CNIT 34220: Network Administration

CNIT34220-001

Group 04

Ethan Hammond

Sean Fitz

Geoffrey Vest

Submitted To: Oscar Wong

Date Submitted: 03/04/23

Date Due: 03/04/23

TABLE OF CONTENTS

BUSINESS CASE

A manufacturing company, ACME, is a growing company that needs to connect a newly acquired location in another city to their existing network architecture. The company is also looking to bring these network infrastructure services in-house. In this search, firewalls, e-mail services, DNS, and other services will need to be integrated into the overall architecture between locations. This comes from the desire to reduce operating costs in order to help fund further research and development for future products. After growing disfavorable towards their network infrastructure services provider, the ACME company is looking to end this relationship. With the information technology consultants building this new architecture, the company can achieve what they are looking for. The ACME company is looking to configure a secure network infrastructure with different zones relating to separate locations and a DMZ. The company would also like to deploy a DNS server to host a domain name related to their company. Company emails should also be handled through the use of a dedicated mail server and a relay with a service in place to filter out spam emails. The company's web services should also be established by deploying web servers accessible from both the internal and public networks. The servers must also support SSL encryption in order to provide security to the sites. For the application delivery system, architecture needs to be implemented in order to handle load balancing and provide access to the mail server. After these requirements are met, the ACME company will have an in-house network architecture service that meets all of the needs they are looking for. This architecture must also account for potential future expansion of the company should the current growth rates and success continue.

PROCEDURES

The formatting key of the following section will obey rules below: buttons are **bold**; options are *italicized*; text entered into the computer is in `Courier New style`; menu, folder navigation, and repetitive commands are shown with the pipe symbol and are *italicized*: *Start* | *Programs* | *MS Office* | *Word*.

Phase I - Infrastructure

Phase 1 procedures consisted of creating a DNS architecture with 4 zones. The four zones that were to be implemented were a CIT 'Internet' zone for all outside traffic, a DMZ for all outside traffic to go through, an internal Remote site, and an internal HQ site. Between all zones, there needed to be something acting as a router and a packet filter. A pfSense virtual machine was placed in the middle of all zones to filter packets and route traffic. DNAT needed to be set up to allow outside traffic bound to an internal interface to get inside the network. DNS then needed to be configured for two DNS servers in the remote and HQ servers as well as a Linux BIND server in the DMZ. This allowed for full DNS and network connectivity between all sites and the outside internet. Lastly, firewall rules and DFS were implemented for network optimization.

Port Group and VM Creation

Port Groups

1. Logged into studentvc.cit.lcl and navigated to CNIT342G04 | Switch, and clicked on networks.
2. Clicked *Actions* and clicked *New Distributed Port Group*.
3. Created port groups for ‘HQ’ ‘DMZ’ and ‘Remote’

Firewall pfSense VM

4. Navigated to the *Cluster* tab in studentvc and right clicked stvmrv04heav.cit.lcl and clicked *Create New VM.*
5. Named the VM “CNIT34220.Group04.pfSense” and selected the Heavilon Cluster using FreeBSD 13 or later version.
6. Selected *thin provision* for the hard drive, added a CD drive for *pfSense* from the ‘rftm’ ISO file, and changed the network adapter to the 34220 G04 adapter.
7. Booted the VM and entered on *Install | BIOS* and let the operating system install.
8. Entered `vmx0` for the *WAN* interface, `vmx1` for the *LAN* interface, `vmx2` for the *OPT1* interface, and `vmx3` for the *OPT2* interface and ended the interface configuration menu.

Creation of Clients

1. Navigated to https://studentvc.cit.lcl to the Heavilon Cluster and right clicked the *CNIT34220Group4* folder and clicked *New Virtual Machine*.
2. Named the machine “CNIT34220.Group04.HQClient” and placed it onto the Heavilon Student Cluster.

3. Changed the HDD to ‘Thin Provision’, selected the ‘HQ’ created distributed port group as the network adapter.
4. Added a CD/DVD drive for the Windows 10 ISO file from RTFM > Windows > Client and connected the device.
5. Booted the VM and completed the basic Windows installation from the provided menu.
6. Went back to the CNIT34220Group4 folder and repeated steps 1-5 for “CNIT34220.Group04.RMClient”.
7. Navigated to the CNIT34220Group4 folder and repeated steps 1-5 with Windows Server 2019 OS for “CNIT34220.Group04.RMServer” and “CNIT34220.Group04.HQServer”.
8. Navigated to the CNIT34220Group4 folder and repeated steps 1-5 with Almalinux 9 OS for “CNIT34220.Group4.DMZServer”.

Configuration of IP addresses

All Windows Machines

1. Navigated to *Control Panel* through the Windows start menu.
2. Clicked on *Network and internet* | *Network Sharing Center* | *Adapter Settings* | *Ethernet0* | *IPv4*.
3. Configured the IP addresses included in Figure 1 below.

Machine	HQServer	HQClient	RMServer	RMClient	DMZ
IP	192.168.1.10	192.168.1.11	192.168.2.10	192.168.2.11	10.20.104.11
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Gateway	192.168.1.1	192.168.1.1	192.168.2.1	192.168.2.1	10.20.104.1
Preferred DNS	192.168.1.10	192.168.1.10	192.168.2.11	192.168.2.10	10.2.1.11
Alternate DNS	10.20.104.11	192.168.2.10	10.20.104.11	192.168.1.10	10.2.1.12

Figure 1: IP Configurations for all machines.

Almalinux Machine

4. Clicked on the network icon in the top right corner of the desktop.
5. Clicked the settings tab on the IPv4 tab and entered the IP configurations for the DMZ server in Figure 1 above.

Initial Configuration of pfSense Firewall

1. Booted the pfSense VM and selected “2) Set Interface IP Address” and set the Interet (WAN) interface to the Internet uplink port group and assigned it a 10.2.4.2/24 IP.
2. Set the DMZ (LAN) interface to 10.20.104.1/24, Remote (OPT1) interface to 192.168.2.1/24, and HQ (OPT2) interface to 192.168.1.1/24.
3. Opened a Firefox browser on the DMZ Alma Linux machine and searched for 10.20.104.1 to get to the pfSense Web Configurator.
4. Clicked *begin* to start the General Setup Wizard and changed the hostname to “CNIT34200Group04pfSense” and the Domain name to acme.lcl.
5. Assigned the DNS Servers as 10.2.1.11 and 10.2.1.12 and the Timeservers as “tick.cit.lcl tock.cit.lcl” and finished the Wizard.

6. Navigated to *Interfaces* on the top menu and gave a description for each interface to define vmx0 as “Internet”, vmx1 as “Remote”, vmx2 as “DMZ”, and vmx3 as “HQ”.
7. Navigated to *Interface Assignments* on the top menu and verified that the network interfaces’ MAC addresses were the same as the MAC addresses defined on the port groups in VMware vCenter.

Firewall Rule Creations

1. Logged into the DMZ Server machine and opened a web browser navigating to 10.20.104.1 (The LAN Interface on the pfSense machine).
2. Selected *Firewall* in the top menu and subsequently *Rules*.
3. Clicked *Add* for each of the 4 interfaces to create a rule for each interface.
4. Set the protocol for each rule to IPv4 any to allow any access from IPv4 on any protocol or service through the firewall.
5. Set the Source IP and Port to any to allow any IPs to be allowed past the machine.
6. Allowed any destination or port through the firewall by selecting any for those categories.
7. Set descriptions for all of the rules for future organization, troubleshooting, and neatness.

DNAT Configs for Traffic from the HQ and Remote Servers

1. Logged into the DMZ Server machine and opened a web browser navigating to 10.20.104.1 (The LAN Interface on the pfSense machine).
2. Selected *Firewall* in the top menu and subsequently *NAT*.

3. Clicked on the *Outbound* section of the NAT rules and changed the outbound NAT mode to *Manual*.

Remote Site Rule

4. Added a rule on the WAN interface for all traffic coming into the Remote to be NATted.
5. Set the Source IP and Port to *any* to allow any IP to enter the NAT rule.
6. Set the destination IP to 192.168.2.0/24 and Port to any to set all incoming traffic to be a 192.168.2.0/24 address.
7. Set the NAT address to be 192.168.2.0/24 to have any traffic be NATted to a Remote address.
8. Set a description for the rule as “RM NAT RULE”.

HQ Site Rule

9. Added a rule on the WAN interface for all traffic coming into the HQ to be NATted.
10. Set the Source IP and Port to *any* to allow any IP to enter the NAT rule.
11. Set the Destination IP to 192.168.1.0/24 and Port to any to set all incoming traffic to be a 192.168.1.0/24 address.
12. Set the NAT address to be 192.168.1.0/24 to have any traffic be NATted to an HQ address.
13. Set a description for the rule as “HQ NAT RULE”.

Active Directory and DNS Server Installation and Configuration

Installation

1. Opened *Server Manager* on the HQ Server and Remote Server.
2. Clicked Manage | Add Roles and Features, and selected Active Directory Domain Services and DNS Services.
3. Clicked “Promote to Domain Controller” when prompted and added a new forest and domain named acme.lcl.
4. Clicked next a few times and then finish to complete the wizard.
5. Rebooted the servers to allow the changes to take place.

Configuration of DNS

6. Opened *Server Manager* and selected *Tools* in the top right menu and launched DNS Services.
7. Right-Clicked the *Forward Lookup Zone* and clicked “Create a New Zone”.
8. Set the zone to all DNS servers running on the domain and named it acme.lcl
9. Added two more zones named “hq.acme.lcl” and “remote.acme.lcl” to act as Organizational Units.
10. Added two name server records to the DNS Forward Lookup Zone for the two DNS Servers for each respective server.
11. Opened the “Forwarders” tab and added the 10.20.104.11 IP and g4dmzsrv.acme04.com FQDN record to have the HQ Server and Remote Server forward their DNS queries to the DMZ.

DMZ DNS Installation and Configuration

1. Navigated to the newly-created DMZ DNS server
2. Entered `sudo dnf -y update` into the prompt and entered the administrator password
3. Typed `sudo dnf install -y bind bind-utils` and pressed Enter
4. Enabled the named service by entering `sudo systemctl enable named` into the command line
5. Checked the status of the named service by entering `sudo systemctl status named`
6. Entered `sudo nano /etc/named.conf` into the terminal
7. Added the acl trusted clients into the top of the configuration file
8. Entered `trustedclients;` into the allow-query and allow-query-cache options
9. Entered `forwarders { 10.2.1.11; };` into the terminal and set the recursion option to no
10. Added the *acme04.com zone* and designated its type as *master*
11. Configured the respective named forward lookup file path
12. Added the *104.20.10.in-addr.arpa* reverse zone and designated its type as *master*
13. Allocated the respective named reverse lookup file path.

Forward Zone Creation

1. Navigated to the named configuration with `cd /etc/named`
2. Entered `sudo nano /var/named/db.acme04.com` into the command prompt and entered the administrator password

3. Set the TTL (Time To Live) at the top of the file to 300 (5 minutes)
4. Entered the SOA record for the g4dmzsrv.acme04.com server and allocated a root email account
5. Allocated the nameserver as g4dmzsrv.acme04.com using a NS record
6. Set the A (address) record for the g4dmzsrv server as 10.20.104.11

Reverse Zone Creation

1. Entered `sudo nano /var/named/reverse.acme04.com` into the command prompt and entered the administrator password
2. Set the TTL to 300 (5 minutes) at the top of the file
3. Set the name server to g4dmzsrv.acme04.com using an NS record and configured a PTR (pointer) record to the same server

Firewall and DNS Configuration

1. Poked holes in the firewall by entering `sudo firewall-cmd –permanent –add-port=53/tcp and sudo firewall-cmd –permanent –add-port=53/udp` into the terminal
2. Entered `sudo firewall-cmd –reload` in order to reload the firewall
3. Restarted the named service by entering `sudo systemctl restart named`
4. Navigated to /etc/resolv.conf by entering `sudo nano /etc/resolv.conf` and entering the administrator password
5. Entered `nameserver 10.2.1.11 and nameserver 10.2.1.12` into the file
6. Pressed Escape and entered `wq` into the file to close it.

DFS Installation and Configuration

1. Opened *Server Manager* on both Windows Servers and clicked *Manage* | *Add Roles and Features.*
2. Selected *File and Storage Services* | *DFS* and installed the service onto the server.
3. Rebooted the machine to allow the changes to take place.
4. Opened "DFS Management" in Server Manager Tools and right clicked the domain to create a new domain namespace called "\\acme.lcl\DFS".
5. Right clicked "Replication" and created a new replication group called "G4REP".
6. Selected the C:\DFS_Share folder on the HQ Server to be shared across G4HQSrv and G4RMSrv.
7. Navigated to *Tools* | *Active Directory Users and Computers* and right clicked acme.lcl and created two new security groups, OUs, and users for HQ and Remote.
8. Booted up the HQ Client and RM Client machines and opened "File Explorer" from the Windows start menu.
9. Clicked *Map Network Drive* and mapped it to \\G4HQSrv\DFS_Share and added a subfolder for Remote and HQ.
10. Changed the permissions on the Remote and HQ DFS folders to match their respective site OU so that each user could only access their OUs folder contents.

Phase II - E-Mail

Procedures for Phase II included adding a Postfix mail server in the DMZ as well as a MS Exchange server in the HQ zone to allow for mail to go through the internal and external network. Postfix needed to be configured to take outside traffic and relay it to the inside Exchange server, and take Exchange traffic and route it out. The exchange server needed to be set up to take in outside mail from the Postfix server as well as send email out of the network through the Postfix server. Along with this, BIND Server configurations and OWA needed to be set up.

Updating DMZ DNS Server

Forward Lookup Zone

1. Navigated to the DMZ DNS VM (Virtual Machine).
2. Entered `sudo nano /var/named/db.acme04.com` and pressed Enter.
3. Configured the A (address) record for the mail server as `10.20.104.20`.
4. Added an MX (Mail Exchange) record for the mail.acme04.com server with a priority of `10`.
5. Set the A (address) record for the acme04.com web server as `10.20.104.13`.
6. Added a CNAME record in the forward zone for g4web1.acme04.com and set it to `www.acme04.com`.
7. Added a CNAME record for acme04.com and set it as `g4web1`.

Reverse Lookup Zone

1. Entered `sudo nano /var/named/reverse.acme04.com`.
2. Entered a PTR (pointer) record for the mail.acme04.com server.

3. Entered a PTR (pointer) record for the g4web1.acme04.com server.
4. Restarted the named service by entering `sudo systemctl restart named` into the command prompt.

Implementing a Complete E-Mail Architecture

Postfix

1. Created a CentOS virtual machine.
2. Navigated to the command line interface and entered yum install postfix.
3. Navigated to the Postfix configuration file by entering `sudo nano /etc/postfix/main.cf.`
4. Set myhostname as `mail.acme04.com`, mydomain as `acme04.com`, inet_interfaces as `all`, mydestination and local_recipient_maps as blank, mynetworks as `192.168.1.0/24`, `127.0.0.0/8`, `192.168.2.0/24`, and `0.0.0.0/24`, and configured the relay_domains line as `acme04.com`.
5. Added the line `transport_maps = hash:/etc/postfix/transport` to the Postfix configuration file.
6. Navigated to the newly-created /etc/postfix/transport file and added `acme04.com smtp:[192.168.1.22]` to the bottom of the file.
7. Started the Postfix process by entering `sudo systemctl start postfix` into the prompt.

SpamAssassin

1. Stayed on the Postfix virtual machine and navigated to the terminal.
2. Entered `yum install spamassassin` into the prompt.
3. Created a new user and group by inputting `groupadd spamd` and `useradd -g spamd -s /bin/false -d /var/log/spamassassin spamd` into the terminal.
4. Inputted `chown spamd:spamd /var/log/spamassassin` into the command line.
5. Navigated to the /etc/postfix/master.cf file.
6. Added `-o content_filter=spamassassin` under the smtp inet n - n - - smtpd line.
7. Navigated to the end of the file and inputted `spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}.`
8. Entered `sudo systemctl enable spamassassin` and `sudo systemctl start spamassassin` to start the spamassassin service.
9. Inputted `sa-update -nogpg` into the command line to update the spam filter rules.
10. Restarted the Postfix service by entering `sudo systemctl restart postfix` into the prompt.

Implementing Microsoft Exchange as an E-Mail Server

1. Created another Windows Server 2019 virtual machine as done in Phase 1.

2. Opened Control Panel through the Windows taskbar and set the network configurations with an IP of 192.168.1.22.
3. Navigated to System and Security | Advanced | Computer name and changed workgroup to domain and entered “acme.lcl” and joined the acme.lcl domain.
4. Opened Server Manager and clicked *Add Roles and Features* and added Active Directory Domain Services under acme.lcl.
5. Used Google to search and install .NET framework 4.7.2, Visual C++ Redistributable Packages for Visual Studio, and Unified Communications Managed API.
6. Opened PowerShell and used the following commands:

```
- Install-WindowsFeature RSAT-ADDS

- Install-WindowsFeature NET-Framework-45-Features,
RPC-over-HTTP-proxy, RSAT-Clustering,
RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt,
RSAT-Clustering-PowerShell, Web-Mgmt-Console,
WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth,
Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing,
Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging,
Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext,
Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase,
Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45,
Web-Request-Monitor, Web-Server, Web-Stat-Compression,
Web-Static-Content, Web-Windows-Auth, Web-WMI,
Windows-Identity-Foundation, RSAT-ADDS
```

7. Used `cd D:\` to get into the Exchange install directory.
8. Used `Setup.EXE /PrepareSchema /IAcceptExchangeLicenseServerTerms` to prepare the active directory schema for installation.
9. Ran `Setup.EXE /PrepareAD /OrganizationName:"acme04" /IAcceptExchangeServerLicenseTerms` to prepare the AD.
10. Opened Windows File Explorer and launched Setup.exe from the exchange D:\ drive.
11. Used the recommended setup settings, selected the mailbox role, named the organization acme04, and started the installation.

Outlook Mailbox and OWA Setup

Exchange Server

1. Opened a Firefox browser tab and searched "localhost/ecp" to access the Exchange administrator center.
2. Opened *mailboxes* and clicked the plus to create a new linked user.
3. Selected a domain user previously created on acme04.com in ADDS.
4. Opened the *mail flow* tab on the left pane and created a new accepted domain of acme04.com.
5. Set the domain as authoritative and the default domain.
6. Navigated to the *email address policies* within *mail flow* and created a new email address format as "SMTP" with a format of "@acme04.com".

7. Clicked *send connectors* within *mail flow* and created a new “internet” connector.
8. Entered 10.20.104.12 as the smart host, no authentication, an SMTP address space with a wildcard as the domain name, and selected the exchange server as the source server.
9. Opened a new Firefox tab and searched “https://192.168.1.25/owa” to access Outlook Web Access for the exchange server.
10. Logged in as a domain user to be able to test email functionality.

Client

11. Logged into the HQClient and RMClient virtual machines and downloaded MS Outlook from the internet.
12. Launched Outlook and clicked ‘Set up new mailbox’ followed by ‘Exchange Server’.
13. Entered the FQDN and IP of the exchange server and logged in with domain credentials to load the mailbox.

Testing with the Mailtest Server

Test from the mailtest to Exchange

1. Logged into the RMClient VM and opened a CMD through the Windows Start Menu.
2. Entered `ssh test4@mailtest.cit.lcl` to SSH into the CIT mailtest server.
3. Entered ‘mutt’ to enter mutt mode for mail testing.
4. Pressed the **m** key to send mail and entered RMClient@acme04.com as the ‘to: ‘, entered a subject, entered text, saved and closed the file, and pressed **y** to send the mail.

Test from Exchange to mailtest

5. Logged into the Exchange server and access OWA as https://localhost/owa.
6. Created a new mail in the GUI and addressed it to RMClient@acme04.com.
7. Logged back into the mailtest server with steps 1-2 above and entered `cat /var/spool/mail/test4` to view the mail received.

Firewall Rule Modifications

1. Logged into the HQServer VM and opened a Firefox tab entering https://10.20.104.1 to reach the pfSense web configurator.
2. Navigated to *Firewall* | *Rules* | *Internet* and created a new rule of type *block*.
3. Set the Source IP as a wildcard on port 25, destination IP address to HQ net on port 25.
4. Created a new rule of type *block* with a source IP as a wildcard on port 25, and destination IP address to Remote net on port 25.

Phase III - Web Services

Phase III procedures included creating two web servers to host the acme04.com domain. These websites needed to be configured with SSL certificates to be used for effective HTTPS connections from users. A Squid proxy server was set up to act as a transparent proxy server between the clients and the web server. Squid was included in BIND configurations to be the host of acme04.com. At the end of the Squid output, an F5 LTM machine was implemented to

act as a load balancer for the two acme04.com web servers. This was configured with the web servers as nodes, node pools, and Virtual Servers to host the two web servers as web pages. On top of the servers being on the LTM, OWA was also configured to be included in the load balancing.

VM Creation

Web Server

1. Navigated to VSphere at https://studentvc.cit.lcl on a personal computer and right-clicked the Heavilon Storage Cluster | New Virtual Machine…
2. Gave the VM a name meeting the lab naming convention standards, selected *Heavilon Storage Cluster* as the storage device.
3. Gave the machine an operating system of Almalinux 9 with thin provisioned hard drive and a DMZ network adapter.
4. Selected the Almalinux ISO from //rtfm.cit.lcl/ and connected it on boot.
5. Installed the operating system and gave it a correct hostname and IP address as follows:

   Hostname: web1.acme04.com

   IP Address: 10.20.104.13

   Netmask: 255.255.255.0

   Default gateway: 10.20.104.1

   DNS Servers: 10.20.104.11,10.2.1.11.

Proxy Server:

6. Repeated steps 1-5 to create the VM for the proxy server.

7. Installed the operating system and gave it a correct hostname and IP address as follows:

   Hostname: g4proxy.acme04.com

   IP address: 10.20.104.15

   Netmask: 255.255.255.0

   Default gateway: 10.20.104.1

   DNS Servers: 10.20.104.11,10.2.1.11

F5 LTM

8. Navigated to VSphere at https://studentvc.cit.lcl on a personal computer and right-clicked the Heavilon Storage Cluster | Deploy OVF Template.
9. Selected the .ova file in \\rtfm.cit.lcl\Pub\CNIT34220\F5 Virtual LTM\2021.
10. Selected thin provision for storage and selected the following network adapters:

    Mgmt: HQ | Adapter 2: DMZ | Adapter 3: DMZ | Adapter 4: DMZ.
11. Booted the machine and reset the default password from username: root | password: default.

Web Server Creation

1. Logged into the web1.acme04.com Almalinux server and opened a terminal window.
2. Entered sudo dnf update followed by sudo dnf install httpd httpd-tools to install Apache services.
3. Started the service with sudo systemctl start httpd followed by sudo systemctl enable httpd.

4. Allowed traffic through the linux firewall by entering the following 2 commands for HTTP and HTTPS:

   Sudo firewall-cmd --permanent --zone=public --add-service=http

   Sudo firewall-cmd --permanent --zone=public --add-service=https
5. Reloaded firewall rules with sudo firewall-cmd --reload.
6. Used sudo nano /var/www/html/index.html to create a display page for the website.

Website Encryption

1. Installed ssl with sudo dnf install mod_ssl.
2. Created SSL Certificates with sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/certs/apache-selfsigned.cert.
3. Entered US as the country, Indiana for State, City as West Lafayette, g4 for Organization Name, g4web1 as the Common Name, and echammon@purdue.edu as the email address.
4. Entered sudo nano /etc/httpd/conf.d/acme04.com.conf to creat a new VirtualHost file.
5. Added the following contents to the file to allow for HTTP and HTTPS traffic (Shown in Figure 2 below).

Figure 2: /etc/httpd/conf.d file on Webservers 1 and 2 to use HTTPS.

6. Checked syntax with sudo apachectl configtest and reloaded the service with sudo systemctl reload httpd.
7. Opened a web browser and searched for https://acme04.com to check the website functionality.

Web2 Configuration

8. Opened vSphere at https://studentvc.cit.lcl on a lab machine and right clicked the web1.acme04.com VM and selected *clone machine.*
9. Logged into the newly created VM and changed the hostname with sudo hostname web2.acme04.com.
10. Changed the IP address in the network GUI settings to 10.20.104.16.

F5 Configuration

1. Booted up the F5 machine, reset the password, and entered config into the terminal to start the initial configuration.
2. Selected the management interface and entered 192.168.1.30 as the IP to connect to the web configurator.
3. Opened a Firefox tab and searched for the IP of the web configurator interface. Clicked on license and entered a license key given by F5 via free trial.
4. Took the dossier that the box output and put it into their license activation website to activate the key.
5. Selected Network | VLANs and created two new VLANs named ‘internal’ and ‘external’, assigning them to the 1.1 and 1.2 interfaces.
6. Selected *Self IPs* and set the IP for the external VLAN to be 10.20.104.129/25 and the internal to be 10.20.104.32/25.
7. Selected *Routes* and set the default route to 10.20.104.1 as that is the IP of the DMZ interface on the firewall machine.

F5 Local Traffic Manager Configuration

1. Logged into the F5 LTM Web Configurator and clicked on *Local Traffic* | *Nodes* and created two nodes: one for each web server and their corresponding IPs.
2. Clicked on *Pools* and created two new pools, adding the two web server nodes to each, one with HTTP and one with HTTPS.
3. Clicked on *Virtual Servers* and created a new one for HTTP.

4. Set the destination address as 10.20.104.29 on port 80.
5. Set the default pool as the created HTTP pool.
6. Created another Virtual Server for HTTPS following steps 3-5 replacing port 80 with port 443.
7. Clicked *Local Traffic* | *Monitors* and created a new health monitor.
8. Created one for HTTP and one for HTTPS with the only modification being changing 'Send String' to "GET \r\n\r\n".
9. Clicked on the created Virtual Servers and added the health monitors as the monitors for that server.

Squid Configuration

1. Created a new CentOS virtual machine and navigated to the command line interface.
2. Entered `yum -y install squid` into the prompt.
3. Started the Squid service by typing `sudo systemctl start squid` and `sudo systemctl enable squid`.
4. Checked the status of the service by entering `sudo systemctl status squid`.
5. Navigated to the Squid configuration file by entering `sudo nano /etc/squid/squid.conf` into the command line interface.
6. Entered `acl hqnet src 192.168.1.0/24`, `acl rmnet src 192.168.2.0/24`, `http_access allow hqnet`, `http_access allow rmnet`, and `http_access allow localhost` into the configuration file to allow access to certain networks.

7. Added `http_port 3129` and `http_port 3128` intercept into the file.
8. Entered `visible_hostname proxy.acme04.com` at the bottom of the configuration file.
9. Restarted the Squid service by typing `sudo systemctl restart squid` into the prompt.

Firewall Modifications

1. Logged into the HQServer VM and opened a Firefox tab entering https://10.20.104.1 to reach the pfSense web configurator.
2. Navigated to *Firewall* | *NAT* | *Port Forward* and created a new redirect entry.
3. Set Interface to HQ, destination to Any, destination port range to HTTP, redirect target IP to Single Host at 10.20.104.15, and Redirect target port to 3128.
4. Created a new redirect entry and set interface to Remote, destination to Any, destination port range to HTTP, redirect target IP to Single Host at 10.20.104.15, and Redirect target port to 3128.

RESULTS

Throughout the three phases that comprised the lab, many servers had to be created and configured along with services that reside on them. As part of phase one of this laboratory assignment, three servers and two clients had to be created in VMware vSphere. This includes the DNS BIND server, the Remote server, and the HQ server. Both the remote server and HQ server had clients in their zones configured as well. A central pfsense firewall was also created to route traffic between these created zones. For phase two, two additional servers were added to the network architecture. An email server running Postfix and Spamassassin was deployed in the DMZ while a mail server running MS Exchange was deployed in the HQ zone. Lastly, in the third and final phase of the lab, four new servers were added to the DMZ. These servers were two web servers running Apache, a proxy server running Squid, and an application delivery controller running F5 Big IP. After these final servers were added and configured, the network architecture was completed. This architecture can be seen in Figures 3 and 4 below in a physical and logical format respectively.

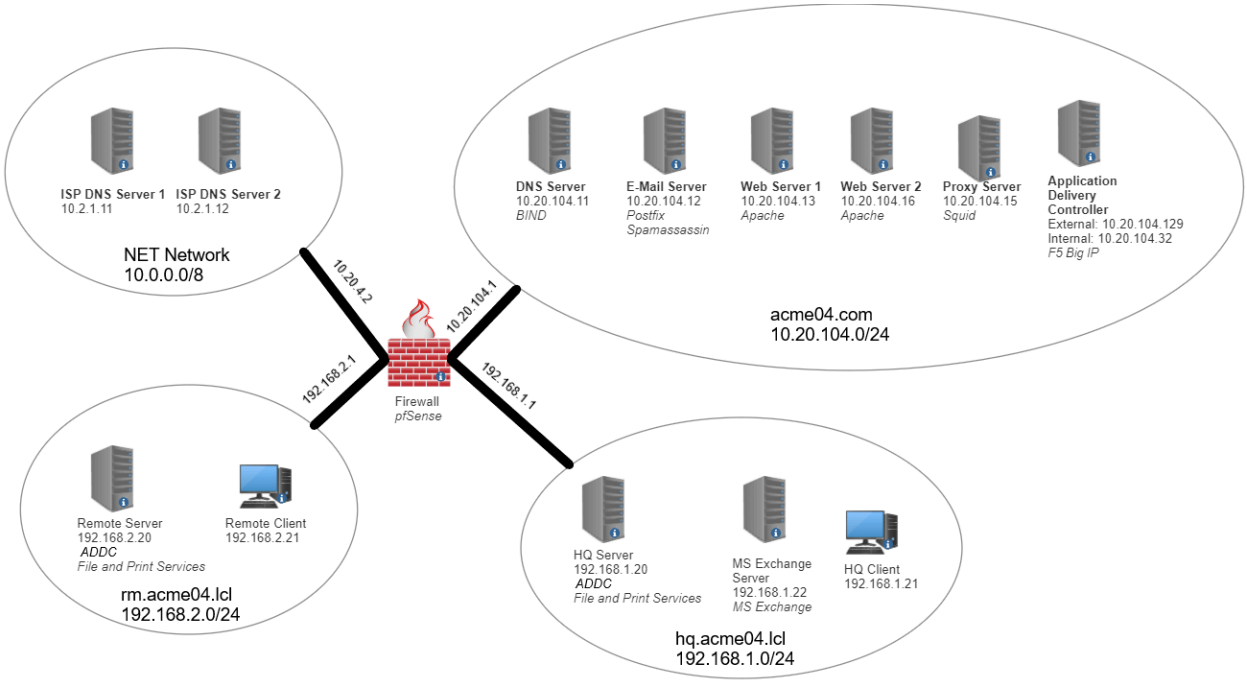

Figure 3: Completed logical network diagram.

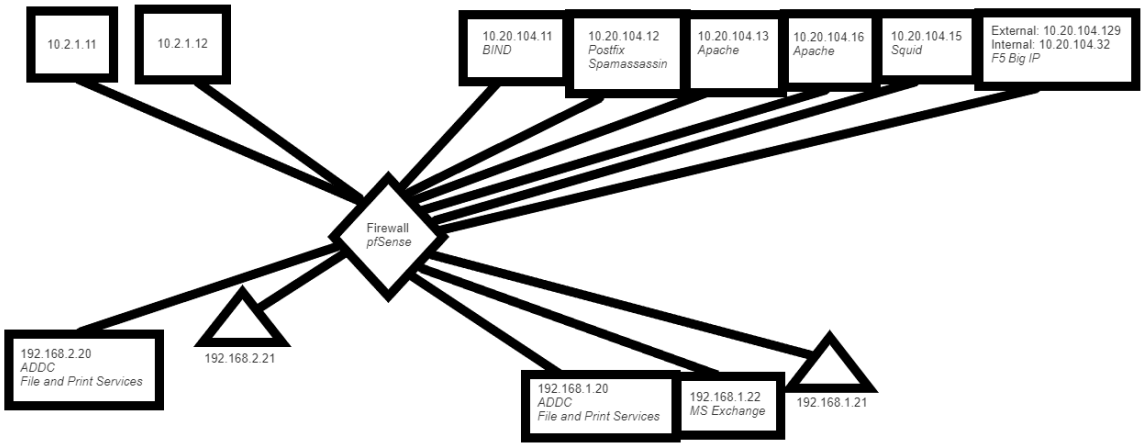

Figure 4: Completed physical network diagram.

CONCLUSIONS AND RECOMMENDATIONS

The overall creation of the network went well. We satisfied all necessary requirements stated within the business case. To address those needs we started with the firewall, a server running pfsense was deployed to handle the security of the network architecture. Three additional zones were also created to distinguish traffic coming from different areas. All traffic coming from the interface was rerouted to the created DMZ in order to further enhance the network's security. DNS services were also deployed using the named service on a dedicated BIND server. The acme04.com and acme.lcl domains were both created and represented external and internal zones respectively. Authentication for the network was established by making Active Directory servers for the acme.lcl domain and provided file and print services to the network. For the e-mail services, a CentOS server running Postfix was deployed. This served as a mail forwarding host for incoming mail and a relay host for outgoing mail. Spam was also filtered through the implementation of Spamassassin on the same server. This assigned scores to each email and flagged them if a certain score threshold was met. A Microsoft Exchange server was also configured in the headquarters zone for administrative purposes and allowed for the use of the Outlook application. In order to ensure that certain servers and clients could be found, the DMZ DNS server records had to be updated to resolve acme04.com hostnames. Finally, web services and application delivery systems had to be integrated into the network architecture. Two CentOS web servers were deployed and were configured to be accessible from both www.acme04.com and acme04.com through the use of DNS CNAME records. Encryption was also supported by self-signing certificates and using HTTPS. The F5 Networks Big-IP Local Traffic Manager (LTM) was configured to load balance the HTTP sites and implement failover. Access to the Exchange OWA through the LTM was also established. In order to re-route traffic

from the headquarters and remote locations, a transparent proxy server running the Squid service was deployed. The ACME corporations network was then successfully finished and configured. It is highly recommended to use FireFox over Internet Explorer as Internet Explorer can slow down work flows because of having to confirm most actions. Another recommendation is to use the free trial when setting up the F5 server as the one supplied within RTFM does not work.

PROBLEM SOLVING

While setting up the network, quite a few different problems arose. In the beginning while establishing the internet for multiple clients and servers, it was noticed that for some reason only the DMZ would get internet. It was immediately figured out that it was a firewall issue as the entirety of the private network was not getting internet. The solution to the issue was to reconfigure the pf sense firewall. So, a new firewall rule was added that allowed all traffic within the network. This allowed all machines on the DMZ and the private network to access the internet. Another issue was run into afterwards and it was that the RM client was unable to ping the RM server. It was deduced that the issue was concerning the alternate DNS server of the RM Client. After reconfiguring the DNS settings on the client it was able to ping the RM server successfully. The last big issue that was run into was Spamassassin not correctly tagging the different spam emails with warnings. After a little investigating, it was noticed that a line within the Postfix main.cf file was incorrect. The last line of the document had a spelling error that was unintentionally created. One of the parameters was incorrectly spelled "spamed" instead of spamd like intended. None of these issues had alternative solutions as the errors were found on core elements. For example, the "spamed" misspelling error could not be resolved in any other manner than spelling it correctly.

REFERENCES

(Admin), X. G. (2021, September 15). *Set up Spamassassin on centos/RHEL to block email spam*. LinuxBabe. Retrieved March 4, 2023, from https://www.linuxbabe.com/redhat/spamassassin-centos-rhel-block-email-spam

14.4.5 Spamassassin configuration examples (Sun Java System Messaging server 6.3 administration guide). (n.d.). Retrieved March 4, 2023, from https://docs.oracle.com/cd/E19563-01/819-4428/bgate/index.html

Alam, A. (2022, December 12). *Install exchange server 2019, complete installing process*. Kernel Data Recovery Blog. Retrieved March 4, 2023, from https://www.nucleustechnologies.com/blog/step-by-step-guide-to-install-exchange-server-2019/

Aleksejs Spiridonovs, 12144 bronze badges, & K-ICTK-ICT 1. (1963, May 1). *How to get spamassassin working with Postfix as a Milter*. Server Fault. Retrieved March 4, 2023, from https://serverfault.com/questions/783401/how-to-get-spamassassin-working-with-postfix-as-a-milter

Anderson, P., & Paul AndersonTwitterPaul is an Avid Tech Geek who Loves writing. (2016, October 3). *DNS/bind TTL settings during domain migrations*. Network Admin Tools. Retrieved March 4, 2023, from https://www.netadmintools.com/art232.html#wbounce-modal

Board index. [SOLVED] postfix/spamassassin/dovecot. (n.d.). Retrieved March 4, 2023, from https://forums.centos.org/viewtopic.php?t=70918

Boucheron, B. (2020, June 30). *How to create a self-signed SSL Certificate for apache on centos 8*. DigitalOcean. Retrieved March 4, 2023, from https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-on-centos-8

Derrick, C., & Subramanian, H. (n.d.). F5 load balancer sample configuration - documentation for BMC TrueSight Operations Management 11.3 - BMC Documentation. Retrieved March 4, 2023, from https://docs.bmc.com/docs/TSOperations/113/f5-load-balancer-sample-configuration-892260471.html

Facebook.com. (2022, September 24). *Setup spamassassin block email spam alma linux 8 / centos 8*. Notes Habibzain. Retrieved March 4, 2023, from https://www.habibza.in/setup-spamassassin-block-email-spam-alma-linux-8/

Google. (n.d.). Google search. Retrieved March 4, 2023, from https://www.google.com/search?q=where%2Bis%2Bspamassassin%2Blocal.cf&rlz=1C1CHBD_enUS915US915&oq=where%2Bis%2Bspamassassin%2Blocal.cf&aqs=chrome..69i57.6397j0j1&sourceid=chrome&ie=UTF-8#ip=1

Google. (n.d.). Google search. Retrieved March 4, 2023, from https://www.google.com/search?q=where%2Bis%2Bthe%2Bmaildir%2Bfile%2Bpath%2

Bpostfi&rlz=1C1CHBD_enUS915US915&oq=where%2Bis%2Bthe%2Bmaildir%2Bfile%2Bpath%2Bpostfi&aqs=chrome..69i57.5677j0j1&sourceid=chrome&ie=UTF-8

How to setup spamassassin with Postfix on ubuntu 16.04. Alibaba Cloud Community. (n.d.). Retrieved March 4, 2023, from https://www.alibabacloud.com/blog/how-to-setup-spamassassin-with-postfix-on-ubuntu-16-04_594878

How to use GREP command in Linux/ unix with examples - nixcraft. (n.d.). Retrieved March 5, 2023, from https://www.cyberciti.biz/faq/howto-use-grep-command-in-linux-unix/

Kaplarevic, V. (2022, August 9). *How to install squid proxy server on centos 7: Phoenixnap KB*. Knowledge Base by phoenixNAP. Retrieved March 4, 2023, from https://phoenixnap.com/kb/install-squid-proxy-server-centos

Linux sendmail command help and examples. Computer Hope. (2021, November 6). Retrieved March 4, 2023, from https://www.computerhope.com/unix/usendmai.htm

Load balancing 101: Nuts and Bolts. F5. (n.d.). Retrieved March 4, 2023, from https://www.f5.com/services/resources/white-papers/load-balancing-101-nuts-and-bolts

Novotny, J. (2023, February 1). *How to install and use Apache on AlmaLinux*. Linode Guides & Tutorials. Retrieved March 4, 2023, from https://www.linode.com/docs/guides/install-and-use-apache-on-almalinux/

Phase 1 Write-up. Login - Purdue University system. (n.d.). Retrieved March 4, 2023, from https://purdue.brightspace.com/d2l/le/content/702044/viewContent/11951583/View

Phase 2 Write-up. Login - Purdue University system. (n.d.). Retrieved March 4, 2023, from https://purdue.brightspace.com/d2l/le/content/702044/viewContent/11951585/View

Phase 3 Write-up. Login - Purdue University system. (n.d.). Retrieved March 4, 2023, from https://purdue.brightspace.com/d2l/le/content/702044/viewContent/11951587/View

Port forwards. Network Address Translation - Port Forwards | pfSense Documentation. (n.d.). Retrieved March 4, 2023, from https://docs.netgate.com/pfsense/en/latest/nat/port-forwards.html

Postfix configuration parameters. (n.d.). Retrieved March 4, 2023, from https://www.postfix.org/postconf.5.html

Postfix not working. FedoraForumorg RSS. (n.d.). Retrieved March 4, 2023, from https://forums.fedoraforum.org/showthread.php?214060-PostFix-not-working

Sending or viewing emails using telnet. Sending or viewing emails using telnet | Media Temple Community. (n.d.). Retrieved March 4, 2023, from https://mediatemple.net/community/products/dv/204404584/sending-or-viewing-emails-using-telnet

Skytech. (2012, June 4). *How to test Postfix mail service using telnet*. Linux Tutorials for Beginners. Retrieved March 4, 2023, from https://webhostinggeeks.com/howto/how-to-test-posfix-mail-service-using-telnet/

spring_64. (2017, September 12). *Solved - mail server error: /USR/lib/dovecot/deliver: No such file or directory*. The FreeBSD Forums. Retrieved March 4, 2023, from

https://forums.freebsd.org/threads/mail-server-error-usr-lib-dovecot-deliver-no-such-file-or-directory.62439/

Wilson, J., el_condor, Admin, Max, Jim, Dcpromo, Rtt, Advisory, A. F. A., & Possamai, L. (2022, June 3). *How to install and integrate Spamassassin with Postfix on a centos 6 VPS*. RoseHosting. Retrieved March 4, 2023, from https://www.rosehosting.com/blog/how-to-install-and-integrate-spamassassin-with-postfix-on-a-CentOS-6-vps/

YouTube. (2016, March 24). *How to configure SMTP postfix mail in linux*. YouTube. Retrieved March 4, 2023, from https://www.youtube.com/watch?v=TJdaLudvCMA

YouTube. (2017, April 21). *02 03 understanding zone files*. YouTube. Retrieved March 4, 2023, from https://www.youtube.com/watch?v=nUht84oLZI0

YouTube. (2019, July 30). *F5 load balancer configuration*. YouTube. Retrieved March 4, 2023, from https://www.youtube.com/watch?v=pi7UKl3EFiw

YouTube. (2021, November 23). *Mail server with Postfix Dovecot mariadb - part 8 - install and integrate spamassassin with Postfix*. YouTube. Retrieved March 4, 2023, from https://www.youtube.com/watch?v=XQtZmaOXuqwhttps%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv

YouTube. (2022, October 30). *Install and configure bind 9 master and slave DNS server for local network using AlmaLinux 9 - 2023*. YouTube. Retrieved March 4, 2023, from https://www.youtube.com/watch?v=4yKN9r48vo0