System Administration

Final Documentation Created by: Dominick Olhava



Table of Contents

Table of Contents	1
Network Overview	2
Project 1: Linux Server	3
Project 2: Windows Server	12
Project 3: pfSense Firewall	
Project 4: Internal Caching DNS	42
Project 5: External DNS	50
Project 6: Static HTTPS Web Server	65
Project 7: Active Directory	78
Project 8: VPN Server	102
Appendix	116

Network Overview

Machine	Service(s)	IP Address	FQDN
pfSense Firewall	 Internal Caching DNS WireGuard VPN 	10.161.21.4	pfsense.slick.firewall
Windows Server	- AD Domain Controller - AD Domain: ad.local	192.168.2.2	slickbrickcentral.com (web server) ubuntu.slickbrickcentral.com
Ubuntu Server	- BIND DNS - Apache Web Server	192.168.2.3	win.slickbrickcentral.com



Project 1: Linux Server

Below contains steps outlining the configuration of an **Ubuntu Linux Server** that will be used to host a Static HTTPS Web Server and BIND for Internal DNS mappings. The Linux Server will start in the WAN under the Static IP Address: **10.161.21.2**.

VM Configuration

Guest Os: Linux (64 Bit) Hardware: 2 CPUs, 8 GB RAM, Thin Provision, Use Datastore ISO file ISO file: Ubuntu 24.04 Live Server

Final VM Specifications:

Virtual Hardware VM Options	
	ADD NEW DEVICE ~
> CPU	2 ~
> Memory	8 v GB v
> Hard disk 1	60 GB v
> SCSI controller 0	VMware Paravirtual
> Network adapter 1	SysAdmin021 ~
> CD/DVD drive 1	Datastore ISO File 🗸 🗹 Connected
> Video card	Specify custom settings 🗸
> Security Devices	Not Configured
VMCI device	
SATA controller 0	AHCI
> Other	Additional Hardware

CANCEL OK

Ubuntu Server Setup

Network Configuration

Subnet: 10.161.21.0/24 (.21 is signifying the subnet I was assigned for the semester) Linux Server Static IP: **10.161.21.2**

Gateway: 10.161.21.1

Nameservers (DNS): UNI DNS Servers - 10.120.16.10 and 10.120.16.11

Network configuration [Help]
Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates.
NAME TYPE NOTES [ens192 eth – ▶] disabled autoconfiguration failed 00:50:56:82:e9:89 / VMware / VMXNET3 Ethernet Controller
[Create bond ►]
Edit ens192 IPv4 configuration
Subnet: 10.161.21.0/24_
Address: 10.161.21.2
Gateway: 10.161.21.1
Name servers: 10.120.16.10, 10.120.16.11 IP addresses, comma separated
Search domains: Domains, comma separated
[Save] [Cancel]

Assigned **NO** Proxy. A proxy is a "middle man" to filter network traffic coming out and/or in Linux Mirror: US Repository Address



Continue **WITHOUT** Updating the Installer Storage Configuration: Use entire disk with 1 partition

Guided storage configuration		[Help]
Configure a guided storage layout,	or create a custom one:	
(<u>Χ</u>) Use an entire disk		
[/dev/sda local disk 60.000G	•]	
[X] Set up this disk as an LV	M group	
[] Encrypt the LVM grou	p with LUKS	
Passphrase:		
Confirm passphrase:		
	Also create a recovery key The key will be stored as ~/recovery–key.txt in the live system and will be copia /var/log/installer/ in the target system.	
() Custom storage layout		

Storage configuration				
FILE SYSTEM SUMMARY				
MOUNT POINT SIZE TYPE DEVICE T [/ 28.996G new ext4 new LVM [/boot 2.000G new ext4 new part	YPE logical volume ition of local disk	►] ►]		
AVAILABLE DEVICES				
DEVICE [ubuntu-vg (new) free space	TYPE LVM volume group	SIZE 57.996G 29.000G	↓ 1	
[Create software RAID (md) ▶] [Create volume group (LVM) ▶]				
USED DEVICES				
DEVICE [ubuntu-vg (new) ubuntu-lv new, to be formatted as ext4,	TYPE LVM volume group mounted at ∕	SIZE 57.996G 28.996G	▶ 1	
[/dev/sda partition 1 new, BIOS grub spacer partition 2 new, to be formatted as ext4, partition 3 new, PV of LVM volume group u	local disk mounted at ∕boot buntu–vg	60.000G 1.000M 2.000G 57.997G	▶] ▶ ▶	

Profile Configuration: Username: **Classified**, Password: **Classified**



SSH Configuration: NO OpenSSH Server



Linux Server Guide

Directories

- **/home** a user's folder that contains personal data and configuration files for programs on the machine. System programs and applications are NOT stored here.
- /var/www a common place to store web content such as HTML, CSS, JavaScript, etc. The var directory is known to store "variable" (changing) data which makes sense since websites frequently update.
- /var/log contains log files generated by system and user applications. The logs can
 include system messages, error messages, security alerts, etc. If someone was
 accessing my server via ssh, I would likely be able to see a log of where and when the
 person logged in.
- /etc contains system-wide configuration files that control various aspects of the
 operating system and system processes. It typically includes configuration files for
 system services, networking, user accounts, and security settings.For example, the
 /etc/passwd file contains usernames and user ids while the /etc/shadow file stores
 hashed passwords.

Commands

- Is -a = the "a" flag stands for ALL so the command Is -a is "listing ALL files"
- sudo = "sudo" is short for "super user do". This is used to allow the current user to have elevated command privileges. It is commonly used to perform administrative tasks within the terminal that require higher clearance than the regular user. The sudo command prompts you for your password to confirm your identity and then allows admin privileges.
 - You can use the sudo command to update packages and software on the device within the terminal using the two commands: sudo apt update and sudo apt upgrade.

Package Management

How do you look for packages to install?

- You can search for packages using the following command: sudo apt search
 cpackage_name>. This command will list all packages that match the search term.
- You can view all available versions of a package with the command: apt list --all-versions
 cpackage_name>
- You can also see what packages have newer versions by running the command: sudo apt update and then: sudo apt upgrade to upgrade all installed packages to their newer versions.

How do you install a package?

- You can install a package using the command: sudo apt install <package_name>. This command will install the specified package and its dependencies.

How do you see what packages are already installed?

- You can check for installed packages using the command: apt list –installed. This command will list all of the system's **installed** packages.

How do you remove a package?

- You can remove a package with the command: sudo apt remove <package_name>. This command will remove the specified package but leave the configuration files. You can use the "purge" keyword to recursively delete package files and its configurations with the command: sudo apt purge <package_name>.
- After removing or purging a package, you can clean up any unused dependencies with the command: sudo apt autoremove.

Services

- You can list all running services with the command: systemctl list-units --type=service --state=running or service --status-all.
- Start a service: sudo systemctl start <service_name>
- Stop a service: sudo systemctl stop <service_name>
- Restart a service: sudo systemctl restart <service_name>
- Service status: systemctl status <service_name>

Cron Jobs

Cron Jobs are automated scripts that run on specific time intervals. You can find cron jobs in a variety of different places within the /etc directory:

- /etc/cron.hourly = hourly scripts
- /etc/cron.daily = daily scripts
- /etc/cron.weekly = weekly scripts
- /etc/cron.monthly = monthly scripts
- /etc/crontab = the system wide cron table where jobs are defined and scheduled, can be accessed by super user -> sudo
- /etc/cron.d = application specific cron jobs and system maintenance tasks
- /var/spool/cron/crontabs/<username> = user specific cron jobs are located here (you can create and edit cron jobs with the command: crontab -e)

Adding Cron Jobs

- You can add cron jobs to the current user using the crontab utility: crontab -e or the root user using the command: sudo crontab -e
- You then can add a cron job with a path to your script in this format: * * * * /path/to/your/script.sh
- You can also add a cron job file to the **/etc/cron.d** directory by using the command: sudo nano /etc/cron.d/my_cron_job. You then add the path to your script with the same format as above!

Crontab Commands:

- crontab -e = create crontab file for current user
- crontab -I = list cron jobs for the current user (my user has none hence the comments only)
- crontab -r = remove crontab file

crontab: installing new crontab onelessone@boontooboiserver:/etc/cron.d\$ crontab -1 # Edit this file to introduce tasks to be run by cron. # Each task to run has to be defined through a single line indicating with different fields when the task will be run # # and what command to run for the task # To define the time you can provide concrete values for # minute (m), hour (h), day of month (dom), month (mon), # and day of week (dow) or use '*' in these fields (for 'any'). # Notice that tasks will be started based on the cron's system daemon's notion of time and timezones. # # Output of the crontab jobs (including errors) is sent through # email to the user the crontab file belongs to (unless redirected). # For example, you can run a backup of all your user accounts # at 5 a.m every week with: # 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/ # For more information see the manual pages of crontab(5) and cron(8) m h dom mon dow command

User Management

Adding Users

- 1. sudo useradd <new_username> = adds new user
- 2. sudo passwd <new_username> = set a password for new user
- 3. sudo useradd -m <new_username> = adds a new user with a home directory (-m flag)

Removing Users

- 1. sudo userdel <username> = deletes a user (does not remove their home directory)
- 2. sudo userdel -r <username> = deletes a user and their home directory (-r flag)

File Permissions

First character indicates the type of file:

- d = directory
- - = regular file
- I = symbolic link

Next nine characters represent the permissions for the owner, group, and others:

Owner Permissions (first three characters): Example -> rwx

- r = read permission
- w = write permission
- x = execute permission

Group Permissions (next three characters): Example -> r-x

- r = read permission
- - = NO write permission
- x = execute permission

Others Permissions (last three characters): Example rw-

- r = read permission
- w = write permission
- - = NO execute permission

Changing Permissions

You can change the permissions by using the chmod command.

Numeric Method

Ex: chmod 755 <filename>

Each permission is represented by a number:

- r (read) = 4
- w (write) = 2
- x (execute) = 1

755 means:

- Owner: 7 (4+2+1 = rwx)
- Group: 5 (4+1 = r-x)
- Others: 5 (4+1 = r-x)

Symbolic Method

Ex: chmod u+rwx,g+rx,o+rx <filename>

- u (user/owner), g (group), o (others)
- + (add permission), (remove permission)

Ex: What does "drwxr-xr-x" mean?

d = directory.

rwx = the owner has read, write, and execute permissions

r-x = the group can read and execute but not write

r-x = others can read and execute but not write

Project 2: Windows Server

Below contains steps outlining the configuration of a **Windows 2022 Server** that will be used to initially configure pfSense through the admin portal in a browser and serve as an Active Directory Domain Controller. The Windows Server will start in the WAN under the Static IP Address: **10.161.21.3**.

VM Configuration

Guest OS: Microsoft Windows Server 2022 Hardware: 4 CPUs, 16 GB RAM, Thin Provision, Use Datastore ISO file ISO File: Windows Server 2022

Final Specifications

Virtual Hardware VM Options		
		ADD NEW DEVICE
> CPU	4 ~	()
> Memory	16 🗸 GB	~
> Hard disk 1	90 GB v	
> SCSI controller 0	LSI Logic SAS	
> Network adapter 1	SysAdmin021 ~	Connected
> CD/DVD drive 1	Datastore ISO File 🗸 🗸	Connected
> USB xHCl controller	USB 3.1	
> Video card	Specify custom settings 🗸	
> Security Devices	Not Configured	
VMCI device		
SATA controller 0	AHCI	



Windows Server Setup

Windows Installer

Select Language and Keyboard and then click "Next".

Microsoft Server Operating System Setup	- • ×
Microsoft	
Language to install: English (United States) <u>T</u> ime and currency format: English (United States) Keyboard or input method: IJS	
Enter your language and other preferences and click "Next" to continue.	<u>N</u> ext
Microsoft Corporation. All rights reserved.	

OS Choice: Windows Server 2022 (Desktop Experience)

Operating system	Architecture	Date modified
Windows Server 2022 Standard	x04	11/5/2022
Windows Server 2022 Datacenter	x64	11/5/2022
Windows Server 2022 Datacenter (Desktop Experience)	хб4	11/5/2022
escription: his option installs the full Windows graphical environment	, consuming extra d	ive space. It can b
escription: his option installs the full Windows graphical environment seful if you want to use the Windows desktop or have an a	, consuming extra d pp that requires it.	rive space. It can b
escription: his option installs the full Windows graphical environment seful if you want to use the Windows desktop or have an a	, consuming extra di pp that requires it.	ive space. It can b
escription: is option installs the full Windows graphical environment eful if you want to use the Windows desktop or have an a	, consuming extra di pp that requires it.	ive space. It can b

Accept Terms and Conditions 🔽

Designate a Custom Install



Do not edit the drive. Click **NEXT** to use the full partition.

		1		
Name		Total size	Free space	Туре
Drive 0 Una	allocated Space	90.0 GB	90.0 GB	
€ <u>p R</u> efresh € Load driver	Delete	Eormat	<mark>₩</mark> N <u>e</u> w	

Sit Tight and Watch the Installation Screen. If you stare too long you might become a Grandpa .

Microsoft Server Operating System Setup	×
Installing Microsoft Server Operating System	
Status	
Copying Microsoft Server Operating System files Getting files ready for installation (69%) Installing features Installing updates Finishing up	

Set Administrator Password

Custonia				
.ustomize	e settings			
Type a password for the	ne built-in administrator account that you can	use to sign in to this compute	r.	
User name				
Password				
Reenter password				
(¹ 7			Back	Finish

You will then be prompted to **restart** the device to solidify the installation.

Windows Server Configuration

Login to Windows after restart and setup Network Settings by right clicking the "Globe" on the bottom right and selecting "Open Network and Internet settings"



Navigate to Ethernet and "Change adapter options"



Right click the Ethernet icon and select "Properties"



Navigate to Internet Protocol Version 4 (IPv4) and select "Properties"



Network Configuration

Subnet: 10.161.21.0/24 (.21 is signifying the subnet I was assigned for the semester) Windows Server Static IP: **10.161.21.3**

Default Gateway: 10.161.21.1

DNS Servers: UNI DNS Servers - 10.120.16.10 and 10.120.16.11

General		
You can get IP settings this capability. Otherwis for the appropriate IP s	assigned automatically if your network suppo e, you need to ask your network administrate ettings.	rts or
Obtain an IP addre	ess automatically	
• Use the following I	P address:	
IP address:	10 . 161 . 21 . 3	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:	10 . 161 . 21 . 1	
Obtain DNS server	address automatically	
• Use the following [DNS server addresses:	
Preferred DNS server	10 . 120 . 16 . 10	
Alternate DNS server	10 . 120 . 16 . 11	
Validate settings u	upon exit Advanced	I
		-

Go to terminal and ping www.google.com to verify network connectivity



Go to Vsphere Esxi and Install "VMware Tools"

Windows Server 2	🐉 Windows Server 2022 P2 🛛 Þ 🗆 😰 🗔 🐼 🕴 🛔 actions							
Summary Monitor Configure Permissions Datastores Networks Snapshots								
		SWITC	H TO NEW VIEW					
1 1 1 1 1 1 1 1 2 1 2 1 3 1 3 1 4 1 4 1 5 1 6 1	Guest OS: Microsoft Windows Server 2022 (64-bit) Compatibility: ESX 7.0 U2 and later (VM version 19) V/Mware Tools: Not running, not installed		CPU USAGE 91 MHZ					
	MORE INFO DNS Name: D Andreases*	m	MEMORY USAGE					
	In Auresses Host: cs-vh3.cs.uni.edu		STORAGE USAGE					
	₩ 3 800 °C							
Mware Tools is not installed	on this virtual machine.	Insta	all VMware Tools					
	1							

Go back to the Windows Server 2022 VM and navigate to File Explorer to open the newly mounted DVD Drive

Vm 🛃 📃 =	Manage	DVD Drive (D:) VMware Tools	-	
File Home Share	View Application Tools			~ 🕐
← → * ↑ m > DV	/D Drive (D:) VMware Tools	ٽ ~	Search DVD Drive (D:) VMwar ,p
	Name	Date modified	Туре	Size
Cuick access Quick access ■ Desktop *	\sim Files Currently on the Disc	: (8)		
Downloads *	Program Files	10/3/2023 3:27 AM	File folder	
Documents *	🐖 autorun	10/3/2023 3:27 AM	lcon	55 KB
	autorun 🐻	10/3/2023 3:27 AM	Setup Information	1 KB
Pictures 🚿	certified	10/3/2023 3:27 AM	Text Document	1 KB
> 💻 This PC	i manifest	10/3/2023 3:27 AM	Text Document	3 KB
	🐻 setup	10/3/2023 3:27 AM	Application	43,976 KB
> I DVD Drive (D:) VMwa	setup64	10/3/2023 3:27 AM	Application	82,168 KB
> 🥏 Network	VMwareToolsUpgrader	10/3/2023 3:27 AM	Application	774 KB

VMWare Tools Install: Typical Once install is complete, **restart** the System



Windows Server Guide

Manage Installed Programs

- 1. You can access the "Control Panel" program through the Start Menu
- 2. Navigate to "Programs"
- 3. Now you can see all of the installed programs and manage them (uninstall, repair, change, etc.)

→ * ↑ 🖸 > Control F	Panel > Programs > Programs and Features			~	ල් Search Program	ns and Features	۶
Control Panel Home	Uninstall or change a program						
View installed updates	To uninstall a program, select it from the list and then	click Uninstall, Change, or Repa	ir.				
Turn Windows features on or							
off	Organize 🔻						(
	Name	Publisher	Installed On	Size	Version		
	💽 Microsoft Edge	Microsoft Corporation	2/7/2025		132.0.2957.140		
	Microsoft Visual C++ 2015-2022 Redistributable (x64)	Microsoft Corporation	2/6/2025	20.6 MB	14.36.32532.0		
	Microsoft Visual C++ 2015-2022 Redistributable (x86)	Microsoft Corporation	2/6/2025	18.0 MB	14.36.32532.0		
	VMware Tools	VMware, Inc.	2/6/2025	102 MB	12.3.5.22544099		

Show Hidden Files and Directories

Navigate to File Explorer and select "View" on the top bar. After selecting "View", select the "Options" module

🗧 📄 📝 🔜 🗢 🛛 File Explo	er		– 🗆 X
File Home Share	View		-# 😮
Navigation Details pane	■ Extra large icons ■ Large icons ■ Medium icons Small icons ■ Extra large icons ■ Extra large icons Small icons ■ Extra large icons ■ Extra large icons Small icons ■ Extra large icons ■ Extra large icons Small icons ■ Extra large icons ■ Extra large icons Small icons ■ Extra large icons ■ Extra large icons Tiles ■ Content ▼	Group by * Hencheck hoxes Mid columns * File name extensions Sort ***** by * Hidden items	9 Options
Panes	Layout	Current view Show/hide	
Desktop 🛪	This PC	This PC	This PC

A popup will appear. Navigate to "View" in the top bar and then select "Show hidden files, folders, and drives".

After selection, click "Apply". Hidden files and folders will now be visible in the File Explorer GUI. **Hidden files and folders will generally appear with less opacity** (transparent) while files that are always visible still appear with full opacity.

Example: ProgramData Folder (now visible)

≝ 🖸 📴 🚽 File Home Share	Manage Loca View Drive Tools	Disk (C:)		
← → × ↑ 🟪 > Th	is PC > Local Disk (C:) >			
	Name	Date modified	Туре	Size
Quick access	SWinREAgent	2/6/2025 5:51 PM	File folder	
Desktop 🖈	PerfLogs	5/8/2021 1:20 AM	File folder	
👆 Downloads 🛛 🖈	Program Files	2/6/2025 5:55 PM	File folder	
🔮 Documents 🛛 🖈	Program Files (x86)	5/8/2021 2:39 AM	File folder	
📰 Pictures 🛛 🖈	ProgramData	2/6/2025 5:55 PM	File folder	
This DC	Users	2/7/2025 1:30 AM	File folder	
inis PC		2/6/2025 5:56 PM	File folder	
🖆 DVD Drive (D:) SSS_Xt				
🥏 Network				

Windows System Logs

Launch "Event Viewer" from the Start Menu

i i	col Convor				
		٢			
	Best match				
	Event App	Viewer			
	𝒫 event Vi	ewer		Ξi	0

Once in the application, you can use the side menu to select from a variety of categories and view their logs



You can	click on	an individual	loa	(event)	and	see i	ts exact	details
rou can		annunuuuu	iug	(CvCnt)	anu	300 1		ucians

Engine sta	te is cha	nged from Available to Sto	pped.		^	
Details: P S	JewEngir PreviousE Requence	neState=Stopped ngineState=Available Number=15			~	4
Log Name: Source:		Windows PowerShell PowerShell (PowerShell)	Logged:	2/6/2025 7:02:42 PM		4
Event ID:		403	Task Category:	Engine Lifecycle		
Level:		Information	Keywords:	Classic		
User:		N/A	Computer:	WIN-U00T4AO1ET9		
OpCode:		Info				
More Infor	mation:	Event Log Online Help				

Windows Services Manager

The Windows Services Manager is a tool that allows you to manage the services running on your Windows operating system. Services are background processes that perform various functions, such as networking, security, and system maintenance.

Launch "Services" from the Start Menu to access the Services Manager.

		Servern							
		Services					-		X
i L		File Action View	Help						
	Best match		🛓 🚺 🖬 🕨 🖉 🖬 🖬 🖬						
		e 💮 Services (Local)	O Septices (Local)						_
	Services	A	Scivices (Eoculy					φ.	
	Ann		Select an item to view its description.	Name	Description	Status	Startup lyp	e l	Log
		1		ActiveX Installer (AxInstSV)	Provides Us		Disabled	1	LOCI
	Apps			AllJoyn Router Service	Routes AllJo		Manual (Tr	ig I	LOCI
	7PP3			App Readiness	Gets apps re		Manual	I	LOCi
	Microsoft Azure Services			Application Identity	Determines		Manual (Tr	ig I	Toci
	- Interosoft Azare Services			Application Information	Facilitates t		Manual (Tr	ig I	Toc
	Component Services			Application Layer Gateway	Provides su		Manual	1	LOCI
	Component Services			Application Management	Processes in		Manual	1	Loci
				AppX Deployment Service (Provides inf		Manual (Tr	ig I	Toci
				Auto Time Zone Updater	Automatica		Disabled	1	Toci
				Background Intelligent Tran	Transfers fil		Manual	1	Toci
				Background Tasks Infrastruc	Windows in	Running	Automatic	1	LOCI
				Base Filtering Engine	The Base Fil	Running	Automatic	a. 1	Loci
				Bluetooth Support Service	The Bluetoo		Manual (Tr	ig I	Toci
				Capability Access Manager	Provides fac	Running	Manual	1	Loci
				CaptureService_9a615c	Enables opti		Manual	1	Loci
				Certificate Propagation	Copies user		Manual (Tr	ig I	Loci
				Client License Service (ClipS	Provides inf		Manual (Tr	ig I	Loci
				Clipboard User Service_9a61	This user ser	Running	Automatic	(Loci
				CNG Key Isolation	The CNG ke	Running	Manual (Tr	ig I	Loci
				COM+ Event System	Supports Sy	Running	Automatic	1	Loci
				COM+ System Application	Manages th	Running	Manual		Loci 🗸
				<					>
			Extended Standard						
	🔎 servcies 📃 🔂								

You can **start/stop/restart** a service in the Services Manager by selecting or right clicking the desired service.

Extensible Authentica	tion P The Extensi		Manual	Loci
Sunction Discover	Chard .	Running	Manual	Loca
🏟 Function Discover	Start	Running	Manual (Trig	Loci
🔍 Geolocation Servic	Stop		Disabled	Loci
GraphicsPerfSvc	Pause		Disabled	Loci
🖏 Group Policy Clier	Resume	Running	Automatic (T	Loci
🎑 Human Interface [Restart		Manual (Trig	Loci
🖏 HV Host Service			Manual (Trig	Loci 🗸
<	All Tasks >			>
	Refresh			
	Properties			
	Help		BPA resu	ults
		70		

You can configure a service to start automatically by navigating to "Properties" after right clicking. You then can customize the Startup type to "Automatic".

Function	Discover	y Provider I	Host Properti	es (Local Cor	nputer)	Х		
General	Log On	Recovery	Dependencie	s				
Service	name:	fdPHost						
e Display	name:	Function D	iscovery Provid	der Host				
Descript	ion:	The FDPH Discovery	OST service h (FD) network d	osts the Funct iscovery provi	ion ders. These	•		
Path to C:\Wind	Path to executable: C:\Windows\system32\svchost.exe +k LocalService -p							
Startup f	type:	Automatic			~	/		
Sentice	atatua:	Automatic Automatic Manual Disabled	(Delayed Start)				
s Service	tart	Stop)	Pause	Resume			
You car from her	n specify th e.	ne start para	meters that app	bly when you s	tart the service			
Start pa	rameters:							
			ОК	Cancel	Арріу	/		

Add/Delete Local Users

Navigate to "Settings" and then the "Accounts" tab. Once in Accounts, select "Other Users".

← Settings		9 <u>00</u>	×
命 Home	Other users		
Find a setting	Other users		-
Accounts	+ Add someone else to this PC		
RE Your info			
🖓 Sign-in options			
A. Other users			

After selecting the "+", a menu should appear with a "Users" and "Groups" folder in the left bar.



Click on the "Users" folder and then right click to bring up a popup menu to add a "New User".



You will be prompted to enter information about the new user. Once the user is created it will show up in the Users directory.

		- 11	
New User		?	×
User name:	Test		
Full name:	Test User		
Description:	This is a test		
Password:	•••••		
Confirm passwo	••••••••		
User must c	hange password at next logon		
User cannot	t change password		
Password n	ever expires		
Account is a	lisabled		
Help	Сгеа	te Clo	se

You can delete a user by right clicking an existing user and selecting "Delete".



Task Scheduler

Windows has a built-in tool called Task Scheduler. It functions similarly to a crontab where you can put when and how often you want a script to execute.



Launch "Task Scheduler" from the Start Menu

Use the left side menu to see existing Windows Tasks

Task Sche	duler				×
File Action	View Help			 	
Task Schee	duler (Local) cheduler Library crosoft	Itask Scheduler Summary (Last refreshed: 2/1 Overview of Task Scheduler Image: Scheduler to create and manage common tasks that your computer will carry out automatically at the Task Status Sta Last 24 hours Summary: 0 total - 0 running, 0 Task Name Last refreshed at 2/10/2025 7:39:02 PM	Actions Task Scheduler (Local) Connect to Another Computer Import Task Display All Running Tasks Enable All Tasks History AT Service Account Configuration View Refresh Help		•
hormanice		renonnance			

Task Scheduler			(12)	×
File Action View Help				
Task Scheduler (Local) Task Scheduler Library Task Scheduler Library Microsoft	Task Scheduler Summary (Last refreshed: 2/1 Overview of Task Scheduler You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the Task Status Sta Last 24 hours Summary: 0 total - 0 running, 0 Task Name Last refreshed at 2/10/2025 7:39:02 PM	Actions Task Scheduler (Local) Connect to Another Computer Create Basic Task Import Task Import Task Display All Running Tasks Enable All Tasks History AT Service Account Configuration View Refresh Help		•
3r				

You can create a new task on the right side menu with "Create Basic Task"

Add "Task Name" and "Description"

Create Basic Task Wizard		×
Create a Basic Task	:	
S		
Create a Basic Task Trigger	Use this wizar such as multi	d to quickly schedule a common task. For more advanced options or settings ple task actions or triggers, use the Create Task command in the Actions pane.
Action	Name:	Test Task
Finish	Description:	Add task desciption here
		< Back Next > Cancel

Add a task "Trigger"

Create a Basic Task	When do you want the task to start?
Trigger	Daily
Daily	O Washing
Action	O Weekly
Start a Program	O Monthly
Finish	One time
	○ When the computer starts
	O When I log on
	O When a specific event is logged

Select when you would like the task to **repeat**

Create a Basic Task	Start: 2/10/2025 T:44:17 PM
Trigger	
Daily	Recur every: 1 days
Action	
Start a Program	
Finish	

Select task Action

Create a Basic Task Trigger Daily	What action do you want the task to perform?
Action	Start a program
Start a Program	○ Send an e-mail (deprecated)
Finish	 Display a message (deprecated)

Configure the script you would like to execute

Create a Basic Task		
Trigger	Program/script:	
Daily	C:\Path\To\Your\Script	Browse
Action		
Start a Program	Add arguments (optional):	
Finish	Start in (optional):	

Confirm your new Task

Create a Basic Task		
Trigger	Name:	Test Task
Daily	Description:	Add task desciption here
Action		
Start a Program		
Finish		
	Trigger	Daily: At 7:44 PM every day
	inggei.	
	Action:	Start a program; C:\Path\To\Your\Script
	Open the	Properties dialog for this task when I click Finish
	When you cli	ck Finish, the new task will be created and added to your Windows schedule.
		< Back Finish Cancel

Server Roles

Open Windows Server Manager and go to the top right and select the drop down menu named "Manage". Then choose "Add Roles and Features".



Set Installation Type to "Role-based or feature-based installation"

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

O Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select the desired server

Select a server or a virtual hard disk on which to install roles and features.

- $\ensuremath{\textcircled{}}$ Select a server from the server pool
- O Select a virtual hard disk

Server Pool Filter:			
Name	IP Address	Operating System	
WIN-U00T4AO1ET9	10.161.21.3	Microsoft Windows Server 2022 Standard	

Designate Server Roles. Ex: Web Server (IIS)

Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	Active Directory Certificate Services	Web Server (IIS) provides a reliable,
Server Roles	Active Directory Domain Services	manageable, and scalable Web
Features	Active Directory Federation Services Active Directory Lightweight Directory Services	application infrastructure.
Web Server Role (IIS)	Active Directory Rights Management Services	
Role Services	Device Health Attestation DHCP Server	
Confirmation	DNS Server	
	Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Volume Activation Services Windows Deployment Services Windows Server Update Services	

Select desired Features

Installation Type Features Server Selection MET Framework 3.5 Features Server Roles Installation Transfer Service (BITS) Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Containers Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management Host Guardian Hyper-V Support I/O Quality of Service IIS Hostable Web Core Internet Printing Client 	server.	
Server Selection Server Roles Peatures Web Server Role (IIS) Role Services Confirmation Results Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management Host Guardian Hyper-V Support I/VO Quality of Service I/S Hostable Web Core I/S Hostable Web Core		Description
Features Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Confirmation Containers Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management Host Guardian Hyper-V Support I/O Quality of Service IIS Hostable Web Core Internet Printing Client 	^	.NET Framework 3.5 co power of the .NET Fran
Web Server Role (IIS) BitLocker Network Unlock Role Services Client for NFS Confirmation Containers Results Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management Host Guardian Hyper-V Support I/O Quality of Service IIS Hostable Web Core IIs Hostable Web Core		APIs with new technolo building applications th
Confirmation Containers Containers Confirmation Containers Data Center Bridging Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management Host Guardian Hyper-V Support V/O Quality of Service IIS Hostable Web Core IIS Hostable Web Core IIs Hostable Web Core		your customers' persor information, enable sea
IP Address Management (IPAM) Server	~	secure communication, the ability to model a r business processes.

nbines the ework 2.0 gies for at offer es, protect al identity mless and and provide nge of

Configure Role Services



Confirm and Install

Before You Begin	To install the following roles, role services, or features on selected server, click Install.
Installation Type	Restart the destination server automatically if required
Server Selection	Optional features (such as administration tools) might be displayed on this page because they have
Server Roles	been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Features	
Web Server Role (IIS)	Web Server (IIS)
Role Services	Management Tools
Confirmation	Web Server
	Common HTTP Features Default Document Directory Browsing HTTP Errors Static Content
	Health and Diagnostics
	Export configuration settings Specify an alternate source path
	< Previous Next > Install Cancel

Remote Desktop

You can track Remote Desktop (RDP) status by going to "Local Server" in the left side menu.



Project 3: pfSense Firewall

Below contains steps outlining the configuration of a **pfSense firewall** for my network cluster. It will be hosted in the WAN and allow me to configure two internal networks: **LAN** and **DMZ**. A DHCP server will be hosted on the LAN for "company workstations" and the DMZ will be reserved for servers that need to operate in a less secure network environment, such as the Ubuntu and Windows servers. The pfSense firewall will be operating within the WAN under the static IP Address: **10.161.21.4**.

A **DMZ (Demilitarized Zone)** is a local network that is separate from a business's private LAN. This isolated network enhances security by allowing external-facing services to communicate with the open internet while keeping the internal network protected.

VM Configuration

Guest OS: Free BSD 13 or later (64 bit) Hardware: 2 CPUs, 8 GB RAM, Thin Provision, 3 Network Adapters Use Datastore ISO file ISO File: pfSense 2.7.2

Virtual Hardware VM Options ADD NEW DEVICE > CPU 2 **(i)** \sim > Memory GB 🗸 \sim > Hard disk 1 30 GB 🗸 > SCSI controller 0 VMware Paravirtual > Network adapter 1 Connected SysAdmin021 ~ > Network adapter 2 Connected SysAdmin021 ~ > Network adapter 3 Connected SysAdmin021 ~ > CD/DVD drive 1 Connected Datastore ISO File > Video card > Security Devices Not Configured VMCI device

Final Specifications

pfSense Setup

Network Configuration

- Use "zfs" partitioning
- Select the" VMware Virtual Disk"
- Enter NICs for the WAN, LAN, and DMZ
 - **WAN =** vmx0
 - **LAN** = vmx1
 - Optional 1 (**DMZ**) = vmx2

LAN (default to **192.168.1.1/24**)

WAN Setup

- Adapter vmx0
- pfSense WAN Address set to: 10.161.21.4/24
- WAN Upstream Gateway set to: 10.161.21.1
- Set as "Default Gateway"
- No IPv6
- No DHCP on WAN

DMZ Setup

- Adapter vmx2
- DMZ Gateway address set to: 192.168.2.1/24
- No WAN Usptream Address
- No IPv6
- No DHCP

Final Configuration:

Reloading routing configuration DHCPD	
The IPv4 WAN address has been set to 1	10.161.21.4/24
Press <enter> to continue. UMware Virtual Machine - Netgate Devic</enter>	ce ID: 1d35710f0c7d1d90a3b5
*** Welcome to pfSense 2.7.2-RELEASE ((amd64) on pfSense ***
WAN (wan) -> VMXØ -> V4: LAN (lan) -> VMX1 -> V4: OPT1 (opt1) -> VMX2 -> V4:	10.161.21.4/24 192.168.1.1/24 192.168.2.1/24
 Ø) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host 8) Shell 	9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) PHP shell + pfSense tools 13) Update from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration 16) Restart PHP-FPM

The interfaces will be assigned as follows:

Do you want to proceed [yin]? y

pfSense Configuration

Navigate to 192.168.1.1 in a browser and sign in

- Default Credentials
- Username: admin
- Password: pfsense

General Information

- Hostname: pfSense
- Domain: home.arpa
- Primary DNS Server: 10.120.16.10
- Secondary DNS Server: 10.120.16.11
- Override DNS: 🔽

Time Server (leave default)

WAN Configuration

Wizard / pfSense	Setup / Configure WAN Interface
	Step 4 of 9
Configure WAN Inter	face
	On this screen the Wide Area Network information will be configured.
SelectedType	Static 🗸
General configuration	n
MAC Address	This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxxxxx or leave blank.
МТU	Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration	on
IP Address	10.161.21.4
Subnet Mask	24 🗸
Upstream Gateway	10.161.21.1


Uncheck RFC1918 Networks and Bogon Networks

RFC1918 Networks	
Block RFC1918 Private Networks	Block private networks from entering via WAN when set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
Block bogon networl	ks
Block bogon networks	Block non-Internet routed networks from entering via WAN when set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

LAN Configuration

Configure LAN Interf	ace
	On this screen the Local Area Network information will be configured.
LAN IP Address	192.168.1.1
	Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24 🗸
	_
	» Next

Final System Info:

System Inform	ation 🥕 🖨 😵
Name	pfSense.home.arpa
User	admin@192.168.1.101 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 1d35710f0c7d1d90a3b5
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT
	Version information updated at Fri Feb 14 18:36:28 UTC 2025 🗲
СРИ Туре	Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	2 Days 00 Hour 06 Minutes 32 Seconds
Current date/time	Fri Feb 14 18:37:19 UTC 2025
DNS server(s)	127.0.0.110.120.16.1010.120.16.11
Last config change	Fri Feb 14 18:35:38 UTC 2025

DHCP Setup

Edit the DHCP Server

all -	Services - VPN	✓ Sta
	Auto Config Backup	
	Captive Portal	
	DHCP Relay	
	DHCP Server	Netga
	DHCPv6 Relay	
ie)	DHCPv6 Server	
	DNS Forwarder	_
Da3b5	DNS Resolver	
	Dynamic DNS	
	IGMP Proxy	If you p
	NTP	Comm
1	PPPoE Server	the NE
	Router Advertisemen	t You als
	SNMP	Suppor
14 18:	UPnP & NAT-PMP	more ti
30GHz	Wake-on-LAN	• Up

Set DHCP Range: 192.168.1.101 to 192.168.1.254

Primary Address Poo	51
Subnet	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	192.168.1.101 192.168.1.254 From To
	The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Configure LAN DNS

Server Options	
WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	10.120.16.10
	10.120.16.11
	DNS Server 3
	DNS Server 4

REMINDER: Save settings at the bottom of the screen and then Apply Changes at the top

Custom DHCP Options	Display Advanced		
	Save		

	Interfaces 🗸	Firewall 🗸	Services 🗸	VPN -	Status 🕶	Diagnostics 🗸
Interfaces / OPT1 ()	Assignments					
interfaces/ of fr(WAN					
General Configuration	LAN					
Enable	OPT1					
Description	MZ					

Change to OPT1 Interface and rename to DMZ -> Save and Apply Changes

Enter a description (name) for the interface here.

Firewall Rules

Navigate to Firewall menu



Use the bottom menu to add, delete, edit, and reorder firewall rules.

• NOTE: Order does matter, rules that are higher on the list have more priority



WAN Firewall Rules



LAN Firewall Rules

F	irew	all / Rule	es/LAN									Lill 📰 😮
F	oatin	g WAN	LAN DI	МZ								
R	ules	(Drag to Cl	hange Order)									
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	1/6.74 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$
	~	0/0 B	IPv4 TCP/UDP	LAN subnets	*	DMZ subnets	*	*	none		ALLOW ALL OUT TO DMZ	ϑ聋▣⊘亩×
	~	5/26 KiB	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none		ALLOW DNS OUT	ϑ聋⊡⊘ <u>ڨ</u> ×
	~	4/1.51 MiB	IPv4 TCP/UDP	LAN subnets	*	*	443 (HTTPS)	*	none		ALLOW HTTPS OUT	ϑ聋▣⊘ <mark>亩×</mark>
0	~	0/4 KiB	IPv4 TCP/UDP	LAN subnets	*	*	80 (HTTP)	*	none		ALLOW HTTP OUT	ϑ聋⊡⊘ā×
	~	0/0 B	IPv4 ICMP echoreg	LAN subnets	*	*	*	*	none		ALLOW PING OUT	ᢤᢧ᠒ᢆ᠐ <u>ᡎ</u> ×

DMZ Firewall Rules

Fi	Firewall / Rules / DMZ									Lill 🗐 🕄		
Flo	pating	WAN	LAN	DMZ								
	Rules (Drag to Change Order)											
Ru	les (Drag to C	hange Or	der)								
Ru	iles (I	Drag to C States	hange Or Protocol	der) Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	iles (l 🐣	Drag to C States 0/4 KiB	Protocol	der) Source DMZ subnets	Port *	Destination LAN subnets	Port *	Gateway *	Queue none	Schedule	Description REJECT ALL TO LAN	Actions

Internal Device Placement

Windows Server (DMZ)

Go into Network and Internet Settings to edit the "Ethernet Adapter" DMZ Static IP: **192.168.2.2**

	Internet Protocol Version 4 (TCP/IPv4) Properties	×
1	General		
h	You can get IP settings assigned auto this capability. Otherwise, you need to for the appropriate IP settings.	matically if your network supports o ask your network administrator	
E	Obtain an IP address automatica	lly	
П	Ouse the following IP address:		
E	IP address:	192.168.2.2	
	Subnet mask:	255.255.255.0	
	Default gateway:	192.168.2.1	
C	Obtain DNS server address auto	matically	
	Use the following DNS server add	dresses:	
	Preferred DNS server:	10 . 120 . 16 . 10	
	Alternate DNS server:	10 . 120 . 16 . 11	
	Ualidate settings upon exit	Advanced	
-		OK Cancel	

Add a firewall rule to allow inbound pinging of the Windows Server

which this rule applies.	Customize ICMP Settings	×
To which ports and protocols does this rule apply?	Apply this rule to the following Internet Control Message Protocol (ICMP) connections:	on
Protocol type: ICMPv4 ✓ Protocol number: 1 ↔ Local port: All Ports ✓ Example: 80, 443, 5000-5010 Remote port: All Ports ✓ Example: 80, 443, 5000-5010 Internet Control Message Protocol (ICMP) settings:	Specfic ICMP types Packet Too Big Destination Unreachable Source Quench Redirect Echo Request Router Advertisement Router Solicitation Time Exceeded Parameter Problem Timestamp Request Address Mask Request	to i
	This ICMP type: Type: 0 V Code: Any Add	
< Back	ОК Салс	el
Inbound Rules		
Name	Group Profile	• ^
🧭 ICMP Echo Request OK	All	

Ubuntu Server (DMZ)

Change directories to /etc/netplan Edit the network config file with: **sudo nano 50-cloud-init.yaml** DMZ Static IP: **192.168.2.3** Refresh the network: **sudo netplan apply**



Windows Client Setup (LAN)

Creating the following 2 Windows clients will simulate workstations in my company. They will be positioned in the LAN and the pfSense DHCP server should automatically issue out individual network configurations.

Windows Setup for Local Accounts (No Microsoft Email Required):

- 1. I disconnected the VM network card once each computer was in the final "windows setup" mode.
- 2. I then ran the following commands to bypass the required network setup so that I could create local system accounts:
 - a. **Shift + f10** -> Brings up a command prompt
 - b. Command: OOBE\BYPASSNRO (Out Of Box Experience command)
- 3. Once through setup without internet, reconnect the network adapter!

Windows 11 Workstation-01

Username: Bill Password: **Classified**

Windows 11 Workstation-02 Username: Fernando

Password: **Classified**

NOTE: "Bob" is the answer for all security questions!!!

Project 4: Internal Caching DNS

Below contains steps outlining the configuration of an **internal caching DNS server** on my **pfSense firewall** which already manages DHCP. The internal DNS server will allow connected machines to have fast internet access due to IP caching. Additionally, its integration with the existing DHCP service will automatically configure DNS settings for LAN clients.

The **DNS Resolver** service within pfSense is easily integrated with the DHCP server. Having pfSense manage both allows clients connecting to the LAN to be issued an IP and the internal caching server simultaneously. The internal caching server also allows configuration of "static IPs" within the LAN for specific use cases. The IP address of the internal caching DNS Server is **192.168.1.1**. Since the DNS server is hosted on the firewall, DMZ clients can access it through the DMZ gateway address, which is **192.168.2.1**. This setup is beneficial as it allows the firewall to maintain a REJECT ALL traffic rule from the DMZ to the LAN.

DNS Resolver Configuration

To configure the internal DNS Resolver (Unbound) navigate to Services > DNS Resolver



Enable the DNS Resolver

Keep all ports default (Port 53)

Set Network Interfaces and Outgoing Network Interfaces to "All"

Disable DNSSEC (does not integrate well with UNI DNS Servers)

Enable DNS Query Forwarding, DHCP Registration, Static DHCP

Add "Host Overrides" at the bottom of the page for the LAN and DMZ

• This will allow the LAN and DMZ to fetch a hostname for the firewall for whichever gateway is being used by the client.

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
pfsense	slick.firewall	192.168.1.1	pfSense LAN DNS	er 🛅
pfsense-dmz	slick.firewall	192.168.2.1	pfSense DMZ DNS gateway	ø 💼
Enter any individual esolver. Standard a somesite.com'. Any	hosts for which the resolver's standard [nd also non-standard names and parent lookup attempt for the host will automa	NS lookup process should be overridden domains can be entered, such as 'test', 'na tically return the given IP address, and the	and a specific IPv4 or IPv6 address should automa s.home.arpa', 'mycompany.localdomain', '1.168.19; usual lookup server for the domain will not be quer	tically be returned by the 2.in-addr.arpa', or ried for the host's records.

LAN: pfsense.slick.firewall

Host Override Option	Host Override Options				
Host	pfsense				
	Name of the host, without the domain part e.g. enter "myhost" if the full domain name is "myhost.example.com"				
Domain	slick.firewall				
	Parent domain of the host e.g. enter "example.com" for "myhost.example.com"				
IP Address	192.168.1.1				
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3				
Description	pfSense LAN DNS				
	A description may be entered here for administrative reference (not parsed).				

DMZ: pfsense-dmz.slick.firewall

Host Override Options		
Host	pfsense-dmz	
	Name of the host, without the domain part e.g. enter "myhost" if the full domain name is "myhost.example.com"	
Domain	slick.firewall	
	Parent domain of the host e.g. enter "example.com" for "myhost.example.com"	
IP Address	192.168.2.1	
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3	
Description	pfSense DMZ DNS gateway	
	A description may be entered here for administrative reference (not parsed).	

DHCP Configuration

To configure DHCP navigate to **Services > DHCP Server** Then make sure you are on the **LAN** tab.

Sense System	 Interfaces - 	Firewall +	Services -	VPN +	
Services / DHCP	Server / LAN		Auto Config B Captive Porta DHCP Relay	3ackup II	
ISC DHCP has reached end	l-of-life and will be rem	oved in a future	DHCP Server		em :
WAN LAN DM2	z		DHCPv6 Rela DHCPv6 Serv DNS Forward	y er er	
General DHCP Option	าร		DNS Resolve		
DHCP Backend	ISC DHCP	_	IGMP Proxy		
Enable	Enable DHCP se	erver on LAN inter	NTP	. [
BOOTP	Ignore BOOTP q	ueries	Router Adver	tisement	
Deny Unknown Clients	Allow all clients		SNMP	1	-
	When set to Allow a interface, any DHCI clients from only th	all clients, any DH P client with a MA is interface, only	UPnP & NAT-		napp tic m

Ensure DHCP is **enabled** on LAN

General DHCP Options				
DHCP Backend	Backend ISC DHCP			
Enable 🖾 Enable DHCP server on LAN interface				
BOOTP Ignore BOOTP queries				
Deny Unknown Clients	Allow all clients			
	When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.			
Ignore Denied Clients	Ignore denied clients rather than reject			
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.				
Ignore Client Identifiers	Do not record a unique identifier (UID) in client lease data if present in the client DHCP request			
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that server behavior violates the official DHCP specification.				

Ensure primary address pool is within the LAN subnet

Primary Address Pool				
Subnet	192.168.1.0/24			
Subnet Range	192.168.1.1 - 192.168.1.254			
Address Pool Range	192.168.1.101	192.168.1.254		
	From	То		
	The specified range for this pool must not be within the range configured on any other address pool for this interface.			
Additional Pools	Pools + Add Address Pool			
	If additional pools of addresses are needed inside of this subnet outside th	e above range, they may be specified here.		

Configure the DHCP issued DNS Server to be the internal caching server: 192.168.1

Serve	Server Options				
	WINS Servers	WINS Server 1			
		WINS Server 2			
	DNS Servers	192.168.1.1			
		DNS Server 2	·]		
		DNS Server 3			
		DNS Server 4			

System Configuration

To ensure requests are forwarded from the internal caching server to the local recursive DNS servers navigate to **System > General Setup**

	System +	Interfaces +
Status / F	Advanced	
	General Setu	p
System Info	High Availab	ility
Name	Package Ma	nager
User	Register	02 (Loci
System	Routing	hine
	Setup Wizard	135710
BIOS	Update	hnologi
	User Manage	er ov 12 20
Version	Logout (adm	in) 164)

Ensure your Local Recursive DNS servers are properly configured In this case I have the UNI DNS Servers: **10.120.16.10** and **10.120.16.11**

DNS Server Settings	DNS Server Settings				
DNS Servers	10.120.16.10	DNS Hostname	Delete		
	10.120.16.11	DNS Hostname	Delete		
	Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).			
Add DNS Server	+ Add DNS Server				
DNS Server Override	Allow DNS server list to be overridden by DHCP/PPP on If this option is set, pfSense will use DNS servers assigned I for its own purposes (including the DNS Forwarder/DNS Ret	WAN or remote OpenVPN server by a DHCP/PPP server on WAN or a remote OpenVPN server). However, they will not be assigned to DHCP client	ver (if Pull DNS option is enabled) s.		
DNS Resolution Behavior	Use local DNS (127.0.0.1), fall back to remote DNS Servers By default the firewall will use local DNS service (127.0.0.1, remote DNS servers otherwise. Use this option to choose al	■ (Default ▼) DNS Resolver or Forwarder) as the first DNS server when ternate behaviors.	possible, and it will fall back to		

Ubuntu DNS Config

To connect the Ubuntu server statically set to 192.168.2.3 in the DMZ to the internal DNS hosted by the pfSense firewall do the following:

Edit the netplan file: sudo nano /etc/netplan/50-cloud-init.yaml

Replace the current name server addresses with **192.168.2.1**

Since the server is on the firewall, the <u>DMZ gateway address</u> should allow the server to utilize the internal DNS Resolver that was configured.



Refresh the network with the command: sudo netplan apply

Test your name server with the command: **resolvectl status** It should output the internal caching DNS IP which is pfsense-dmz.slick.firewall:**192.168.1.1**



Test the DNS connection with the command: nslookup google.com

onelessone@boon Server: Address:	tooboiserver:/etc/netplar 127.0.0.53 127.0.0.53#53	\$ nslookup	google.com
Non-authoritation Name: google. Address: 142.25 Name: google. Address: 2607:f8	ve answer: com 1.32.14 com 8b0:4009:81c::200e		

Windows DNS Config

To connect the Windows server statically set to 192.168.2.2 in the DMZ to the internal DNS hosted by the pfSense firewall do the following:

Navigate to edit the server's ethernet connection



Edit the "Properties" of the adapter and then select "Internet Protocol Version 4"



Set the "Preferred DNS server" to 192.168.2.1

neral	
ou can get IP settings assigned aut is capability. Otherwise, you need r the appropriate IP settings.	omatically if your network supports to ask your network administrator
Obtain an IP address automatic	cally
Use the following IP address: –	
IP address:	192.168.2.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.2.1
Obtain DNS server address aut	omatically
Use the following DNS server a	ddresses:
Preferred DNS server:	192 . 168 . 2 . 1
Alternate DNS server:	

Test your name server with the command: **nslookup** It should output the internal caching DNS IP which is pfsense-dmz.slick.firewall:192.168.1.1

Administrator: Windows PowerShell PS C:\Users\Administrator> nslookup Default Server: pfsense-dmz.slick.firewall Address: 192.168.2.1

Test the DNS connection with the command: nslookup google.com

```
PS C:\Users\Administrator> nslookup google.com
Server: pfsense-dmz.slick.firewall
Address: 192.168.2.1
Non-authoritative answer:
Name: google.com
Addresses: 2607:f8b0:4009:819::200e
142.250.191.174
```

LAN Client Testing

If you properly configured the internal caching DNS server, you should be able to do the following in a terminal from a LAN machine:

Test the functionality and verify the DNS Server is the correct address with the command: **nslookup google.com**

The DNS Address came back as **192.168.1.1** which is perfect because that is what was configured!



Test caching with the dig command: dig mlb.com

Run the command twice. The first query should be much longer than the second!



Project 5: External DNS

Below contains steps outlining the configuration of an **external DNS server**. The external DNS server will be hosted on the **Ubuntu Server** using **BIND**. This server will respond to queries on the public and private side of the firewall and will resolve requests made to the two servers in the DMZ (Windows and Ubuntu). Within the BIND configuration, FQDNs will be created and mapped to each DMZ server. Doing this will allow clients to query the DMZ servers by a domain name such as "www.mywebsite.com" instead of by IP address.

DNS Information

pfSense firewall: 10.161.21.4

FQDN Mappings: www.slickbrickcentral.com -> **192.168.2.3** ubuntu.slickbrickcentral.com -> **192.168.2.3** win.slickbrickcentral.com -> **192.168.2.2**

Ubuntu DNS Server

BIND (Berkeley Internet Name Domain) is a software that maps **FQDNs** (Fully Qualified Domain Names) to IP addresses. It is open source and can be configured to serve as an authoritative DNS server, a caching DNS server, or both. A **local authoritative DNS** server will be hosted under the static DMZ IP address: **192.168.2.3**.

BIND Installation

Run the following commands to install BIND:

- 1. sudo apt update
- 2. sudo apt install bind9 bind9utils bind9-doc

Configure BIND to use IPv4 protocol: **sudo nano /etc/default/named** Add -4 to the end of the **OPTIONS** parameter:



Restart BIND to implement the changes: sudo systemctl restart bind9

BIND Configuration

Main Configuration File: named.conf.options Open the config file: sudo nano /etc/bind/named.conf.options

If you want to forward unknown queries, uncomment and update the "forwarders" section with your DNS servers: **UNI DNS Servers**: **10.120.16.10** and **10.120.16.11**.



I however do NOT want to forward queries. I want BIND to resolve only mappings I configure locally!

Add the following lines to disable forwarding



Additional lines for logging in a new section below "options"



Access logs with the command: sudo tail -f /var/cache/bind/named.log

DNS Zones

Edit the local configuration file to define your DNS Zones: sudo nano /etc/bind/named.conf.local

This file specifies the DNS zones that BIND will manage.

I will be using *slickbrickcentral.com* as my company domain (you can change this out). Also, since the DNS is in the DMZ subnet (192.168.2.0/24), I will use **2.168.192** in the second zone designation!



Forward Lookup Zone

Create the forward lookup zone file: sudo nano /etc/bind/db.slickbrickcentral.com

This file maps domain names to IP addresses.

Add the following content to the newly created file:

GNU	nano 7.2		/etc/bind/db.slickbrickcentral.com *
\$TTL	604800		
C	IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
; @	IN	NS	ns1.slickbrickcentral.com.
ns1	IN	A	192.168.2.3
ພພພ	IN	A	192.168.2.3
-			

Reverse Lookup Zone

Create the reverse lookup zone file: sudo nano /etc/bind/db.192

This file maps IP addresses back to domain names.

Add the following content to the newly created file:

GNU	nano 7.2		/etc/bind/db.192 *
\$TTL	604800		
Q	IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
, e o	IN IN	NS PTR	ns1.slickbrickcentral.com. www.slickbrickcentral.com.

<u>Check for Errors</u> Check the config files for syntax errors: sudo named-checkconf sudo named-checkzone slickbrickcentral.com /etc/bind/db.slickbrickcentral.com sudo named-checkzone 2.168.192.in-addr.arpa /etc/bind/db.192

If there are no errors the command output should be as follows:

onelessone@boontooboiserver:/etc/netplan\$ sudo named-checkconf onelessone@boontooboiserver:/etc/netplan\$ sudo named-checkzone slickbrickcentral.com /etc/bind/db.slickbrickcentral.com zone slickbrickcentral.com/IN: loaded serial 2 OK onelessone@boontooboiserver:/etc/netplan\$ sudo named-checkzone 2.168.192.in-addr.arpa /etc/bind/db.192 zone 2.168.192.in-addr.arpa/IN: loaded serial 2

Restart BIND9 to apply changes: sudo systemctl restart bind9

Configure UFW to allow DNS traffic (if applicable): sudo ufw allow Bind9

Test DNS with a dig command: dig @localhost www.slickbrickcentral.com

onelessone@boontooboiserver:/etc/netplan\$ dig @localhost www.slickbrickcentral.com							
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost www.slickbrickcentral.com ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20642 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1							
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 1232 ; COOKIE: cb8715302e6b6a940100000067ccad4b3be4bffaf3940bf5 (good) ;; QUESTION SECTION: ;www.slickbrickcentral.com. IN A							
;; ANSWER SECTION: www.slickbrickcentral.com. 604800 IN A 192.168.2.3							
;; Query time: 1 msec ;; SERVER: 127.0.0.1#53(localhost) (UDP) ;; WHEN: Sat Mar 08 20:49:15 UTC 2025 ;; MSG SIZE rcvd: 98							

FQDN Records

To add **FQDN** records for the two static DMZ machines, we will have to update the forward and reverse zone files!

Update Forward Zone

Edit the forward lookup zone file: sudo nano /etc/bind/db.slickbrickcentral.com

Add **A record** for the machines:

Ubuntu Server

- FQDN = ubuntu.slickbrickcentral.com
- IP: 192.168.2.3

Windows Server 2022

- FQDN = win.slickbrickcentral.com
- IP: 192.168.2.2

The file should look like this:

GNU	nano 7.2		/etc/bind/db.slickbrickcentral.com *
\$TTL	604800		
0	IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
; @	IN	NS	ns1.slickbrickcentral.com.
ns1	IN	A	192.168.2.3
ພພພ	IN	Ĥ	192.168.2.3
ubuntu	IN	A	192.168.2.3
win	IN	A	192.168.2.2

Update Reverse Zone

Edit the reverse lookup zone file: sudo nano /etc/bind/db.192

Add PTR (Pointer) records for the machines:

Ubuntu Server

- FQDN = ubuntu.slickbrickcentral.com
- IP: 192.168.2.3

Windows Server 2022

- FQDN = win.slickbrickcentral.com
- IP: 192.168.2.2

NOTE: Add the last octet of the IP to the first entry in each PTR record! For example: $192.168.2.55 \rightarrow 55$ IN PTR yay.slickbrickcentral.com The file should look like this:

GNU	nano 7.2		/etc/bind/db.192 *
\$TTL	604800		
0	IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
, @	IN	NS	ns1.slickbrickcentral.com.
3	IN	PTR	_www.slickbrickcentral.com
3	IN	PTR	ubuntu.slickbrickcentral.com.
2	IN	PTR	win.slickbrickcentral.com.
-			

Check the config files for syntax errors:

sudo named-checkconf

sudo named-checkzone slickbrickcentral.com /etc/bind/db.slickbrickcentral.com sudo named-checkzone 2.168.192.in-addr.arpa /etc/bind/db.192

Restart BIND9 to apply changes: sudo systemctl restart bind9

pfSense Integration

In order to have your caching DNS server hosted on the pfSense firewall forward to the local DNS you just created, you need to configure pfSense to forward requests to 192.168.2.3 for your custom domain: slickbrickcentral.com.

Do this by going to the pfSense browser portal: <u>https://192.168.1.1</u>

Navigate to Services > DNS Resolver in the top bar and scroll to the bottom of the page.



Next, locate "Domain Overrides" at the bottom of the page.

You will need to add 2 records so your local FQDNs will resolve. One record will be the forward lookup zone and the other will be the reverse lookup zone.

Referencing the earlier DNS configuration:

Forward Zone:

- slickbrickcentral.com
- 192.168.2.3

Reverse Zone:

- 2.168.192.in-addr.apra.
- 192.168.2.3

Add both rules:

Domain Overrides								
Domain	Lookup Server IP Address	Description	Actions					
slickbrickcentral.com 192.168.2.3		Forward all DNS requests for slickbrickcentral.com to external DNS	d 🗇					
2.168.192.in-addr.arpa.	192.168.2.3	Reverse Lookup Zone for slickbrickcentral.com on Ubuntu Server	A 🗇					
Enter any domains for which t invalid' and local domains, an treated as the authoritative lo available for a domain then m	he resolver's standard DNS lookup pro d subdomains, can also be entered, su okup server for the domain (including a ake a separate entry for each, using th	cess should be overridden and a different (non-standard) lookup server should be queried ch as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somes ill of its subdomains), and other lookup servers will not be queried. If there are multiple au e same domain name.	d instead. Non-standard, site.com'. The IP address uthoritative DNS servers					
			+ Ad					

Note: Make sure to select **Apply Changes** on the top of the page to lock in your changes. Then refresh the DNS Resolver service \rightarrow



Test the Domain Overrides by using a LAN Client to **ping**, **nslookup**, and **dig** one of the FQDNs you created.

I will test win.slickbrickcentral.com -> 192.168.2.2

```
Run the command: ping win.slickbrickcentral.com
```

```
PS C:\Users\Bill> ping win.slickbrickcentral.com
Pinging win.slickbrickcentral.com [192.168.2.2] with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
```

Run the command: nslookup win.slickbrickcentral.com

```
PS C:\Users\Bill> nslookup win.slickbrickcentral.com
Server: pfSense.slick.firewall
Address: 192.168.1.1
Non-authoritative answer:
Name: win.slickbrickcentral.com
Address: 192.168.2.2
```

Run the command: dig win.slickbrickcentral.com

WAN Configuration

VM Configuration

REMEMBER: Thin Provision Storage and TPM Module!!!

	ADD N	IEW DEVIC
Encryption	VM configuration files are encrypted. ①	
> CPU	4 ~	í
> Memory	16 🗸 GB 🗸	
> Hard disk 1	60 GB ~	
> SCSI controller 0	LSI Logic SAS	
> Network adapter 1	SysAdmin021 ~	onnected
> CD/DVD drive 1	Datastore ISO File 🗸 🗸 🗸	onnected
> USB xHCl controller	USB 3.1	
> Video card	Specify custom settings 🐱	
> Security Devices	ТРМ	
VMCI device		

Windows Setup for Local Accounts (No Microsoft Email Required):

- 1. I disconnected the VM network card once each computer was in the final "windows setup" mode.
- 2. I then ran the following commands to bypass the required network setup so that I could create local system accounts:
 - a. Shift + f10 -> Brings up a command prompt
 - b. Command: **OOBE\BYPASSNRO** (Out Of Box Experience command)
- 3. Once through setup without internet, reconnect the network adapter!

Windows 11 Workstation-WAN

Username: Rebecca Password: **Classified**

NOTE: "Bob" is the answer for all security questions!!!

Workstation Network Configuration

Workstation IP: **10.161.21.20** DNS Servers: **10.161.21.4** and **10.120.16.10**

General You can get IP settings assigned autr this capability. Otherwise, you need for the appropriate IP settings.	omatically if your network supports to ask your network administrator
Obtain an IP address automatic	ally
OUse the following IP address:	
IP address:	10 . 161 . 21 . 20
Subnet mask:	255.255.255.0
Default gateway:	10 . 161 . 21 . 1
Obtain DNS server address auto	omatically
O Use the following DNS server ad	ldresses:
Preferred DNS server:	10 . 161 . 21 . 4
Alternate DNS server:	10 . 120 . 16 . 10
Validate settings upon exit	Advanced
	OK Cancel

I also installed the **Chocolatey** package manager and the dig command. Powershell: **choco install bind-toolsonly**

pfSense Address (WAN): 10.161.21.4

I am going to <u>forward</u> any request from WAN to pfSense on port 53 straight to my "external DNS server": **192.168.2.3** which then will reply back to the WAN client.

pfSense NAT

In the admin web interface: http://192.168.1.1

Navigate to **Interfaces > WAN**. Scroll to the bottom of the page and make sure that "Block private networks" is unchecked!



Navigate to System > Advanced > Firewall and NAT Tab.

	System -	Interfaces 🗸	Firewall -	Services -	VPN -	Status -	Diagnostics -
System / A	Advanced,	/ Firewall 8	& NAT				
Admin Access	Admin Access Firewall & NAT		Networking Misce		System Tunables	Notifica	ations

In the "Network Address Translation" section further down the page:

- Set "NAT Reflection Mode for Port Forwards" to Pure NAT
- Enable (Check the box) for "Enable NAT Reflection for 1:1 NAT"

Network Address Tra	nslation
NAT Reflection mode for	Pure NAT 🗸
port forwards	 The Pure NAT mode uses a set of NAT rules to direct packets to the target of the port forward. It has better scalability, but it must be possible to accurately determine the interface and acteury IP used for computing will the target at the time the rules are loaded. There are no inherent
	 limits to the number of ports other than the limits of the protocols. All protocols available for port forwards are supported. The NAT + Proxy mode uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. This feature does not support IPv6. Only TCP and UDP protocols are supported.
	Individual rules may be configured to override this system setting on a per-rule basis.
Reflection Timeout	2000
	Enter value for Reflection timeout in seconds. Note: Only applies to Reflection on port forwards in NAT + proxy mode.
Enable NAT Reflection for	Automatic creation of additional NAT redirect rules from within the internal networks.
1:1 NAT	Note: Reflection on 1:1 mappings is only for the inbound component of the 1:1 mappings. This functions the same as the pure NAT mode for port
	role basis.
Enable automatic	Automatic create outbound NAT rules that direct traffic back out to the same subnet it originated from. Activat
outbound NAT for Reflection	Required for full functionality of the pure NAT mode of NAT Reflection for port forwards or NAT Reflection for 1:1 NAT. Note: This only works 🕫 to Se assigned interfaces. Other interfaces require manually creating the outbound NAT rules that direct the reply packets back through the router.

NAT Port Forwarding Rule

Navigate to Firewall > NAT > Port Forward Tab.

Fire	Firewall / NAT / Port Forward									
Port	Forward	1:1 Outbo	ound NPt							
Rule	s									
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
						Add	l Add	🛅 Delete 🚫	Toggle 📑 Save	+ Separator

Add a new Rule with following configurations:

- Interface: WAN
- Protocol: TCP/UDP
- Destination: WAN Address
- Destination Port Range: DNS (Port 53 Only)
- Redirect Target IP: Internal DNS Server (BIND) → 192.168.2.3
- Redirect Target Port: DNS (Port 53)

Interface	WAN		~		
	Choose which interface this	rule applies to. In most cases	s "WAN" is specified.		
Address Family	IDv4				
Address Fulling	Celect the Internet Drotocol	version this rule applies to	¥		
	Select the Internet Protocol	version this fulle applies to.			
Protocol	TCP/UDP		~		
	Choose which protocol this	rule should match. In most ca	ases "TCP" is specified.		
Source	😳 Display Advanced				
Destination	 Invert match. 	WAN address	*		/ *
		Туре		Address/mask	
Destination port range	DNS		DNS 🗸		
	From port	Custom	To port	Custom	
	Specify the port or port rang	e for the destination of the pa	acket for this mapping. The 'to' fiel	ld may be left empty if only mapping	a single port.
		(Generation	
Redirect target IP		Address or Alias	~	192.168.2.3	
		Туре		Address	1
	Enter the internal IP address	of the server on which to ma	ap the ports. e.g.: 192.168.1.12 for	r IPv4	
	In case of IPv6 addresses, in	n must be from the same "sco	ope",		
	i.e. it is not possible to redire	act from link-local addresses	scope (fe80:*) to local scope (::1)		
Redirect target port	DNS		~		
	Port		Custom		
	Specify the port on the mac	nine with the IP address enter	red above. In case of a port range	specify the beginning port of the ra	nge (the end port will be
	calculated automatically).	and manufactor address critici	rea assets. In case or a port range,	opeony the beginning port of the re-	inge (one end port will be

This is usually identical to the "From port" above.

Final NAT Rule:

Port Forward	1:1	Outbound	NPt							
Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□ ✓ ≭	WAN	TCP/UDP	*	*	WAN address	53 (DNS)	192.168.2.3	53 (DNS)		A 🗋 🛅

Corresponding Firewall Rule Created:

Firewa	all / Rules	VAN									Lui 🗉 😧
Floating	WAN	LAN DMZ									
Rules (Drag to Cha	nge Order)									
0	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
• 🗸	0/164 KiB	IPv4 TCP/UDP		*	192.168.2.3	53 (DNS)	*	none		NAT	৻৳৶ঢ়ঢ়ঢ়
							1 Add	Add 间	Delete	Toggle 🚺 Copy	🗟 Save 🕇 Separato

WAN Client Testing

Go to the WAN Client (10.161.21.20) created earlier and use the dig command to verify proper configuration and local DNS resolution.

First, we will show that DNS requests are properly being port forwarded from pfSense (**10.161.21.4**) to FQDNs mapped in the local BIND server (**192.168.2.3**).

Run the command: dig win.slickbrickcentral.com



As you can see above, the **A record** for win.slickbrickcentral.com is 192.168.2.2 which is correct!

Next, we will show that requests **NOT** mapped in the BIND server are redirected to the alternate UNI DNS (**10.120.16.10**) configured on the WAN Machine.

Run the command: dig google.com

PS C:\Users\Rebecca> dig www.google.com						
; <<>> DiG 9.16.28 <<>> www.google.com ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64239 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1						
;; OPT PSEUDOSECTION: ; EDNS: version: 0, f ;; QUESTION SECTION: ;www.google.com.	lags:; u	dp: 4000	IN	A		
;; ANSWER SECTION:						
www.google.com.	210	IN	А	142.250.191.132		
;; Query time: 0 msec ;; SERVER: 10.120.16. ;; WHEN: Mon Mar 24 1 ;; MSG SIZE rcvd: 59	10#53(10 6:42:29	.120.16. Pacific	10) Daylight	: Time 2025		

Project 6: Static HTTPS Web Server

Below contains steps outlining the configuration of a static **HTTPS** server using **Apache** on the existing **Ubuntu Linux** server (**192.168.2.3**) within the local DMZ. This server will server static HTML content to the frontend so no scripting language or database will be needed. Proper configuration of DNS records, a self signed certificate for SSL connections, and integration of **NAT port forwarding** in pfSense will allow clients in the LAN and WAN to access the web server.

Web Server mapping:

slickbrickcentral.com and www.slickbrickcentral.com \rightarrow 192.168.2.3 (Ubuntu Linux Server)

BIND DNS Records

Edit the forward lookup zone to add A records for slickbrickcentral.com.

Edit the configuration file: sudo nano /etc/bind/db.slickbrickcentral.com

Add the following A Records:

GNU	nano 7.2		/etc/bind/db.slickbrickcentral.com *
\$TTL	604800		
0	IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
0	IN	NS	ns1.slickbrickcentral.com.
(d	IN	A	10.161.21.4
Q	IN	A	192.168.2.3
ns1	IN	A	192.168.2.3
ພພພ	IN	Ĥ	192.168.2.3
ubuntu	J IN	Ĥ	192.168.2.3
win	IN	Ĥ	192.168.2.2

Next update the reverse lookup zone.

Edit the configuration file: sudo nano /etc/bind/db.192

	GNU	nano 7.2		/etc/bind/db.192 *
\$	₿TTL	604800		
Ċ		IN	SOA	ns1.slickbrickcentral.com. admin.slickbrickcentral.com. (2 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800); Negative Cache TTL
, 10	3	TN	NS	ns1 slickbrickcentral com
3	}	TN	PTR	www.slickbrickcentral.com.
3	}	IN	PTR	slickbrickcentral.com
З	3	IN	PTR	ubuntu.slickbrickcentral.com.
2	-	IN	PTR	win.slickbrickcentral.com.

Add the following reverse lookup records:

Apply changes with the command: sudo systemctl restart bind9

Verify Records on WAN Client

Run the command: **nslookup slickbrickcentral.com** Run the command: **nslookup 192.168.2.3**

Apache Web Server

The **Apache HTTP Server**, commonly known as Apache, is a powerful, open-source web server software that allows websites to be hosted and served over the internet. It is highly customizable and supports a wide range of features, including SSL/TLS encryption, URL redirection, and load balancing.

Install and Configuration

I will be installing Apache on the Ubuntu Linux Server in the DMZ under the IP 192.168.2.3.

Update system packages with: sudo apt update

To begin the installation run the command: **sudo apt install apache2** Start the service with the command: **sudo systemctl status apache2** Verify that it is running with the command: **sudo systemctl status apache2**



Since the Ubuntu Server is within the DMZ, verify the website is being hosted <u>locally</u> by using a DMZ client and navigating to <u>http://192.168.2.3</u> in a browser.



SSL Configuration

In order to ensure that our website connection is secure, we need to enable **SSL** so our network traffic is HTTPS. To enable SSL we can create a **self-signed certificate**.

Enable SSL Module

We will start by enabling an Apache module that provides support for SSL encryption.

Use the command: sudo a2enmod ssl

Restart Apache to activate the module: sudo systemctl restart apache2

onelessone@boontooboiserver:~\$ sudo a2enmod ssl
[sudo] password for onelessone:
Considering dependency mime for SSI:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
onelessone@boontooboiserver:~\$ sudo systemctl restart apache2

Create the SSL Certificate

Create a directory for the certificate: **sudo mkdir /etc/ssl/private** NOTE: The directory is created with sudo so it can only be accessed by privileged users!

Generate a Private Key and Self-Signed Certificate: sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

After running the command, you will be prompted to fill out some information for your certificate: NOTE: Make sure to put the proper FQDN of your website in the **Common Name** section!

You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. -----Country Name (2 letter code) [AU]:US State or Province Name (full name) [Some-State]:Iowa Locality Name (eg, city) []:Cedar Falls Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNI-SYS-ADMIN Organizational Unit Name (eg, section) []:University of Northern Iowa Common Name (e.g. server FQDN or YOUR name) []:slickbrickcentral.com Email Address []:olhavad@uni.edu

Configure Apache to use SSL

We need to create a **VirtualHost** that will facilitate HTTPS requests on port 443.

Create a new file with: sudo nano /etc/apache2/sites-available/slickbrickcentral.conf NOTE: Make sure to match the ServerName with the Common Name you chose when setting up the certificate! \rightarrow slickbrickcentral.com



Let's now make a new DocumentRoot and put an HTML file for testing purposes! Create your website's root directory: **sudo mkdir /var/www/slickbrickcentral.com**

Create the landing page of the website: sudo nano /var/www/slickbrickcentral.com/index.html



Next we need to enable the configuration file: **sudo a2ensite slickbrickcentral.conf** Test the configuration file with the command: **sudo apache2ctl configtest** Activate changes with the command: **sudo systemctl reload apache2**

```
onelessone@boontooboiserver:/etc/ssl$ sudo a2ensite slickbrickcentral.conf
Enabling site slickbrickcentral.
To activate the new configuration, you need to run:
   systemctl reload apache2
onelessone@boontooboiserver:/etc/ssl$ sudo apache2ctl configtest
Syntax OK
onelessone@boontooboiserver:/etc/ssl$ sudo systemctl reload apache2
```

Test HTTPS Connection

Go to your DMZ Client and visit your website with HTTPS! In a browser enter <u>https://slickbrickcentral.com</u>

Upon navigating to your page you will see a warning about the self-signed certificate. You can click "Advanced" towards the bottom of the warning graphic and then proceed to the website!



You then should see your website landing page render with the simple message coded earlier. Notice that the browser URL is using **HTTPS**!



Redirect HTTP to HTTPS

Currently, our configuration will only respond to HTTPS requests on port 443. It is good practice to also respond on port 80, even if you want to force all traffic to be encrypted. Let's set up another **VirtualHost** to respond to these unencrypted requests and redirect them to HTTPS.

Open the same Apache configuration file: sudo nano /etc/apache2/sites-available/slickbrickcentral.conf



Next we need to refresh the configuration file: **sudo a2ensite slickbrickcentral.conf** Test the configuration file with the command: **sudo apache2ctl configtest** Activate changes with the command: **sudo systemctl reload apache2**

onelessone@boontooboiserver:/etc/ssl\$ sudo a2ensite slickbrickcentral.conf Site slickbrickcentral already enabled onelessone@boontooboiserver:/etc/ssl\$ sudo apache2ctl configtest Syntax OK onelessone@boontooboiserver:/etc/ssl\$ sudo systemctl reload apache2

Test the redirect by trying to access your website with HTTP protocol! You can do this by navigating in a browser to <u>http://slickbrickcentral.com</u>

			New	rtab × +
\leftarrow	С	(\bigcirc	http://slickbrickcentral.com
C, Im	port fav	orite	s	For quick access, place your favorites here on the favorites bar. Manage favorites now

The website should redirect the HTTP request to HTTPS!



Test Page

Disable the default configuration file: **sudo a2dissite 000-default.conf** Reload Apache to apply changes: **sudo systemctl reload apache2**
Static HTML Page

After verifying the server is running on our **Ubuntu Server at 192.168.2.3**, we need to create a customized static HTML page to display!

I downloaded external images to a DMZ client and then used **scp** to transfer them to the Apache Web Server:

scp <the/local/file/path> user@[ip_address]:[the/server/destination/path]



I then used ssh on the DMZ client to connect to the Apache server: **ssh onelessone@192.168.2.3**

After logging in, I created an images directory within the website's root directory: **sudo mkdir /var/www/slickbrickcentral.com/images**

I then copied the uploaded files within the /static directory and transferred them to /images: sudo cp /home/onelessone/static/* /var/www/slickbrickcentral.com/images/

onelessone@boontooboiserver:/var/www/slickbrickcentral.com\$ ls ./images
lego_logo.png lego_star_wars.gif

After copying my website resources, I edited the base HTML page: sudo nano /var/www/slickbrickcentral.com/index.html



After saving the file, render the new page contents in a browser: https://slickbrickcentral.com

\leftarrow	C	😣 Not secure	https://slickbrickcentral.com	
				Welcome to SlickBrickCentral Here we sell aftermarket Legos!
				azo
				Our Website is currently a Work in Progress!

pfSense Integration

I will have to **port forward** http and https traffic entering my pfSense address from the WAN to the internal Apache Web Server.

To do this I can create a port forward rule to forward traffic on ports 80 (http) and 443 (https) from 10.161.21.4 (pfSense WAN) to 192.168.2.3 (Apache Web Server).

First, go onto a LAN machine and navigate to the pfSense configuration portal: <u>http://192.168.1.1</u>

In the top bar, navigate to Firewall > NAT > Port Forward



Add a new rule for HTTP traffic (port 80)

Firewall / NAT /	Port Forward / Ed	lit			
dit Redirect Entry					
Disabled	 Disable this rule 				
No RDR (NOT)	Disable redirection for This option is rarely need	r traffic matching this rule ed. Don't use this without thorou	gh knowledge of the implicati	ions.	
Interface	WAN Choose which interface t	his rule applies to. In most cases	♥ "WAN" is specified.		
Address Family	IPv4 Select the Internet Protoc	ol version this rule applies to.	~		
Protocol	TCP Choose which protocol th	is rule should match. In most ca	► ses "TCP" is specified.		
Source	Display Advanced				
Destination	Invert match.	WAN address Type	```````````````````````````````````````	Address/mask	1
Destination port range	HTTP V From port	Custom	HTTP To port	Custom	a single port.
Redirect target IP	Enter the internal IP addre	Address or Alias Type ess of the server on which to map	o the ports. e.g.: 192.168.1.12	192.168.2.3 Address 2 for IPv4	
	In case of IPv6 addresses i.e. it is not possible to rec	, in must be from the same "scop direct from link-local addresses s	cope (fe80:*) to local scope ((::1)	
Redirect target port	HTTP Port Specify the port on the mic calculated automatically). This is usually identical to	achine with the IP address entere , , the "From port" above.	Custom	nge, specify the beginning port of the ran	ge (the end port w
Description	Port forward HTTP traffic A description may be enter	c to Apache Web Server red here for administrative refere	ence (not parsed).		
No XMLRPC Sync	Do not automatically s This prevents the rule on	ync to other CARP members Master from automatically synci	ng to other CARP members. T	This does NOT prevent the rule from bein	g overwritten on S
NAT reflection	Use system default		~		
Filter rule association	Add associated filter rul	e	~		

Add a new rule for HTTPS traffic (port 443)

dit Redirect Entry							
Disabled	 Disable this rule 						
No RDR (NOT)	Disable redirection for This option is rarely nee	or traffic matching this rule ded. Don't use this without thoroug	gh knowledge of the	implications			
Interface	WAN Choose which interface	this rule applies to. In most cases	WAN" is specified.				
Address Family	IPv4 Select the Internet Proto	col version this rule applies to.	*				
Protocol	TCP Choose which protocol t	this rule should match. In most cas	► ses "TCP" is specifie	ed.			
Source	🔅 Display Advanced						
Destination	Invert match.	WAN address Type		*	Address/mask	1	
Destination port range	HTTPS •	Custom	HTTPS To port	~	Custom	D	
Redirect target IP		Address or Alias		~	192.168.2.3 Address		
	Enter the internal IP addr In case of IPv6 addresses i.e. it is not possible to re	ess of the server on which to map s, in must be from the same "scop direct from link-local addresses so	the ports. e.g.: 192 e", cope (fe80:*) to loca	.168.1.12 for al scope (::1)	IPv4		
Redirect target port	HTTPS Port Specify the port on the m	achine with the IP address entere	✓ d above. In case of	Custom a port range,	specify the beginning port	of the range (the end port	tv
	calculated automatically) This is usually identical to	o the "From port" above.					
Description	Port forward HTTPS traf	ffic to Apache Web Server ered here for administrative refere	nce (not parsed).				
No XMLRPC Sync	 Do not automatically This prevents the rule on 	sync to other CARP members Master from automatically syncin	g to other CARP me	embers. This	does NOT prevent the rule	from being overwritten or	1 5
NAT reflection	Use system default		~				
ilter rule association	Add associated filter ru	le	V It will only work a	n an interfac	e containing the default ga	feway	

Final Port Forward Rules (make sure to Apply Changes)

Po	ort Fo	rwar	d 1:1	Outbo	ound NPt							
Ru	ıles											
			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	~	*	WAN	TCP	*	•	WAN address	443 (HTTPS)	192.168.2.3	443 (HTTPS)	Port forward HTTPS traffic to Apache Web Server	/ 💭 🖻
	~	24	WAN	TCP	*	•	WAN address	80 (HTTP)	192.168.2.3	80 (HTTP)	Port forward HTTP traffic to Apache Web Server	
	~	2\$	WAN	TCP/UDP	*	.t.	WAN address	53 (DNS)	192.168.2.3	53 (DNS)		/ 💭 1
										1 Add	Add 🛅 Delete 🚫 Toggle 🖬 Save	Separator

Go to your WAN machine and verify you can access your Apache Web Server. In the browser I will check by using my chosen domain name: **slickbrickcentral.com**



Project 7: Active Directory

Below contains steps outlining the configuration of an **Active Directory Domain**. The **Windows 2022 Server** (**192.168.2.2**) in the DMZ will be designated as the **Domain Controller**. Active Directory **Roaming Profiles** will enable my employees to log into any LAN workstation and maintain their user files and settings.

AD Information

AD Domain Controller: **192.168.2.2** AD Domain: **ad.local** Usernames: AD\Administrator, bill, fernando Employee Password: **Classified**

AD Setup

Active Directory is a Microsoft tool that helps manage users and computers in a network. It organizes and controls access to resources like files and applications. I will be installing Active Directory on my Windows 2022 Server within the DMZ under the IP Address 192.168.2.2!

Installing AD Role and Features

After logging into the Windows 2022 Server, open the Server Manager application. Then in the upper right corner navigate to **Manage > Add Roles and Features**



Installation Type: Role-based or feature-based installation.



Server Selection: Select your local server where you wish to install the AD DS role. This menu shows our local server, WIN-U00T4AO1ET9, its IP and OS.

Refore You Regin	Select a server or a virtu	al hard disk on whicl	n to install roles and features.		
Installation Type	Select a server from the se	the server pool			
Server Selection	 Select a virtual hard of 	disk			
Server Roles	Server Pool				
Features					
	Filter:				
	Name	IP Address	Operating System		_
	WIN-U00T4AO1ET9	192.168.2.2	Microsoft Windows Server 20	022 Standard	
					-
	1 Computer(s) found				

Server Roles: Select "Active Directory Domain Services". Once you choose that option, a new pop-up window will appear. This window shows the features required for AD DS that you will need to include. Select "Include management tools" and click on "Add Features".

NOTE: Disregard the DNS selection. That is not needed for Active Directory!

🚘 Add Roles and Features Wizard		– 🗆 X	
Add Roles and Features Wizard	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Pomain Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DeVice P server Month Directory Content of 12 installed) Fax Server	– C × DESTINATION SERVER WIN-JOOTAAOTETS Domain Name System (DNS) Server manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services pODS Server and Active Directory Domain Services to work together.	Add Roles and Features Wizard X Add features that are required for Active Directory Domain Services? You cannot install Active Directory Domain Services unless the following role services or features are also installed. [Tools] Group Policy Management A Remote Server Administration Tools A Dol S and AD LDS Tools A DD S Tools
	Host Guardian Service Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) Windows Deployment Services Windows Server Update Services Vervious Next >	Install Cancel	Active Directory module for Windows PowerShell AD DS Tools [Tools] Active Directory Administrative Center [Tools] AD DS Snap-Ins and Command-Line Tools Include management tools (if applicable) Add Features Cancel

Features: Select "Next" AD DS: Select "Next" Confirmation: Verify the Active Directory configuration and select "Install"



NOTE: Keep the installation wizard **OPEN** until the installation is complete! Then select "Promote this server to a domain controller"



A new setup window will appear. This contains three options for deployment: "Add a domain controller to an existing domain", "Add a new domain to an existing forest", or "Add a new forest". Since we are starting from scratch, we are going to create a brand new forest.

AD Forest and Domain Controller

Deployment Configuration: Select "Add a new forest" and specify the Root domain name.

Root domain name: ad.local

🔁 Active Directory Domain Services Configuration Wizard	– 🗆 ×
Active Directory Domain Services Configuration Wizard Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	- C X
More about deployment configurations	
< Previous Next >	Install Cancel

Domain Controller Options: Since this is the first AD domain controller, check the "DNS server" and "Global Catalog" boxes. Give the Directory Services Restore Mode (DSRM) a password. Then click on "Next".

DSRM Password: **Classified**

Active Directory Domain Services	Configuration Wizard		-		×
Domain Controller	Options		TAR WIN-U	GET SER 00T4AO1	VER ET9
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest a Forest functional level: Domain functional level: Specify domain controller capabilities I Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mode Password: Confirm password: More about domain controller options	nd root domain Windows Server 2016 V Windows Server 2016 V e (DSRM) password V V V V V V V V V V V V V			
	< Pre	vious Next > Insta		Cancel	

DNS Options: SKIP, no need for DNS Delegation right now

Additional Options: Displays the NetBIOS domain name taken from the root domain. Ex: AD Paths: You can specify the location of the AD DS database, log files, and SYSVOL folders. Review Options: Check your configuration and go back if you want to make any changes before installation. If everything looks good, click "Next".

Active Directory Domain Services	Configuration Wizard —		×
Review Options	T. WIN	ARGET SERVER	R 9
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Review your selections: Configure this server as the first Active Directory domain controller in a new forest. The new domain name is "ad.local". This is also the name of the new forest. The NetBIOS name of the domain: AD Forest Functional Level: Windows Server 2016 Domain Functional Level: Windows Server 2016 Additional Options: Global catalog: Yes DNS Server: Yes Create DNS Delegation: No These settings can be exported to a Windows PowerShell script to automate additional installations	View script	
	< Previous Next > Install	Cancel]

Prerequisites Check: Shows you a checklist with warnings or critical alarms. If the check passes, it will show a green light, and you'll be able to install AD DS with the new domain controller and forest. You can take care of these warnings later on.

Click "Install". The server will then install and restart automatically.



After the server restarts, verify your configuration by opening the Server Manager application.

Then in the upper right corner navigate to **Tools > Active Directory Users and Computers**. You should see the domain name you picked! My domain was **ad.local**.



AD DNS Server Zones

You already installed AD DS, the DNS role, and created a new Forest and Domain Controller (DC). Now you only need to configure the DNS zones.

A DNS zone is formed by the mappings of IPs and hostnames used to resolve DNS queries. The most common zone type in Active Directory is the **Active Directory-integrated DNS zone**.

Forward Lookup Zone

In the upper right corner navigate to Tools > DNS



Expand the "Forward Lookup Zones" directory and you will see the root domain name chosen earlier (**ad.local**) and the **_msdcs** zone which is created by default.

🏯 DNS Manager			8	– 🗆 X
File Action View Help				
🗢 🔿 🗖 🖬 🖉 🖥				
 DNS WIN-U00T4AO1ET9.ad.local Forward Lookup Zones msdcs.ad.local ad.local Reverse Lookup Zones Trust Points Conditional Forwarders 	Name msdcs.ad.local ad.local	Type Active Directory-Integrated Pr Active Directory-Integrated Pr	Status Running Running	DNSSEC Status Not Signed Not Signed

Reverse Lookup Zone

The Forward Lookup Zone is already pre-populated but the Reverse Lookup Zone is not. Create a new zone by right clicking the "Reverse Lookup Zones" directory and selecting "New Zone".

🔰 📔 Reverse Lookur📑		
Trust Points	New Zone	
🦰 Conditional Fo	View	>
	Refresh	
	Help	

Zone Type: Check "Primary Zone" and "Store the zone in Active Directory"



AD Zone Replication Scope: Check "To all DNS servers running on domain controllers in this

domain: <your domain>"



Reverse Lookup Zone Name: Select "IPv4 reverse lookup zone" and click "Next"

Reverse Lookup Zone Name: Specify the **Network ID** of the reverse zone to help identify the reverse lookup zone. The **first three octets** of your Windows Server's IP are used for the Network ID.

Windows 2022 Server: **192.168.2**.2

New Zone Wizard X
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone. Network ID: 192 168 192 168 Ine network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order. If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10.0 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.ion-addr.arpa. O Reverse holes a zero area is a set of the s
2,168.192.in-addr.arpa
< Back Next > Cancel

Then, click "Next > "Next" > "Finish".

Check your new Reverse Lookup Zone. Inside, you should see two DNS resource records, **SOA** and **NS**.

🚊 DNS	Name	Туре	Data	Timestam
VIN-U00T4AO1ET9.ad.local	(same as parent folder)	Start of Authority (SOA)	[1], win-u00t4ao1et9.ad.lo	static
Forward Lookup Zones medes ad local	(same as parent folder)	Name Server (NS)	win-u00t4ao1et9.ad.local.	static
> 🔂 ad.local	*			
✓ ☐ Reverse Lookup Zones				1
📋 2.168.192.in-addr.arp	·			1
> Irust Points				
> Conditional Forwarders				

Update A Records

Open your domain name directory within the Forward Lookup Zone and then double-click the Host A record.

DNS V UN-U00T4AO1ET9.ad.local WIN-U00T4AO1ET9.ad.local	Name msdcs	Туре	Data	Timestam
Solution Solution	sites tcp udp DomainDnsZones			
 2.168.192.in-addr.arp Trust Points Conditional Forwarders 	ForestDnsZones	Start of Authority (SOA) Name Server (NS)	[21], win-u00t4ao1et9.ad.l win-u00t4ao1et9.ad.local.	static
	(same as parent folder)	Host (A)	192.168.2.2	4/9/2025 2
	win-u00t4ao1et9	Host (A)	192.168.2.2	static

A popup window will open and make sure to select "Update associated pointer (PTR) record". Then click on "Apply" and "Ok" to save changes.

win-u00t	lao1et9 Properties	?	×
Host (A)	Security		
Host (us	es parent domain if left blank):		
win-u0	It4ao1et9		
Fully qu	alified domain name (FQDN):		
win-u0	It4ao1et9.ad.local		
IP addr	355:		
192.16	8.2.2		
Î			
	OK Cancel	Ap	ply

Verify Reverse Lookup Zone

If you don't see the PTR record in the reverse lookup zone, you'll need to refresh. Click the refresh button on the top bar and the new PTR record should appear.



AD Domain Controller Verification

Verify your server is the AD Controller by navigating in the top right corner of Server Manager to **Tools > Active Directory Users and Computers**.

Once the pop-up opens, expand your domain name and then look into the "Domain Controllers" section. Your current machine should be listed!



Creating AD Users

In order to create users for your Active Directory open the Server Manager application. Next, in the upper right hand corner navigate to **Tools > Active Directory Users and Computers**.



A pop-up window will appear. Right-click on your domain and then navigate to **New > Organizational Unit**.

ad.local ad.local B C C D F F N U	ory Users and Com leries Delegate Control Find Change Domain Change Domain Controller Raise domain functional level Operations Masters	Tyj	pe iltinDomain htainer anizational htainer htainer htainer	Description Default container for up Default container for do Default container for sec Default container for ma Default container for up
	New	>	Compute	er
	All Tasks	>	Contact	
	View	>	Group	
	Refresh Export List Properties		InetOrgP msDS-Sh msImagii MSMO 0	erson adowPrincipalContainer ng-PSPs weue Aliar
			Organiza	tional Unit
	Help		Printer User	
	-	_	Shared Fe	older

Name your Organizational Unit. I will be naming mine *Employees* since it will contain worker data.

ew Objec	ct - Organiza	tional Uni	it	
N	Create in:	ad.local/	,	
Name:				
Employe	es			
Prote	ct container fr	om accider	ntal deletion	
Prote	ct container fr	om accider	ntal deletion	
Prote	ct container fr	om accider	ntal deletion	
✓ Prote	ct container fr	om accide	ntal deletion	

Right-click the newly created OU and then navigate to **New > User**.

> Users	Delegate Control Move Find		
	New	>	Computer
	All Tasks	>	Contact
	View	>	Group
< Creates a new iter	Cut Delete Rename Refresh Export List		InetOrgPerson msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias Organizational Unit Printer
Creates a new iter	Properties	Г	User
	Help		Shared Folder

I will be creating two users for my workforce: **Bill** and **Fernando**

Note: Make sure to check the box "Password never expires" so you will not have to change it on the first logon for your users.

Usernames: bill or fernando

Password: **Classified** (same for both users)

New Object - User	×	New Object - User	×
Create in: ad Jocal/Employees		Create in: ad Jocal/Emplo	yees
First name: Bill	Initials:	First name: Fernando	Initials:
Last name: Bob		Last name: Minecraft	
Full name: Bill Bob		Full name: Femando Minec	raft
User logon name:		User logon name:	
bill @ad.local	\sim	femando	@ad.local ~
User logon name (pre-Windows 2000):		User logon name (pre-Windows 2000):	
AD\ bill		AD\	femando
< Back	Next > Cancel		< Pack Next > Cancel
New Object - User	×	New Object - User	×
Create in: ad.local/Employees		Create in: ad Jocal/Emplo	yees
Password:		Password:	
Confirm password:		Confirm password:	•••••
User must change password at next logon		User must change password at next	logon
User cannot change password		User cannot change password	
Password never expires		Password never expires	
Account is disabled		Account is disabled	
		·	
2 De alt	Novt > Concel		< Back Next > Cancel
< Back	INEXL 2 Califer		

After creating both users you should see them under the *Employees* OU!

Name	Туре	Description	
📥 Bill Bob	User		
📥 Fernando Mi	User		

To validate they are in your Active Directory Domain, right-click each user and then select "Properties". Then navigate to "Member Of" and verify your domain is listed.

Bill Bob Properties				? ×
Remote control General Address Member Of	Remote [Account Dial-in	Desktop Se Profile Envi	rvices Profile Telephones ironment	COM+ Organization Sessions
Member of:	Active Direct	on Domain	Services Folde	
Domain Users	ad.local/Use	rs		
Add	Remove			
Primary group: D	omain Users			

Success! Next, we'll join two workstations to our AD domain, allowing us to sign in with the users we've just created.

Joining Clients to AD

In order to add a windows workstation to an Active Directory, it must be able to connect to a network with an AD Domain Controller. Luckily, our LAN workstations can communicate with DMZ hosts like the AD Domain Controller!

Client DNS Setup

In the Windows 2022 Server, open the Server Manager application, navigate to the top right corner and select **Tools > DNS**.

A DNS Manager pop-up will appear. Within the window, right-click the DNS server name and select "Properties". Navigate to the Forwarders section, input your preferred DNS server forwarder, and click "Apply". I will be choosing to forward to my pfSense server at **192.168.2.1**.

Debug Legging	Event Lenging	Manitaria	- Cee	
Lebug Logging	Forwarders	Advanced	Dept Hi	unic
Forwarders are DN queries for records	S servers that this se that this server canno	ver can use to re ot resolve.	solve DNS	
IP Address	2	Server FQDN		
192,168,2,1		Unable to resolve	>	
			5.0	
☑ Use root hints if	no forwarders are av	ailable	Edit	
Use root hints if Note: if conditional used instead of ser forwarders, navigal	no forwarders are av forwarders are defin ver-level forwarders. ie to the Conditional f	ailable Id for a given dom To create or view orwarders node in	Edit nain, they will y conditional n the scope tr	be

This will ensure all unknown queries given to the AD Domain Controller will be forwarded elsewhere to resolve.

Next, open the pfSense Admin portal in a browser at <u>http://192.168.1.1</u> and login. Once in the portal navigate in the top bar to **Services > DHCP Server**. Make sure you are in the "LAN" tab and then scroll until you see DNS servers and assign the AD Domain Controller as <u>primary</u> DNS (**192.168.2.2**) and then pfSense as <u>secondary</u> DNS (**192.168.1.1**).

WINS Servers	WINS Server 1	
	WINS Server 2	
DNS Servers	192.168.2.2	
	192.168.1.1	
	DNS Server 3	
	DNS Server 3	

Doing this will allow all LAN workstations to be automatically issued the AD Domain Controller for DNS: **ad.local**.

Renaming Client Device

On your Windows workstation open the Settings app. Then navigate to **System > About**. Click "Rename this PC" in the upper right hand corner and create a unique name to the two client computers.

Workstation Names: WS-1 and WS-2

DESk VMw	KTOP-UAHLEPK are7,1		Rename this PC
(i)	Device specificat	tions	Сору
	Device name	DESKTOP-UAHLEPK	
	Processor	Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz 2.30 GHz (2 processors)	
	Installed RAM	8.00 GB	
	Device ID	0160C75F-1C8F-4294-BBD2-BECC37E7761E	
	Product ID	00331-10000-00001-AA031	
	System type	64-bit operating system, x64-based processor	
	Pen and touch	No pen or touch input is available for this display	

After renaming each workstation, restart the device!

Connecting Client to AD

Open the Settings app again and navigate to **System > About** menu, and then select "Advanced system settings".



A pop-up window will open. Navigate to "Computer Name" on the top bar and click the "Change" button.

System Properties		\times				
Computer Name Hardwar	e Advanced System Protection Remote					
Windows uses on the network	the following information to identify your computer					
Computer description:	I					
	For example: "Kitchen Computer" or "Mary's Computer".					
Full computer name:	WS-1					
Workgroup:	WORKGROUP					
To use a wizard to join a domain or workgroup, click Network ID						
To rename this computer workgroup, click Change.	or change its domain or Change]				

You then need to enter your domain name: ad.local and then click "Ok".

Computer Name/Domai	n Changes		×
You can change the name computer. Changes might a	and the memb affect access to	ership of t o network	his resources.
Computer name:			
WS-1			
Full computer name: WS-1 Member of Domain: ad.local			More
O Workgroup: WORKGROUP			
	OK		Cancel

Enter the credentials of one of the AD users configured earlier to join the domain! Username: **bill** or **fernando** Password: **Classified**



If login is a success, you will see the following message.



Restart to apply changes!



After restart, select "Other user" login and you should see your AD domain listed. You then can sign in with one of the AD user accounts.

	Other user
	User name
	Password → Sign in to: AD
Bill Other user	How do I sign in to another domain?

Delete Local Accounts

There is no need for the local account on our Windows workstation since we have Active Directory connected. Let's delete it!

Login to your workstation with the Administrator Active Directory user. Username: **AD\Administrator**



Right-click the Windows button and select "Computer Management".



Navigate into Local Users and **Groups > Users** and right-click the local user you want to delete.



After deletion, there should be no local users remaining!

Name	Full Name
🛃 Administrator	
🛃 DefaultAcco	
🛃 Guest	
WDAGUtility	

Description Built-in account for administering... A user account managed by the s... Built-in account for guest access t... A user account managed and use...

Roaming Profiles

Active Directory **Roaming Profiles** are a Windows Server feature that allow users to access their personal desktop settings and files from any computer within the domain.

Before configuring a Roaming Profile, we need to create a Share. Open the Server Manager application and navigate to **File and Storage Services > Shares**.



Create a new Share.

Filter	2 total	(€) ▼		TASKS VOLUMI New Share New Share Refresh New Share	
Share	Local Path	Protocol	Availability Type	17.5% L	lse
▲ WIN-U00T	4AO1ET9 (2)				
NETLOGON	C:\Windows\SYSVOL\sysvol	ad.loc SMB	Not Clustered		
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered		

Select Profile: SMB Share - Quick

Share Location: C:\Roaming_Profiles\$

ET9	Status Online	Cluster Not Clu	Role stered	Owner Node	
ET9	Online	Not Clu	stered		
ne:					
	Free Space	Capacity	File Syster	n	
	73.7 GB	89.3 GB	NTFS		
ın	ıme:	rme: Free Space 73.7 GB	rme: Free Space Capacity 73.7 GB 89.3 GB	ime: Free Space Capacity File Syster 73.7 GB 89.3 GB NTFS	me: Free Space Capacity File System 73.7 GB 89.3 GB NTFS

Share Name: Click "Next"

Other Settings: Make sure to check "Enable access-based enumeration".



Permissions: Click "Customize Permissions".

w Share Wizard				- (
ecify permiss	sions to co	ntrol access			
lect Profile	Permissions	to access the files on a sha	are are set using a	combination of folder permission	
Tare Location	permissions	, and, optionally, a central	access policy.		
nare Name	Share permissions: Everyone Full Control				
ther Settings	Folder perm	hissions:			
ermissions	Туре	Principal	Access	Applies To	
	Allow	CREATOR OWNER	Full Control	Subfolders and files only	
onfirmation					
onfirmation	Allow	BUILTINUSers	Special	This folder and subfolders	
onfirmation esults	Allow	BUILTIN/Users BUILTIN/Users	Special Read & execu	This folder and subfolders This folder, subfolders, and files	
onfirmation esults	Allow Allow Allow	BUILTIN Users BUILTIN Users BUILTIN VAdministrators	Special Read & execu Full Control	This folder and subfolders This folder, subfolders, and files This folder, subfolders, and files	

"Add" a new permission.

lame:	C:\Roaming_Profiles\$			
)wner:	Administrators (AD\Administr	Administrators (AD\Administrators) Change		
Permissio	ns Share Auditing	Effective Access		
or additio ermission	nal information, double-click a pern entries:	hission entry. To modify a	permission entry, select	the entry and click Edit (if available).
iype	сустем	Access Full control	Innented from	This folder, subfolders and files
	SYSTEM Administration (AD) Administra	Full control	C:\	This folder, subfolders and files
	Administrators (AD\Administr	Pull control	C:\	This folder, subfolders and files
Allow	Users (AD\Users)	Read of execute	C:\	This folder, subfolders and files
Allow Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only
Add	Remove View			
Disable	inheritance			

Click "Select a principal" and then enter "Domain Users" in the pop-up window. Select "Check Names" to validate your selection and then choose "Ok" to lock in configurations.

Principal:	Select a principal	Select User, Computer, Service Account, or Group	×
Туре:	Allow	Select this object type:	
Applies to:	This folder, subfolders and files	User, Group, or Built-in security principal Object Typ	es
		From this location:	
		ad local Location	s
asic perm	issions:	Enter the object name to select (examples):	niss
	Full control	Domain Users	mes
	Modify		lica
	✓ Read & execute		
	✓ List folder contents		
	✓ Read	Advanced OK Cano	xel .
	Write		
	Special permissions		

Ensure the following permissions are set so AD users have close to full access to their own file systems. Click "Ok" when done!

Permission	n Entry for Roaming_Profiles\$				- 0
Principal:	Domain Users (AD\Domain Users)	elect a principal			
Туре:	Allow	~			
Applies to:	This folder, subfolders and files	~			
Basic permi	issions:				Show advanced permissio
	Full control				
	☐ Modify				
	🖌 Read & execute				
	List folder contents				
	🗹 Read				
	🗹 Write				
	Special permissions				
Only app	oly these permissions to objects and/or	containers within this	container		Clear all
Add a cond	lition to limit access. The principal will	he granted the specifi	ad permissions only if con	ditions are met	
	and to mill decess the principal time	be granted the specifi	cu permissions only in com		
Add a cond	lition				

In the original popup-window select "Apply" and then "Ok".

click Edit (if available).
to
der, subfolders and files
der, subfolders and files
der, subfolders and files
der. subfolders and files
der and subfolders
ers and files only

Confirmation: Click "Create" when ready.

🔁 New Share Wizard			<u></u>		×
Confirm selection	IS				
Select Profile Share Location Share Name Other Settings Permissions	Confirm that the following SHARE LOCATION Server: Cluster role: Local path:	are the correct settings, a WIN-U00T4AO1ET9 Not Clustered C:\Roaming_Profiles\$	nd then click Cr	eate.	
Confirmation Results	SHARE PROPERTIES Share name: Protocol: Access-based enumeration: Caching: BranchCache: Encrypt data:	Roaming_Profiles\$ SMB Enabled Enabled Disabled Disabled			
		< Previous Next >	Create	Cance	el

Navigate to **Tools > Active Directory Users and Computers > Employees**. Then, right click on a user and select "Properties". Within the popup window, open the "Profile" section and specify the following Profile path: \\server_name\profile_folder_name\%username%. I used: **WIN-U00T4AO1ET9\Roaming_Profiles\$\%username%**

Active Directory Users and Computers		Bill Bob Properties			? ×
File Action View Help	🛿 🗔 浅 🗽 🗃 🍸 🚨 🍇	Member Of Remote control	Dial-in Remote De	Environment esktop Services Profile	Sessions COM+
 Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers Fernance ForeignSecurityPrincipal: Managed Service Accour Users 	TypeDescriptionCopyAdd to a groupAdd to a groupDisable AccountReset PasswordMoveOpen Home PageSend MailAll Tasks>CutDeleteRenamePropertiesHelpImage: Contemport of the second	General Address User profile Profile path: Logon script: Home folder () Local path: () Connect:	Account μυοσταλο 1ΕΤ	Profile Telephones 9\Roaming_Profiles\$\%us	Organization
Resets the password for the current selection.			OK Ca	ancel Apply	Help

Click "Apply" and "Ok" when done!

Project 8: VPN Server

Below contains steps outlining the configuration of a **WireGuard** service on my **pfSense firewall** (10.161.21.4). The VPN server will be used to allow approved external clients to connect to an **internal VPN subnet** enabling them to access select internal services. In a real world scenario, this is very helpful for remote work since employees can use a VPN to securely connect to the organization's network from anywhere.

VPN Information

pfSense Firewall: **10.161.21.4** WireGuard Port: **51820** (default) Internal VPN Subnet: **192.168.3.0/24** WAN Client IP: **10.161.21.20** Internal Client IP Assignment: **192.168.3.2**

pfSense Configuration

I will be using WireGuard to host a vpn service on my pfSense firewall.

Install WireGuard

WireGuard is a modern, lightweight VPN protocol that operates in the Linux kernel for high performance and minimal overhead, making it ideal for both mobile and server environments. As a VPN server, WireGuard can be deployed to allow remote clients to securely access private networks, route internet traffic through encrypted tunnels, or connect multiple networks across locations.

I will create a 3rd subnet managed by pfSense to facilitate my VPN server. LAN: 192.168.1.0/24 DMZ: 192.168.2.0/24 VPN: 192.168.3.0/24 Login to the pfSense admin dashboard within a browser at http://192.168.1.1

	System - Inte	rface					
Status / F	Advanced						
Status / L	Certificates General Setup						
System Info	High Availability						
Name	Package Manager						
User	Register	2					
System	Routing	in					
	Setup Wizard	3					
BIOS	Update	n					
	User Manager	v					
Version	Logout (admin)	64					
	built on Wed Dec	5 20:1					

Navigate to System > Package Manager > Available Packages

Search for "WireGuard"

Search					-
Search term	WireGuard		Both	~	Q Search Clear
	Enter a search string or *nix regular expression to search package nam	nes ar	nd descriptions.		

Once the WireGuard package is located, click Install.

WireGuard 0.2.1 WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.

Confirm the installation.

pfSense-pkg-WireGuard installation successfully completed.

Create WireGuard Tunnel

Navigate to **VPN > WireGuard** using the top bar and click **Add Tunnel**.

	Se System - ITION	Interfaces - Firev	vall - Services -	VPN - S	Status -	Diagnostics 👻	Help 🗕	0
VPN /	WireGuard /	Tunnels						₩ 8
Tunnels	Peers Setti	ngs Status						
11/1-0								
Name	ard Tunnels Description	Public Key	Address / A	ssignment		Listen Port	Pee	rs Actions
Name No Wire	ard Tunnels Description Guard tunnels have be	Public Key	Address / A	ssignment		Listen Port	Pee	rs Actions
Name No Wire	ard Tunnels Description Guard tunnels have be	Public Key	Address / A	ssignment w to create one.		Listen Port	Pee	rs Actions

WireGuard Configuration

- **Port:** 51820
- Public Key: YSZ33x1OWiYAYQHVc4geSH9jx5zhngwWLarokCGA4XI=

Tunnel Configuration	ı (tun_wg0)		
Enable	Enable Tunnel Note: Tunnel must be enabled in order to be assigned to a	pfSense interface.	
Description	Description Description for administrative reference (not parsed).		
Listen Port	51820 Port used by this tunnel to communicate with peers.		
Interface Keys	Private key for this tunnel. (Required)	YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4XI Public key for this tunnel. (Copy)	P Generate New Keys
Interface Configurati	on (tun_wg0)		
Assignment	🕂 Interface Assignments		
Firewall Rules	WireGuard Interface Group		
Hint	These interface addresses are only applicable for unassign	ed WireGuard tunnel interfaces.	
Interface Addresses	192.168.3.0 / 24 v IPv4 or IPv6 address assigned to the tunnel interface.	Description Description for administrative reference (not parsed).	
Add Address	+ Add Address		

Navigate to the **Settings** tab and "Enable WireGuard".

Tunnels Pe	ers	Settings Status	
General Settir	ngs		
	Enable	 Enable WireGuard Note: WireGuard cannot be disabled when one or more tunnels is assign 	ied to a pfSense interface.
Keep Config	uration	 Enable Note: With 'Keep Configurations' enabled (default), all tunnel configurations 	ons and package settings will persist on install/de-install.
Endpoint Hos Resolve I	stname Interval	300 Interval (in seconds) for re-resolving endpoint host/domain names. Note: The default is 300 seconds (0 to disable).	☐ Track System Resolve Interval Tracks the system 'Aliases Hostnames Resolve Interval' setting. Note: See System > Advanced > Firewall & NAT
Interface Memi	e Group bership	All Tunnels Configures which WireGuard tunnels are members of the WireGuard inte Note: Group firewall rules are evaluated before interface firewall rules. Do	rface group. efault is 'All Tunnels.'

Result:

VPN / WireGuard / Tunnels Co = 1								
Tunnels	Peers Setti	ings Status						
WireGuard	Tunnels							
Name	Description	Public Key	Address / Assignment	Listen Port	Peers	Actions		
> tun_wg0		YSZ33x10WiYAYQHVc4geSH9jx5zhngwW	192.168.3.0/24	51820	0	≗ +∥ ≵ ⊘ ڨ		
						+ Add Tunnel		

Interface Assignment

I now need to configure the network interface for WireGuard.

Navigate to Interfaces > Assignments using the top bar



Select Add to enable the VPN interface.

Interface	Network port		
WAN	vmx0 (00:50:56:82:4a:58)	*	
LAN	vmx1 (00:50:56:82:c8:d7)	•	Delete
DMZ	vmx2 (00:50:56:82:95:7a)	•	Delete
Available network ports:	tun_wg0 (tun_wg0)	~	+ Add

Click on the new interface name "OPT2" to open the configuration menu.



VPN Interface Configuration

- Enable the Interface
- Static IPv4
- IP Range: 192.168.3.1/24
- Keep "Block private networks" and "Block bogon networks" unchecked

General Configuratio	n
Enable	Z Enable interface
Description	VPN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
МТU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and ivate minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Static IPv4 Configura	ation
IPv4 Address	192.168.3.1
IPv4 Upstream gateway	None Add a new gateway
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.
Reserved Networks	
Block private networks and loopback addresses	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (f±00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	Blocks traffe from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
	This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local trafficate Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings. Go to Sett

Click **Save** at the bottom when you are done and then **Apply Changes**.

Result:

Interfaces / Interface Assignments								<u>Im</u> 🚱		
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs	
Interface	Network port									
WAN	vmx0 (00:50):56:82:4a:58)						*		
LAN	vmx1 (00:50):56:82:c8:d7)						*	Delete	
DMZ	vmx2 (00:50):56:82:95:7a)						¥	Delete	
VPN	tun_wg0 (tu	n_wg0)						*	Delete	
Save										
Firewall Rules

VPN Rules

I want the VPN subnet to not allow any communication to the LAN and allow all communication to the DMZ.

Navigate to Firewall > Rules using the top bar.



Within the **VPN** tab, create new firewall rules.

Rule 1: REJECT ALL to LAN

- Source: VPN Subnets
- Destination: LAN Subnets
- This rule will block all traffic traveling to the LAN

Edit Firewall Rule	
Action	Reject Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	 Disable this rule Set this option to disable this rule without removing it from the list.
Interface	VPN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which IP protocol this rule should match.
Source Source	□ Invert match VPN subnets ✓ Source Address / ✓
Destination Destination	Invert match LAN subnets Destination Address /

Rule 2: ALLOW ALL

- Source: VPN Subnets
- Destination: Any (*)
- This rule will allow the VPN devices to communicate with the WAN and DMZ

Edit Firewall Rule		
Action	Pass Choose what to do with pac Hint: the difference between whereas with block the pack	kets that match the criteria specified below. block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, let is dropped silently. In either case, the original packet is discarded.
Disabled	Disable this rule Set this option to disable thi	s rule without removing it from the list.
Interface	VPN Choose the interface from w	hich packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol	version this rule applies to.
Protocol	Any Choose which IP protocol th	▼ is rule should match.
Source		
Source	Invert match	VPN subnets VPN subnets / v
Destination Destination	Invert match	Any Destination Address / V

Final VPN Firewall Rules

• NOTE: The REJECT ALL to LAN rule is listed as first priority. This will ensure that traffic to the LAN will not be allowed!

Firewall / Rules / VPN									Lill 📰 😢			
Fle	pating	Wire	Guard \	WAN LAN	DMZ	VPN						
Ru	les (Drag to	Change Or	·der)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	۲	States 0/60 B	Protocol	Source VPN subnets	Port *	Destination LAN subnets	Port *	Gateway *	Queue none	Schedule	Description REJECT ALL to LAN	Actions
	⊘ ✓	States 0/60 B 0/0 B	Protocol IPv4 * IPv4 *	Source VPN subnets VPN subnets	Port *	Destination LAN subnets	Port *	Gateway * *	Queue none none	Schedule	Description REJECT ALL to LAN ALLOW ALL	Actions ♣��□♡面 ♣��□♡面×

WAN Rules

I need to allow VPN traffic from WAN clients into pfSense so they can properly connect.

Rule: ALLOW WireGuard VPN

- Pass
- Protocol: UDP
- Source: Any (*)
- Destination: WAN Address (pfSense public IP: 10.161.21.4)
- Port: 51820 (WireGuard Port)

Edit Firewall Rule		
Action	Pass	
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RS whereas with block the packet is dropped silently. In either case, the original pack	T or ICMP port unreachable for UDP) is returned to the sender, et is discarded.
Disabled	 Disable this rule Set this option to disable this rule without removing it from the list. 	
Interface	WAN Choose the interface from which packets must come to match this rule.	
Address Family	IPv4 Select the Internet Protocol version this rule applies to.	
Protocol	UDP Choose which IP protocol this rule should match.	, G
Source Source	Invert match Any	 ✓ Source Address ✓ ✓
	Display Advanced The Source Port Range for a connection is typically random and almost never ex- its default value, any.	qual to the destination port. In most cases this setting must remain at
Destination Destination	Invert match WAN address	Destination Address
Destination Port Range	(other)51820(other)FromCustomTo	✓ 51820 Custom
	Specify the destination port or port range for this rule. The "To" field may be left	empty if only filtering a single port.

New WAN Firewall Rules

Rule	es	(Drag to	Change Orde	∍r)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	/	0/0 B	IPv4 UDP	*	*	WAN address	51820	*	none		ALLOW WireGuard	∜ ⁄ ⁄ □ ⊘ ল ×
	/	1/3.24 MiB	IPv4 TCP/UDP	*	*	192.168.2.3	53 (DNS)	*	none		NAT	ৼৢ৻ঢ়৾৾৾৾৾ঀ৾৾৾৾৾৾৾৾৾
	/	0/24 KiB	IPv4 TCP	*	*	192.168.2.3	80 (HTTP)	*	none		NAT Port forward HTTP traffic to Apache Web Server	ৼৢ৻ঢ়৾৾৾৾ঀ৾৾৾৾ঢ়৾৾৾ঢ়৾
	1	0/2.63 MiB	IPv4 TCP	*	*	192.168.2.3	443 (HTTPS)	*	none		NAT Port forward HTTPS traffic to Apache Web Server	ৼৢ৻৻৻৻৻
									E	Add	Add 🛅 Delete 🛇 Toggle 📮 Copy 🖬	Save + Separator

WireGuard Client Setup

In order to connect to the newly created WireGuard VPN service on pfSense, we have to install the proper client software on our WAN device. There is no need to install the software on the LAN workstations since they are already on the internal network.

Login to your WAN client device

Open a browser and navigate to <u>https://www.wireguard.com/install/</u> Download the Windows Installer



Open the WireGuard application and go to the bottom left corner. Open the dropdown menu and select "Add empty tunnel..."

🚍 Add Tunnel 💌 🗙 🚞		
Import tunnel(s) from file	Ctrl+O	
Add empty tunnel	Ctrl+N	c

Public Keys

Client Public Key

Add a name for your tunnel and remember your client's public key.

Tunnel Name: pfSense

Public Key: AqEDALWCBVqLzbh8YEI9PRokwWBzH++0J7p0EGaJ/g4=

🔠 Edit tunr	hel	×
Name:	pfSense	
Public key:	AqEDALWCBVqLzbh8YEI9PRokwWBzH++0J7p0EGaJ/g4=	

Server Public Key

Go back to pfSense and access your WireGuard VPN Tunnel to get the server's public key. WireGuard Server Public Key: YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4XI= pfSense public WAN IP and Port: 10.161.21.4:51820

VPN / WireGuard	/ Tunnels / Edit		C® 幸 ⊡ 0
Tunnels Peers	Settings Status		
Tunnel Configuration	(tun_wg0)		
Enable	Enable Tunnel Note: Tunnel cannot be disabled when assigned to a pfSen	se interface.	
Description	Description Description for administrative reference (not parsed).		
Listen Port	51820 Port used by this tunnel to communicate with peers.		
Interface Keys	Private key for this tunnel. (Required)	YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4X Public key for this tunnel. (Copy)	P Generate New Keys

Peer Creation

Stay in pfSense and create a peer connection by navigating to **VPN > WireGuard > Peers** and selecting **Add Peer**.

Note: Public Ke	y is the Windows	Client public key	y!
-----------------	------------------	-------------------	----

Enable	Enable Peer Note: Uncheck this option to disable this peer without removing it from	the list.	
Tunnel	tun_wg0 WireGuard tunnel for this peer. (Create a New Tunnel)	•	
Description	WAN Windows Client (Rebecca) Peer description for administrative reference (not parsed).		
Dynamic Endpoint	Dynamic Note: Uncheck this option to assign an endpoint address and port for th	ils peer.	
Keep Alive	Keep Alive Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).		
Public Key	AqEDALWCBVqLzbh8YEI9PRokwWBzH++0J7p0EGaJ/g4= WireGuard public key for this peer.		
Pre-shared Key	Pre-shared Key Optional pre-shared key for this tunnel. (Copy)	Cenerate	

Address Configuration	on							
Hint	Allowed IP entries here will be transformed into proper su multiple peers on the same tunnel. Otherwise, traffic to th	wed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must be unique between iple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.						
Allowed IPs	192.168.3.2 / 32 🗸	Description						
	IPv4 or IPv6 subnet or host reachable via this peer.	Description for administrative reference (not parsed).						
Add Allowed IP	+ Add Allowed IP							

Client Tunnel Configuration

Navigate back to your client device and finish configuring the new tunnel.

- [INTERFACE]
 - Public Key = the static internal IP assignment when the client is connected
- [PEER]
 - Public Key = pfsense's public key for WireGuard
 - Allowed IPs = the allowed subnets for traffic to route through
 - Endpoint = public socket to connect to the VPN -> pfSenseIP:WireGuard Port

Final Tunnel File

```
[Interface]
PrivateKey = +O+mVPd7VVyrhH8e+Vi3bejQQT7QxKfosRE/odqngmg=
Address = 192.168.3.2/24
```

```
[Peer]
PublicKey = YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4XI=
AllowedIPs = 192.168.3.0/24, 192.168.2.0/24
Endpoint = 10.161.21.4:51820
```

Note: The AllowedIPs section specifies which subnets will be routed through the VPN tunnel. In this configuration, the client device will route traffic destined for 192.168.3.0/24 and 192.168.2.0/24 through the WireGuard tunnel. All other traffic will be sent via the device's regular network interface (NIC), effectively creating a "split tunnel" setup.

```
Edit tunnel
X

Name:
pfSense

Public key:
AqEDALWCBVqLzbh8YEI9PRokwWBzH++0J7p0EGaJ/g4=

[Interface]
PrivateKey = +0+mVPd7VVyrhH8e+Vi3bejQQT7QxKfosRE/odqngmg=
Address = 192.168.3.2/24
[Peer]
PublicKey = YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4XI=
AllowedIPs = 192.168.3.0/24, 192.168.2.0/24
Endpoint = 10.161.21.4:51820
Save Cancel
```

VPN Testing

Client Testing

Once you have a proper tunnel file on the client device and a configured peer on pfSense, **Activate** the tunnel within the WireGuard application.

) pfSense	Interface: pfSense Status: Inactive Public key: AqEDALWCBVqLzbh8YEI9PRokwWBzH++0J7p0EGaJ/g Addresses: 192.168.3.2/24 Activate	4=	
	Peer Public key: YSZ33x10WiYAYQHVc4geSH9jx5zhngwWLarokCGA4 Allowed IPs: 192.168.3.0/24, 192.168.2.0/24 Endpoint: 10.161.21.4:51820	XI=	
- Add Tuppel		Edit	

Once the tunnel is active, open a terminal to verify you are within the private VPN subnet with the command: **ipconfig**

You should be able to see 2 network interfaces with an internal VPN IP and a personal IP.



After verifying you are on the internal VPN subnet, try pinging a service in the DMZ such as the web server (**192.168.2.2**) and then try pinging the LAN gateway (**192.168.1.1**).

The DMZ ping should succeed and the LAN ping should fail.

PS C:\Users\Rebecca> ping 192.168.2.1									
Pinging 192.168.2.1 with 32 bytes of data: Reply from 192.168.2.1: bytes=32 time=6ms TTL=64 Reply from 192.168.2.1: bytes=32 time<1ms TTL=64 Reply from 192.168.2.1: bytes=32 time=1ms TTL=64 Reply from 192.168.2.1: bytes=32 time<1ms TTL=64									
<pre>Ping statistics for 192.168.2.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 6ms, Average = 1ms PS C:\Users\Rebecca> ping 192.168.1.1</pre>									
Pinging 192.168.1.1 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out.									
Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),									

Server Testing

Within pfSense, navigate to **VPN > WireGuard > Status** and select the dropdown menu for your tunnel. This will display current connections and successful VPN handshakes.

Status / WireGuard C										
Tunnels	Peers	Settings	Status	-						
WireGuard Status										
Tunnel	Descrip	Description		Public Key	Address / Assignment		MTU	Listen Port	RX	тх
✓ ↑ tun_wg0			1	YSZ33x10WiYAYQHV	VPN (opt2)		1500	51820	52 KiB	1.36 MiB
Peers	Desc	ription		Latest Handshake	Public Key	Endpoint		Allowed IPs	RX	тх
	181	WAN Winde	ows Clie	40 seconds ago	AqEDALWCBVqLzbh8	10.161.21.2	20:54092	192.168.3.2/32	52 KiB	1.36 MiB

Appendix

The 3 Most Important Skills I have learned from CS 4400

1. Firewall and Local Network Configuration

Early in the course, I was tasked with configuring a pfSense firewall. Although I have participated in numerous Cyber Defense competitions through the UNISEC Cyber Security club at UNI, I had never been the teammate responsible for setting up a network-level firewall. My experience was limited to host-based firewalls like UFW for Linux or Windows Defender. Booting from the pfSense ISO, setting it up via the terminal, and then transitioning to the browser GUI was a significant learning experience. It provided a refresher on networking concepts such as subnetting, as I had to create two main internal subnets: LAN and DMZ. pfSense also introduced me to creating firewall rules, NAT port forwarding from the WAN into the internal subnets, and setting up services hosted on the firewall, such as the DNS Resolver, DHCP for the LAN, and a WireGuard VPN service. It was incredibly rewarding to finally put computer networking concepts into practice, physically seeing machines and services populate internal networks and connect with each other. Overall, having experience in creating my own Home Lab/Network Cluster will be a great topic to discuss during future job interviews!

2. DNS Configuration

After completing the firewall setup, properly configuring DNS was crucial for ensuring a fully connected network cluster. I had never touched DNS settings on personal devices nor had I ever configured a standalone DNS server before taking this course. My experience was limited to understanding how DNS queries are forwarded through nameservers worldwide to resolve domain names. The progression from setting up an internal caching DNS service on pfSense to installing and configuring a standalone DNS server using BIND was highly beneficial. I started with configuring a simple DNS caching mechanism and then advanced to setting up FQDN mappings using Forward and Reverse lookup zones. DNS setup also involved getting familiar with the nslookup and dig commands. nslookup is used to query DNS servers to obtain domain name or IP address mapping information, while dig provides detailed information about DNS queries and responses, allowing for more advanced troubleshooting and analysis.

3. Active Directory Configuration

The most tedious task of this course was setting up Active Directory on the Windows server. I learned that setting up services on Windows devices involves a lot of "wizards" and GUIs while services on Linux involve the command line and simple configuration files. I prefer the former but it was definitely beneficial to set up AD since it is a common enterprise deployment. For example, my own university uses AD for everything! After completing the initial installation and designating the Windows Server as a Domain Controller, it was fascinating to set up Forward and Reverse lookup zones. Active Directory actually uses DNS to connect to and authenticate client workstations. The setup concluded with creating a new forest and establishing an Organizational Unit (OU). Having some experience with AD will help with enterprise scenarios.