1. Scenario

Design, draft, and implement a multi-forest enterprise environment, with multiple networks and routing, VPN access, virtualized infrastructure, cloud-hosted resources, and a web presence.

2. Layout: Overview

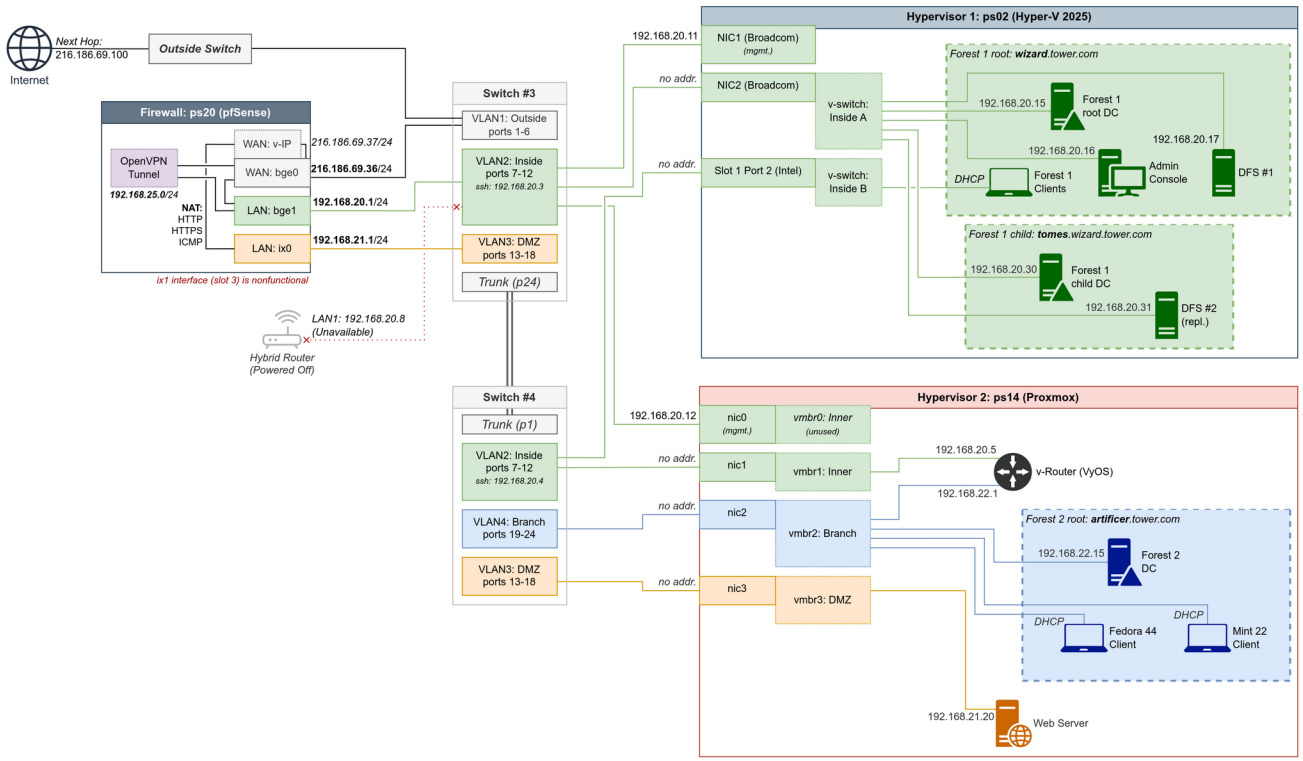

Fig. 1: Overview of logical layout of networking infrastructure (not including cloud).

3. Special information: Project-wide specifications

Certain high-level project specifications were decided prior to starting the project. Some of these were delivered to instructor on day 1.

- Project domain: ***tower.com***
- Web DNS: *tower.itio.rocks*
- Forest 1 root domain: *wizard.tower.com*
- Forest 1 child domain: *tomes.wizard.tower.com*
- Forest 2 root domain: *artificer.tower.com*
- Hypervisor 2: *Proxmox VE 9.1*
- Web Server OS: *AlmaLinux 10.1*
- Forest 2 client OS 1: *Fedora 44*
- Forest 2 client OS 2: *Mint 22.3*
- Custom GPO 1: *Block Chrome usage for non-admin users*
- Custom GPO 2: *Set homepage in browser to project web server*
- IP addressing:
  - Inside network: *192.168.20.0/24*
  - DMZ network: *192.168.21.0/24*
  - Branch network: *192.168.22.0/24*
  - VPN tunnel: *192.168.25.0/24*

3.1. Network and host access

Inside network is accessed directly through wireless access point (if hybrid router is on), or through prepared VPN connection. Branch network and DMZ can be accessed from inside network.

Host access varies depending on OS:

- Windows servers are accessible through RDP. Most are accessible through SSH as well.
- Linux and Unix-based hosts are accessible through SSH (port 22).
- The web server is also accessible through Cockpit (HTTPS port 9090) from internal networks.
- The *cuneo* account can be used on all Windows hosts except ps02 (Hyper-V server).

4. Hardware infrastructure

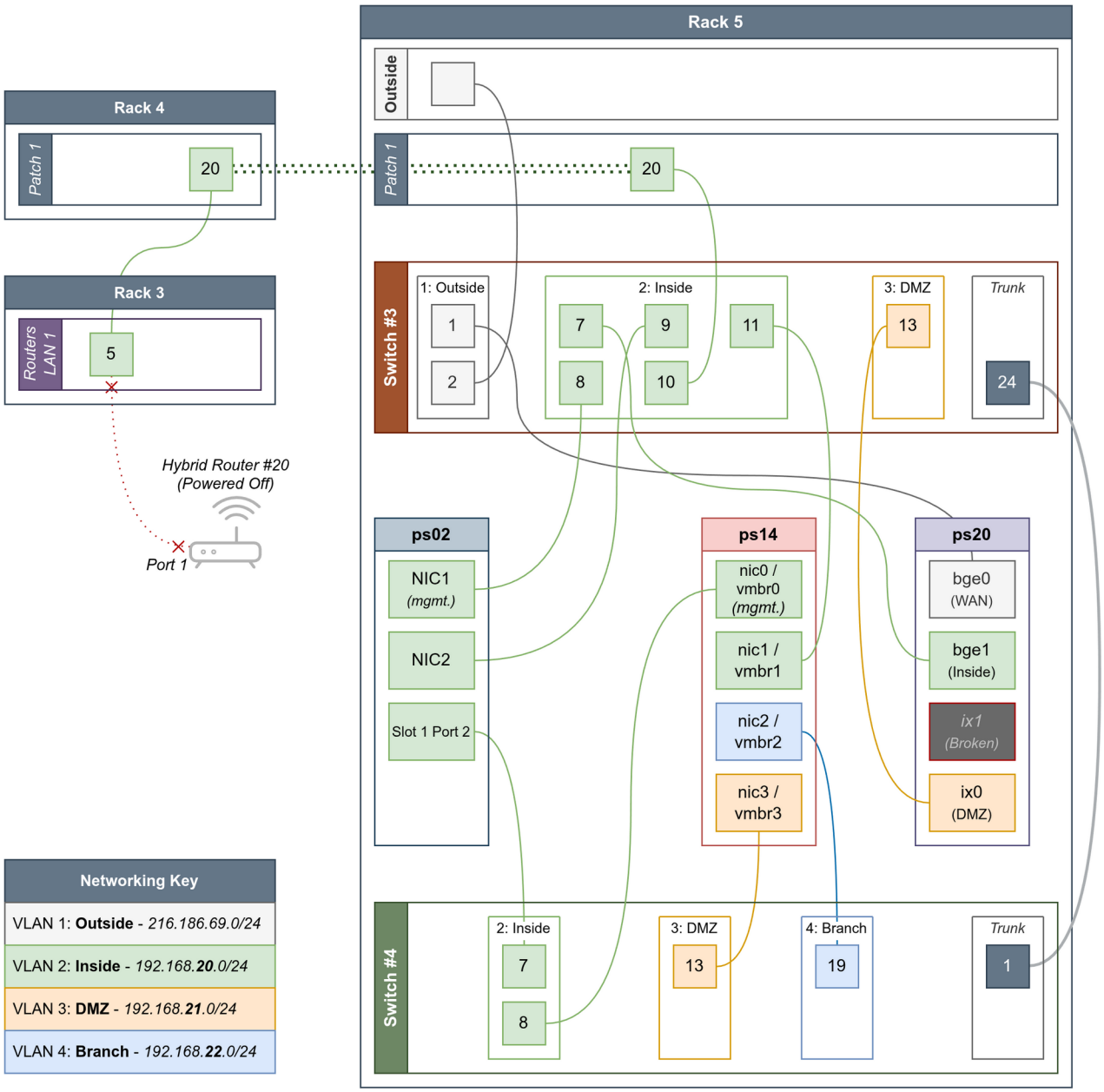

Fig. 2: Diagram of physical topology between hardware devices and associated network segmentation.

Note: We discovered the third port of ps20 (pfSense router) was nonfunctional in its connection between the port on the "LAN 3" patch panel and the pfSense OS (interface "ix1"). Thankfully, only three ports were needed on the host.

4.1. Switching: VLAN structure

4.1.1. VLAN 1: Outside

WAN connections go through this VLAN on the way to the outside switch and the internet. The only host connection is the pfSense router WAN port (ps20:bge0).

This VLAN is assigned ports on both switches, but only the connections on switch #3 are used.

4.1.2. VLAN 2: Inside

The main *Inside* network (192.168.20.0/24) makes use of this VLAN. Host connections are split across both switches:

- Gateway connection on pfSense router (ps20:bge1), to switch #3
- Management connections on hypervisors (ps02:NIC1, ps14:vmbr0), to switch #3
- Hyper-V “Inside A” connection (ps02:NIC2) to switch #3
- Hyper-V “Inside B” connection (ps02:Slot1Port2) and Proxmox inside bridge (ps14:vmbr1) to switch #4
- Hybrid router LAN access (powered off) to switch #3

Inside network servers and network infrastructure is generally accessed through switch #3, while client traffic passes through switch #4 and the trunk (see below).

4.1.3. VLAN 3: DMZ

Less trusted boundary traffic is routed into the *DMZ* network (192.168.21.0/24). Currently the only residing host is the web server, residing on the Proxmox host.

- Gateway connection on pfSense router (ps20:ix0), to switch #3
- Proxmox DMZ bridge (ps14:vmbr3), to switch #4

All traffic to the web server goes through the trunk.

4.1.4. VLAN 4: Branch

Secondary location *Branch* network (192.168.22.0/24). Has no direct connection to the pfSense router; all traffic is instead routed through a virtual router on Proxmox host into the *Inside* network. The only connection is the Proxmox host (ps14:vmbr2), to switch #4.

This VLAN is defined on both switches, but only switch #4 assigns ports to it. It is included in the trunk, but no traffic of this VLAN will pass through it.

4.1.5. Trunk

A “trunk”-like connection between switches is set up for VLAN traffic to pass through the switch fabric. While HP switches include a “trunk” feature for ports, it functions differently than the 802.1q VLAN tagging functionality typically named “trunking” in Cisco switches. For our purposes, the trunk ports are instead assigned the above VLANs as “tagged”.

Traffic in non-trunk ports is assigned only untagged VLANs, to avoid the burden of configuring VLAN tag recognition on hosts. VLAN traffic to untagged ports passes through tagged trunk ports seamlessly, no additional configuration was needed to achieve desired behavior.

4.2. Hybrid router and rack 4 patch connection

Hybrid router (#20) is only used as a wifi access point, accessible in the classroom and about 10ft out into the hallway. It was used for project setup and remains powered off for submission.

Its “LAN 1” connection is only accessible on rack 3 (“Routers LAN 1” panel). To connect it to the main infrastructure on rack 5, the linked patch panels between racks 4 and 5 were used. Its traffic went through switch #3.

4.3. Troubleshooting

Problem: Switches were not passing VLAN traffic correctly.

- **Cause**: HP “trunk” mode is not comparable to Cisco trunking.
- **Solution**: Configure each VLAN to pass tagged traffic through the trunk port. HP switches automatically handle tagging/untagging of traffic between trunk and non-trunk ports.

Problem: Port #3 on ps20 (ix1) reporting as disconnected even when all ports are physically connected to ethernet cables. Switching cable to switch does not help.

- **Cause**: Connection between pfSense OS and patch panel appears to be nonfunctional. Most likely a bad cable or possibly physical interface on host.
- **Workaround**: Use port #4 (ix0) instead; pfSense router only needs 3 ports to function. Should be investigated further after hardware baselining.

Incident: VLANs suddenly and unexpectedly started misbehaving; ps14 went offline.

- **Cause**: Switch #3 was unwittingly reset to factory defaults by another team.
- **Recovery**: Restore switch #3 configuration from previously saved copy. Re-create logins, SSH host keys and certificates. Set hostnames to be more clear to prevent future mishaps.

4.4. Potential improvements

Changes in implementation of project that may have helped in retrospect.

Switch port and VLAN ranges could be arranged more conveniently and consistently. VLAN 1 (Inside) space on switch #3 is currently very tight and could use additional ports, while VLAN 3 (DMZ) and VLAN 4 (Branch) have very little use for more than a couple ports on each switch.

Hyper-V and Proxmox both support sharing a “management” port used for outside access with internal virtual switches/bridges. This could reduce the number of cables used. We had forgotten this during their setup and assigned a dedicated “management” port to not be used for VMs. Hyper-V host could be configured to share “Inside A” v-switch traffic with host traffic. Proxmox could have VMs use vmbr0 v-bridge alongside the host.

5. Routing, NAT, and firewall

Networks are arranged in a hub-and-spoke layout, with the Inside, DMZ, and WAN (Outside) networks connected to the pfSense router.

- Inside gateway: *192.168.20.1*
- DMZ gateway: *192.168.21.1*
- WAN “next hop” gateway: *216.186.69.100 (default route)*

The Branch network is connected to a VyOS v-router on ps14:

- Inside interface: *192.168.20.5 (default route)*
- Branch gateway: *192.168.22.1*

Only simple routing is used, bridging the Inside and Branch networks in both directions, though this means the Branch network has no internet access. (See improvements below.)

NAT is used to port forward traffic to the web server in the DMZ. Incoming traffic directed at the public registered web DNS address is picked up by a “virtual IP” on the WAN interface. HTTP (tcp/80), HTTPS (tcp/443), and ICMP traffic is forwarded to the web server (192.168.21.20); other traffic is dropped.

The default outbound NAT rules are left at default for WAN traffic.

5.1. Firewall

The pfSense router is also a firewall configured to manage traffic flow between networks. For this project, a simple ACL-based implementation is used.

WAN interface:

- Block private/bogon networks.
- Allow HTTP/HTTPS/ICMP traffic to the web server on the DMZ.
- Allow OpenVPN (udp/1194) traffic outward to the internet.

Inside interface:

- Allow HTTP/HTTPS traffic from inside network (anti-lockout).
- Allow all Inside and Branch traffic to anywhere.

DMZ interface:

- Allow HTTP/HTTPS inward from anywhere (web server access).
- Block inbound traffic from DMZ to Inside network.
- Allow ICMP to web server from anywhere (web server ping).
- Allow ICMP from web server to pfSense (web server to gateway ping).
- Allow DNS (udp/53) traffic to router (DNS functionality in DMZ).

OpenVPN (see “VPN” section below):

- Allow inbound traffic from VPN to Inside and Branch networks.
- Allow outbound traffic from VPN to anywhere.

The VyOS v-router has no firewall enabled; all traffic flows freely between the Inside and Branch networks.

5.2. Troubleshooting

Problem: VPN clients could not access devices on the Inside network reliably.

- **Cause**: VPN-sourced traffic was being blocked by firewall in certain corner cases.
- **Solution**: Add allow rules to firewall to allow these cases through.

Problem: Traffic between VPN and Branch network and between Branch and internet failed.

- **Cause**: Lack of routing protocol that could synchronize routes between pfSense and v-router.
- **Resolved**: No action needed; beyond the scope of project requirements.
- **Workaround**: If Branch network clients need internet access, reconfigure VM with an interface connected to inside network for the duration of needs.

5.3. Potential improvements

VyOS router should be configured with routing protocol along with pfSense to synchronize routes between them for LAN networks. Static routes were attempted but could not be set up successfully. RIPv2 does not seem to be supported in pfSense UI. Perhaps OSPF is more appropriate?

Firewall rules on DMZ should be cleaned up quite a bit; the current setup is in a “if it works” setup. More thorough testing and planning would be required.

Specifying IP addresses of trusted networks directly in firewall rules poses possible security risk. This could be improved by reworking rules to not trust the IP of any client directly, relying on interface crossings insead. Extensive planning would be needed for this.

6. Networking services

6.1. DHCP and DNS

DHCP and DNS services were not hosted by the pfSense router in most cases. Instead, the DCs of the root domain of each forest hosted these services through Windows Server features.

In both cases, DHCP was scoped to the entire network range, using only reserved addresses to avoid lease interference. No zones were to be used to reduce the size of the scope.

Hybrid router offered a DHCP service, which was turned off once the service was set up elsewhere.

DNS was included as a service with each AD/DS installation on a root domain DC. This was mainly used to resolve hostnames within the network without mDNS. No special static records were used to force name resolution.

6.2. VPN

pfSense supports acting as an OpenVPN server to allow access to LAN networks remotely. For the most part this followed a “wizard” process in the web UI.

A TLS certificate authority and child certificate was created for use by the VPN first.

- CA is self-signed (RSA 2048-bit)
- Server certificate prepared for DNS:magiccircle.tower.com, IP:216.186.69.36
- Client certificates prepared for each VPN user, signed by the CA, associated with the user in user management.

VPN was configured using the wizard, which created additional NAT and firewall rules as needed.

- Use previously prepared CA and server certificates.
- VPN accessed via WAN interface, UDP port 1194.
- Put VPN clients into tunnel network *192.168.25.0/24*.
- Grant access to *192.168.20.0/24* (Inside) and *192.168.22.0/24* (Branch)
- Assign DNS server of matching forest 1 root DC.

Used client export utility (package “openvpn-client-export”) to download .ovpn file from “Most Clients” inline configuration. File loaded depending on desktop environment and OpenVPN client.

6.3. Problems and potential improvements

Problem: DHCP zones defined in hybrid router did not appear to be respected consistently.

- **Cause**: DHCP services were running from multiple source in the network, with overlapping scopes. These were accepted on a first-come first-serve basis, rather than means of network access.
- **Solution**: Disable DHCP server on hybrid router to allow service on forest 1 root DC.

In situations with much network infrastructure, defining reserved addresses for every host can be tedious. Defining DHCP zones to avoid static IPs used by servers and network infrastructure improves clarity in client IPs (such as a DHCP IP in between two reserved static IPs). It also gives room for growth in server/networking infrastructure if needed.

7. Hypervisors

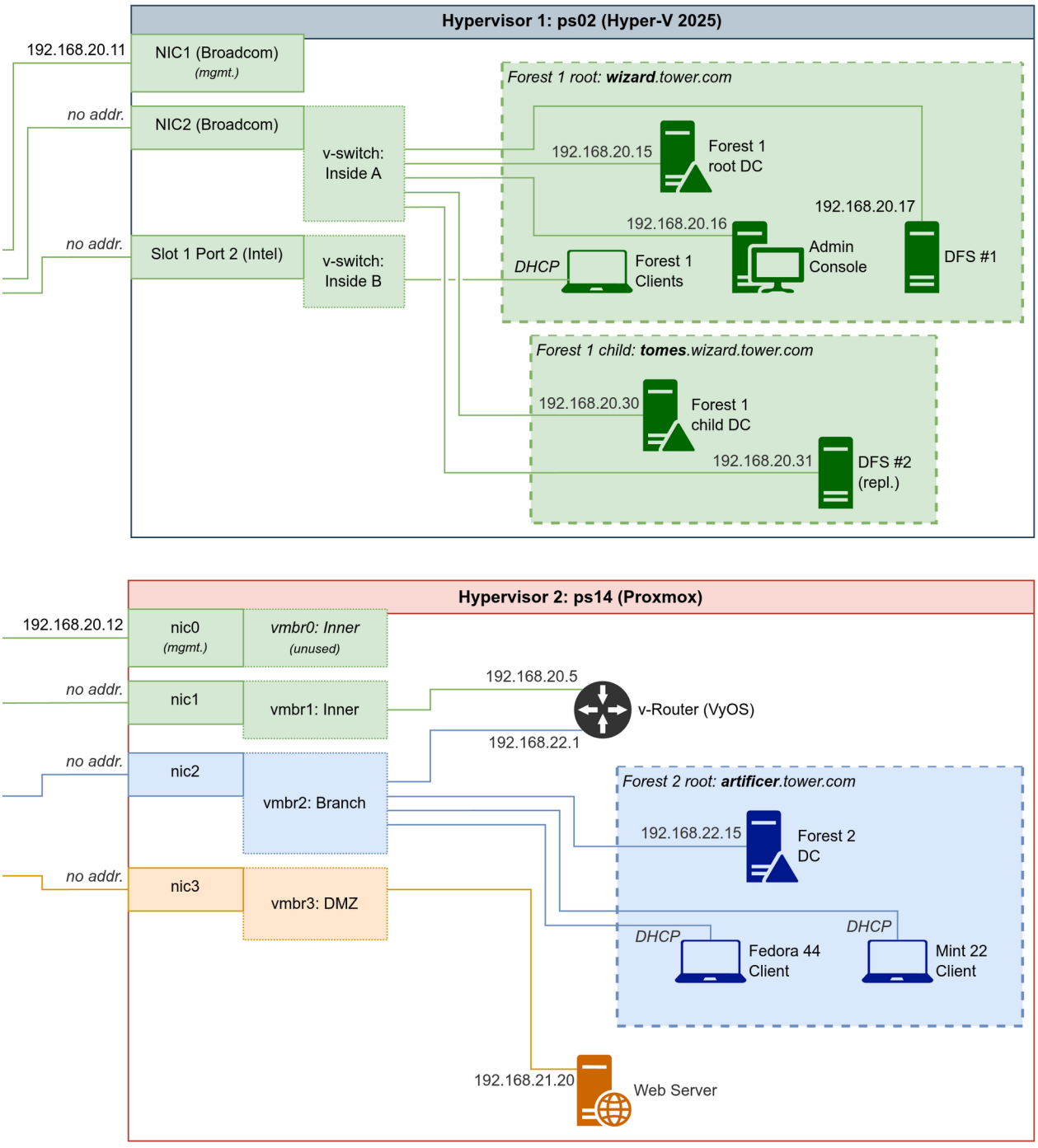

Fig. 3: Hypervisor network layout close-up, including VMs and domains. Dotted-border network interfaces are virtual, associated with the adjacent physical interface.

7.1. Hyper-V

Server ps02 was used as the Hyper-V host. This server would host the majority of Inside network hosts, aside from network infrastructure.

Instead of a fresh install, the existing licensed installation of Windows Server 2025 Datacenter used. This placed restrictions on configuration:

- Only one new account was to be created, for project work to avoid conflicts. (This is why ps02 is the only host without any form of “cuneo” account.)
- Server was not to be joined to a domain.
- No new software was to be installed aside from the Hyper-V role.

The host was set up with two v-switches, each directing to one physical switch. Servers (including admin console) were connected to “Inside A” v-switch, connected to physical switch #3. Clients were connected to “Inside B” v-switch, to physical switch #4. The management interface was excluded from any v-switch traffic (see above). No DMZ or Branch network guests exist on the server.

Hyper-V was configured to use the D: drive (second HDD) for VMs. This included VM configuration files, virtual disks, and exported “template” backups.

While Hyper-V Manager doesn’t support cloning or template VMs, the export tool allows a rudimentary workaround to duplicate VMs, though doing so requires some file renaming and editing.

7.2. Proxmox

Server ps14 was used for the secondary hypervisor, decided as Proxmox. All Branch network hosts, as well as the web server and v-router, would reside on this hypervisor.

As a fresh install of Proxmox VE 9.1, some basic configuration was put in place:

- User accounts created for both “rpeaco” and “djoyce”, both for command-line and web login.
- APT package sources were fixed in /etc/apt/sources.list.d/ to allow installing and updating system packages.
- System given a FQDN “ps14.tower.com”, at level above forest 1 root (“wizard.tower.com”).

Host was configured with a v-bridge for each physical interface, used by VMs to connect to each network. Two interfaces go to Inside network (one to each physical switch, with “management” interface going to switch #3).

Several “basevm” templates were prepared for Windows OSs, as well as the web server’s AlmaLinux install, to reduce waiting time during initial setup for hosts.

7.3. Troubleshooting

Problem: Installing Fedora on VM seemed to cause the VM to be nonresponsive.

- **Cause**: Anaconda installer struggles with less than 2GiB of RAM available.
- **Solution**: Allocate more RAM for Fedora VM.

Problem: Setting up Windows desktop clients is very time consuming.

- **Cause**: Windows desktop editions are badly designed OS.
- **Solution**: Prepare “basevm” images where feasible, with guest prepared to a usable state.

Incident: ps14 failed to reboot properly while away.

- **Cause**: Unknown. Most likely cause is interactive notification from the BIOS.
- **Resolved**: Unknown how. If there was a message waiting for boot, instructor may have pressed necessary key to resume boot normally.

7.4. Potential improvements

Setting up a WAC server could help with management of Hyper-V guests. Hyper-V Management snap-in does not allow cloning VMs, but WAC does, which would have been quite helpful during this project.

Proxmox was set up with only one disk of storage during configuration. Setting up the second disk as an LVM physical extent would expand storage available. In a production environment, a SAN or NAS solution would be more desirable for redundancy, flexibility, and separation of concerns.

8. Hosts

8.1. Domain structure

Three domains were created for this project, across two forests:

- **wizard**.tower.com (forest 1)
  - **tomes**.wizard.tower.com (forest 1)
- **artificer**.tower.com (forest 2)

Members of WIZARD and TOMES exist in the Inside network (192.168.20.0/24), while members of ARTIFICER are on the Branch network (192.168.22.0/24). Only one Domain Controller was used for each domain.

8.1.1. Trust relationships

The three domains are granted access to each other through domain trust relationships. These allow users from one domain to log on and gain access to domain resources from any domain host.

The child domain “TOMES” was automatically granted a parent-child trust relationship with its parent “WIZARD” during creation.

The forest trust between “WIZARD” and “ARTIFICER” required more setup:

- DNS conditional forwarding was set up so that DNS servers on each DC could forward requests to each other. This was set up on each DC.
- Lookups were tested with *nslookup* utility to confirm functionality both ways.
- Create two-way forest trust, providing credentials for the remote forest to authenticate.

8.2. Hostnames and IPs

A total of 12 virtual hosts were set up across the enterprise infrastructure.

wizard.tower.com:

- “SCRYING” (192.168.20.15) – DC for domain. Hosts DNS, DHCP, and shared printers.
- “TINYHUT” (**192.168.20.16**) – Admin console for instructor.
- “SECRETCHEST-01” (192.168.20.17) – DFS server #1, namespace and replication.
- “IDENTIFY” (DHCP) – Client PC for Divination dept.
- “FINDFAMILIAR” (DHCP) – Client PC for Conjuration dept.

tomes.wizard.tower.com:

- “LEGENDLORE” (192.168.20.30) – DC for domain.
- “SECRETCHEST-02” (192.168.20.31) – DFS server #2, replication only.

artificer.tower.com:

- “ARCANEEYE” (192.168.22.15) – DC for domain. Hosts DNS and DHCP.
- *“sanctuary” (DHCP) – Linux client PC (not directly joined, FQDN only)*
- *“curewounds” (DHCP) – Linux client PC (not directly joined, FQDN only)*

Network infrastructure:

- “majorimage” (192.168.21.20) – Web server in DMZ
- “sending” (192.168.20.5, 192.168.22.1) – VyOS v-router between Inside and Branch networks

8.3. Operating systems

Various OSs were used as per project needs:

- Windows Server 2022 Standard used for most servers – DCs, DNS, DHCP, DFS.
- Windows 10 Pro used for Windows clients in wizard.tower.com domain.
- AlmaLinux 10.2 used for web server.
- VyOS 2026.03 used for v-router.
- Fedora 44 used for Linux client #1 in Branch network (“sanctuary”)
- Mint 22 used for Linux client #2 in Branch network (“curewounds”)

8.4. Troubleshooting

Problem: Forest 1 computers appeared unable to join the domain.

- **Cause**: Windows clients must be Pro edition and set DNS to the DC.
- **Solution**: Reinstall with Windows Pro, set DNS to the DC. Once DHCP is running on DC, configure clients to use it as DNS.

Problem: Forest trust refused creation from failure to resolve domain.

- **Cause**: Forest trusts require either a shared parent DNS server, or conditional forwarding.
- **Solution**: Add DNS conditional forwarding between DCs (“SCRYING” and “ARCANEEYE”) before adding forest trusts.

8.5. Potential improvements

Linux clients could be joined to domain through *sssd* for LDAP authentication. Domain resources could be accessed with *Samba*. Lack of practice with this and being not necessary for the project left this unimplemented.

IP addresses could be condensed and reorganized with better planning. Network services such as DNS and DHCP are typically placed in low host IPs. Instead they were placed relatively high for their role as domain-specific infrastructure rather than network infrastructure.

9. File Sharing

9.1. DFS shares

Distributed File Services adds redundancy to SMB sharing, as well as scoping shares within the domain as a “namespace”.

In this project, DFS was configured across two servers:

- DFS #1 (“SECRETCHEST-01”) – DFS namespacing and replication roles installed
- DFS #2 (“SECRETCHEST-02”) – DFS replication only installed

Because the shares are distributed between a parent and child domain, additional permissions were prepared for the service. The “Domain Admins” group from WIZARD was granted membership of the local “Administrators” group on SECRETCHEST-02 in TOMES, allowing DFS from server #1 to write to files on server #2.

Additionally, the location for the share needed to be prepared on each server. For both servers, this is at C:\DFS.Data.

To set up the DFS share itself, a namespace was created for wizard.tower.com on server #1. Default settings were used.

A replication group “DFSRepl” was then configured for the share paths:

- Two way replication
- Primary server: SECRETCHEST-01
- SECRETCHEST-01 location: C:\DFS.Data
- SECRETCHEST-02 location: C:\DFS.Data

Once replication was set up, the group was “published” to the directory:
\\wizard.tower.com\DFS\Data

9.2. Printer sharing

For GPO configuration, a fake printer (local FILE: port, XPS driver) was set up for each of two departments. Printer was configured to be shared and then listed on the directory.

See “GPO configuration” below for further information on deployment.

9.3. Troubleshooting

Many issues were encountered with DFS setup.

Problem: DFS namespace creation refused to connect to the domain, when server was already joined to domain. *(Could not be reproduced on separate hardware.)*

- **Cause**: DFS namespace configuration seems to require domain admin membership at login.
- **Solution**: Re-login as domain admin and retry.

Problem: DFS replication group fails to access destination server in child domain.

- **Cause**: Domain admin in parent domain does not have local admin permissions on server in child domain.
- **Solution**: Add parent domain's "Domains Admins" group membership in local "Administrators" group on second server in child domain.

Problem: DFS share was not granting write permissions to regular domain users.

- **Cause**: DFS shares use NTFS folder permissions for remote access, rather than SMB share permissions.
- **Solution**: Grant write and modify permissions to "Domain Users" group in parent domain, to the local directory of the share on primary DFS server.

10. Active Directory

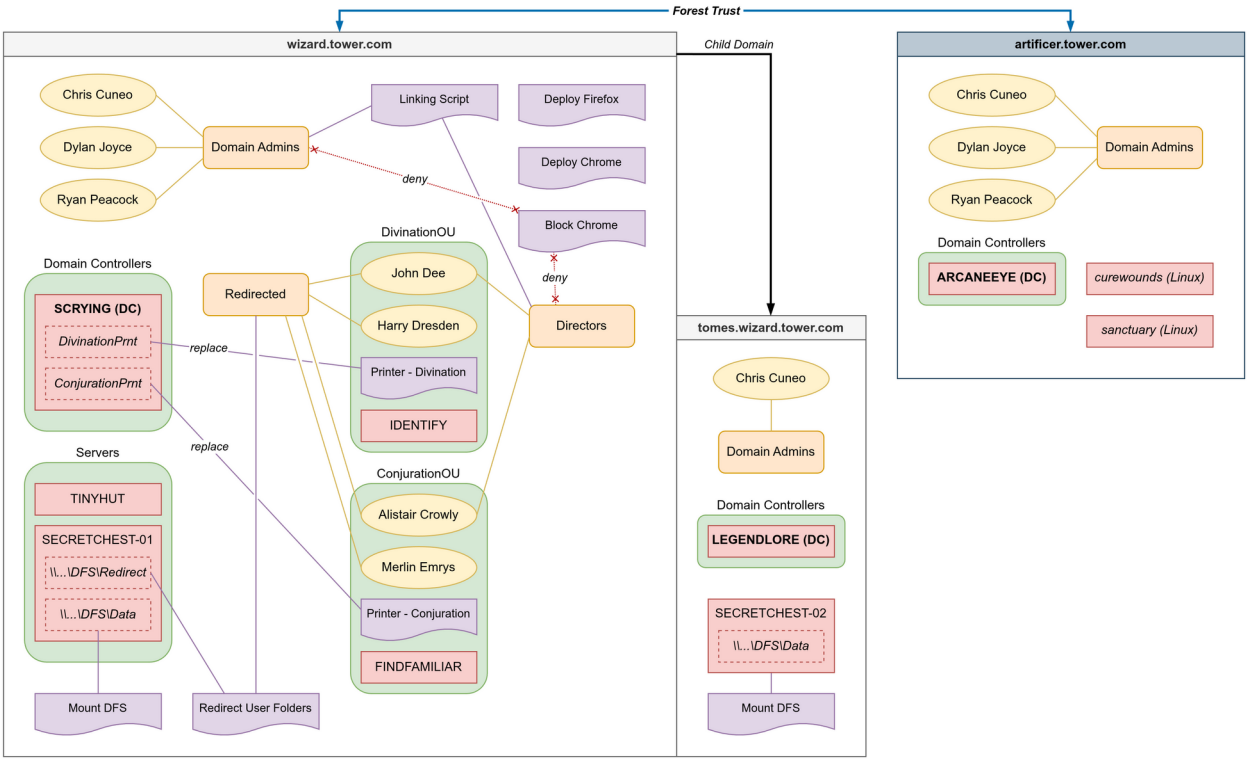

Fig. 4: Active directory layout, with users, computers, groups, OUs, and policies.

10.1. Organization units

Organization units were set up for associated policies and some mild scoping. An object can only be part of one OU at most, which required some workarounds for implementing scoping correctly.

Only the WIZARD domain needed extra OUs to be created. One was created for servers, distinguishing them from client PCs. However, the main OUs at use were the two created for the two departments, “DivinationOU” and “ConjurationOU”. Two users and one client computer were added to each. A GPO was linked into each department OU to map the associated pseudo-printer.

10.2. Users and groups

Administrator accounts were created for project members as well as the instructor. These should have unrestricted access to all domain and forest configuration:

- Ryan Peacock (rpeaco)
- Dylan Joyce (djoyce)
- Chris Cuneo (cuneo)

These users were created again on the forest 2 root (artificer.tower.com); these are separate accounts, but due to the forest trust, they may access resources from the other forest.

Additionally, an instructor account was added to the forest 1 child domain in case of access problems.

For client PC logins, four wizard logins were created with lesser permissions:

- John Dee (Director, Divination dept.)
- Harry Dresden (Divination dept.)
- Alistair Crowley (Director, Conjuration dept.)
- Merlin Emrys (Conjuration dept.)

Two users were added to a “Directors” group. This is used in several group policies for including or excluding certain users (see below).

A “redirected” group was prepared for user folder redirection. This includes only the four client users above; administrators do not have folder redirection.

10.3. Policies (GPOs)

10.3.1. Mount DFS

This GPO maps the DFS share \\wizard.tower.com\DFS\Data to the S: drive of all users. It is linked to the domain, unrestricted by delegation.

This policy was recreated in all domains. As there is no way to scope a GPO to multiple domains, it was duplicated.

Policy paths:

- GPO:\User Configuration\Preferences\Windows Settings\Drive Maps
  - “\\wizard.tower.com\DFS\Data” mapped to S: as “DFS Data”
  - Run in user’s context

10.3.2. Run script

This runs a simple powershell script to create a Windows .lnk shortcut on the desktop to a hidden share, where the script itself resides.

A hidden share was created on DC for the script, made readable by all users but remaining hidden.

Policy paths:

- GPO:\User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)
  - Logon: “\\SCRYING\GPO$\linktoshare.ps1”

10.3.3. Set Edge homepage

This sets Edge settings such that the project website loads when the user clicks the home button.

Since Windows does not come with policy templates for Edge in Server 2022, they needed to be downloaded from Microsoft, and installed to *C:\Windows\PolicyDefinitions* on the DC.

Policy paths:

- GPO:\User Configuration\Policies\Administrative Templates\Microsoft Edge\Startup, home page, and new tab page\
  - Set the new tab page as the home page: Disabled
  - Configure the home page URL: Enabled, “https://tower.itio.rocks”
  - Show Home button on toolbar: Enabled

10.3.4. Deploy Chrome, Firefox

A custom GPO is set to block Chrome for certain users. To do this, Chrome needs to be installed first.

A version of Chrome “for Enterprise” is available, its MSI installer was downloaded and copied to the NETLOGON share of the DC. The policy then deploys it as a software package.

To avoid failures to install due to race conditions, system is configured to wait for network and a pre-set time for installation.

Policy paths:

- GPO:\Computer Configuration\Policies\Software Settings\Packages
  - \\SCRYING\NETLOGON\googlechromestandaloneenterprise64.msi
- GPO:\Computer Configuration\Policies\Administrative Templates\System\Logon\
  - Always wait for the network at computer startup and logon
- GPO:\Computer Configuration\Policies\Administrative Templates\System\Group Policy\
  - Specify startup policy processing wait time: 40 seconds

This was repeated for Firefox “ESR” edition.

10.3.5. Deploy printers

The pseudo-printers defined for each department (“Printer sharing” above) can be deployed with GPO.

Two GPOs were created, one for each department, each linked to the respective OU.

Policy paths:

- GPO:\User Configuration\Preferences\Control Panel Settings\Printers
  - Replace: “\\SCRYING\DivinationPrnt” (remove if not applied)

10.3.6. Block Chrome

To block a program, group policy allows setting the computer to not run specific programs.

The GPO uses delegation to “deny” (exclude) applying it to administrators.

Policy paths:

- GPO:\User Configuration\Policies\Administrative Templates\System\
  - Don’t run specified Windows applications: “C:\...\chrome.exe”

Delegation:

- Deny: “Apply group policy” to: Administrators, Domain Admins, Directors

Note: If the user copies the Chrome folder to a new location and renames chrome.exe, they will be able to run it. Denying specific programs in Windows can be unreliable; the preferred practice is to specify a list of allowed programs instead, though this can be time-consuming.

10.3.7. User folder redirection

Folder redirection requires some initial setup to work:

- Create a new DFS shared folder at *C:\DFS.Redirect*, published to directory as “\\wizard.tower.com\DFS\Redirect”
- Alter filesystem permissions on DFS server #1:
  - Disable inheritence on root folder
  - Assign “read & execute” and “create folders” permissions to Domain Users
- Test with a user account creating a folder within \\wizard.tower.com\DFS\Redirect

GPO uses basic redirection; it will create a folder for each user and subfolder for each redirect automatically, within the share root.

Delegation is configured to

Policy paths:

- GPO:\User Configuration\Policies\Windows Settings\Folder Redirection
  - Folders: Desktop, Documents, Pictures, Contacts
    - Basic redirection: “\\wizard.tower.com\DFS\Redirect”
    - Move the contents to the new location
    - Removal: Redirect the user folder back to local userprofile location when removed

Delegation:

- Uncheck “Apply group policy” for Authenticated Users
- Check “Apply group policy” for Redirected group (see above)

10.4. Troubleshooting

Problem: On computers logged in from members of two different department OUs, both pseudo-printers are visible.

- **Cause**: Preferred printers set to “Update” in GPO are applied once and left in place after user switch.
- **Solution**: Specify printer as “Replace” in GPO, and check “Remove this item when it is no longer applied”.

Problem: Windows Server 2022 does not contain policy definitions for Edge

- **Solution**: Download ADMX and ADML files from Microsoft and install to DC.

10.5. Potential improvements

Home page GPO could be reproduced for Firefox and Chrome as well. Both Google and Mozilla offer policy definitions to configure their browsers in enterprise environments. This would be fairly easy to set up.

As noted above, blocking specific programs with a fixed block list is prone to workarounds. While Windows offers a means to block a program by file hash or publisher certificate, these policies are deprecated legacy functionality and do not appear to work anymore (at least with Chrome). Instead, a more thorough approach to only allow specific programs necessary would be more useful. This takes much more research and effort though.

11. Web presence

11.1. Web server

Project web server was set up on Proxmox host:

- OS: AlmaLinux 10.2
- FQDN: “majorimage.tower.com”
- IP: 192.168.21.20 (DMZ)
- Forwarded (virtual) IP: 216.186.69.37
- External domain name: tower.itio.rocks

Server was set up to be ready for web hosting with basic Linux configuration:

- No GUI desktop environment installed, just TTY
- Installed and enabled Apache httpd
- Enabled Cockpit for easier remote management (accessed at HTTPS port 9090)
- Added HTTP, HTTPS, ICMP, and Cockpit to public zone of *firewalld*
- Set SELinux to "Enforce"
- Installed EPEL and Certbot for TLS certificate

In the meantime, index.html was set to a simple placeholder page to confirm functionality.

TLS was enabled in Apache config. Initially this was with a self-signed certificate from the pfSense router, but since the server was reachable from a public DNS record, this actually wasn't necessary. Let's Encrypt, a free public TLS certificate authority, could validate the website connection with minimal configuration.

The ACME client (Certbot) could validate and install the certificate on the server. This placed the certificate in the correct directory and added the necessary config lines for Apache. Restarting httpd now showed a valid TLS certificate in a browser.

11.1.1. Secure access directory

A private directory was added at /var/www/html/access for private uploaded files. Currently this only includes the OpenVPN client configuration for instructor access (see below). A basic HTTP login dialog is used, though the TLS certificate should encrypt the login in transit.

Apache is configured with "AllowOverride AuthConfig" in the /var/www/html document root. This is paired with a *.htaccess* file in it to require authentication.

11.2. Web site

A rudimentary HTML and CSS website was set up to match the "Wizard Tower Construction Co." design requirements. The site adopted an early-2000s "clip art" design with simple styling for pages.

PDFs are viewable through iframes to enable viewing within the main page. Diagram images are also viewed this way.

11.3. Cloud hosting

This document is hosted on AWS in an S3 bucket for documentation.

S3 buckets were configured to allow public access to image files at static URLs, allowing the resources to be displayed in the web site. Two buckets were used:

- “itio-final-b” for PDF documentation (stand-in for Azure, see below)
- “itio-final-bucket” for diagrams and images

Images and PDFs on the website link to the static public URLs in these buckets. Enabled public access on these files to allow this.

The initial plan was to use Azure to host documentation, but due to issues with Microsoft account setup, this was not possible. Instead, documentation was to be moved to another S3 bucket.

11.3.1. EC2 instance

Another web server was to be set up as an EC2 instance, running httpd and containing only a link to the main website.

- Used default Amazon Linux 2023 AMI
- Permissions opened for inbound HTTP and HTTPS traffic in its security group.
- Installed Apache httpd package and started its service.
- Edited /var/www/html/index.html to display a simple link to our main web page.

This instance is accessible at: http://**18.215.162.253**

11.4. Troubleshooting

Problem: Files in bucket were not visible in website.

- **Cause**: Files were not set for public URL access.
- **Solution**: Configure public URL access for each file.

Problem: EC2 instance was not accessible from public IP.

- **Cause**: Startup script to install httpd did not complete due to *dnf* prompting interactively.
- **Solution**: Specify -y in *dnf* command.

11.5. Potential improvements

EC2 instance could be set as new image/template to deploy to a public DNS name. This could be connected to an elastic IP (though this would be quite expensive).

Cloud infrastructure could be laid out in a more clear and organized way, with better separation of concerns.

Cloud hosting could be used to set up permissions to require login to view specific items.

12. Instructor access

Following verification of the project, an ethernet cable was set up connecting the fourth port of Hyper-V host (ps02) to ITIO. This was configured with a static IP.

For accessing the network, the OpenVPN client configuration can be reached with a link at the bottom of the “Final Project Deliverables” page. This requires instructor login.

For host access:

- All hosts have either a local or domain *cuneo* account for instructor.
- RDP is enabled on all Windows hosts.
- SSH is enabled on all Linux hosts, and most Windows Server hosts.
  - SSH for switches requires *cuneo* login.
- Cockpit (HTTPS, port 9090) is also enabled on web server.
- VyOS uses a separate login.