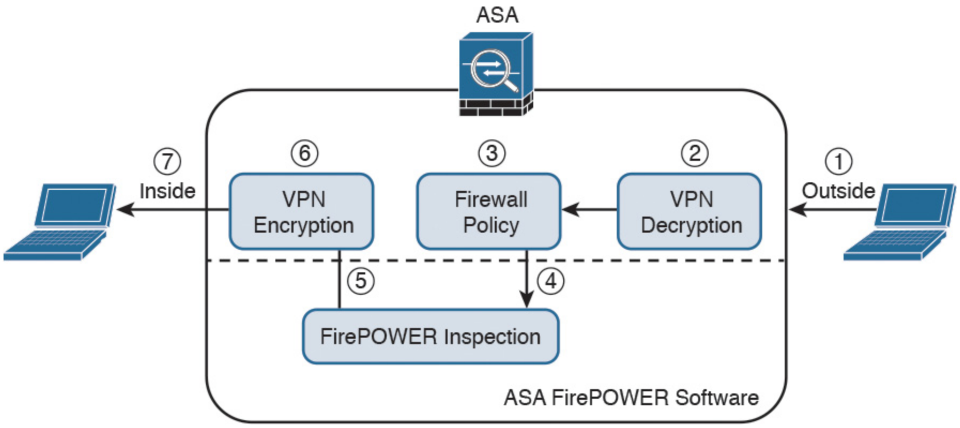
2.2 INFRASTRUCTURE SECURITY

The infrastructure security within the design for Challenge 1 was built around leveraging VMware NSX along with Palo Alto & Cisco firewalls and security policies.

2.2.1 Cisco

At datacenters MAC & DNB, we have deployed the Cisco ASA 5585-X with FirePOWER Services for external threat detection and prevention as well as site-to-site VPN between datacenters. This firewall allows our MAC & DNB datacenters to gain granular control over the applications layer and leverage risk-based controls that can launch threat detection policies to optimize security at each site. Intrusion Policies are used to examine the network traffic and identify anything malicious. The FirePOWER module is being used in IPS mode to generate alerts and block malicious traffic.

Logical Flow of Cisco ASA



2.2.2 NSX

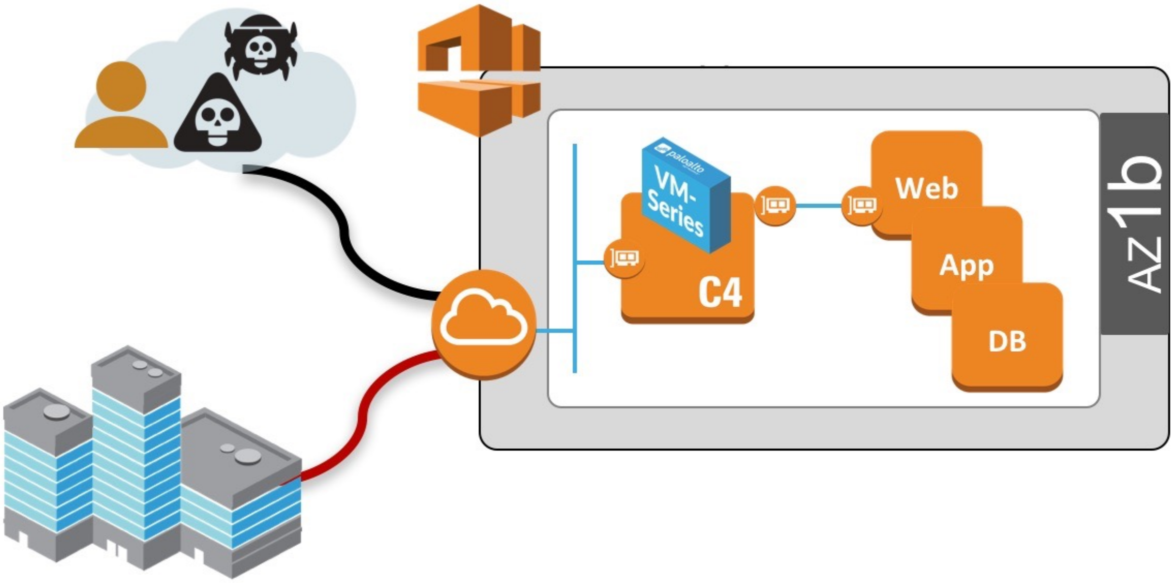
Along with the Cisco firewalls we have also designed VMware NSX to handle micro-segmentation within the MAC & DNB datacenters. The goal of NSX is to help create a zero trust network security outcome by only allowing the necessary network communications between datacenter systems to reduce any attack surfaces. NSX re-direction rules will be used so that any traffic meant for critical systems is re-routed to the Cisco FirePOWER IDS/IPS detection systems to evaluate any indicators of an attack.

Within the NSX distributed firewall we are monitoring port 445 to provide visibility into SMB traffic to be aware of attacks or attempted attacks. Next we are using an NSX Security Group that includes any virtual machines that run Windows OS to help identify vulnerable machines in the environment. NSX Endpoint Monitoring is enabled for any VMs that run Windows. If excessive traffic to port 445 is detected we will know because an NSX distributed firewall rule is set to immediately block & monitor all traffic if the destination is port 445, when coming from the subnet(s) of the Windows VMs. RDP blocking rules are also in play within NSX.

2.2.3 Palo Alto

In this design we are also using the Palo Alto VM-Series firewall in our AWS datacenter. The VM-Series firewall works in conjunction with AWS security groups to classify & control AWS traffic and based on application identity. This process can then apply threat prevention policies to block threats across ports and applications. With many of the same rules as we are using in NSX, the Palo Alto VM-Series firewall is protecting or AWS perimeter and applications.

Logical Flow of Palo Alto VM-Series



2.2.4 Port Blocking

Along with the latest and greatest networking tools, software, appliances we are also blocking particular ports to limit our surface of attack from the outside even further within all datacenters. This list is below.

Port	Description/Detail
80	Linux Systems ONLY
25	Sendmail
143	IMAP
110	POP
21	FTP

2.3 FIND THE BREACH

The process of finding the breach will entail us reviewing logs/alerts within NSX & Endpoint Monitoring. This will lead us to the system(s) that have been comprised in the datacenter. All of the network security that is in place, we will be able to quickly and visibly find the breach. We will leverage NSX to isolate these systems from the rest of the network.

2.4 RECOVERY

Once the breach has been discovered and isolated, recovery of the systems will begin by utilizing the virtual machine backups from Veeam. Since we are using the 3-2-1 model for backups, we will have multiple copies to refer to if required when restoring the compromised system.

The recovery process will begin removing all network adapters from the compromised machine after it has been isolated. Next the virtual machine will be powered off and removed from the VSAN Datastore and transferred to a temporary Datastore for future forensics work. Once the compromised system is offline and removed, the backup copy of the VM from Veeam will be imported into the environment, AFTER a Veeam SureBackup verification test has been performed on the VM. Once the VM passes this test, the VM can be moved to the production environment to replace the compromised VM.

The compromised virtual machine will then have its virtual network card removed before boot up. This will help us determine if there are any further problems with the Veeam backup copy of this recently resorted VM prior to bringing it online in the datacenter. If no issues or detected at this time, the virtual network card will be added back to the system and activated on the proper network.

This process is the same for all virtual machines within the datacenter regardless if they support or run HumanityLink software or not. Once the restored virtual machine is once again in a healthy state, and if it connects to any part of the HumanityLink software, all application services will be restarted to allow new connections.

3 REFERENCES

Use a Zero Trust Approach to Protect Against WannaCry
https://blogs.vmware.com/networkvirtualization/2017/05/use-zero-trust-protects-against-wannacry.html/

Use WildFire to Detect and Block Threats
https://www.paloaltonetworks.com/documentation/60/wildfire/wf_admin/wildfire-reporting/use-case-use-wildfire-to-detect-and-block-threats

Configure Intrusion Policy and Signature Configuration in Firepower Module
http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-firepower-services/200451-Configure-Intrusion-Policy-and-Signature.html

NSX for vSphere
https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html

Advanced VMware NSX Security Services with Check Point vSEC
https://blogs.vmware.com/networkvirtualization/2016/02/advanced-vmware-nsx-security-services-with-check-point-vsec.html/

Cisco Firewall
http://www.cisco.com/c/en/us/support/security/asa-5585-x-firepower-ssp-10/model.html

Cisco Switches
http://www.cisco.com/c/en/us/products/switches/nexus-92160yc-switch/index.html

Palo Alto Networks | GlobalProtect - Scalable Remote Access for AWS White Paper
https://www.paloaltonetworks.com/resources/whitepapers/building-scalable-globalprotect-deployment

Next Generation Security with VMware® NSX and Palo Alto Networks® VM-Series
https://www.paloaltonetworks.com/resources/whitepapers/vm-series-integration-technical-whitepaper

Veeam Backup & Replication 9.5
https://helpcenter.veeam.com/docs/backup/vsphere/system_requirements.html?ver=95

Veeam SureBackup
https://helpcenter.veeam.com/docs/backup/vsphere/surebackup_recovery_verification.html?ver=95