

Introduction

Information Systems Security is the art and science of protecting digital information technology infrastructure. To be successful in their mission, information security practitioners must first understand what they are defending. While IT infrastructures are constantly evolving and vary widely in their scale and complexity, almost every IT infrastructure will share common components and follow certain basic architectural principles. For example, all IT infrastructures contain client workstations and servers, and rely on common networking protocols and devices to connect those workstations and servers. In a globalized economy where Bring Your Own Device policies and remote workers are increasingly commonplace, most IT infrastructures will also include a VPN solution to secure off-network workers and devices. Collectively, the common assets and design principles of an IT infrastructure can be viewed through several different paradigms, but for the purposes of this lab, they will be introduced using a model referred to as the Seven Domains of a Typical IT Infrastructure. Under this model, an IT infrastructure is classified according to the following domains:

- User Domain: the people who access an organization's information system.
- Workstation Domain: any device that connects to an organization's private Local Area Network (LAN), including desktop computers, laptops, smartphones, and tablets.
- LAN Domain: the collection of devices that are connected on an individual segment of the organization's private network.
- LAN-to-WAN Domain: the point in the network where an organization's IT infrastructure connects to the Wide Area Network (WAN) and public Internet.
- WAN Domain: the connection between an organization's different remote sites, as well as the broader Internet, typically via an Internet Service Provider (ISP).
- Remote Access Domain: the connection between a remote user's workstation domain and LAN Domain, and the organization's private network.
- System/Application Domain: an organization's mission-critical systems, applications, and data, typically stored within a data center.

Each of these domains is accompanied by its own range of unique and overlapping security concerns. As an information security practitioner, it is your responsibility to ensure each of these domains is protected by multiple security controls – a process known as hardening. For example, the Workstation

Domain should be hardened by installing antivirus software, while the LAN-to-WAN Domain should be hardened using thoughtfully crafted firewall rules. Collectively, the process of applying multiple security controls across multiple domains is a concept referred to as Defense-in-Depth, which is predicated on the assumption that at some point or another, one or more of these security controls will fail or be defeated, at which point another control must be ready to take its place as the next line of defense.

In this lab, you will explore the seven domains within the context of a virtual lab environment. Along the way, you will review several foundational IT concepts, including operating systems, server roles, and network connectivity.

Lab Overview

SECTION 1 of this lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will review basic security controls on a Windows workstation.
2. In the second part of the lab, you will explore additional devices on the LAN segment, including a Linux-based switch and a FreeBSD-based file server.
3. In the third part of the lab, you will connect to a router-firewall device and learn about the network perimeter.

SECTION 2 of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will extend your exploration of the lab environment to the WAN, Remote Access, and System/Application Domains.

Finally, you will explore the virtual environment on your own in **SECTION 3** of this lab to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work - similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

1. Identify and navigate the seven domains of a typical IT infrastructure.
2. Use common command-line utilities to gather relevant system information.
3. Use PuTTY to remotely connect to network devices.
4. Identify common network devices, including switches, routers, and firewalls.
5. Identify common server roles, including domain controllers, web servers, and file servers.

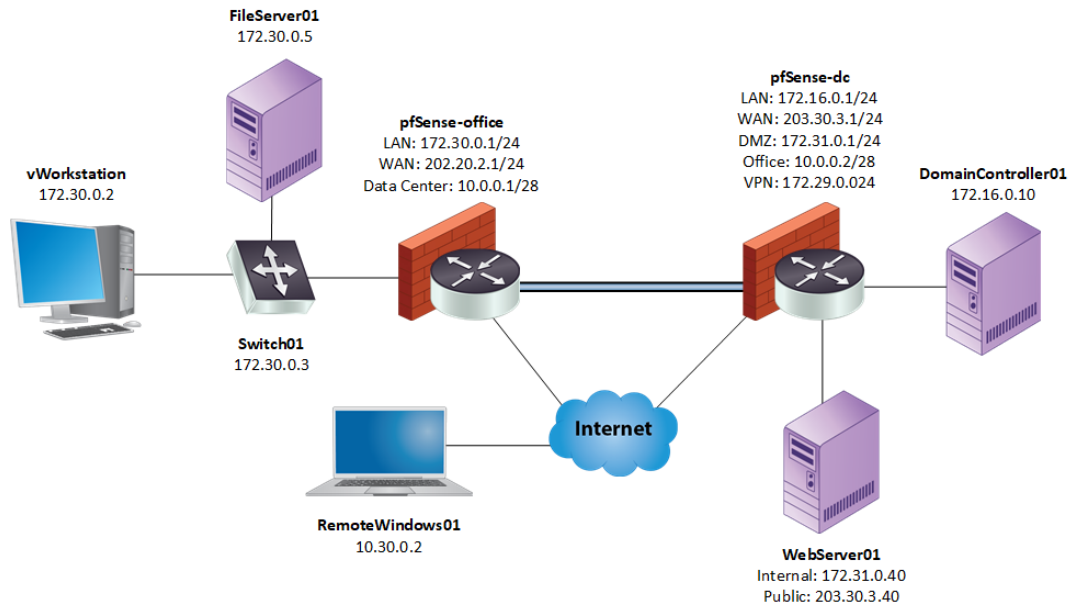
Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- vWorkstation (Windows: Server 2022)
- Switch01 (Linux: Debian 11)
- FileServer01 (FreeBSD)
- pfSense-office (FreeBSD)
- pfSense-dc (FreeBSD)
- DomainController01 (Windows: Server 2019)
- WebServer01 (Linux: Ubuntu 20)
- RemoteWindows01 (Windows: Server 2019)
- AttackLinux01 (Linux: Kali)

Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- PuTTY
- Ping
- Open vSwitch
- TrueNAS
- pfSense
- Traceroute
- Nslookup
- OpenVPN
- OWASP Juice Shop

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

SECTION 1

1. Lab Report file including screen captures of the following:

- Sign-in options for Alice's account
- View configured update policies page
- Virus & Threat Protection Settings
- Security warning from attempting to run an executable file
- Blocked attachment message
- Successful connection to the adodson user folder
- Failed connection to another user folder
- Successful connection to the Marketing shared folder
- Failed connection to another shared folder
- vWorkstation's original ARP table
- vWorkstation's updated ARP table
- Switch01 forwarding table
- Contents of the Employees directory
- Outbound NAT settings
- Permissive LAN rules
- Static Routes page
- Result of your tracert to the pfsense-dc appliance
- Port Forward rules for the web server
- DMZ firewall rules

2. Any additional information as directed by the lab:

- None

SECTION 2

1. Lab Report file including screen captures of the following:

- Static route for the point-to-point connection
- BPG neighbor ping results
- Traceroute to the file server
- Successful connection to the email server
- Successful reverse DNS lookup for the internal host
- Whoami results

- Members of the Developers AD group
- Password policy settings in the Group Policy Management Console
- DNS entries
- Docker service status
- Juiceshop.com web page
- Disks in the tank volume

2. Any additional information as directed by the lab:

- Document whether the VPN connection is split tunnel or full tunnel, based on the tracert results.

SECTION 3

1. Lab Report file including screen captures of the following:

- None

2. Any additional information as directed by the lab:

- Based on your research, identify at least two compelling threats to the User Domain and two effective security controls used to protect it. Be sure to cite your sources.
- Based on your research, identify security controls that could be implemented in the Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application Domains. Recommend and explain one security control for each domain. Be sure to cite your sources.

Section 1: Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverables.

1. Review the Tutorial.

Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

2. Proceed with Part 1.

Part 1: Explore the Workstation Domain

Note: In this part of the lab, you will learn about the Workstation Domain by exploring your local workstation within the lab environment: the vWorkstation. For the purposes of this lab, the vWorkstation is equivalent to a physical desktop computer that is located within a corporate or government office. Like most individual workstations intended for employee use, the vWorkstation is running the Windows operating system. While many organizations also rely on MacOS-based devices (as well as Android and iOS smartphones and tablets), Windows is still the most popular desktop operating system for day-to-day business functions, such as email, word processing, and web browsing.

The Workstation Domain intersects closely with the User Domain, which is comprised of the many individuals who interact with an organization's devices and assets. Given the fallibility and unpredictability of human beings, the User Domain is typically the weakest link in any IT infrastructure. For this reason, the Workstation Domain is home to the first line of defense against most risks, threats, and vulnerabilities in the User Domain. For example, consider the widespread threat posed by phishing, where attackers send misleading emails to thousands of users across multiple organizations in the hope that a few of them will be tricked into sharing their credentials or downloading malware. When regular security awareness training fails (and someone in your organization is *eventually* going to click a link that they shouldn't), Workstation Domain controls provide the next line of defense.

Common Workstation Domain controls include strict access controls, password policies, regular software updates, anti-malware software, mobile device monitoring, content filtering, and other forms of commercial end-point protection solutions. Critically, the end user is not responsible for managing any of these controls, and in many cases may not even be aware of their existence. Instead, the primary responsibilities for the Workstation Domain are shared between the Desktop Support team and the Information Security team.

In the next steps, you will assume the role of a desktop support engineer working at the fictional Secure Labs on Demand organization. Imagine that you have recently finished updating an older

Exploring the Seven Domains of a Typical IT Infrastructure (4e)

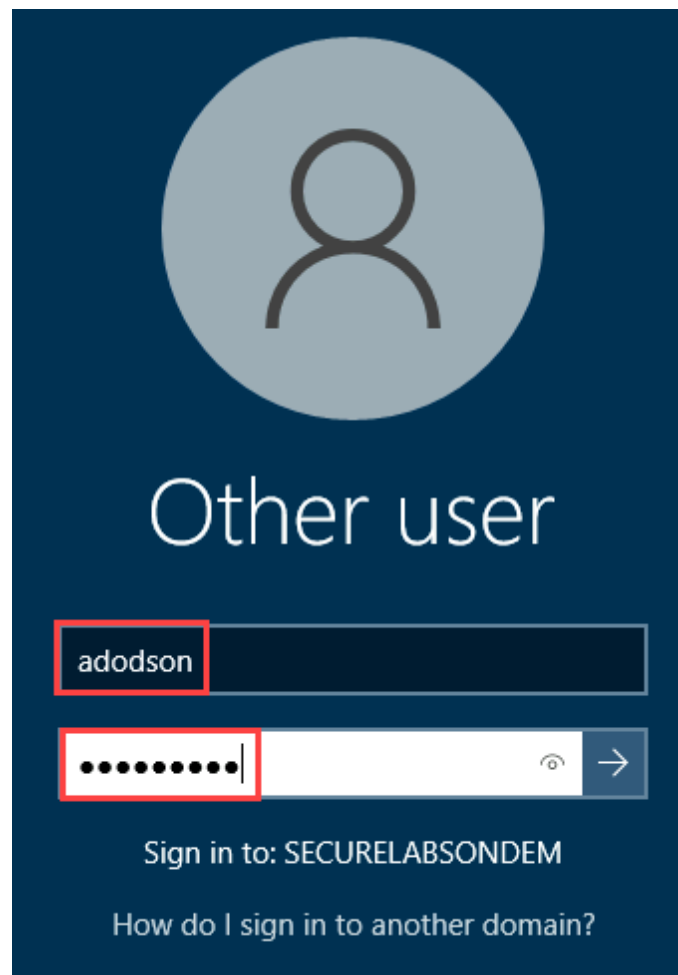
Fundamentals of Information Systems Security, Fourth Edition - Lab 01

employee workstation to the latest version of Windows. To ensure that the workstation is still compliant with your organization's security policies, you will log in using the employee's credentials and validate several basic Workstation Domain security controls.

1. At the vWorkstation log-in page, **click Other user**, then **type** the following credentials and **press Enter** to log in as the workstation's primary user.

User: **adodson**

Password: **P@ssw0rd!**



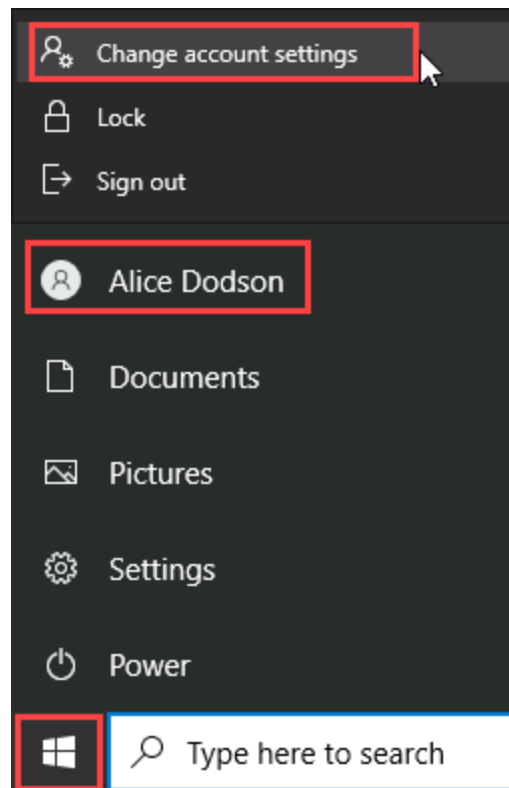
vWorkstation log-in screen

Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Note: As a first step, you will verify that system admin rights have been disabled for Alice's account. This critical control ensures that Alice does not have more access than is required to perform their job, and – in the event that Alice's workstation or credentials are compromised – neither will an attacker.

2. On the vWorkstation taskbar, **click** the **Start icon** and **hover** your cursor over the **User icon**, then **click** the **Alice Dodson icon** and **select Change account settings** to open the Your info page in the Settings application.



Change account settings

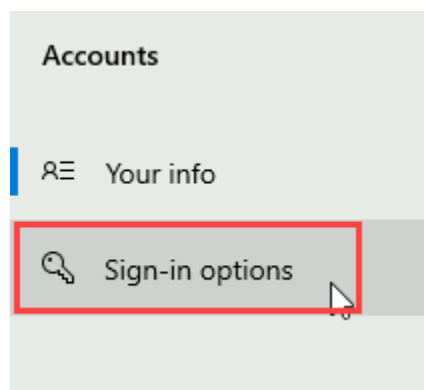
Note: The Your Info page shows basic information about Windows accounts. For accounts with Administrator privileges, you will see *Administrator* under the account name. Since you do not see that here, you know that Alice Dodson's account is not an Administrator account. You should also notice that Alice's account name (adodson) is preceded by *SECURELABSONDEM*, which indicates that Alice is a Domain User on a Domain Member computer. The use of the term "domain" here refers to a group of computers and devices that Windows can manage together, making it easy to share accounts and settings among domain members. You will learn more about domains in Section 2, Part 3, when you explore the System/Application Domain.

Your info



Your Info page

3. In the Settings window, **click** the **Sign-in options** link to display the Sign-In options page.



Sign-in options link

Note: On the Sign-in options page, you should see a message stating that “some of these settings

are hidden or managed by your organization.” This message is an example of an IT security policy being enforced by the organization. The Secure Labs on Domain organization has decided to manage some account settings at the organization level, rather than allowing each user to change them individually. This approach is one way of enforcing standards that can make organizations more secure.

Sign-in options

**Some of these settings are hidden or managed by your organization.*

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.



Security Key

Sign in with a physical security key



Password

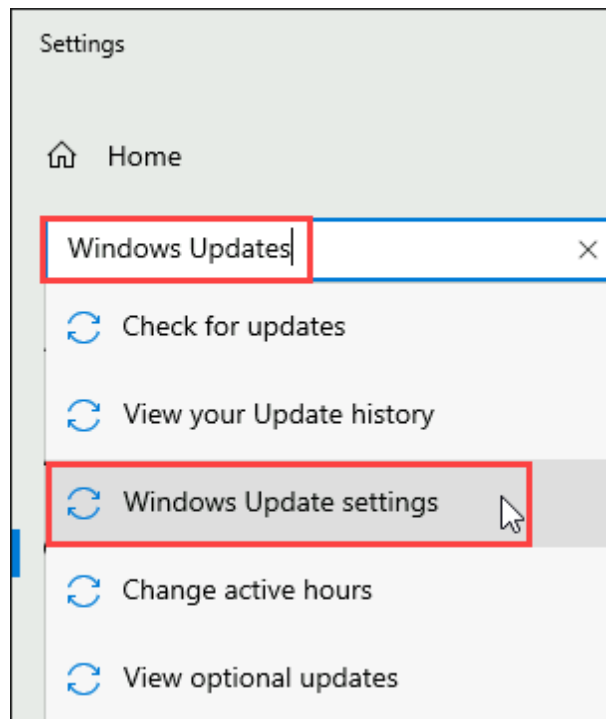
Sign in with your account's password

Sign-in options page

4. **Make screen capture** showing the **Sign-in options for Alice's account**.

Note: In the next steps, you will inspect the Windows Update settings to verify that the vWorkstation is automatically receiving system software updates. Attackers will never stop finding new ways to attack systems, so it is important to ensure that every system has the latest security updates installed. Fortunately, Microsoft allows administrators to create policies that ensure that systems are regularly updated with security patches, rather than leaving this critical responsibility to individual users. Automatically keeping computers and other devices up to date is one of the most important security practices in the Workstation Domain.

5. In the Settings window, **type Windows Updates** in the Find a setting field, then **select Windows Update settings** from the results to open the Windows Update settings page.



Search for Windows Updates

6. On the Windows Update page, **click the View Policies link** to open the View configured update policies page.

Windows Update

*Some settings are managed by your organization [\(View policies\)](#)



You're up to date

Last checked: 10/20/2021, 12:50 PM

Check for updates

*This option is managed by your organization.

[View Policies link](#)

Note: On this page, you can see a list of update policies that have been set on Alice Dodson's workstation. Collectively, these policies ensure that updates are handled the same way for all devices in an organization and prevent users from accidentally or intentionally interfering with the update process.

Policies set on your device

Disable check for updates by user

Source: Administrator

Type: Group Policy

Download the updates automatically and notify when they are ready to be installed

Source: Administrator

Type: Group Policy

Set Automatic Update options

Source: Administrator

Type: Group Policy

Disable Pause updates by user

Source: Administrator

Type: Group Policy

[Update policies](#)

7. Make a screen capture showing the **View configured update policies** page.

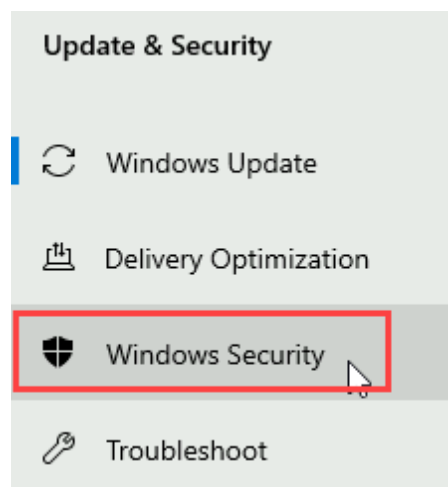
Note: Downloading and installing operating system and software updates is only one part of a comprehensive security strategy. Patching software with the latest security updates goes a long way toward reducing the number of known software vulnerabilities, but these efforts must be accompanied by real-time monitoring to detect suspicious activity. One of the more common types of real-time activity monitoring is anti-virus software. In the next steps, you will review the Windows Security application to verify that the Windows anti-virus software is enabled on the vWorkstation.

8. Click the **Back button** to return to the Windows Update page.



Back button

9. From the navigation menu on the left, click the **Windows Security** link to open the Windows Security settings page.

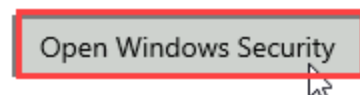


Windows Security link

10. On the Windows Security settings page, click the **Open Windows Security button** to open the Windows Security application in a new window.

Windows Security

Windows Security is your home to view and manage the security and health of your device.

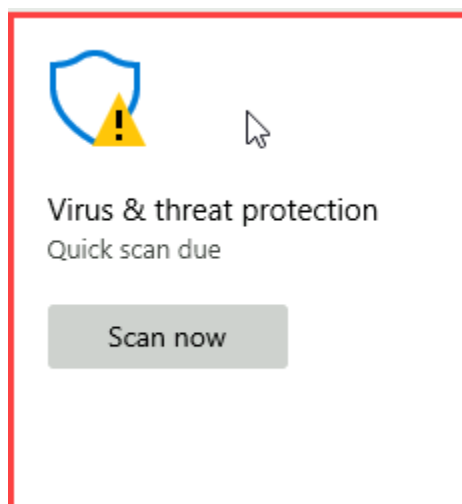


Open Windows Security button

Note: The Windows Security application provides four main areas of protection: Virus & threat protection, Firewall & network protection, App & browser control, and Device security. In the next steps, you will review Virus & threat protection settings.

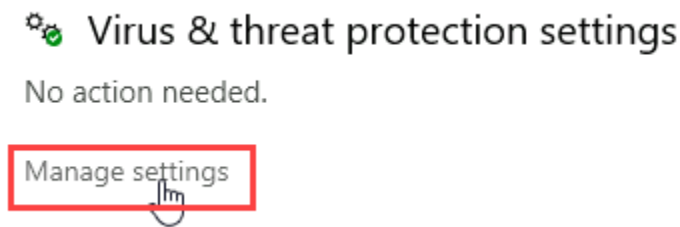
You may notice that Windows is recommending a Quick anti-virus scan. Ordinarily, regular scans should be automatically scheduled and managed by the organization, but for the purposes of this lab, automatic scans have been disabled to minimize interference with the lab exercise.

11. In the Windows Security window, **click the Virus & threat protection module** to open the Virus & threat protection page.



Virus & threat protection module

12. Under the Virus & threat protection header, **click** the **Manage settings link** to open the Virus & threat protection settings page.



Manage settings link

13. On the Virus & threat protection settings page, **attempt to deactivate** the Real-time protection, Cloud-delivered protection, and Tamper Protection settings.

Note: Although it appears you can turn off real-time, cloud-delivered, and tamper protection, you cannot. In this case, the local administrator has implemented a policy that blocks users from changing these settings. If you toggle any of these values, the switch immediately goes back to its previous setting (on).

14. **Make a screen capture** showing the **Virus & Threat Protection Settings**.

15. **Close** the **Windows Security** and **Settings windows**.

Note: Although policies like the ones you just reviewed can enforce an organization's rules to protect devices and software, there is always the possibility that an attacker will get past your defenses. To minimize the damage an attacker can do once they have gained access to a user's account, it is important to adhere to the Principle of Least Privilege. The Principle of Least Privilege simply means

that a user account only has the privileges necessary to carry out functions related to its assigned job function. If an attacker gains access to an account, they will not be able to use the account for anything beyond tasks within the owner's job function.

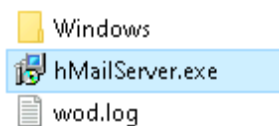
In the next steps, you will attempt to install a new application to verify that Alice's account has appropriately limited permissions.

16. On the vWorkstation taskbar, **click** the **File Explorer icon** to open a new File Explorer window.



File Explorer icon

17. In the File Explorer, **navigate** to the **C:** directory and **double-click** the **hMailServer.exe** file to attempt to run it.



hMailServer.exe

Note: You should see an error message stating that you must be logged in as administrator to install this program. While some users may find this policy inconvenient, restricting standard users from installing software without administrator approval is a critical security control for preventing malicious actors from installing tools that could further compromise a system.

18. **Make a screen capture** showing the **security warning from attempting to run an executable file**.
19. **Click OK** to close the error dialog box, then **close** the **File Explorer window**.

Note: As previously mentioned, many of the security controls deployed in the Workstation Domain are designed to function as defenses against threats that originate in the User Domain. For example, many attacks begin with a user clicking on a malicious link in an email message, which could trigger a malware download or trick the user into divulging private information, such as a password. To protect users from email-based threats, many organizations use specialized software and services (such as those offered by Mimecast) to filter email for potential malicious content before it ever reaches a user's Inbox.

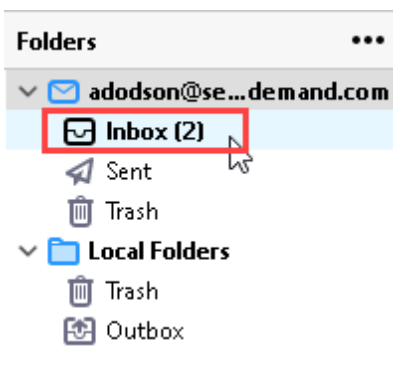
In the next steps, you will inspect Alice's email account. In order to test the email security solution managed by your organization, you previously sent a few test emails to Alice's account to verify the expected handling of incoming mail.

20. On the vWorkstation desktop, **double-click** the **Mozilla Thunderbird icon** to open the Thunderbird email client application.



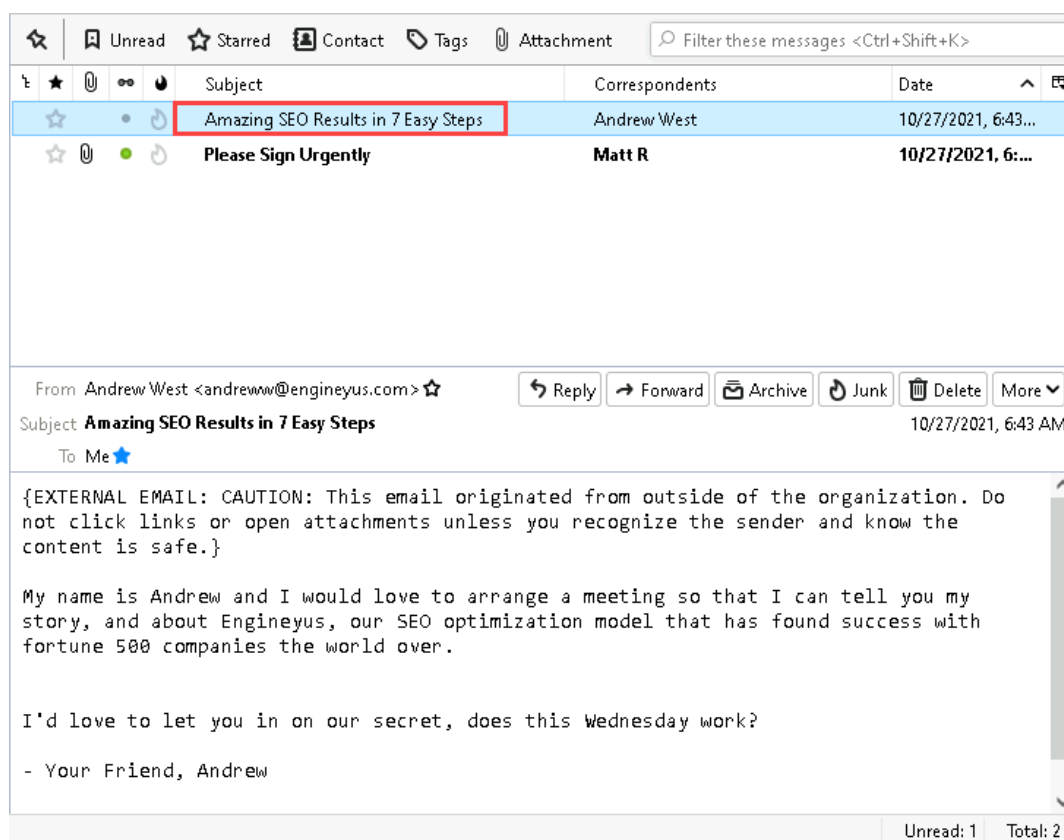
Thunderbird icon

21. In the left-hand Folders pane, **click** the **Inbox link** to open Alice's email Inbox.



Inbox

22. In the Inbox pane, **select** the **first email** (Amazing SEO Results in 7 Easy Steps) to display the message contents in the Preview pane.

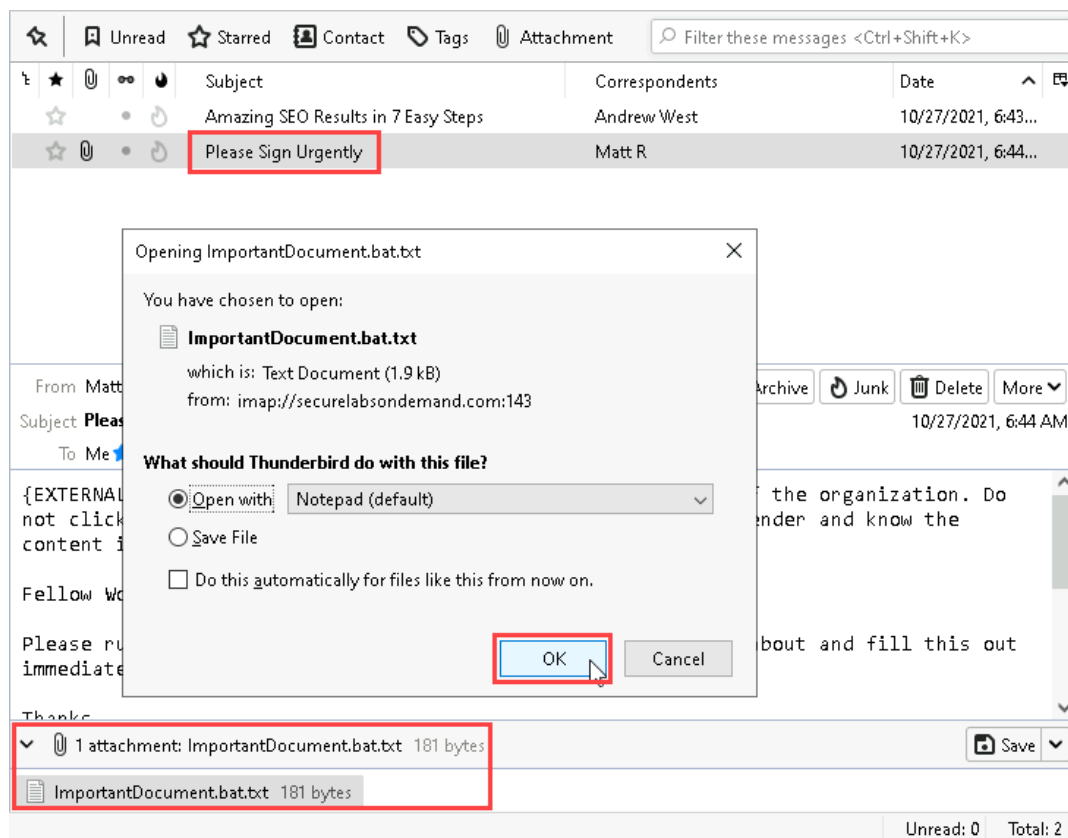


First email

Note: Pay attention to the EXTERNAL EMAIL: CAUTION warning in the body of the message. This message indicates that this message originated from outside the organization. In other words, this email was not sent by someone else in this organization. Email filters can be configured to automatically add this warning any time the server receives a message from an external server, regardless of the sender's email address. Although it is perfectly normal for users to regularly receive emails from outside their organization, adding this warning is a simple security measure that can remind users to handle these emails with caution. Additionally, if a seemingly internal email contains this warning, this could be a sign of a targeted phishing attempt, where the attacker is attempting to impersonate another person within the organization.

23. Select the **second email** (Please Sign Urgently), then **double-click** the **attachment** to open it.

When prompted, **click the OK button** to continue.



Second email

Note: You may notice that the ImportantDocument attachment is a .bat file with a .txt extension. Files with a .bat extension are Windows batch files, which contain commands that run when the file is opened. Malicious actors often use batch files to carry out attacks when unsuspecting victims open the attachment. In this case, the simulated email security service appears to have blocked the .bat file and replaced it with a harmless text file, which contains a warning that the original attachment was blocked.

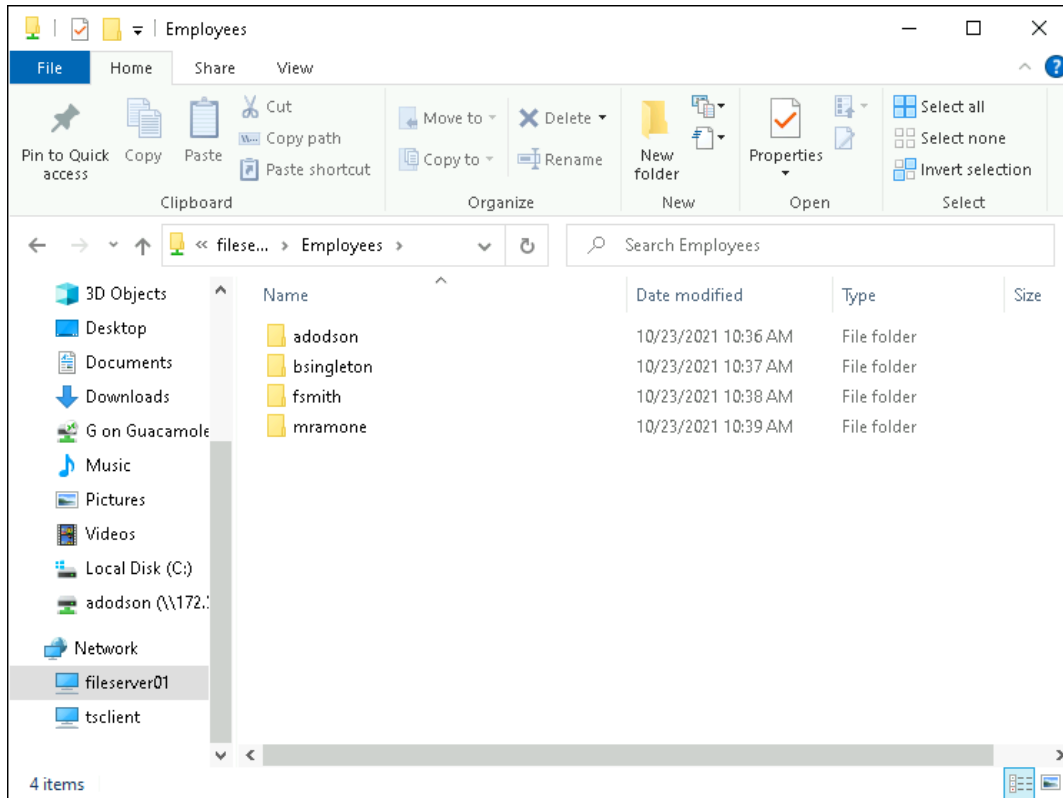
24. **Make a screen capture** showing the **blocked attachment message**.

25. **Close** the **Notepad** and **Thunderbird** windows.

Note: As a final check, you will verify that Alice's account has been assigned the correct permissions on Secure Labs on Demand's shared file server. For the purposes of this exercise, you will verify that Alice – a member of the marketing department – only has access to her own private folder and the Marketing team's shared folder.

26. On the vWorkstation taskbar, **click** the **File Explorer icon** to open a File Explorer window.

27. In the left-hand pane, **navigate** to **Network > fileserver01 > Employees**.



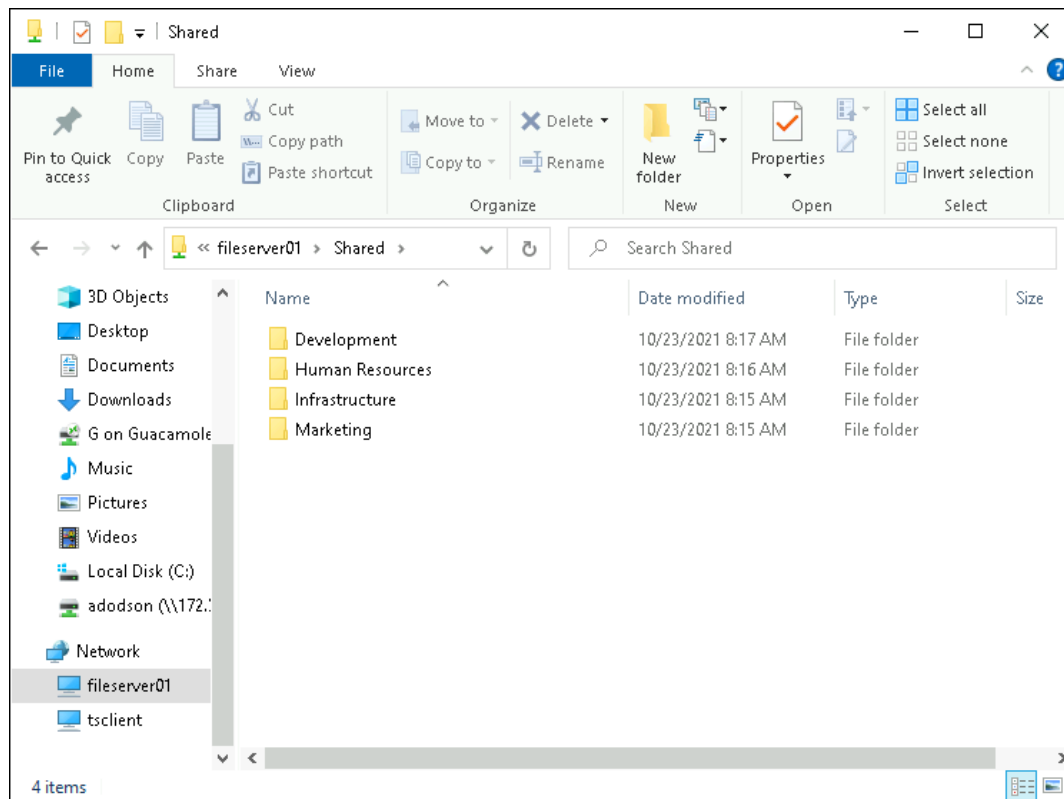
Employees folder

Note: Network shares are folders that are physically stored on other systems, but are accessible to authorized users as if they were local folders. In this case, Secure Labs on Domain uses a file server that is attached to its network. The file server provides individual folders for each user and a globally shared folder with individual folders for each department. The share permissions are configured to limit each user to their own folder and the shared folder for their department.

28. **Make a screen capture** showing a **successful connection to the adodson user folder**.

29. **Make a screen capture** showing a **failed connection to another user folder**.

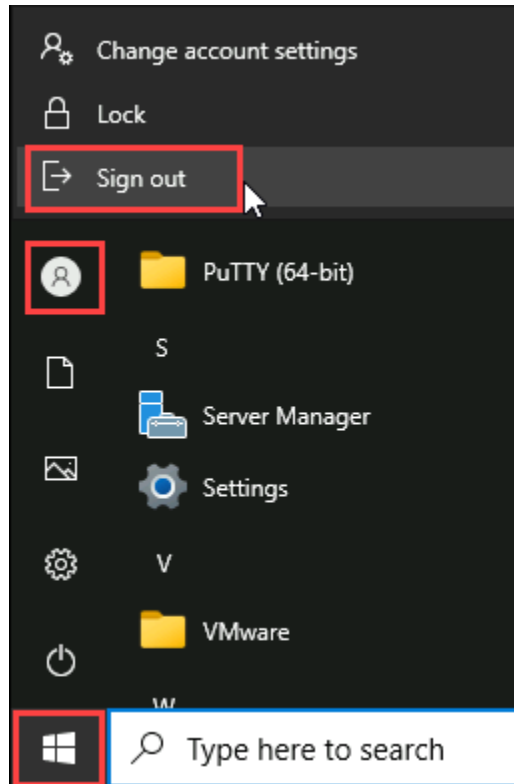
30. On the File Explorer toolbar, **click the Back button** to return to the FileServer01 directory, then **double-click the Shared folder** to open it.



Shared folder

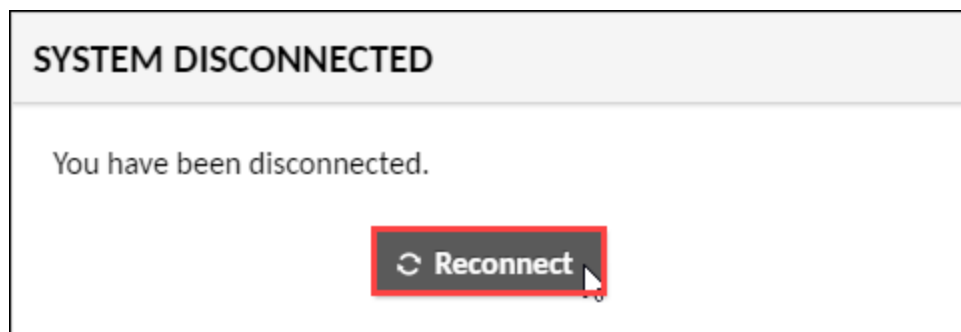
Note: While all authorized users can access the Shared folder, users can only access the folders associated with the department. In this case, Alice Dodson is a member of the Marketing department. Therefore, her account should be able to access the Marketing folder, but no others.

31. **Make a screen capture** showing a **successful connection to the Marketing shared folder**.
32. **Make a screen capture** showing a **failed connection to another shared folder**.
33. From the vWorkstation taskbar, **click the Start icon** and **hover** your cursor over the **User icon**, then **click the Alice Dodson icon** and **select Sign out** to log out of the Alice Dodson account.



Sign out

34. When prompted, **click** the **Reconnect** button to return to the vWorkstation log-in screen.



Reconnect button

Part 2: Explore the LAN Domain

Note: In this part of the lab, you will explore the LAN Domain within the virtual lab environment. Along with the LAN-to-WAN Domain, WAN Domain, and the Remote Access Domain, the LAN Domain is predominantly concerned with networking and network security. While these four domains are closely intertwined with overlapping security concerns, the LAN Domain deals specifically with security concerns in an organization's private Local Area Network, including the networking hardware that comprises the network, as well as the devices connected to it.

For the purposes of exploring the LAN Domain, it may be helpful to briefly review the foundational networking concepts outlined in the OSI Reference Model, which provides a convenient vocabulary for discussing network communications. The model consists of 7 layers, each of which plays a specific role in supporting communication between nodes in a network. The top-most layer is the Application Layer (also called Layer 7) and facilitates communications between the applications running on each networked node – for example, email. The bottom-most layer is the Physical Layer (or Layer 1) and consists of the physical connections between network nodes – for example, the Cat5 cables that connect a computer to a router or the radio signals that enable WiFi. Each intervening layer serves a specific purpose in translating the physical Layer 1 signals into useful information and ensuring that information reaches its intended destination.

Within the OSI Reference Model, the most relevant layer to the LAN Domain is Layer 2 – the Data Link Layer. While Layer 1 deals with individual bits of data, transmitted over a physical medium, Layer 2 protocols organize those bits into collections called frames, each of which is assigned the address of the intended recipient. These Layer 2 addresses are called Media Access Control addresses – or MAC addresses for short. Each node on a network has one or more unique MAC addresses, which are used by Layer 2 networking devices to determine where a frame should be sent on a LAN. The Layer 2 networking devices that facilitate communications on a LAN are commonly referred to as switches or bridges.

For the remainder of the lab, you will assume the role of a security engineer working at the fictional Secure Labs on Domain organization. You have been assigned the responsibility of familiarizing yourself with organization's network and critical systems. In the next steps, you will gather information about the vWorkstation's network configuration, verify connectivity with other devices on the LAN, and remotely connect to two of those devices.

1. At the vWorkstation log-in screen, **type P@ssw0rd!** to log in as the local Administrator.
2. On the vWorkstation taskbar, **click the Command Prompt icon** to open a new Command Prompt window.



Command Prompt icon

Note: While many of today's computer users prefer to use a Graphical User Interface (GUI), the Command Line Interface (CLI) is alive and well. Administrators and security practitioners often prefer the CLI for its efficiency and flexibility. CLI utilities typically perform very specific tasks and can easily be chained together to quickly build more complex solutions. They can even be included in scripts for repeated and scheduled operation. The CLI may take a little time to learn, but it is among the most important tools in a security practitioner's toolbox.

3. At the command prompt, **type** `ipconfig /all` and **press Enter** to display the vWorkstation's network interfaces.

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : vWorkstation
    Primary Dns Suffix . . . . . : securelabsondemand.com
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : securelabsondemand.com

Ethernet adapter Student:

    Connection-specific DNS Suffix . : 
    Description . . . . . : vmxnet3 Ethernet Adapter
    Physical Address. . . . . : 00-50-56-AB-90-03
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 172.30.0.2(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.30.0.1
    DNS Servers . . . . . : 172.16.0.10
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Truelab:

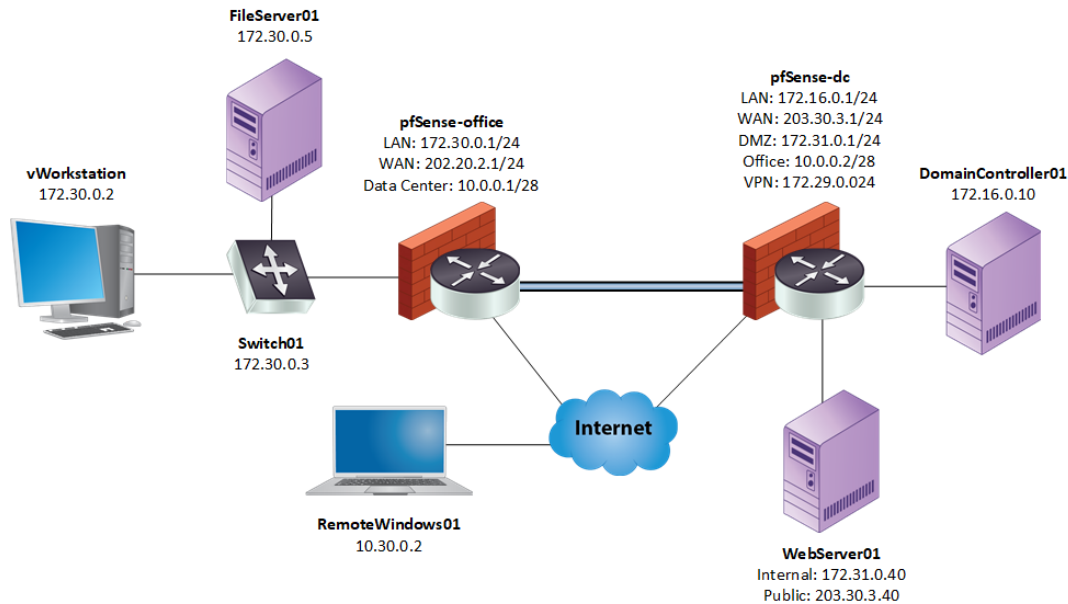
    Connection-specific DNS Suffix . : 
    Description . . . . . : vmxnet3 Ethernet Adapter #2
    Physical Address. . . . . : 00-50-56-AB-0E-31
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.156.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
    NetBIOS over Tcpip. . . . . : Disabled

C:\Users\Administrator>
```

Network interfaces

Note: Ipconfig is a Windows-based CLI utility used to display the configuration values assigned to its Network Interface Card(s), including the MAC address. Network Interface Cards (NICs) are hardware components that facilitate communications between a computer and a LAN. When we talk about a device's MAC address, we are actually referring to its NIC's unique hardware identifier.

In the command output, you should see two different Ethernet adapter results for the vWorkstation, which has two network interface cards. For the purposes of this lab, the only interface you are interested in is the Student interface, which facilitates communication with the network represented in the topology diagram that you reviewed in the Introduction (provided below for reference).



Network topology diagram

In the ipconfig output and on the network topology diagram, you will likely notice the four-part dotted numerical labels. These are Internet Protocol (IP) addresses, which are associated with OSI Layer 3 in a similar manner to which MAC addresses are associated with Layer 2. Although Layer 3 is most closely aligned to the LAN-to-WAN Domain, which you will explore in the next part of this lab, it is difficult to fully appreciate Layer 2 concepts without the added context of Layer 3 – the Network Layer. Just as Layer 2 protocols organize individual bits into frames and assign them the MAC address of the intended recipient, Layer 3 protocols encapsulate those frames into units called packets, which provide an additional layer of dynamic addressing. It is that additional layer of dynamic addressing – IP addressing – that allows packets to travel outside the LAN to reach devices on other networks via Layer 3 networking devices, commonly referred to as routers. In this case, the vWorkstation and its LAN are served by the pfSense-office firewall-router, which is identified in the ipconfig output as the Default Gateway.

While Layer 2 addresses are static and unique to individual NICs, Layer 3 addresses can change based on the network to which the device is currently connected. As demonstrated in the vWorkstation's ipconfig output, the relationship between a device's own MAC address and IP address is managed by its NIC. However, in order to communicate with other devices on the LAN, the vWorkstation must also keep track of their MAC/IP address relationships. Those relationships are managed by the Address Resolution Protocol (ARP), a Layer 2 protocol that is used to organize MAC/IP mappings into a table known as the ARP table or ARP cache.

In the next steps, you will review the ARP table associated with the Student NIC.

4. At the command prompt, **type** `arp -a` `172.30.0.2` and **press Enter** to display the ARP

table for the Student NIC.

```
C:\Users\Administrator>arp -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
    Internet Address      Physical Address      Type
    224.0.0.22            01-00-5e-00-00-16    static
C:\Users\Administrator>
```

ARP table

Note: The `arp -aN` command displays all IP/MAC address mappings associated with the Student NIC in the vWorkstation's ARP table. However, you may notice that none of the IP addresses for the other devices on the vWorkstation's LAN are listed here. When the vWorkstation attempts to communicate with an IP address on the same LAN that it does not currently have in its ARP table, it will first send out an ARP Request packet as a broadcast to the entire LAN. Upon receiving the broadcast, the device with the IP address in question will reply to the vWorkstation with an ARP Response, which provides the required IP/MAC address mapping. Upon receiving the response, the vWorkstation will update its ARP table accordingly.

In the next steps, you will generate traffic to the pfSense-office, Switch01, and FileServer01 devices in order to update the vWorkstation's ARP table.

5. Make a screen capture showing the vWorkstation's original ARP table.

Note: In the next steps, you will use the Ping utility to test connectivity between the vWorkstation and the other devices on the LAN. Initially released in 1983, ping stands for Packet Internet Groper and operates on OSI Layer 3 using the Internet Control Message Protocol (ICMP). The Ping utility allows you to test host availability and connectivity by measuring the round-trip time of ICMP packets transmitted between an originating host to a destination host.

- At the command prompt, **type** `ping 172.30.0.1` and **press Enter** to ping the pfSense-office device.

```
C:\Users\Administrator>ping 172.30.0.1

Pinging 172.30.0.1 with 32 bytes of data:
Reply from 172.30.0.1: bytes=32 time=1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64
Reply from 172.30.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>_
```

Ping the pfSense-office device

7. At the command prompt, **type** `ping 172.30.0.3` and **press Enter** to ping the Switch01 device.
8. At the command prompt, **type** `ping 172.30.0.5` and **press Enter** to ping the FileServer01 device.
9. **Repeat step 4** to display the vWorkstation's updated ARP table.

Note: The vWorkstation's ARP table should now include three additional entries – one for each of the three hosts that you pinged in the previous steps.

10. **Make a screen capture** showing the vWorkstation's updated ARP table.
11. **Close the Command Prompt window.**

Note: In the next steps, you will open a remote shell connection to the Switch01 device and review its networking configuration. As the name implies, Switch01 is a switch, which is the common name for networking devices that operate at OSI Layer 2 by directing frames across the network using MAC

addresses.

Given that Switch01 is a Layer 2 device, you may be wondering why it has an IP address. Although the term "switch" is often used to refer to a single type of the device, there are actually two types of switches: unmanaged and managed. An unmanaged switch is a simple hardware device that provides basic frame-forwarding capabilities. A managed switch can be a physical device or a program running on a computer, and can be configured to meet a wide range of networking needs. Because managed switches require administrative input, they will typically support remote connections via an IP address.

12. On the vWorkstation desktop, **double-click** the **PuTTY icon** to open the PuTTY configuration window.



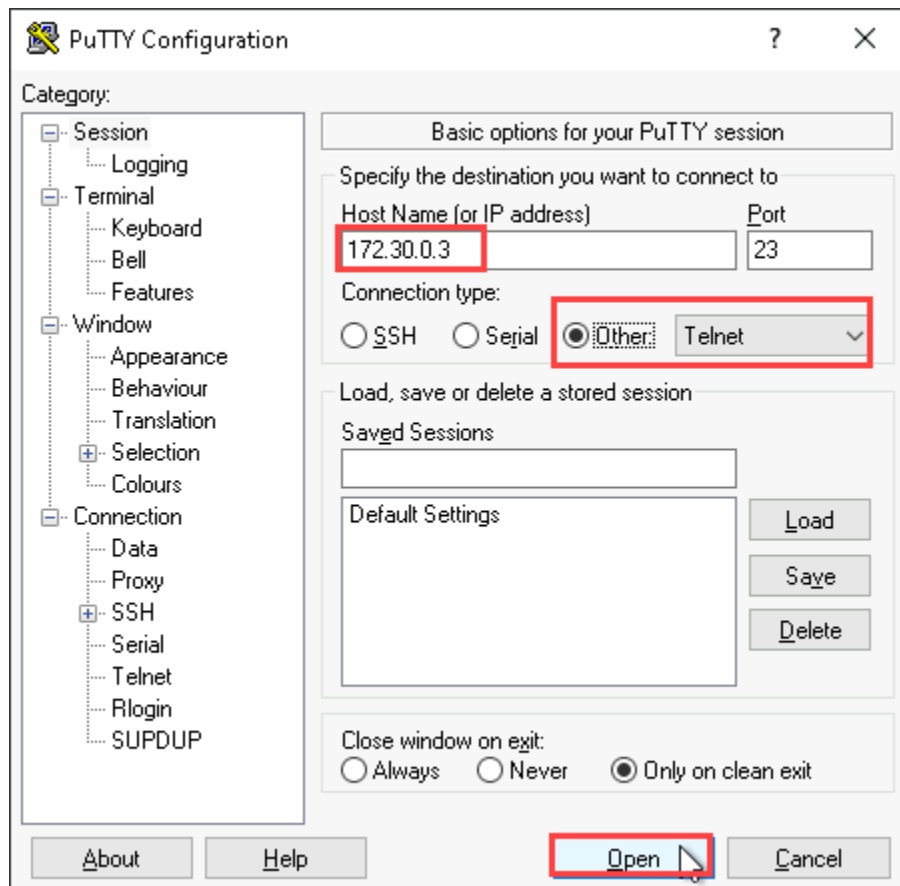
PuTTY icon

Note: PuTTY is a free and open-source terminal emulator, serial console, and network file transfer application that can be used to connect to other devices across a LAN (or even a WAN). In the next steps, you will configure PuTTY to open a remote connection with the Switch01 device.

13. In the PuTTY configuration window, **type** **172.30.0.3** in the Host Name field to specify the host you wish to connect to.
14. **Click** the **Other radio button** to select the Telnet protocol as your connection type.

Note: Telnet (an abbreviation of “teletype network”) provides command-line access to a remote host. Originally developed in 1969, Telnet transmits data in plain text, a detail that was not so concerning in the less security-conscious days of the early Internet. Naturally, it has since fallen out of favor, with protocols that support encrypted communications, such as SSH (Secure SHell), now being the recommended approach in nearly all cases.

15. **Click Open** to open a Telnet connection to the Switch01 device.

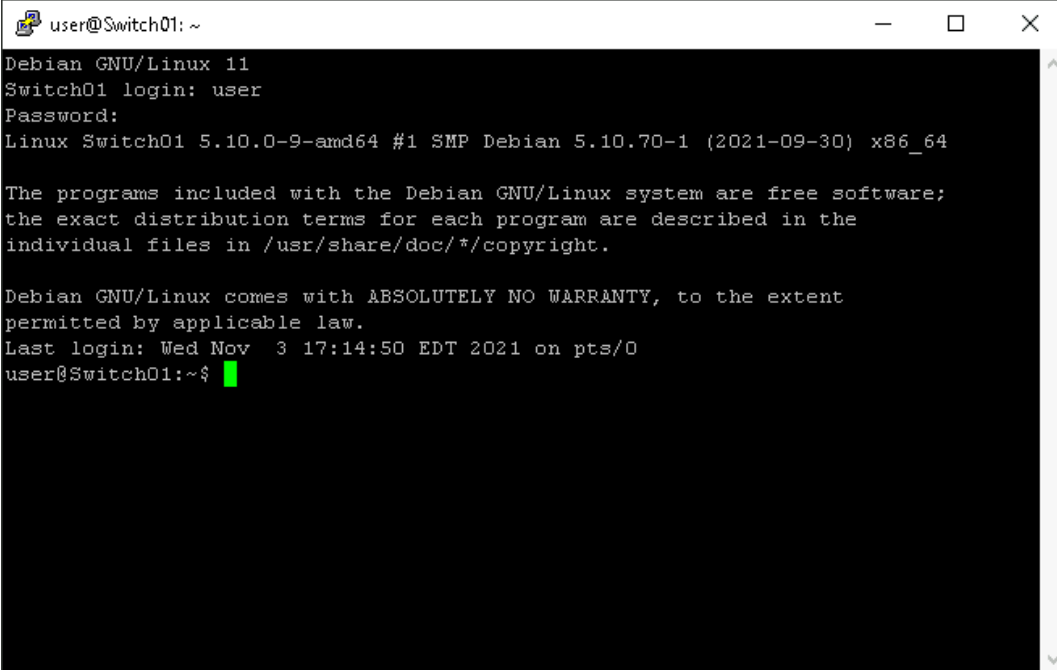


PuTTY configuration window

16. When prompted, **type** the following credentials and **press Enter** to authenticate your Telnet session.

Username: **user**

Password: **password**



```
user@Switch01: ~  
Debian GNU/Linux 11  
Switch01 login: user  
Password:  
Linux Switch01 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Wed Nov  3 17:14:50 EDT 2021 on pts/0  
user@Switch01:~$
```

Log-in prompt

Note: For security purposes, terminals typically do not show password inputs on-screen, but rest assured that your inputs are being recorded.

Although it functions as a dedicated switch in this lab environment, the Switch01 device is actually a Linux computer running the popular open-source Open vSwitch software, which allows general-purpose computers to perform switching functions. While the terms "switch" and "router" might invoke images of dedicated physical appliances, many networking devices in modern IT infrastructures are actually just software running on Linux-based virtual machines or containers.

Because Switch01 is running Linux, you will need to use the `sudo` (super user do) command and enter your password in order to elevate your privileges while running certain commands. To draw a comparison to Windows, you can think of Linux users as running as Standard accounts by default, with the option to temporarily become an Administrator when necessary.

In the next step, you will use `sudo` to run the Linux-version of the `ipconfig` command and review the Switch01 device's network interfaces.

17. At the command prompt, **type** `sudo ifconfig` and **press Enter** to display the network interfaces on the Switch01 device.

When prompted, **type password** to authorize your privilege escalation.

```
user@Switch01:~$ sudo ifconfig
[sudo] password for user:
br0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.0.3 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::250:56ff:feab:3534 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:35:34 txqueuelen 1000 (Ethernet)
    RX packets 239 bytes 22510 (21.9 KiB)
    RX errors 0 dropped 45 overruns 0 frame 0
    TX packets 103 bytes 8796 (8.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:3534 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:35:34 txqueuelen 1000 (Ethernet)
    RX packets 751 bytes 112690 (110.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 627 bytes 113032 (110.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:c707 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:c7:07 txqueuelen 1000 (Ethernet)
    RX packets 1091 bytes 138431 (135.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 943 bytes 125240 (122.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::250:56ff:feab:ef9d prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:ab:ef:9d txqueuelen 1000 (Ethernet)
    RX packets 1237 bytes 200388 (195.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1814 bytes 252409 (246.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5142 bytes 417034 (407.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5142 bytes 417034 (407.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

user@Switch01:~$
```

Network interfaces on Switch01

Note: You should see five network interfaces in the ifconfig output. The first, br0, has been assigned an IP address (labeled as "inet" in the ifconfig output) of 172.30.0.3. This is the administrative interface that you are currently using for your Telnet connection. The next three – ens192, ens224, and ens256

– are associated with the three devices connected to Switch01 (the vWorkstation, FileServer01, and pfSense-office). You should notice that none of these interfaces have IP addresses assigned, which makes sense, given that this is a Layer 2 device that relies solely on MAC addresses. In the ifconfig output, MAC addresses are labeled as "ether" in reference to Ethernet, the most common Layer 2 communication system. For the purposes of this lab, you can disregard the final interface (lo).

In the next steps, you will use Open vSwitch to display the interfaces in its configuration database.

18. At the command prompt, **type** `sudo ovs-vsctl show` and **press** **Enter** to display the current Open vSwitch configuration database.

If prompted, **type** `password` to authorize your privilege escalation.

```
user@Switch01:~$ sudo ovs-vsctl show
[sudo] password for user:
fca948bb-05a2-4b83-b264-38e926fb0ac1
    Bridge br0
        Port ens224
            Interface ens224
        Port ens256
            Interface ens256
        Port ens192
            Interface ens192
        Port br0
            Interface br0
                type: internal
    ovs_version: "2.15.0"
user@Switch01:~$
```

Open vSwitch configuration database

Note: Once again, you should see ens192, ens224, and ens256. In the Open vSwitch configuration database, you will see these values listed as both ports and interfaces. In this context, port refers to the physical port on the switch (even though this one is virtualized) and interface refers to the software representation of that port.

19. At the command prompt, **type** `sudo ovs-appctl fdb/show br0` and **press** **Enter** to display the Open vSwitch forwarding table.

If prompted, type **password** to authorize your privilege escalation.

```
user@Switch01:~$ sudo ovs-appctl fdb/show br0
port  VLAN  MAC                Age
  3      0  00:50:56:ab:8d:29    22
  1      0  00:50:56:ab:55:98     4
LOCAL    0  00:50:56:ab:1f:4d     4
  2      0  00:50:56:ab:99:fb     3
user@Switch01:~$
```

Open vSwitch forwarding table

Note: Much like the ARP table on the vWorkstation, the forwarding table is used to map Switch01's ports to the MAC addresses of the devices connected to them. If you compare the forwarding table with the ipconfig results in step 3 and the ARP table in step 9, you should recognize the MAC addresses for the vWorkstation, FileServer01, and pfSense-office. The fourth entry, labeled as "Local," again refers to the administrative interface to which you are currently connected.

20. **Make a screen capture** showing the **Switch01 forwarding table**.

21. **Close** the **PuTTY window**.

When prompted, **click** the **OK button** to continue.

Note: So far you have inspected the vWorkstation and the switch on the Local Area Network. In the final exercise in this part, you will examine the file server that you previously accessed from Alice's account in Part 1. Although you will learn more about file servers and other server roles in Section 2, in the next steps you will take the opportunity to complete your exploration of the LAN by connecting to the file server and gathering some basic information about it.

22. **Repeat steps 12-16** using the following information:

Host Name or IP address: **172.30.0.5**

Connection Type: **SSH**

User: **root**

Password: **password**

Note: You may notice that the banner that appears after you log in to this server identifies its operating system as FreeBSD. The FreeBSD kernel and the Linux kernel both are based on the UNIX operating system kernel, which was an early and highly influential multi-user operating system developed by AT&T in the late 1960's and early 1970's. While there are some differences between Linux and FreeBSD, both are typically accessed via the Command Line Interface and share many of the same basic commands.

In the next steps, you will use several common Unix commands to gather more information about the file server.

23. At the command prompt, **type `pwd`** and **press Enter** to display the current directory.

```
root@Fileserver01[~]# pwd
/root
root@Fileserver01[~]#
```

Pwd output

Note: The `pwd` command (**p**rint **w**orking **d**irectory) is a useful command for confirming your current location in the Linux file system. Everything in a Linux system begins in the root directory, which is represented as `/`. All the folders, hard drives, USB drivers – everything rolls up to the root directory. For Windows users, it may be useful to think of the root directory as similar to the C: drive (although there are limits to the comparison).

In this case, the word "root" in the output actually refers to the root user folder, which contains files that are specific to the root user. In Linux systems, the root user is equivalent to the Administrator user in Windows systems. When operating in a live production environment, logging in as root is not recommended at any time.

24. At the command prompt, **type `whoami`** and **press Enter** to display the current user account.

```
root@Fileserver01[~]# whoami
root
root@Fileserver01[~]#
```

Whoami output

Note: Similar to `pwd` and file system location, the `whoami` command is used for confirming your current user. As you confirmed by the `pwd` output, the current user is the root user.

25. At the command prompt, **type** `cd /mnt` and **press Enter** to change your working directory to `/mnt`.

```
root@Fileserver01[~]# cd /mnt
root@Fileserver01[/mnt]#
```

Change to `/mnt` directory

Note: In the Linux CLI, the `cd` command is used to navigate the file system. In this case, you have specified the `/mnt` directory as your desired location. The `/mnt` directory is commonly used as a mount point in UNIX-like operating systems. A mount point is a directory that represents the root directory of a storage device's file system.

26. At the command prompt, **type** `ls -l` and **press Enter** to list the contents of current directory.

```
root@Fileserver01[/mnt]# ls -l
total 1
-rw-r--r-- 1 root  wheel  5 Oct 12 10:19 md_size
drwxr-xr-x 4 root  wheel  4 Oct 28 09:10 tank
root@Fileserver01[/mnt]#
```

Ls -l output

Note: The `ls` command is used to display the contents of the current working directory – in this case, `/mnt`. Appending the `-l` option to the `ls` command will display additional information about the files and directories within the working directory, including the file type, permissions, file owner, group, file size, last modified date, and finally, the file or directory name. In this case, the output includes one file (`md_size`) and one directory (`tank`).

27. At the command prompt, **type `ls tank`** and **press Enter** to list the contents of the `tank` directory.

```
root@Fileserver01[/mnt]# ls tank
Employees      Shared
root@Fileserver01[/mnt]#
```

Ls tank output

Note: As you can see, using `ls` without the `-l` option will simply display the contents of the specified directory. In this case, you have instructed the shell to display the contents of the `tank` directory.

28. At the command prompt, **type the command** to change the working directory to the `tank/Employees` directory.
29. At the command prompt, **type the command** to list the contents of the current directory.
30. **Make a screen capture** showing the **contents of the Employees directory**.
31. **Close the PuTTY window**.

When prompted, **click OK** to continue.

Part 3: Explore the LAN-to-WAN Domain

Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Note: In this part of the lab, you will extend your exploration of the network in the virtual lab environment to the LAN-to-WAN Domain. While the LAN Domain is primarily composed of switches that serve only the private network, the LAN-to-WAN Domain is primarily composed of routers and extends to the point in the network where the private, protected network is connected to the Internet and broader WAN. It is also important to note that the distinction between the LAN and the WAN is not just conceptual, but logically divided at the network layer using separate private and public IP addresses.

In this lab environment, routing functions are provided by the open-source pfSense firewall/router software distribution. pfSense is a highly versatile and extensible tool that can be configured using both a CLI and GUI to provide a wide range of networking functions. Like the TrueNAS file server, pfSense is based on the FreeBSD operating system and is running on a dedicated virtual machine. For the purposes of this lab, all of the required pfSense functionality has been pre-configured.

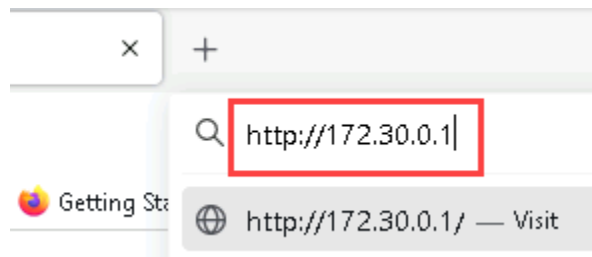
In the next steps, you will access the local pfSense firewall/router that serves the Secure Labs on Demand office via the pfSense webGUI. You will explore several critical functions of the pfSense application, including routing, Network Address Translation (NAT), and packet filtering.

1. On the vWorkstation taskbar, **click** the **Firefox icon** to open a new browser window.



Firefox icon

2. In the Firefox navigation bar, **type** **http://172.30.0.1** and **press Enter** to connect to the webGUI for the pfSense-office device.



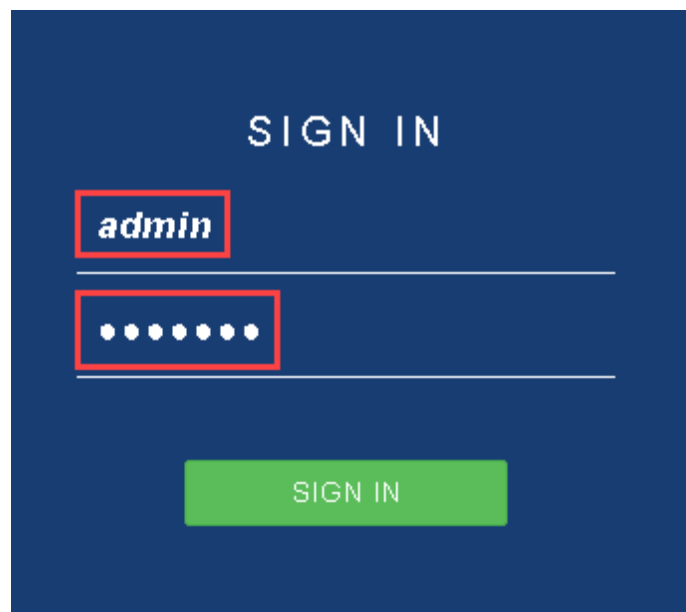
Firefox navigation bar

Note: Although web browsers like Firefox are typically used for accessing popular websites on the public Internet, they can also be used to connect directly to local servers by specifying the device's IP address in the same manner as a domain name (such as jblearning.com).

3. At the pfSense log-in screen, **type** the following credentials and **press Enter** to log in to the pfSense webGUI.

User: **admin**

Password: **pfsense**



pfSense log-in screen

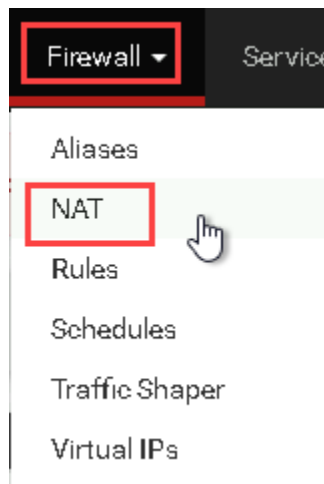
Note: Take some time to explore the pfSense dashboard, which contains important information about the pfSense system, including version, uptime, memory usage, and more. If you scroll down slightly, you will see a table displaying three network interfaces labeled as LAN, WAN, and DCLINK. In this lab environment, the LAN interface is connected to the local area network that you explored in Part 2, the WAN interface is connected to the simulated public Internet, and the DCLINK interface is connected to the Secure Labs on Demand organization's data center via a dedicated point-to-point connection.

Next to each network interface, you will see the IP address that the pfSense appliance uses to connect to that network. You may notice that the first two segments of each IP address are different from the other two, in contrast with the IP addresses you observed within the LAN, which all began with 172.30. The reason for these differences is the fact that IP addresses are actually composed of two distinct segments – the network address and the host address. While the mechanism used for differentiating the network address from the host address (called a Subnet Mask) is outside the scope of this lab, the important thing to know is the 172.30.0.x, 202.20.1.x, and 10.0.0.x each refers to a distinct network, while the last segment (.1 for all three) refers to the pfSense-office device's address on that network.

This brings us to one of the core functions of modern routers – Network Address Translation (NAT). NAT is a mechanism that allows a NAT-enabled router to keep track of connections between internal and external hosts and replace internal IP addresses with public (external) IP address(es), typically assigned by an Internet Service Provider (ISP). To the outside world, all traffic appears to originate from the router's public IP address(es). Meanwhile, the router knows the true destination for traffic based on its internal connection table and makes the appropriate address substitutions when receiving traffic from, or sending traffic to, the Internet.

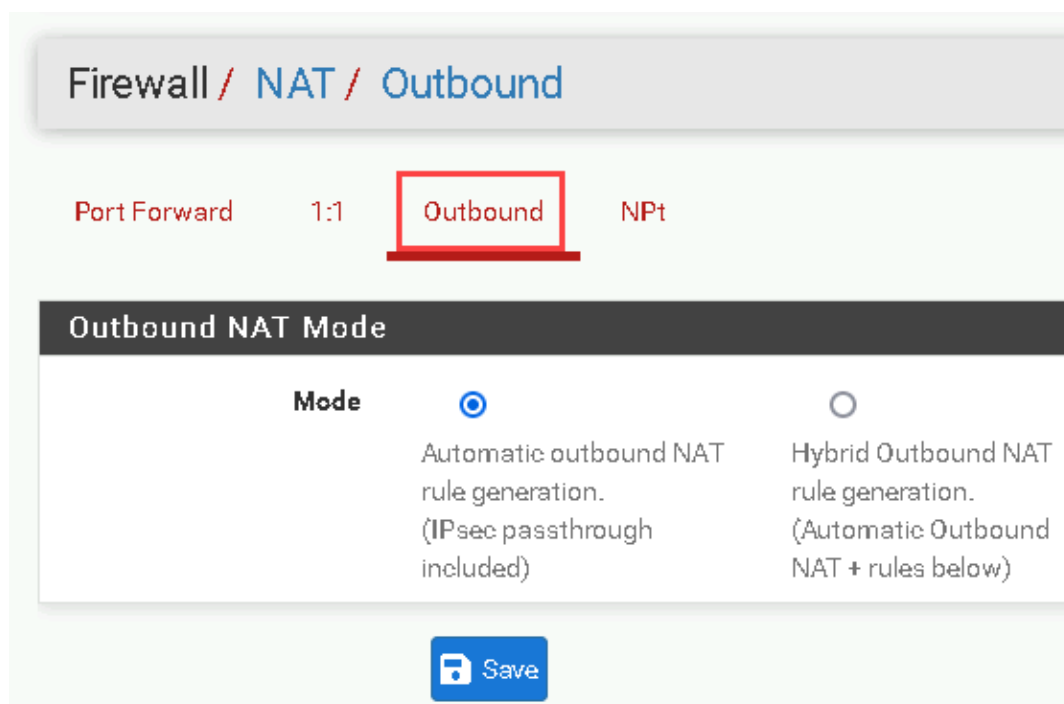
In the next steps, you will review the NAT table for the pfsense-office appliance.

4. On the pfSense menu bar, **click** the **Firewall menu** and **select NAT** to open the NAT settings.



Firewall > NAT

5. On the NAT page, **click** the **Outbound tab** to open the Outbound NAT settings.



Outbound NAT Settings

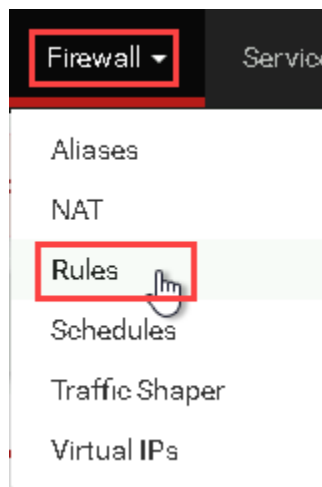
Note: At the top of the page, you should see that the Automatic outbound NAT rule generation option is selected. Although there are multiple forms of NAT, this configuration offers basic NAT functionality in which the router dynamically replaces all internal (private) IP addresses with a public IP address.

In the Automatic Rules table, you should see four entries – two associated with the WAN interface and two associated with the DCLINK interface. Counting down from the top, the second rule states that for all outbound connections from the LAN to the WAN interface (the Internet), from any source port to any destination port (a Layer 4 addressing scheme), and to any destination IP address, assign a public IP address. The fourth rule serves the same function for all outbound connections to the DCLINK interface (the Secure Labs on Demand data center). The other two rules are related to IPsec, a network protocol suite used for implementing secure communications, and are outside the scope of this lab.

6. **Make a screen capture** showing the **Outbound NAT settings**.

Note: In the next steps, you will review the Firewall rules.

7. On the pfSense menu bar, **click the Firewall menu** and **select Rules** to open the WAN Rules page.



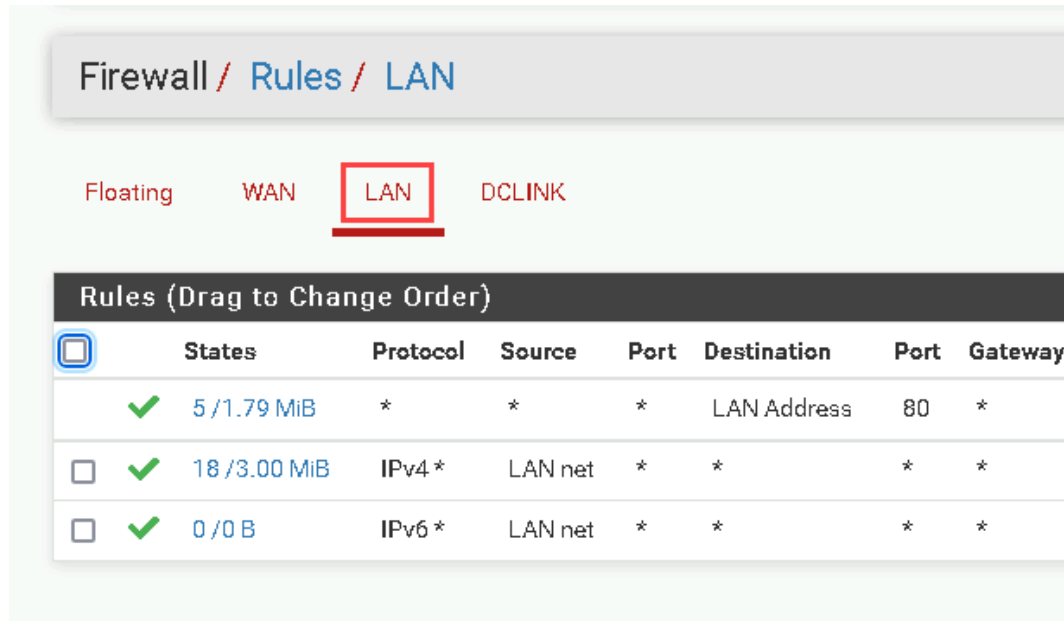
Firewall > Rules

Note: Among its many functions, pfSense's packet filtering capabilities are arguably the most important. Packet filtering is the core function of traditional firewalls, which effectively function as the network's bouncer. Just like a human bouncer, packet filtering firewalls use Access Control Lists (ACLs) to make decisions about which inbound packets (ingress) are allowed into the network and which packets are turned away. Similarly, a packet filtering firewall will make decisions about which outbound packets (egress) are allowed to leave the network.

One common ACL model is to automatically deny all inbound traffic and allow all outbound traffic. However, you might wonder how this model allows any two-way communications if all inbound traffic is blocked. Under this default deny model, two-way communications are facilitated by the fact that packet filtering firewalls are also stateful. In this context, stateful means that the firewall will consider the state of connections in addition to the basic inbound/outbound rules. When an outbound connection is initiated by a host inside the firewall perimeter, a stateful firewall makes note of this and grants exceptions for inbound packets associated with that connection.

Upon navigating to the pfSense Firewall Rules page, you will land on the WAN Rules table by default, which governs traffic on the WAN interface. The first rule is automatically generated by pfSense and will block any traffic originating from a source IP address that has been reserved exclusively for private (internal) networks by the IETF and IANA (per [RFC 1918](#)), which is a common sign of an IP spoofing attack. The second rule is also automatically generated by pfSense and will block any traffic originating from a source IP address that is not part of an IANA-approved IP address space (commonly referred to as [bogon filtering](#)). The third rule approves any ICMP packets directed to a WAN address.

8. On the WAN Rules page, **click the LAN tab** to display the rules table for the LAN interface.



LAN rules

Note: Just as the WAN rules table governs traffic on the WAN interface, the LAN rules table governs traffic on the LAN interface. Once again, pfSense has automatically populated the rules table with some default rules:

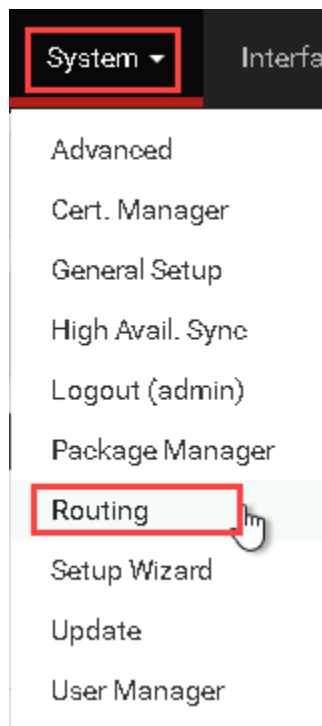
- **Anti-Lockout Rule** prevents users from locking themselves out of the pfSense WebGUI.
- **Default allow LAN to any rule** allows any traffic that originates on the Local Area Network (LAN). It is common for organizations to allow unrestricted outbound access and the pfSense firewall adds this unrestricted rule by default. However, from a security standpoint, you should allow only the type of access you want your users to have, and block everything else. This is what LAN rules are for: limiting access from a trusted network to an untrusted network.
- **Default IPv6 any rule** is equivalent to the second rule, but instead applies to IPv6 addresses. You will not be generating any IPv6 traffic in this lab.

It is worth noting that as packets traverse the pfSense firewall from the LAN to the WAN and vice-versa, they will be subject to the rules defined on both the LAN and WAN rules tables. For example, if a rule were added to the WAN interface that blocks all HTTP traffic, and a device on the LAN attempted to connect to a web server on the public Internet, the HTTP packets generated by that connection would be allowed through the LAN interface (keeping with the *Default allow LAN to any* rule), but would ultimately be blocked by the anti-HTTP rule on the WAN rules table.

9. **Make a screen capture** showing the **permissive LAN rules**.

Note: In the next steps, you will explore the Routing configuration.

10. On the pfSense menu bar, **click the System menu** and **select Routing** to open the Routing page.



System > Routing

Note: While pfSense's firewall capabilities are arguably its most important feature, they are only possible because of the Layer 3 routing capabilities that packet filtering relies on. Upon navigating to pfSense's Routing configuration, you will land on the Gateways tab by default. Just as individual devices on a LAN use a default gateway to connect to devices outside the local network, routers also have a default gateway to which they direct traffic. For a simple home set-up, your router's default gateway will be a router in your ISP's network. While the same is true for larger organizations when it

comes to traffic directed to the public Internet, many modern organizations typically operate a more complex private network of routers, each of which must be assigned one or more gateways. In this case, you will notice that the pfSense-office device has two gateways: one for traffic directed to the WAN interface and one for traffic directed to the Data Center. You should also notice that the WAN gateway is defined as the default gateway.

11. On the Routing page, **click** the **Static Routes** tab to open the Static Routes page.

System / Routing / Static Routes

Gateways

Static Routes

Gateway Groups

Static Routes

	Network	Gateway	Interface
✓	172.16.0.0/24	DC - 10.0.0.2	DCLINK
✓	172.31.0.0/24	DC - 10.0.0.2	DCLINK

Static Routes

Note: Static routing refers to the process of routing packets via paths that are manually defined on a router (contrasted with dynamic routing, where the route may change according to network conditions). In a sense, the Static Routes page is similar to the Forwarding Table that you reviewed on the Switch01 device, but organized around Layer 3 addresses. The first entry on this page states that all traffic directed to the 172.16.0.x network (the private LAN at the data center) pass through the DC 10.0.0.2 gateway. The second entry states that all traffic directed to the 172.31.0.x network (the Demilitarized Zone, another network segment at the data center) also pass through the DC 10.0.0.2. Without any other static routes in place, all other outbound traffic will be automatically routed to the default gateway – in this case, the WAN gateway that connects to the simulated public Internet.

12. **Make a screen capture** showing the **Static Routes** page.

Note: In the next steps, you will demonstrate the routing functions enabled by the pfSense firewall/router by running traceroutes to a local host on the LAN side of the router-firewall and a remote host on the WAN side. The traceroute CLI utility, called `tracert` in Windows, sends ICMP Echo Request (Windows) or UDP packets (UNIX-like OS) from a source to a destination IP address. Each time the packet is received and forwarded by a network node, that node responds with a hop count and time. The `tracert` utility uses the received packets to determine the path a packet took to reach its destination and how long the journey took.

13. On the vWorkstation taskbar, **click** the **Command Prompt icon** to open a new Command Prompt window.
14. At the command prompt, **type** `tracert 172.30.0.5` and **press Enter** to trace your path to FileServer01.

```
C:\Users\Administrator>tracert 172.30.0.5

Tracing route to fileserver01.securelabsondemand.com [172.30.0.5]
over a maximum of 30 hops:

  1    2 ms    <1 ms    <1 ms  fileserver01.securelabsondemand.com [172.30.0.5]

Trace complete.

C:\Users\Administrator>
```

Traceroute results

Note: The command output should report that the path to the FileServer01 device took only one hop. Despite the fact that the vWorkstation and FileServer01 are connected by the Switch01 device, Switch01 is not counted as a hop in the `tracert` output, due to the fact that it is a Layer 2 device. The pfSense firewall/router was not needed because the vWorkstation already has the FileServer01 IP/MAC address mapping in its ARP table, and the Switch01 device was capable of directing the traffic to the FileServer01 based on the MAC address.

15. At the command prompt, **type** `tracert 172.16.0.1` and **press Enter** to trace your path to the pfSense firewall located in the remote data center.

Note: In this case, the results should be slightly more interesting. You should see two hops: one for

the pfsense-office device and one for the pfsense-dc device.

16. **Make a screen capture** showing the **result of your tracert to the pfsense-dc appliance**.

17. **Close the Command Prompt window**.

Note: In the final steps, you will examine the second router-firewall, which serves the Secure Labs on Demand organization's remote data center site. Although the space between your local firewall/router and the remote firewall/router is technically considered the WAN Domain, which you will explore in the next section, the protected network within the data center is still considered part of the LAN Domain, including a specialized area of the LAN Domain – the DMZ.

18. In the Firefox navigation bar, **type `http://172.16.0.1`** and **press Enter** to open the pfSense webGUI for the pfSense firewall-router that serves your network's data center.

19. At the pfSense log-in screen, **type** the following credentials and **press Enter** to log in.

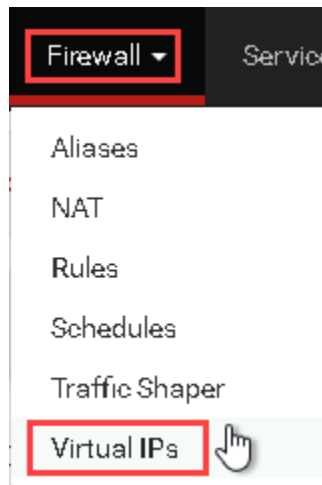
User: **admin**

Password: **pfsense**

Note: Once again, you should direct your attention to the interfaces table on the pfSense dashboard. This time, you should see four interfaces: one for the LAN, one for the WAN, one for the office site (OFFICELINK), and one labeled DMZ. The DMZ – short for De-Militarized Zone – is a separate network for an organization's public-facing resources, such as a web server running the organization's primary website. Because that website must be readily accessible to anyone on the Internet, it requires a more permissive ACL than devices on the LAN – one that does not automatically block all inbound connections. However, devices located in the DMZ are still considered part of the LAN Domain and use private IP addresses. Just as pfSense can provide outbound NAT for devices on the LAN, it can also provide inbound NAT for devices in the DMZ.

In the next steps, you will review the NAT configuration and firewall rules that facilitate access to the WebServer01 device in the pfSense-dc DMZ.

20. On the pfSense menu bar, **click the Firewall menu** and **select Virtual IPs** to open the Virtual IPs page.



Firewall > Virtual IPs

Note: A virtual IP (VIP) is an IP address that does not correspond to a physical interface on the firewall/router. In addition to the pfSense-dc device's WAN IP address, this pfSense firewall-router uses another public IP address, a VIP address, to represent the web server on the privately-addressed DMZ network. When Secure Labs on Demand's customers need to reach their website, they will input `securelabsondemand.com` in their browser, which will resolve to the public VIP address. When the request reaches the pfSense-dc firewall/router's WAN address, it will automatically redirect that request to the private IP in the DMZ via NAT.

21. On the pfSense menu bar, **click** the **Firewall menu** and **select NAT** to open the NAT Port Forwarding page.

Note: Port forwarding is another form of NAT and relies on a combination of Layer 3 and Layer 4 addresses. While Layer 3 uses IP addresses to enable connections across networks, Layer 4 (the Transport Layer) is responsible for ensuring reliable communications between the two hosts making the connection via the TCP or UDP protocols. Addresses at Layer 4 are referred to as Ports and are used to direct traffic for specific services on a host. A useful analogy in this situation might be an apartment building. If you are attempting to send a letter to a resident in a 50-resident complex, it's not enough to simply send it to the complex (the IP address) – you also need to specify which unit your resident lives in (the port).

On the Port Forwarding page, you should see two rules. The first rule specifies that all traffic directed to the 203.30.3.40 VIP on port 443 be re-directed to 172.31.0.40 private IP on port 443. The second rule specifies the same thing, but for port 80. Port 443 and 80 are the designated ports for web traffic

using the HTTPS and HTTP protocols, respectively. Because the WebServer01 device in the DMZ is intended solely as a web server, using port-forwarding NAT helps to limit the traffic that actually reaches it. For example, if someone outside the organization attempted to open an SSH connection (port 22) to 203.30.3.40, pfSense would not recognize the 203:30.3.40:22 address (together referred to as a socket) in its port forwarding NAT table.

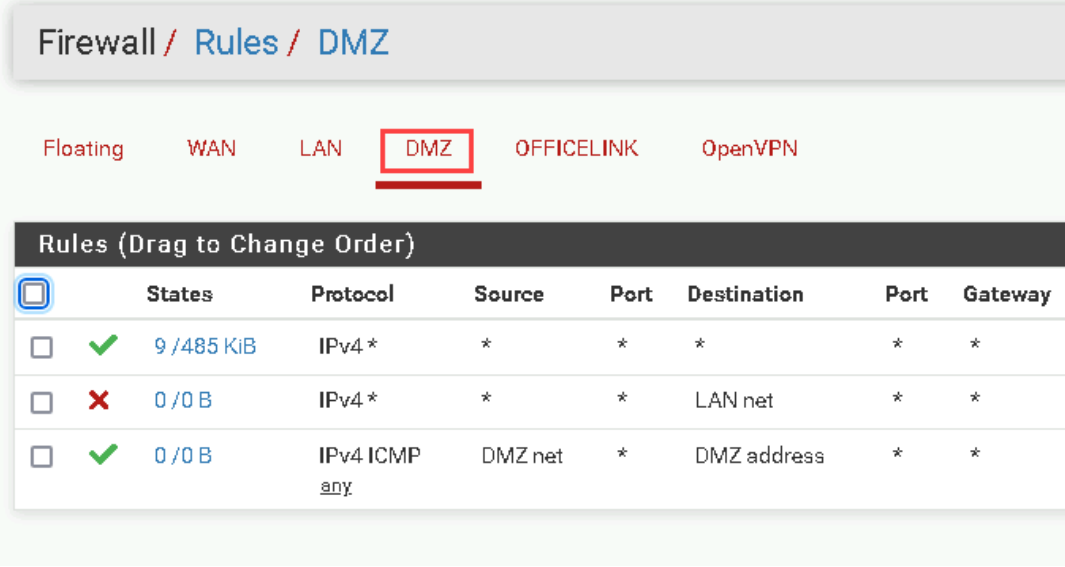
22. **Make a screen capture** showing the **Port Forward** rules for the web server.

Note: In the next steps, you will examine the firewall rules on the WAN and DMZ interfaces that support access to WebServer01.

23. On the pfSense menu bar, **click** the **Firewall menu** and **select Rules** to open the WAN Rules page.

Note: In addition to the same three rules you observed on the WAN rules table for the pfSense-office device, you should see three additional rules here. Two of the rules mirror the port forward rules that you just examined, and permit any traffic directed to 172.31.0.40 on ports 80 or 443. In this case, the private IP is specified because the NAT conversion has already occurred by the time the packets reach the WAN firewall. The third new rule pertains to the organization's Virtual Private Network, which you will examine in Section 2 of this lab.

24. On the WAN Rules page, **click** the **DMZ tab** to display the rules table for the DMZ interface.



Firewall / Rules / DMZ

Floating WAN LAN **DMZ** OFFICELINK OpenVPN

Rules (Drag to Change Order)

<input checked="" type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway
<input type="checkbox"/>	✓ 9 / 485 KiB	IPv4 *	*	*	*	*	*
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 *	*	*	LAN net	*	*
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 ICMP any	DMZ net	*	DMZ address	*	*

DMZ rules

Note: Of the three rules listed in the DMZ rules table, the single most important rule is the second one, which blocks all traffic to the LAN interface. This rule is the defining feature of the DMZ. In the event that an attacker is able to compromise one of the devices located in the DMZ, this rule helps mitigate the risk that they might use the compromised device to gain access to the private LAN.

25. **Make a screen capture** showing the **DMZ firewall rules**.

Note: This concludes Section 1 of the lab.

Section 2: Applied Learning

Note: **SECTION 2** of this lab allows you to apply what you learned in **SECTION 1** with less guidance and different deliverables, as well as some expanded tasks and alternative methods. You will extend your exploration of the lab environment to the WAN, Remote Access, and System/Application Domains.

Part 1: Explore the WAN Domain

Note: In this part of the lab, you will explore the WAN Domain, which encompasses the space on the far side of the WAN interfaces on an organization's routers. The term WAN – a Wide Area Network – refers to any network that extends over a large geographical area. Many people think of the term WAN as synonymous with the Internet, but that is not strictly accurate. While it is true that the Internet itself is the largest WAN, many large organizations use leased lines to create their own private WANs to accommodate multiple physical sites, such as offices and data centers. Private WANs are generally more secure and may be faster than using the public Internet for the same access.

For most organizations, the public Internet is the WAN that they use to connect with customers, partners, and services across wide geographical distances. Each node on a WAN needs a connection to an Internet Service Provider (ISP) to act as its gateway to the Internet. One of the fastest growing categories of services provided via a WAN is cloud services, wherein Cloud Service Providers (CSPs) use the WAN domain to offer their services to customers around the world.

In the previous section of the lab, you used the pfSense WebGUI to review several key functions that support the LAN-to-WAN Domain. In the next steps, you will return to the pfSense WebGUI and examine the routes between Secure Labs on Demand's two remote sites, as well as their connection to the simulated public Internet. You will then use the simulated ISP's Looking Glass server to examine simulated public Internet directly.

1. From the vWorkstation taskbar, **open the Firefox application**.
2. In Firefox, **navigate** to **http://172.16.0.1** and **log in** using the following credentials:

Username: **admin**
Password: **pfsense**
3. From the pfSense menu bar, **navigate to System > Routing** to display the Gateways list.

Note: As you previously observed on the pfSense-office firewall/router in Section 1, Part 3, the

Gateways page lists two gateways. The first, WANGW, serves the public Internet via an ISP (or in this case, a simulated public Internet). The OFFICELINK gateway serves as the entry and exit point for traffic to and from the office LAN. At the other end of this connection is the DCLINK interface that you observed in the pfSense-office WebGUI. The connection between the two routers is a simulated point-to-point (P2P) connection, which is a dedicated, private connection offered by a P2P service provider. While an in-depth discussion of WAN technologies is outside the scope of this lab, P2P connections are just one of the many options available to organization that need to operate their own WAN.

4. Click the **Static Routes tab** to display the static routing table.

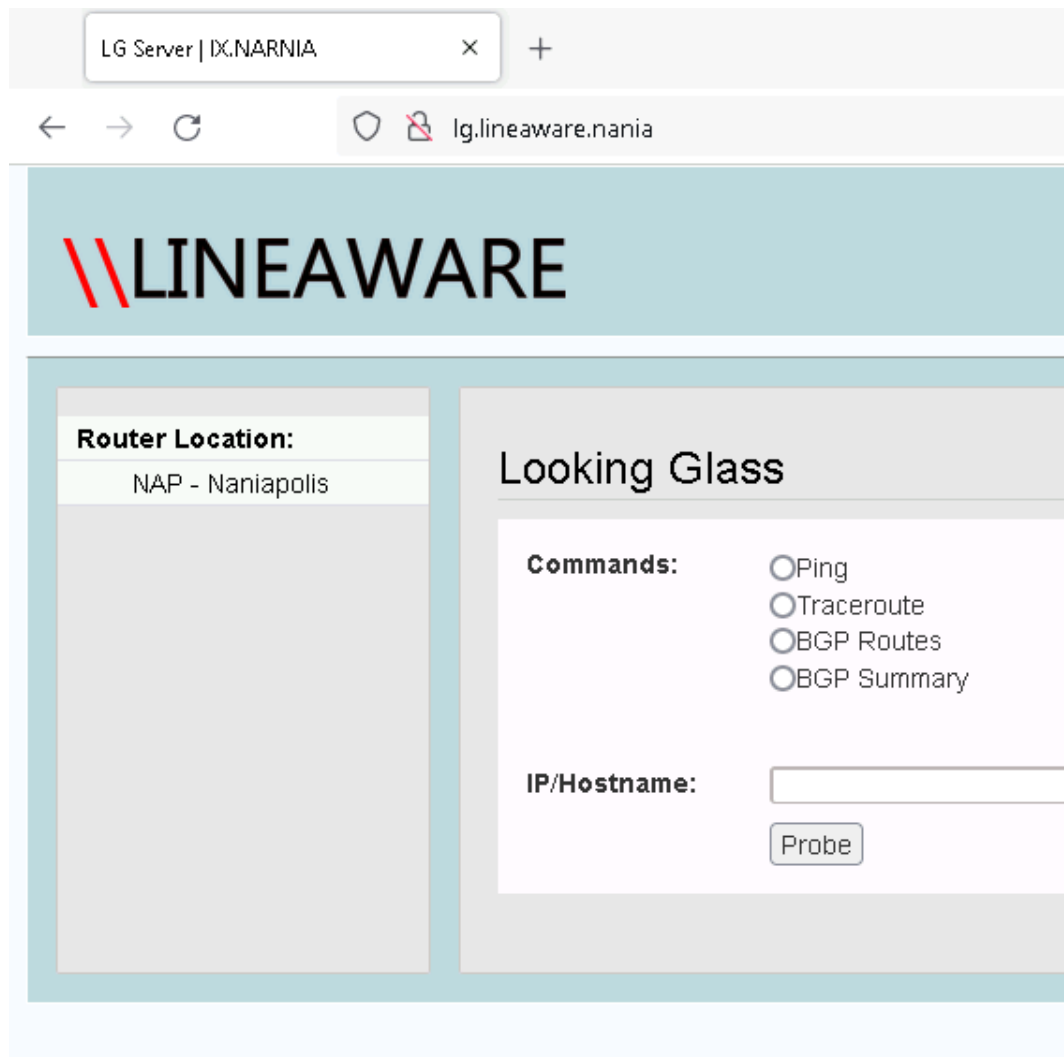
Note: There is only one static route defined, which states that all traffic destined for the 172.30.0.0/24 network should be forwarded to the OFFICELINK upstream gateway. For all other traffic, pfSense will use the default gateway defined on the Gateways page, which in this case is the WANGW gateway.

5. Make a screen capture showing the **static route for the point-to-point connection**.

Note: One common area of confusion is what happens to network traffic that a gateway sends to the public Internet. In simple terms, an organization connects to the public Internet through an Internet Service Provider (ISP) interface. For a fee, the ISP provides a connection an Internet backbone, which it may own directly or lease through a Network Service Provider (NSP). To route traffic across multiple ISPs, ISPs connect to one another using gateways called Internet Exchange Points (IXs). Together, this collection of ISPs, NSPs, and IXs provide the ability to build the Internet-connected networks that provide many of the cloud services in use today.

In the next steps you will connect to something called a Looking Glass server. A Looking Glass server is typically run by an ISP or NSP and allows public users to review high-level ISP/NSP routing information.

6. Using the Firefox address bar, **navigate** to **<http://lg.lineaware.nania>** to access the Looking Glass server operated by this lab environment's simulated ISP.



Lineaware LG server interface

Note: The Looking Glass server interface offers four command options: Ping, Traceroute, BGP Summary, and BGP Route. Ping and Traceroute both require a target IP address, while the BGP options do not.

BGP is an acronym for the Border Gateway Protocol. BGP is a Layer 3 routing protocol that provides edge routers with the ability to exchange routing information and optimize network traffic on a global scale. The protocol is very slow and only concerns itself with a high-level view of routes between autonomous systems. You can think of BGP as the BiGPicture view of Internet connectivity, made possible by companies peering with one another to share routes. Within this lab environment, the public Internet is simulated using a single BGP router.

7. At the Looking Glass interface, **select the BGP Summary radio button**, then **click the Probe button** to display the BPG summary.

Note: The BGP Summary command should return information on two neighbors to the BGP router: the pfSense-office and pfSense-dc routers, each identified by the IP address for their WAN interface. You should also see a column labeled AS, which contains a unique 10-digit (32-bit) number for each neighbor. In this context, AS is short for Autonomous System, which refers to a collection of IP networks run by a single operator collection. The unique 10-digit number is known as an Autonomous System Number (ASN), which is used as an IP routing prefix for BGP routing. At the top of the output, you should see another ASN for the simulated ISP, here labeled *local AS number*. Although the border gateways in this lab are all single routers using fictional ASNs, in a real-world environment, a single ASN could actually represent a collection of multiple routers using a shared ASN.

In the BGP summary output, you can also see messages sent and received (MsgRcvd and MsgSent). Given that the numbers in these columns are not zeros, it appears things are working. In the next step, you will use the Ping command to verify connectivity with one of the BGP neighbors.

8. **Select the Ping radio button** and **type the IP address for either of the BGP neighbors displayed in the BGP summary** in the IP/Hostname field, then **click the Probe button** to ping the BGP neighbor.
9. **Make a screen capture** showing the **BPG neighbor ping results**.

Note: The most revealing utilities on this page are the Traceroute and BGP Routes options. These utilities provide the ability to inspect all known routes and determine which routes are being selected for traffic to specific networks and nodes. In the next steps, you will review the BGP routing table and verify one of the routes using Traceroute.

10. **Run the BGP Routes command**.

```
BGP table version is 8, local router ID is 201.10.1.2, vrf id 0
Default local pref 100, local AS 4260000000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop           Metric LocPrf Weight Path
*  10.0.0.0/28    202.20.2.1          1             0 4230000000 ?
*>               203.30.3.1          1             0 4200000000 ?
*  172.16.0.0/24  202.20.2.1          0             0 4230000000 ?
*>               203.30.3.1          1             0 4200000000 ?
*> 172.29.0.0/24  203.30.3.1          1             0 4200000000 ?
*  172.30.0.0/24  202.20.2.1          1             0 4230000000 ?
*>               203.30.3.1          0             0 4200000000 ?
*  172.31.0.0/24  202.20.2.1          0             0 4230000000 ?
*>               203.30.3.1          1             0 4200000000 ?
*  202.20.2.0/24  202.20.2.1          1             0 4230000000 ?
*>               0.0.0.0            0          32768 i
*  203.30.3.0/24  203.30.3.1          1             0 4200000000 ?
*>               0.0.0.0            0          32768 i
*> 204.40.4.0/24  0.0.0.0             0          32768 i

Displayed 8 routes and 14 total paths
```

BGP routing table

Note: In real-world implementation, the output of this command would be limited to routes on the public Internet. In this case, the Looking Glass server displays all of the networks within the lab environment, including private networks. For the purposes of this lab, this is not a problem, and in fact may be fractionally more representative of the massive scale at which real-world BGP routing tables operate.

While most of the information displayed on-screen is outside the scope of this lab, you should be able to interpret the Network and Next Hop columns. For each network listed in the Network column, the BGP routing table lists one or more IP addresses in the Next Hop column, which represent the neighboring routers through which the BGP router can connect to the target network. For each network, the BGP routing table also identifies one of the Next Hop options as the best route, represented as the > sign on the far left.

In the next step, you will confirm the current path to the WebServer01 machine (172.31.0.40) in the pfSense-dc DMZ is the one identified as the best route in the BGP routing table.

11. Select the Traceroute radio button and type **172.31.0.40** in the IP/Hostname field, then

click the **Probe** button to run a traceroute to WebServer01.

Note: The traceroute results should confirm that the first hop to the WebServer01 host is the same IP address identified as the best route in the BGP routing table.

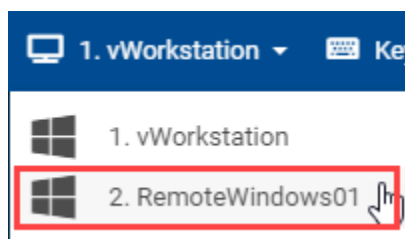
12. **Make a screen capture** showing the **traceroute to the file server**.

Part 2: Explore the Remote Access Domain

Note: In this part of the lab, you will explore the Remote Access Domain. The Remote Access Domain encompasses the connection between an organization's private network and any workstations or other devices that are physically located outside of an organization's private network, but must still connect to the private network. To ensure remote workers are protected by the same network security measures as workers connected directly to the network at an office, most organizations use Virtual Private Network (VPN) solutions. A VPN allows a remote endpoint to establish a secure tunnel with a trusted server that can encrypt all traffic and provide a secure channel between the endpoint and the internal network. In effect, VPNs extend an organization's security perimeter beyond traditional physical boundaries and across public networks.

In the next steps, you will assume the role of a remote worker who needs to connect to the corporate network.

1. On the Lab View toolbar, **select RemoteWindows01** from the Virtual Machine menu to connect to the RemoteWindows01 system.



Virtual Machine menu

2. **Sign in** using the following credentials:

User: **mramone**

Password: **P@ssw0rd!**

Note: This computer represents Matthew Ramone's work-provided laptop. Matt Ramone is a developer at the fictional Secure Labs on Demand organization. Matt's laptop was created using the company's standard image, and then configured with remote access so that he can securely access the internal resources despite being hundreds of miles away from the office.

In the next steps, you will confirm that Matt can access email, which requires access to the company's internal mail server.

3. From the RemoteWindows01 desktop, **open** the **Thunderbird** application.

Note: Upon opening the Thunderbird email client, you should receive an error message stating that Thunderbird failed to connect to the server at securelabsondemand.com. This confirms that your laptop is not connected to the private Secure Labs on Demand network.

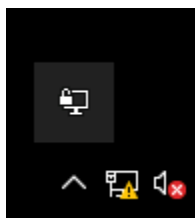
4. **Minimize** the **Thunderbird** window.

Note: On the RemoteWindows01 desktop, you should see an application shortcut titled OpenVPN — this is your ticket to the private company network. OpenVPN is an open-source VPN solution that provides Layer 2 or 3 VPNs using its own custom security protocol, which relies heavily on the TLS protocol. OpenVPN will set up an encrypted tunnel between your endpoint (RemoteWindows01) and the organization's VPN server, which in this case is running on the pfSense-dc firewall/route. This tunnel will allow you to communicate securely with resources on the private Secure Labs on Demand network, including the company email server.

5. From the RemoteWindows01 desktop, **double-click** the **OpenVPN GUI icon** to launch the OpenVPN application.

Note: Once OpenVPN is launched, a new icon will briefly appear on the RemoteWindows01 taskbar, then be replaced by carrot (^) menu icon.

6. On the RemoteWindows01 taskbar, **click** the **carrot icon**, then **double-click** the **OpenVPN icon** to open the OpenVPN GUI.



OpenVPN icon

7. When prompted, **log in** using the following credentials:

User: **mramone**

Password: **P@ssw0rd!**

8. **Restore** the **Thunderbird window**, then **click** the **Get Messages button** to reattempt a connection to the email server.

Note: Thunderbird should now be able to receive email messages from the securelabsondemand.com email server. In fact, you should have received a message from fsmith about your full stack needing an update. Success!

9. **Make a screen capture** showing the **successful connection to the email server**.
10. **Close** the **Thunderbird application**.

Note: There are 2 main types of VPNs: routed VPNs, which function at Layer 3, and bridged VPNs, which function at Layer 2. In the next steps, you will inspect your workstation's network interface cards to determine which type of VPN RemoteWindows01 is using.

9. Open the Windows Command Prompt.

11. At the command prompt, **execute** `ipconfig` to list the RemoteWindows01 machine's network interfaces.

Note: In addition to the TrueLab and Student interfaces that you also saw on the vWorkstation, you should see two unknown adapters, designated as OpenVPN Wintun and OpenVPN TAP-Windows6. TUN and TAP are both virtual network interfaces. TUN simulates a Layer 3 network device. This is the "routed" flavor of VPN, which functions by routing packets through the network that connects the remote client to the internal network. TAP simulates a Layer 2 network device. This is the "bridge" flavor, which function by forwarding frames across the VPN connection without ever traversing Layer 3, such that all hosts on either end communicate as if they are on the same local network. In practice, TUN VPNs are more common, due to the fact that TAP VPNs introduce more overhead and complexity. If you review the two unknown adapters in the ipconfig output, you should see that the OpenVPN Wintun adapter has an IP address assigned (172.19.0.2), while the OpenVPN TAP-Windows6 adapter is listed as disconnected, confirming that your VPN type is routed.

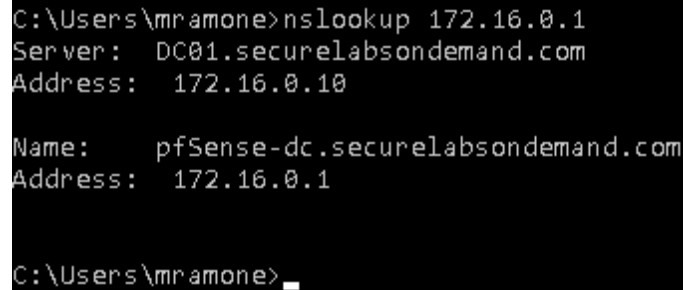
The term "tunnel" is also used to refer to the connection between the VPN client and server. Tunnels can be full or split, where full tunnels route all network traffic through the VPN and split tunnels provide the option to send some network traffic through the VPN and the rest through your local network. In the next steps, you will use the `tracert` command to determine whether the VPN in this lab is running as a full tunnel or split tunnel implementation. If a full tunnel is in use, you can expect the first hop to always be the gateway for the 172.29.0.x network. If a split tunnel is enabled, when attempting to access IP addresses outside the private network, your first hop will be the gateway for the 10.30.0.x network.

12. At the command prompt, **execute** `tracert 172.31.0.40` to display the path taken to the internal IP address of the web server.
13. At the command prompt, **execute** `tracert 203.30.3.40` to display the path taken to the external IP of the web server.
14. **Document** whether the VPN connection is split tunnel or full tunnel, based on the `tracert` results.

Note: Remote access configurations will push out settings that facilitate communications, such as routes and DNS servers. In the final step for this part of the lab, you will confirm that the internal DNS server was pushed to the remote host by performing a reverse DNS lookup on an internal host. A DNS lookup takes a domain as an input and returns the corresponding IP address, while a reverse DNS

lookup takes an IP address as an input and returns its domain name.

15. At the command prompt, **execute** `nslookup 172.16.0.1` to display the DNS records associated with 172.16.0.1.



```
C:\Users\mramone>nslookup 172.16.0.1
Server:  DC01.securelabsondemand.com
Address:  172.16.0.10

Name:     pfSense-dc.securelabsondemand.com
Address:  172.16.0.1

C:\Users\mramone>
```

Reverse DNS lookup

Note: The reverse DNS lookup for 172.16.0.1 should be successful, which confirms that RemoteWindows01 was able to access the DNS server for the Secure Labs on Demand network. Otherwise, because the IP address 172.16.0.1 is assigned to a host located on the private network, the reverse DNS lookup would be unable to locate it.

16. **Make a screen capture** showing the **successful reverse DNS lookup for the internal host**.
17. **Close the Command Prompt window**.

Part 3: Explore the System/Application Domain

Note: The System/Application Domain contains the critical systems and applications that support and provide various services for the organization. Systems in this domain perform core functions like authentication, authorization, and data management, as well as various other services/microservices. Most of the computers in this domain are servers, which typically have unique, dedicated roles. Although it is not strictly a networking concept, the System/Application Domain is typically located on one or more dedicated LAN segments, separate from the LANs that serve user workstations. The most common physical location for the System/Application Domain is in an environmentally controlled datacenter with service level agreements for quality of service and uptime guarantees.

In the next steps you will examine several of Secure Labs on Demand's key systems, including a domain controller, web server, and file server. You will begin with the most important system in the Secure Labs on Demand IT infrastructure — the domain controller.

1. On the Lab View toolbar, **select DomainController01** from the Virtual Machine menu.

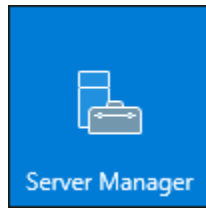
Note: The Microsoft Windows operating system provides the Active Directory Domain Services (AD DS) feature to make administration of networked computers easier. Active Directory allows users and configuration settings to be managed from a central location and applied to computers in a managed group. Windows uses the term "domain" to refer to a managed group of computers and devices. Domains are designated using domain names, which is typically based on the organization's name and represented as DOMAINNAME\. One or more central servers, called Domain Controllers, manage shared user account and configuration settings for all computers and devices in a specific domain.

2. From the DomainController01 taskbar, **open a Command Prompt window**.
3. At the command prompt, **execute whoami** to display information about your current user account.

Note: Not all administrators are created equal. A local administrator is a user account that has the authority to do pretty much anything on a single computer. A domain administrator can make changes to global policies that impact all computers and users in a domain. Generally speaking, a domain administrator is more powerful than a local administrator.

In this case, whoami has confirmed that your current account is a domain administrator, represented by the securelabsondem\ prefix that precedes the account name (administrator).

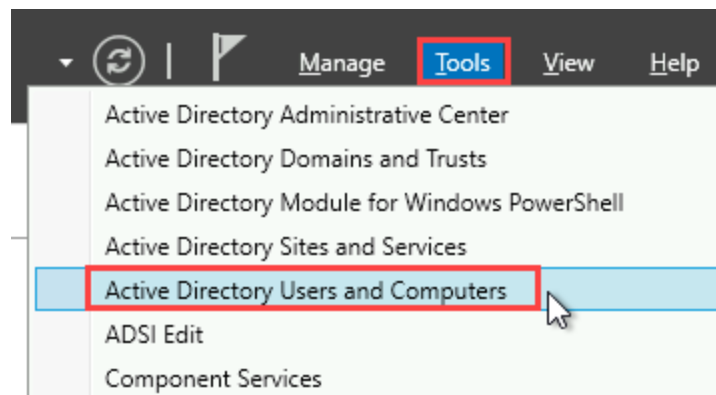
4. **Make a screen capture** showing the **whoami results**.
5. **Close the Command Prompt window**.
6. From the DomainController01 Start menu, **open the Server Manager**.



Server Manager icon

Note: The Server Manager is a specialized application included on Server editions of Windows. It provides a centralized management dashboard for the various roles and features that a Windows server can provide. In the next several steps, you will explore three of those roles: Active Directory Users and Computers, Group Policy Management, and Domain Name Services.

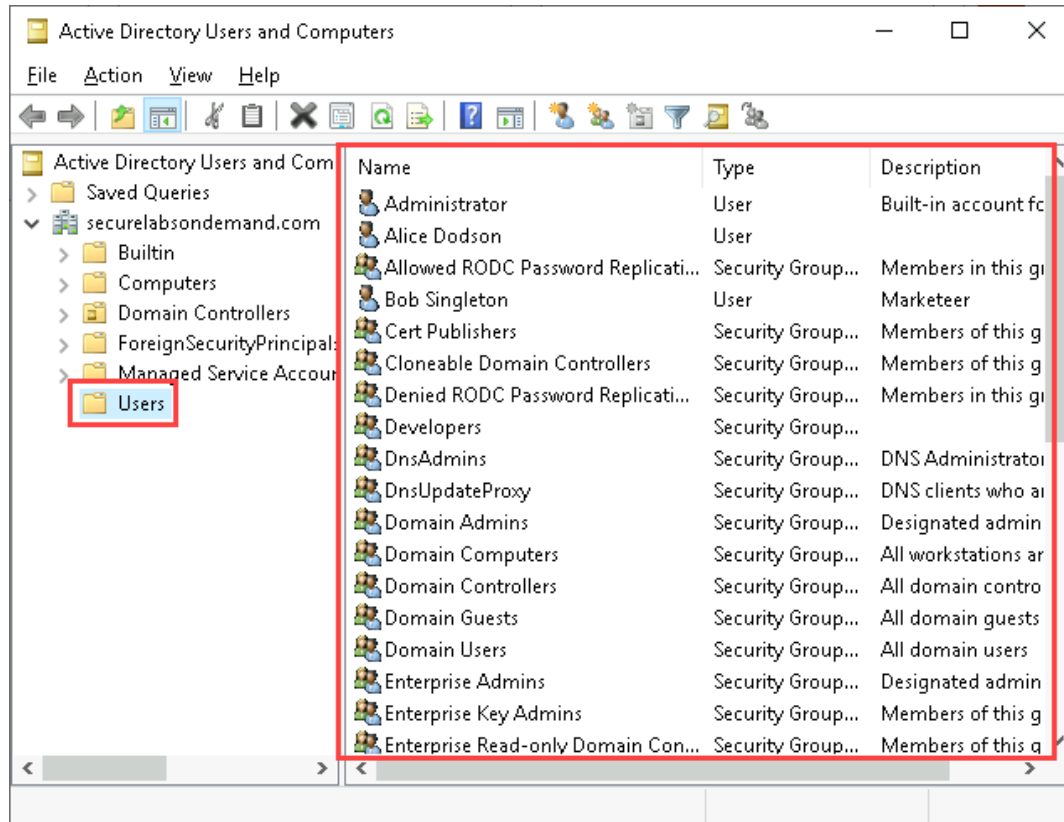
7. From the Server Manager menu bar, **navigate to Tools > Active Directory Users and Computers**.



Tools > Active Directory Users and Computers

Note: The Active Directory Users and Computers tool is part of the Active Directory Domain Services role, which is the defining feature of a Windows Domain Controller. From the Active Directory Users and Computers console, you can manage users and computers across a domain.

8. In the Active Directory Users and Groups console, **open** the **Users** folder and **review** the contents.



Users folder

Note: The built-in Users container contains both individual users and groups, which are typically used to organize users according to their function within an organization. For example, you may recognize Matt Ramone from Section 2, Part 2. You may recall that Matt was a remote developer, which means he is probably a member of the Developers group in Active Directory.

9. Within the Users folder, **double-click** the **Developers group** to open the Developers Properties dialog box, then **click** the **Members tab** and **review** the list of users within this group.

Note: Sure enough, there's Matt — proud (and only) member of the Developers group.

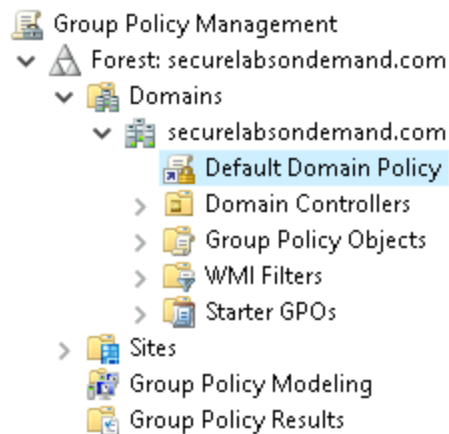
Carefully managing AD relationships such as group membership is not only good hygiene, but a critical security consideration. If an attacker were able to obtain access to a Domain Controller (which is a worst-case scenario in itself), they might be able to deploy tools like Bloodhound, which can quickly document the relationships between users and computers, as well as privilege levels. With this information in hand, an attacker can quickly move across systems and solidify their foothold in your network.

10. **Make a screen capture** showing the **members of the Developers AD group**.
11. **Close** the **Active Directory Users and Groups console**.
12. From the Server Manager menu bar, **navigate to Tools > Group Policy Management**.

Note: The Group Policy Management Console (GPMC) is another tool associated with the Active Directory Domain Services role. Used in tandem with AD Users and Computers, the GPMC provides centralized configuration settings for domain-level policies. Password policies, Windows updates, program execution privileges — many of the security controls you encountered in your survey of the Workstation Domain are configured here.

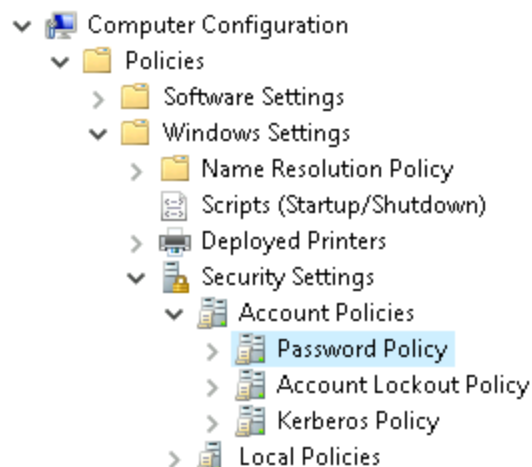
Policies generally fall into one of two categories: User and Computer configurations. User policies relate to user accounts and privileges, while computer configuration policies govern how computers operate and allow users to interact with their resources.

13. In the Group Policy Management Console, **navigate to Forest: securelabsondemand.com > Domains > securelabsondemand.com > Default Domain Policy**.



Default Domain Policy

14. **Right-click** the **Default Domain Policy** object and **select Edit** to open the Group Policy Management Editor.
15. In the Group Policy Management Editor, **navigate** to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy**.



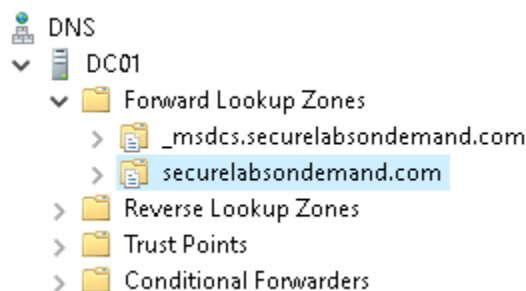
Password Policy

Note: From this page, you can define different aspects of the default password policy for the Secure Labs on Demand domain, including minimum password length, minimum password age, and password complexity.

16. **Make a screen capture** showing the **password policy settings in the Group Policy Management Console**.
17. **Close the Group Policy Management Editor and Console**.
18. From the Server Manager menu bar, **navigate to Tools > DNS**.

Note: As you reviewed earlier in this lab, all of the hosts in this mock IT infrastructure have an IP address that can be used to communicate with other networked hosts. While IP addresses are very effective at facilitating communications, they are not necessarily easy for humans to remember. As you probably know from browsing the Internet, websites are typically accessed via human-legible Uniform Resource Locators (URLs), such as microsoft.com or amazon.com — also known as domains. While you may never see them, these domains are actually surrogates for IP addresses. Like the MAC/IP address mappings maintained by the ARP table, domain/IP address mappings are managed by a protocol called the Domain Name System (DNS). DNS services are typically run from dedicated servers called DNS servers. For the purposes of this lab, the DNS server role has been installed on DomainController01.

19. In the DNS console, **navigate to DNS > DC01 > Forward Lookup Zones > securelabsondemand.com** to display the DNS records in the securelabsondemand.com domain.



DNS console

Note: Within the securelabsondemand.com domain, you should see several records corresponding to different devices on the Secure Labs on Demand network. The most common type is a Host or A type record, which refers to a specific IP address within the domain. Another common type is the MX record, which identifies a mail server.

20. **Make a screen capture** showing the **DNS entries**.

21. **Close** any **open windows**.

Note: In the next steps, you will inspect another common server role in IT infrastructures: a web server. A web server is a computer running specialized software, such as Apache or NGINX, which allows it to accept inbound requests from web browsers via the HTTP and HTTPS protocols.

22. From the Lab View toolbar, **select vWorkstation** from the Virtual Machine menu.

23. At the vWorkstation log-in screen, **type P@ssw0rd!** to log in as the local Administrator.

Note: Although web servers are typically accessed via web browsers, you will begin by connecting directly to the Linux computer running the web server using PuTTY.

24. From the vWorkstation, **launch the PuTTY application** and **open an SSH session** to **172.31.0.40**.

25. When prompted, **log in** using the following credentials:

User: **user**

Password: **password**

26. At the command prompt, **execute sudo netstat -tulpn** to view open connections on the WebServer01 system.

If prompted, **type password** to authorize your privilege escalation.

```
user@WebServer01:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      881/docker-proxy
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      596/sshd: /usr/sbin
tcp6       0      0 :::80                  :::*                    LISTEN      886/docker-proxy
tcp6       0      0 :::22                  :::*                    LISTEN      596/sshd: /usr/sbin
udp        0      0 0.0.0.0:5353           0.0.0.0:*                LISTEN      356/avahi-daemon: r
udp        0      0 0.0.0.0:43538          0.0.0.0:*                LISTEN      356/avahi-daemon: r
udp6       0      0 :::5353                :::*                    LISTEN      356/avahi-daemon: r
udp6       0      0 :::33412               :::*                    LISTEN      356/avahi-daemon: r
user@WebServer01:~$
```

Netstat

Note: Netstat is a CLI utility used to display various statistics about a computer's network status, including ports that are listening for connections, established connections, and the services associated with those connections. Within the netstat output, you should see a service titled "docker-proxy" running on port 80. Docker is a lightweight virtual machine that runs limited services to perform specific functions. Docker VM's, called containers, can even be run on top of traditional virtual machines. The fact that the docker-proxy service is running on port 80 (the port for HTTP) indicates that the web server software is actually running on a Docker container atop the WebServer01 Linux system. The addition of the word "proxy" suggests that connections are being redirected to another container, perhaps on a different port.

In the next step, you will use a common Linux services wrapper to check the status of Docker.

27. At the command prompt, **execute sudo service docker status** to check the status of the Docker container.

```
• docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-12-01 11:33:12 EST; 19min ago
   TriggeredBy: • docker.socket
     Docs: https://docs.docker.com
    Main PID: 608 (dockerd)
      Tasks: 21
     Memory: 139.9M
        CPU: 984ms
    CGroup: /system.slice/docker.service
            └─608 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
              └─881 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 80 -container-ip 172.17.0.2 -container-port 3000
                └─886 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80 -container-ip 172.17.0.2 -container-port 3000
```

Docker status

Note: Within the output, you should see that port 80 on the host is being redirected to IP address 172.17.0.2 and port 3000 on the container. This is a typical configuration for a container running on a host system, wherein the host and container both have their own set of TCP ports, which requires a mapping to ensure traffic flows from one to the other.

28. **Make a screen capture** showing the **Docker service status**.

29. **Close the PuTTY window**.

30. From the vWorkstation taskbar, **open Firefox** and **navigate** to **juiceshop.com** to access the website being hosted on the web server.

Note: At juiceshop.com, you can interact with the website that WebServer01 is hosting. Juice Shop is an open-source web application developed by the Open Web Application Security Project (OWASP) to demonstrate common web application vulnerabilities. You can learn more about Juice Shop at <https://owasp.org/www-project-juice-shop/>.

31. **Make a screen capture** showing the **juiceshop.com web page**.

Note: In the final steps, you will examine one additional server type — a file server, represented by the FileServer01 system, which you may recall from earlier in the lab. File servers are dedicated computer systems used to provide shared disk access to multiple users, typically over a network. File servers are commonly hosted on specialized appliances called Network Attached Storage (NAS) systems, which contain multiple storage drives. These drives are typically organized in a RAID configuration for redundancy — a key design feature in information security and assurance. Although self-hosted file servers are rapidly being overtaken in popularity by bundled cloud services such as Microsoft's OneDrive, they are still very common as legacy systems and can pose a pressing security risk if not properly maintained.

32. Using the Firefox address bar, **navigate** to **fileserver01.securelabsondemand.com** to access the file server's web GUI.

33. At the TrueNAS log-in screen, **log in** using the following credentials:

User: **root**

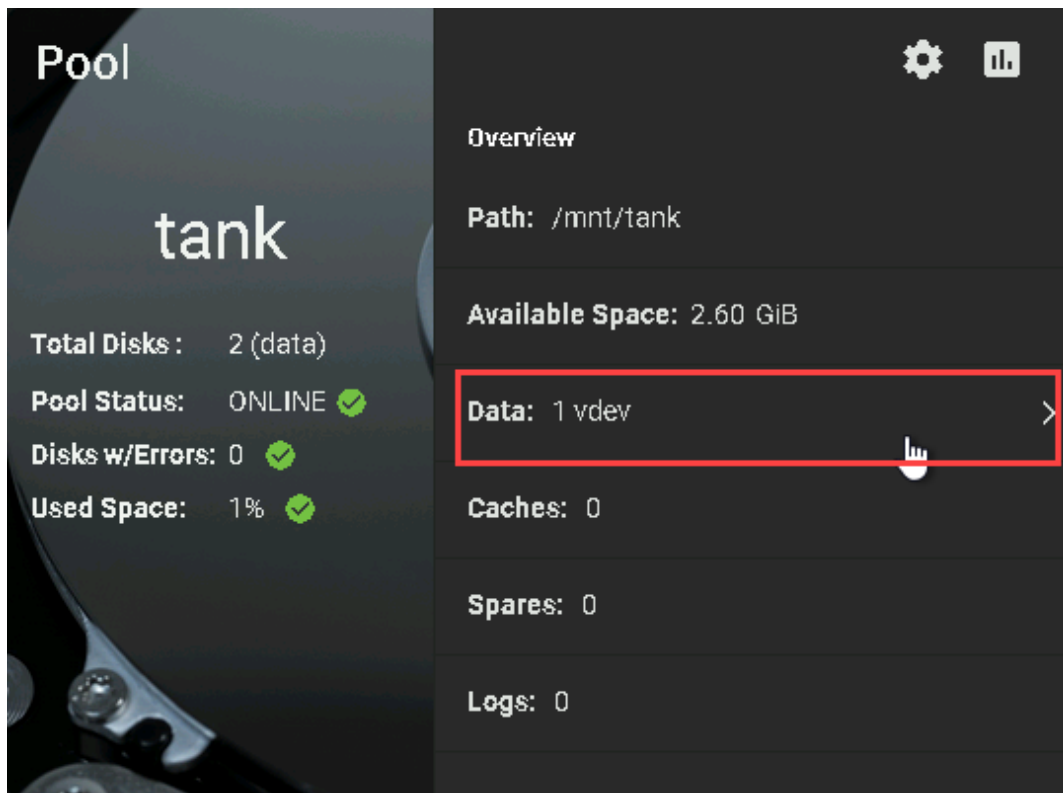
Password: **password**

Note: FileServer01 is running TrueNAS, a FreeBSD-based family of NAS operating systems. After logging in, you should be greeted by the TrueNAS dashboard. Like the pfSense dashboard, the TrueNAS dashboard displays important details about the NAS configuration and its current status. Within the Pool tile, you should see two data disks associated with the Tank pool. In TrueNAS parlance, Pooling is a means of representing multiple physical volumes as a single logical volume. In this case, the single logical volume is Tank, a virtual device (or vdev).

34. When prompted, **close** the **Get Started dialog box**.

35. In the Pool / tank tile, **click** the **Data row** to display the disks in the tank volume.

You may need to scroll down to see the Pool / tank tile.



Pool/tank tile

Note: The two disks (da0 and da1) are organized in a mirrored configuration, which ensures that if one fails, the other can continue to function. NAS systems like this one can play an important role in supporting a comprehensive data security strategy, enabling offering redundancy, backup management, generating alerts for unusual behavior, scanning content for malicious code, and more.

36. **Make a screen capture** showing the **disks in the tank volume**.

Note: This concludes Section 2 of the lab.

Section 3: Challenge and Analysis

Note: The following exercises are provided to allow independent, unguided work using the skills you learned earlier in this lab — similar to what you would encounter in a real-world situation.

Part 1: Explore the User Domain

While the User Domain was briefly discussed in conjunction with the Workstation Domain, it was not explored in length due to the present limitations of virtualizing human beings. In some ways, the challenges of developing a virtual lab exercise that explores the User Domain mirror the challenges that security practitioners face in attempting to secure the User Domain. Human beings are not machines, which makes them much more unpredictable and, consequently, more difficult to secure.

For this exercise, use the Internet to conduct research on the risks, threats, and vulnerabilities associated with the User Domain, as well as security controls used to protect it.

Based on your research, **identify** at least **two compelling threats** to the User Domain and **two effective security controls** used to protect it. Be sure to cite your sources.

Part 2: Research Additional Security Controls

For this exercise, imagine that you have recently been hired as a security analyst at a small/medium-sized business (SMB) called the Juice Shop. The Juice Shop runs a small office network for its employees and an off-site data center for its mission-critical applications. The Juice Shop already has several basic security controls in place, such as packet filtering firewalls and Active Directory Domain Services, but until recently, cybersecurity has not been a top priority for the company. That changed after an employee was tricked into sharing their credentials by a spear phishing campaign.

Your manager, the Director of IT, has asked you to review the Juice Shop IT Infrastructure and recommend additional security controls that could be implemented in each of the technical domains of a typical IT infrastructure (everything but the User Domain, for which you already have some recommendations in hand). Using the Internet, conduct research on common security controls that could be implemented at the Juice Shop. While conducting your research, you should use your knowledge of each domain to search for security controls specific to the technologies within each domain, rather than the domain itself.

Based on your research, **identify** security controls that could be implemented in the Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application Domains. **Recommend** and **explain** one security control for each domain. Be sure to cite your sources.

Note: This concludes Section 3 of the lab.