

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Student:

Patrick Kierzkowski

Email:

pxk405@francis.edu

Time on Task:

24 hours, 57 minutes

Progress:

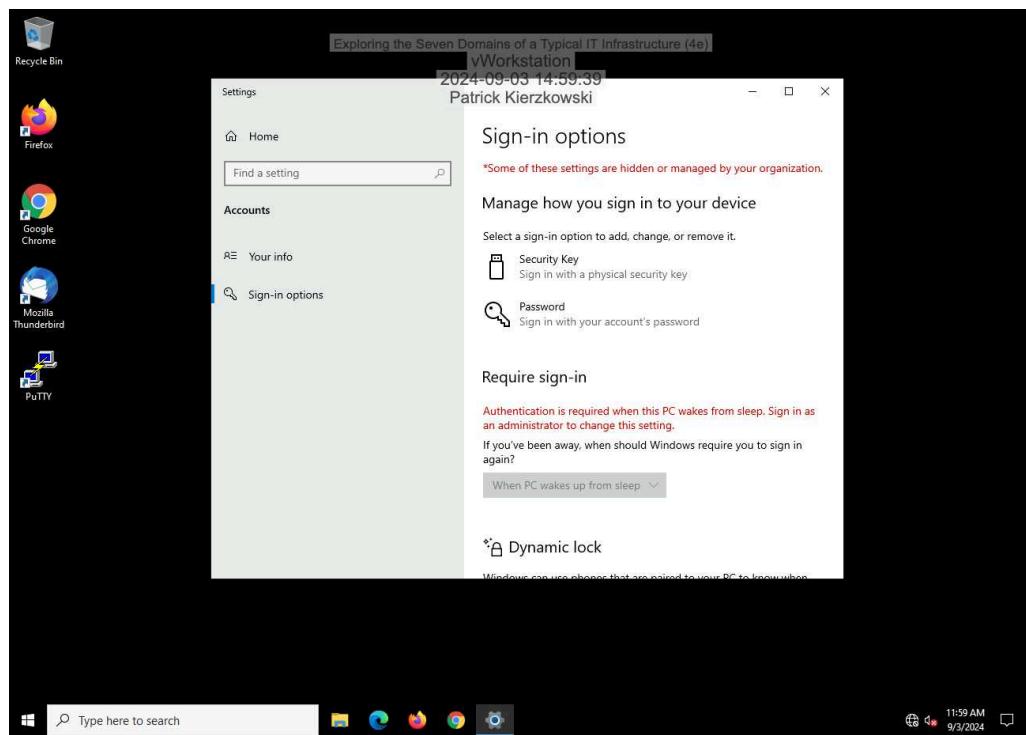
100%

Report Generated: Monday, July 7, 2025 at 9:49 PM

Section 1: Hands-On Demonstration

Part 1: Explore the Workstation Domain

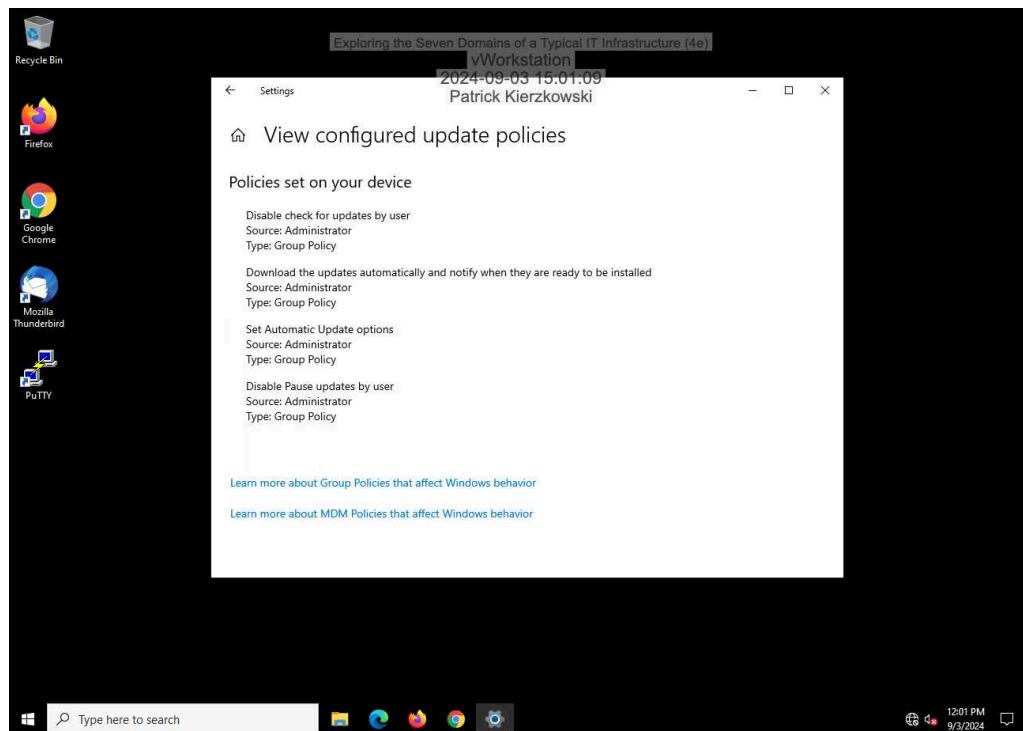
4. Make screen capture showing the Sign-in options for Alice's account.



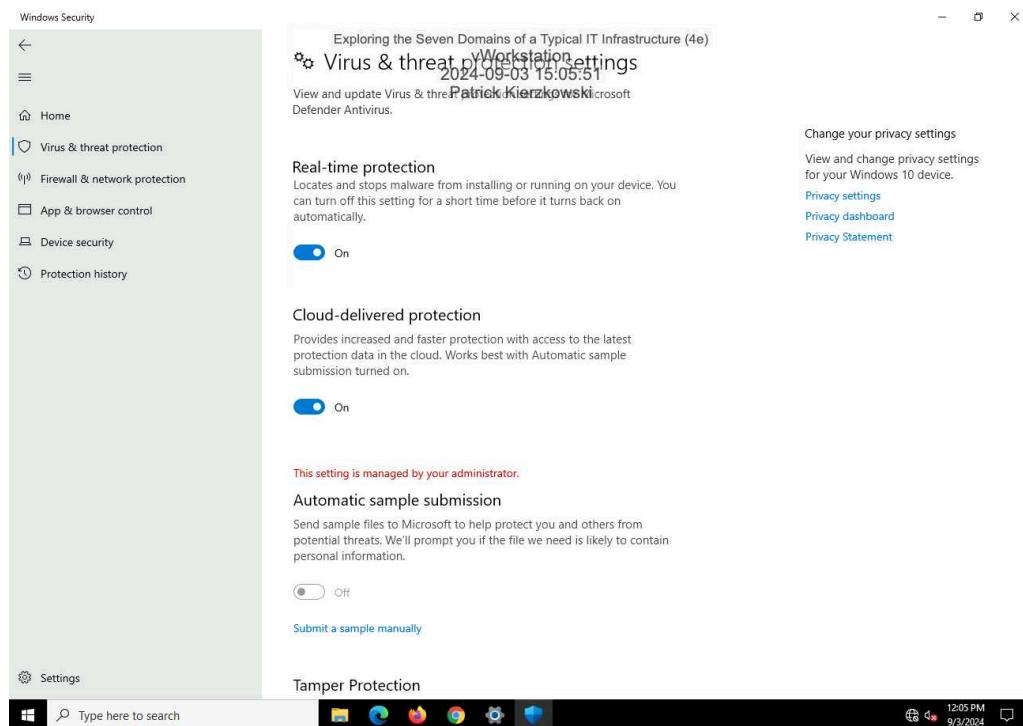
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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



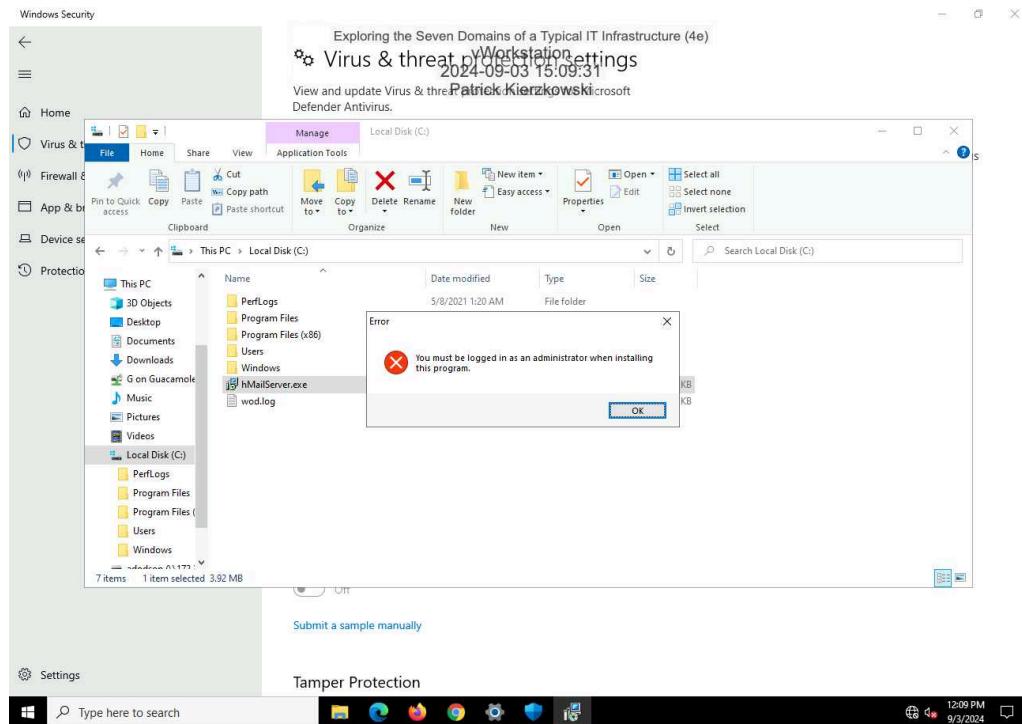
14. Make a screen capture showing the Virus & Threat Protection Settings.



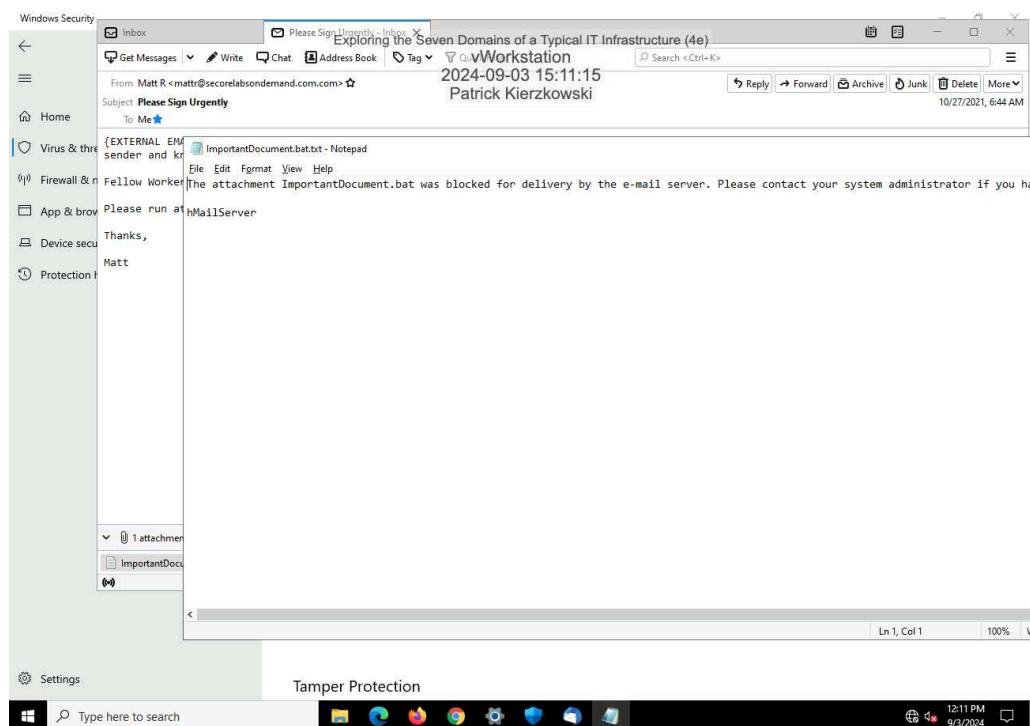
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

18. Make a screen capture showing the security warning from attempting to run an executable file.



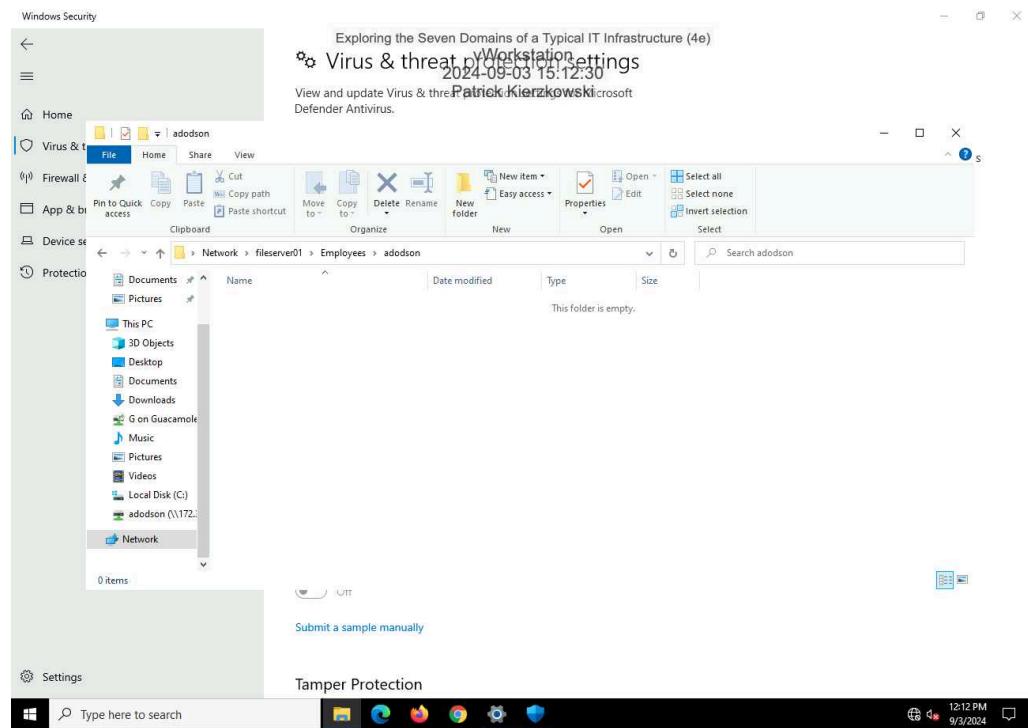
24. Make a screen capture showing the blocked attachment message.



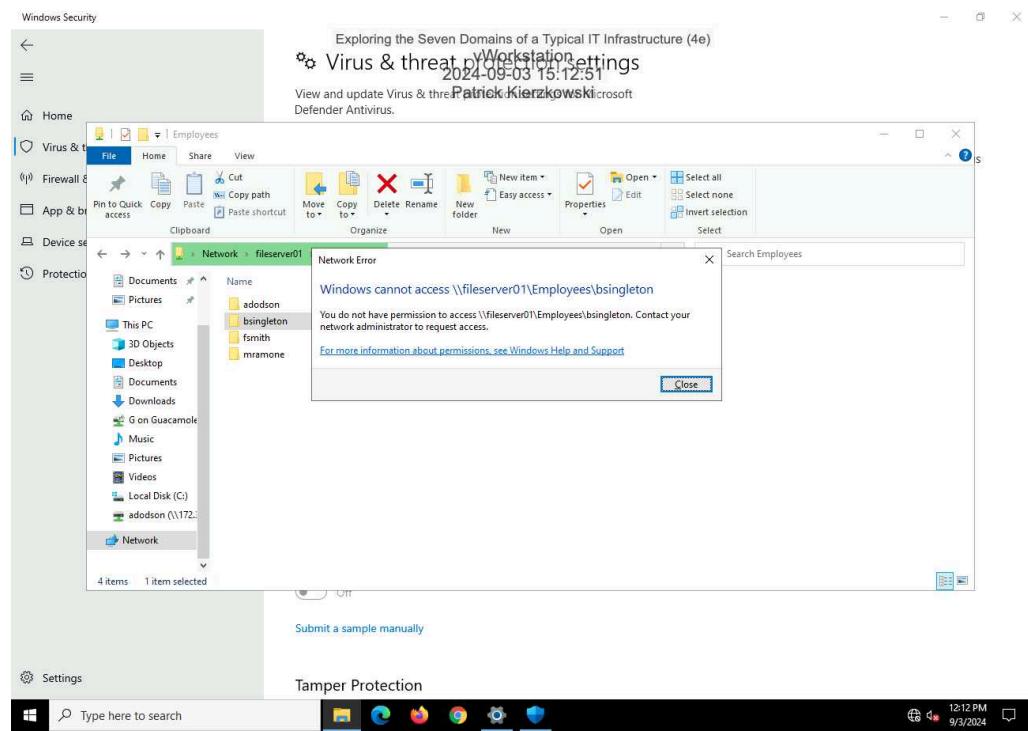
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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



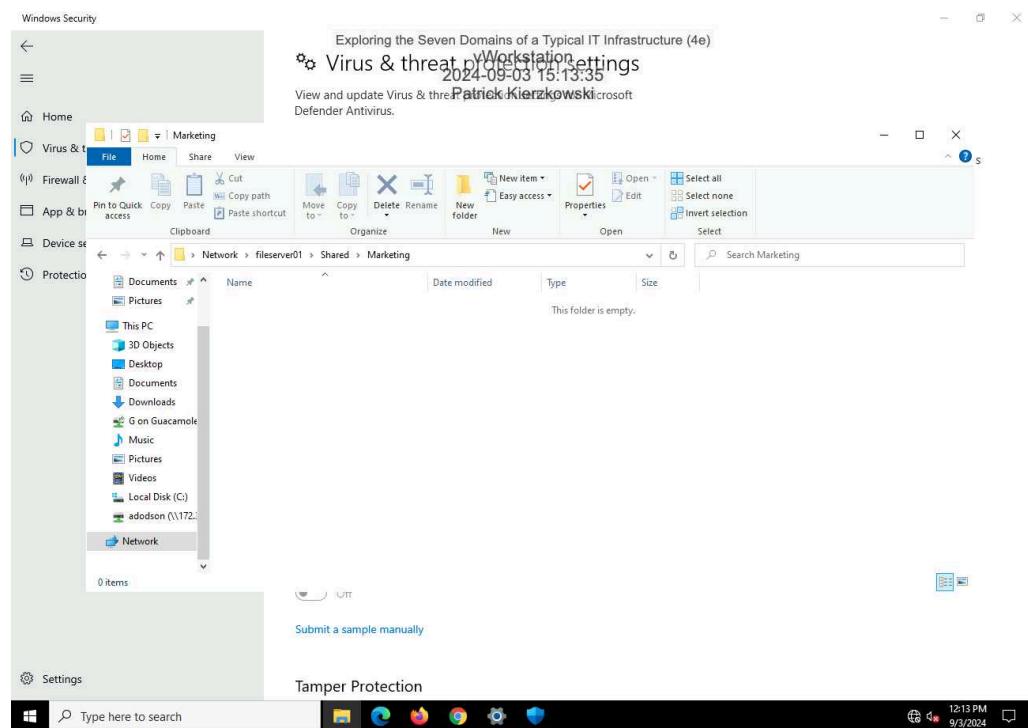
29. Make a screen capture showing a failed connection to another user folder.



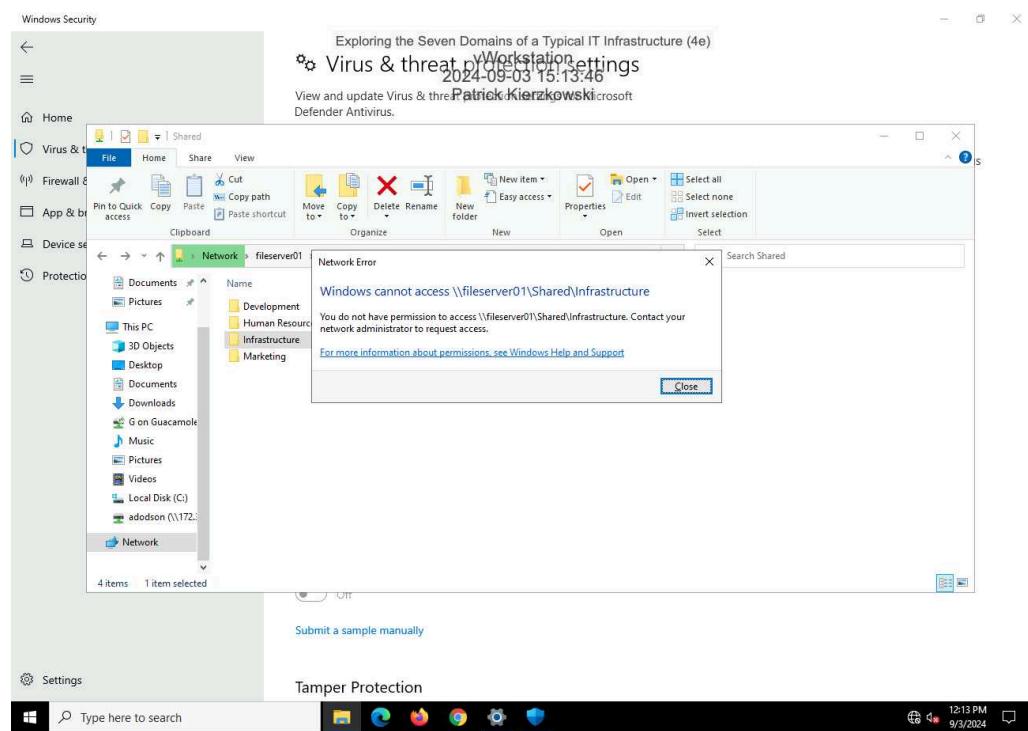
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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.

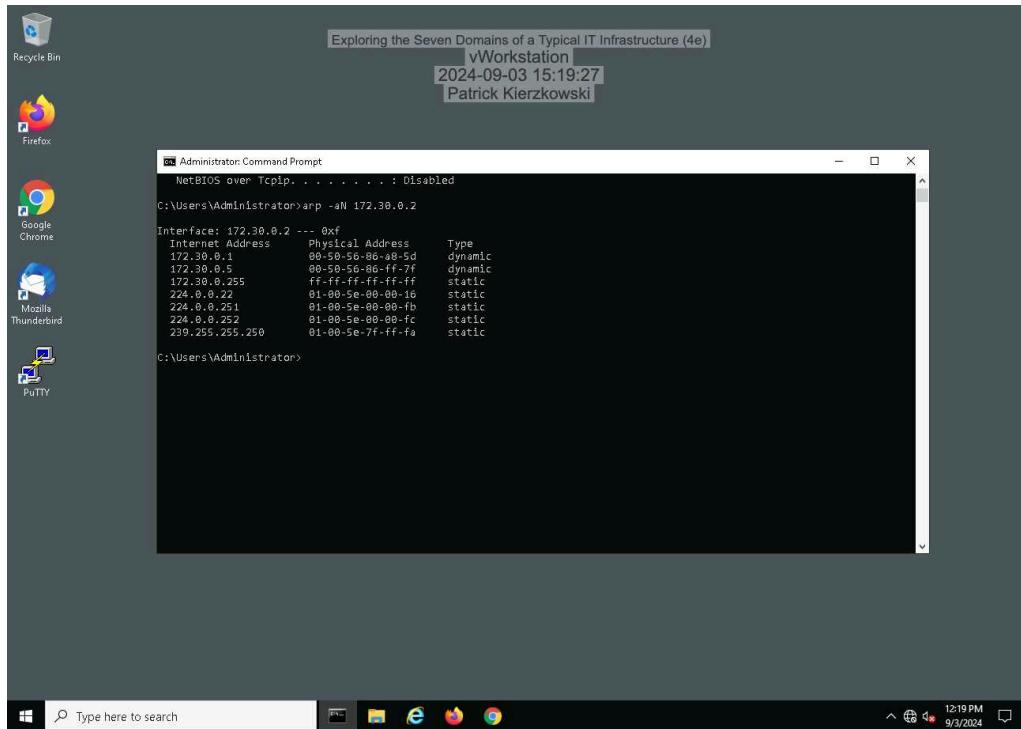


Part 2: Explore the LAN Domain

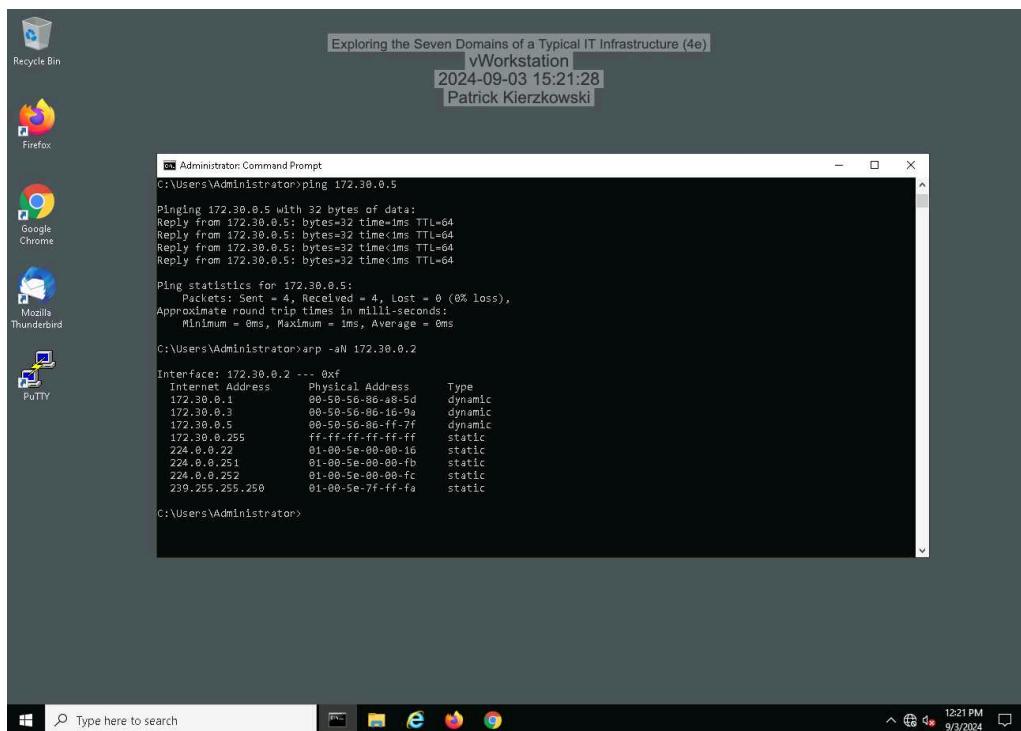
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

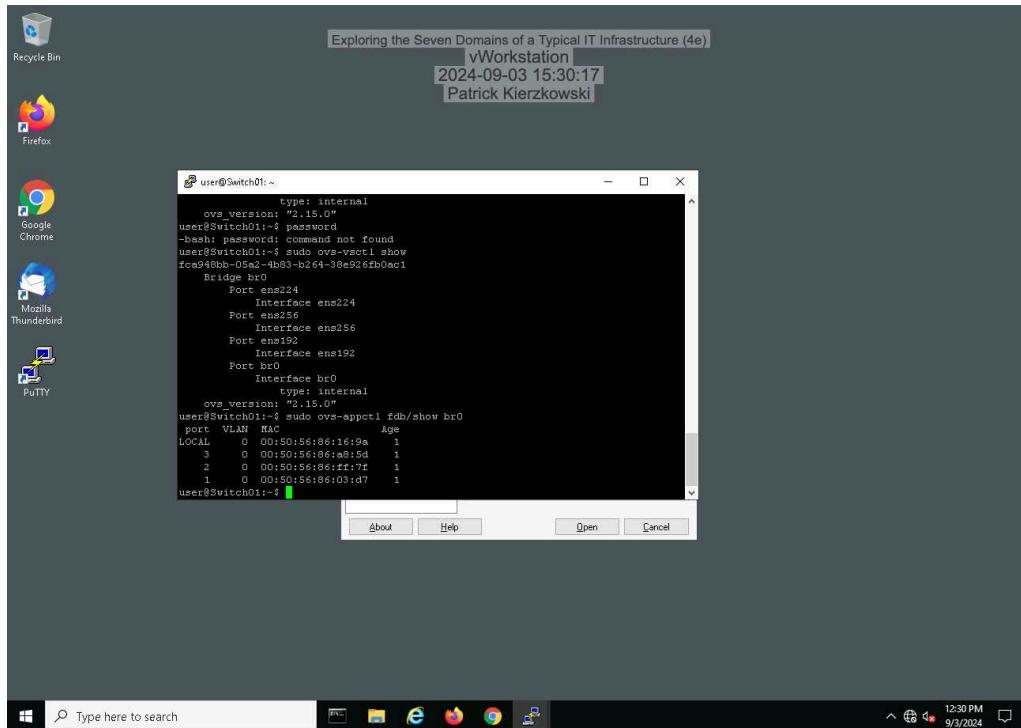
5. Make a screen capture showing the vWorkstation's original ARP table.



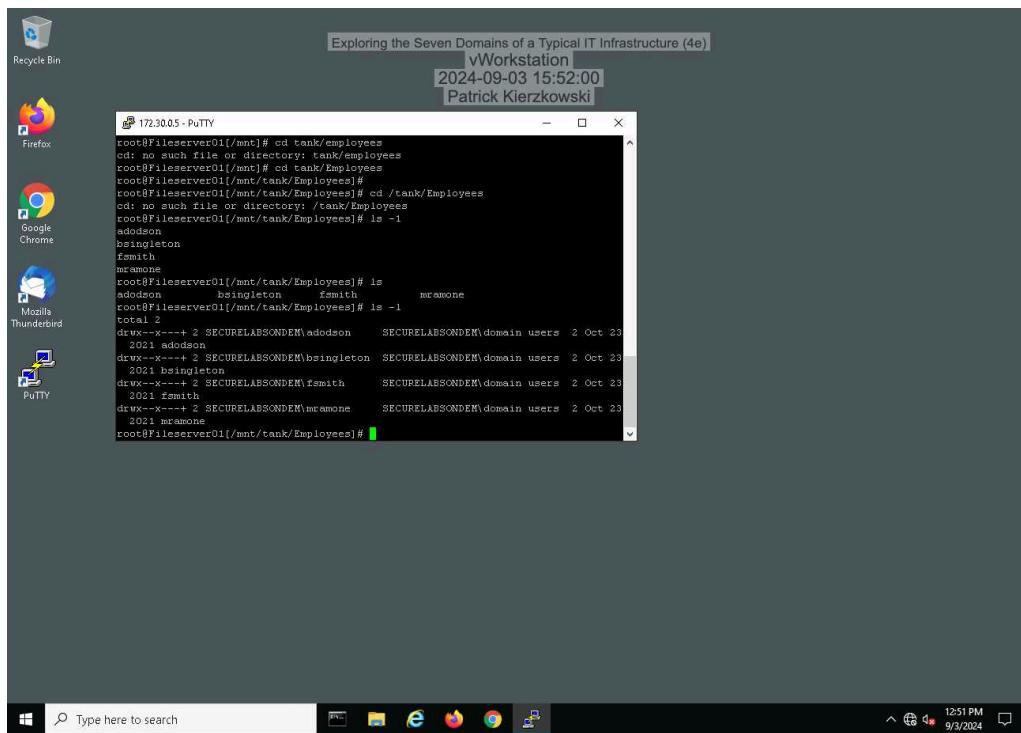
10. Make a screen capture showing the vWorkstation's updated ARP table.



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



30. Make a screen capture showing the contents of the Employees directory.



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

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

The screenshot shows the pfSense web interface under the 'Firewall / NAT / Outbound' tab. The 'Outbound' tab is selected. A warning message at the top says: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, the 'Outbound NAT Mode' section shows four options: Automatic outbound NAT rule generation (selected), Hybrid Outbound NAT rule generation, Manual Outbound NAT rule generation, and Disable Outbound NAT rule generation. The 'Mappings' section displays a table of automatic rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
WAN	127.0.0.0/8 -> 128.172.16.0/24	*	172.31.0.0/24	*	500	WAN address	*	✓	Add Edit Delete Save

At the bottom of the interface, there is a search bar and a status bar showing '12:54 PM 9/3/2024'.

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

The screenshot shows the pfSense web interface under the 'Firewall / Rules / LAN' tab. The 'LAN' tab is selected. A warning message at the top says: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, the 'Rules (Drag to Change Order)' section displays a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 3/1.19 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 22/1.52 MiB	IPv4*	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6*	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the interface, there is a search bar and a status bar showing '12:54 PM 9/3/2024'.

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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

The screenshot shows the pfSense web interface under the 'System / Routing / Static Routes' section. The 'Static Routes' tab is selected. A table lists two static routes:

Network	Gateway	Interface	Description	Actions
172.16.0.0/24	DC-10.0.0.2	DCLINK	DC Internal	Edit Delete Details
172.31.0.0/24	DC-10.0.0.2	DCLINK	DC DMZ	Edit Delete Details

Below the table is a green 'Add' button. The browser's address bar shows '172.30.0.1/system_routes.php'. The status bar at the bottom indicates '12:55 PM 9/3/2024'.

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

The screenshot shows a Windows Command Prompt window titled 'Administrator: Command Prompt'. The user has run the 'tracert' command twice:

```
Microsoft Windows [Version 10.0.20348.288]
(c) Microsoft Corporation. All rights reserved.

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

C:\Users\Administrator>tracert 172.16.0.1
Tracing route to pfsense-dc.securelabsondemand.com [172.16.0.1]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  pfsense-office.securelabsondemand.com [172.30.0.1]
  2  <1 ms  <1 ms  <1 ms  pfsense-dc.securelabsondemand.com [172.16.0.1]

Trace complete.
```

The browser's address bar shows '172.30.0.1/system_routes.php'. The status bar at the bottom indicates '12:56 PM 9/3/2024'.

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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

The screenshot shows the pfSense Firewall / NAT / Port Forward configuration. The interface has tabs for Port Forward, 1:1, Outbound, and NPt. The Port Forward tab is selected. A table lists two port forwarding rules:

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	203.30.3.40	443 (HTTPS)	172.31.0.40	443 (HTTPS)	Pass	
<input type="checkbox"/>	WAN	TCP	*	*	203.30.3.40	80 (HTTP)	172.31.0.40	80 (HTTP)	Pass	

A legend at the bottom left indicates that a green arrow points right means "Pass" and a red double-headed arrow means "Linked rule".

At the bottom of the browser window, the taskbar shows icons for File Explorer, Edge, and other applications, along with the date and time (9/3/2024, 12:58 PM).

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

The screenshot shows the pfSense Firewall / Rules / DMZ configuration. The interface has tabs for Floating, WAN, LAN, DMZ, OFFICELINK, and OpenVPN. The DMZ tab is selected. A table lists three DMZ rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	4/457 KB	IPv4 *	*	*	*	*	*	none		Open Mail Relay	
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	LAN net	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	DMZ net	*	DMZ address	*	*	none			

At the bottom of the browser window, the taskbar shows icons for File Explorer, Edge, and other applications, along with the date and time (9/3/2024, 12:58 PM).

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Section 2: Applied Learning

Part 1: Explore the WAN Domain

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

The screenshot shows the pfSense web interface for managing static routes. The URL is 172.16.0.1/system_routes.php. The page title is "Exploring the Seven Domains of a Typical IT Infrastructure (4e) vWorkstation". A warning message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a sub-navigation for System / Routing / Static Routes. Under "Static Routes", there is a table with one entry:

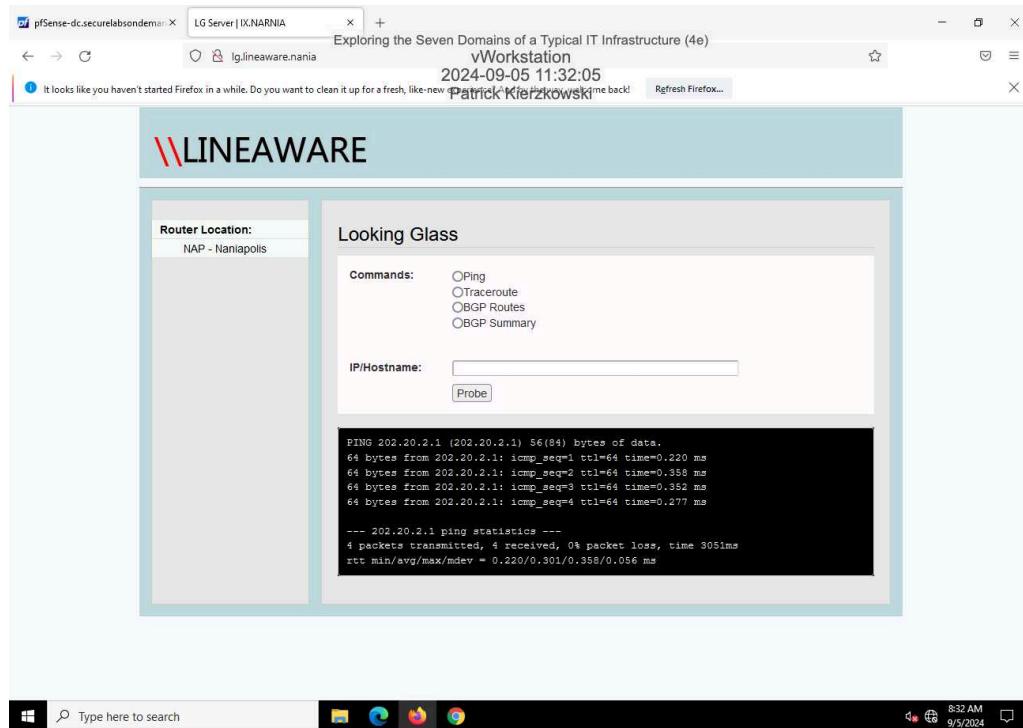
Network	Gateway	Interface	Description	Actions
172.30.0.0/24	Office - 10.0.0.1	OFFICELINK	Office	Edit Delete Details

At the bottom of the page, it says "pfSense is developed and maintained by Netgate. © ESF-2004 - 2024 View license." The taskbar at the bottom shows icons for File Explorer, Task View, Edge, Firefox, and Chrome. The system tray shows the date and time as 8:26 AM 9/5/2024.

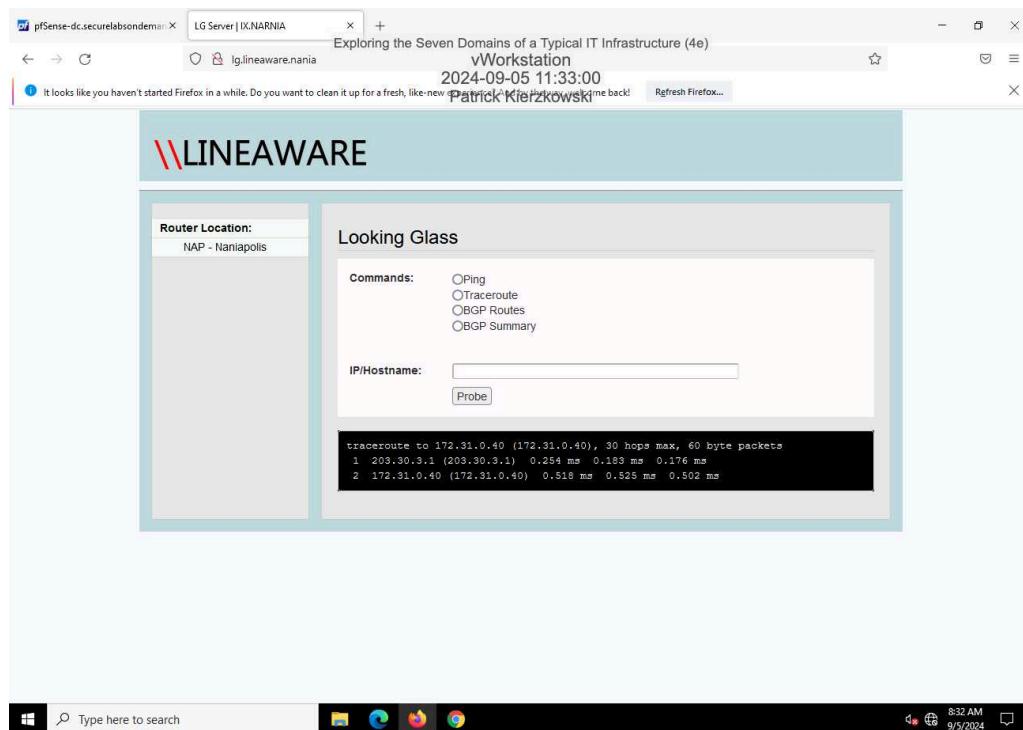
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

9. Make a screen capture showing the BPG neighbor ping results.



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

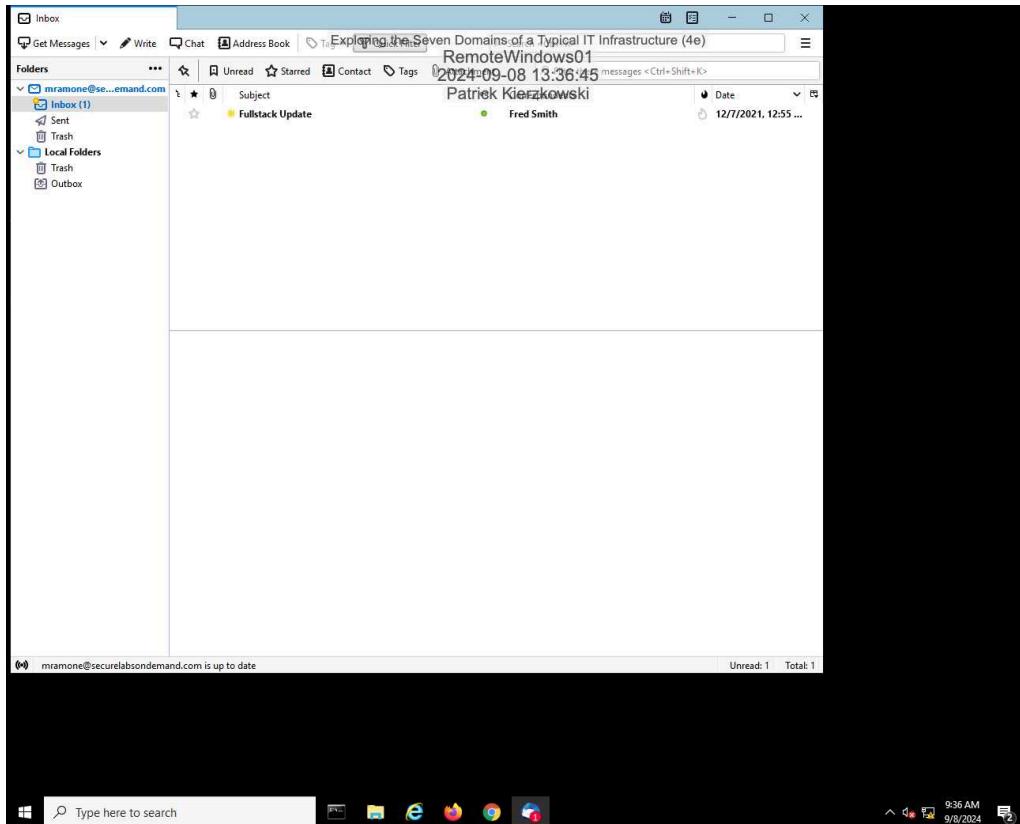


Part 2: Explore the Remote Access Domain

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

9. Make a screen capture showing the successful connection to the email server.



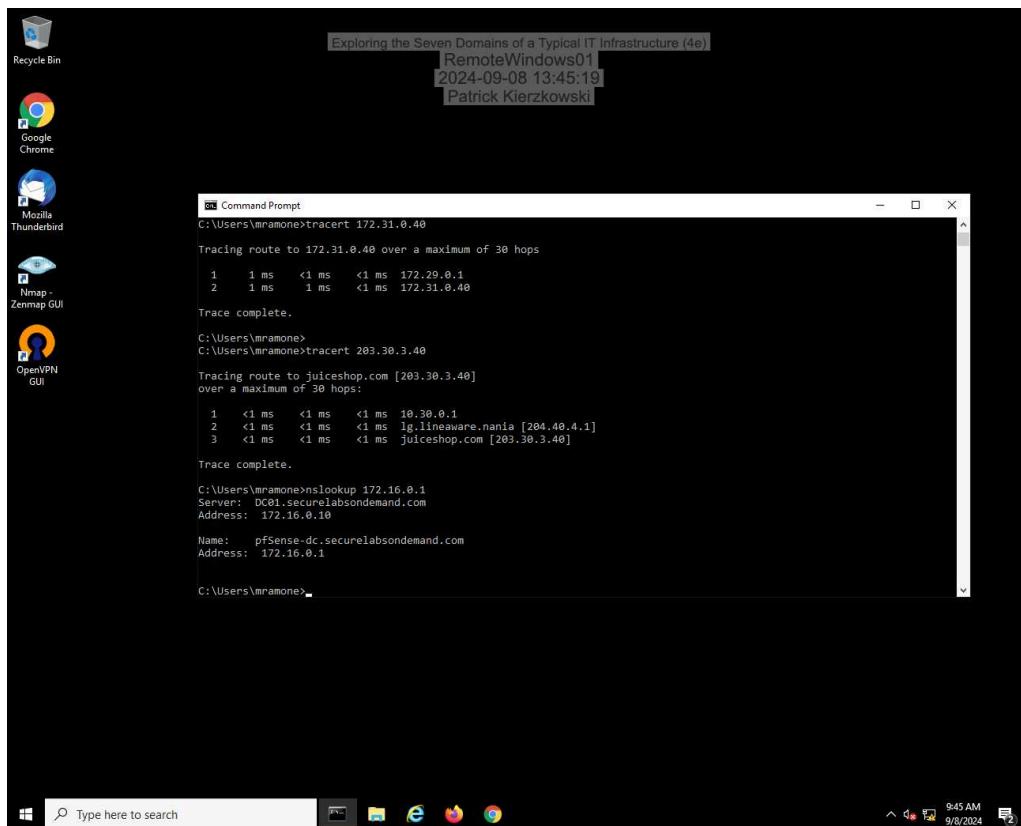
14. Document whether the VPN connection is split tunnel or full tunnel, based on the tracert results.

The first one was a full tunnel, meanwhile the second one was a split tunnel

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

16. Make a screen capture showing the successful reverse DNS lookup for the internal host.

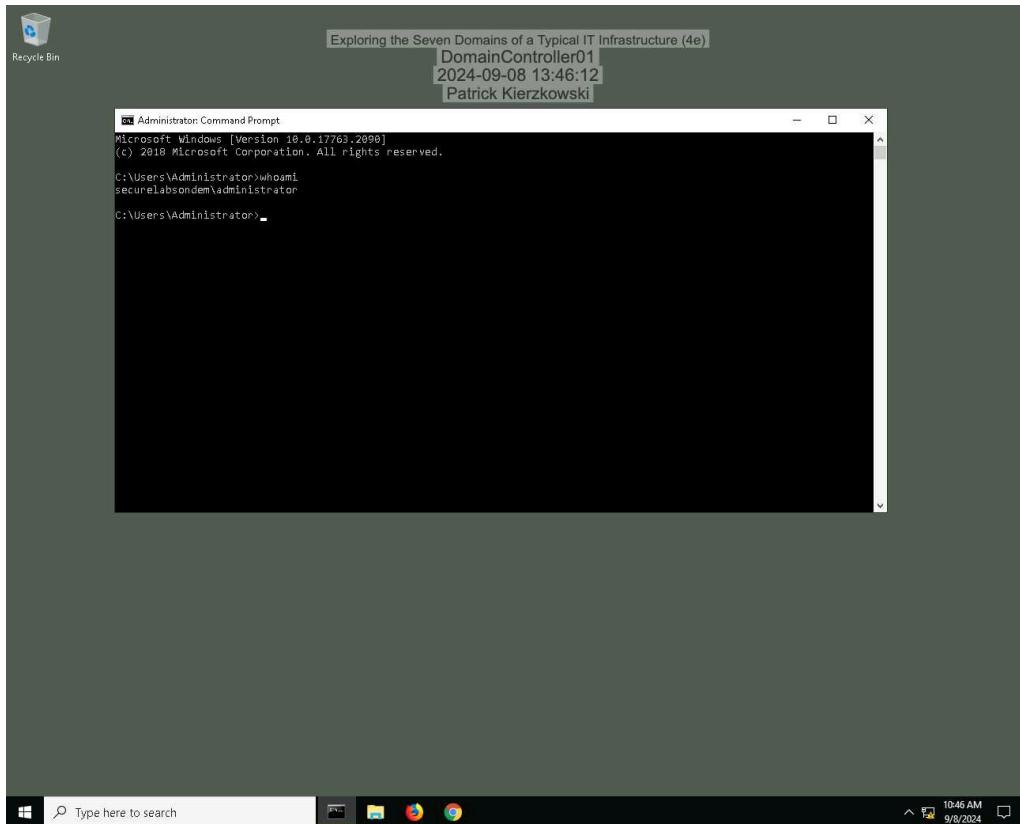


Part 3: Explore the System/Application Domain

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

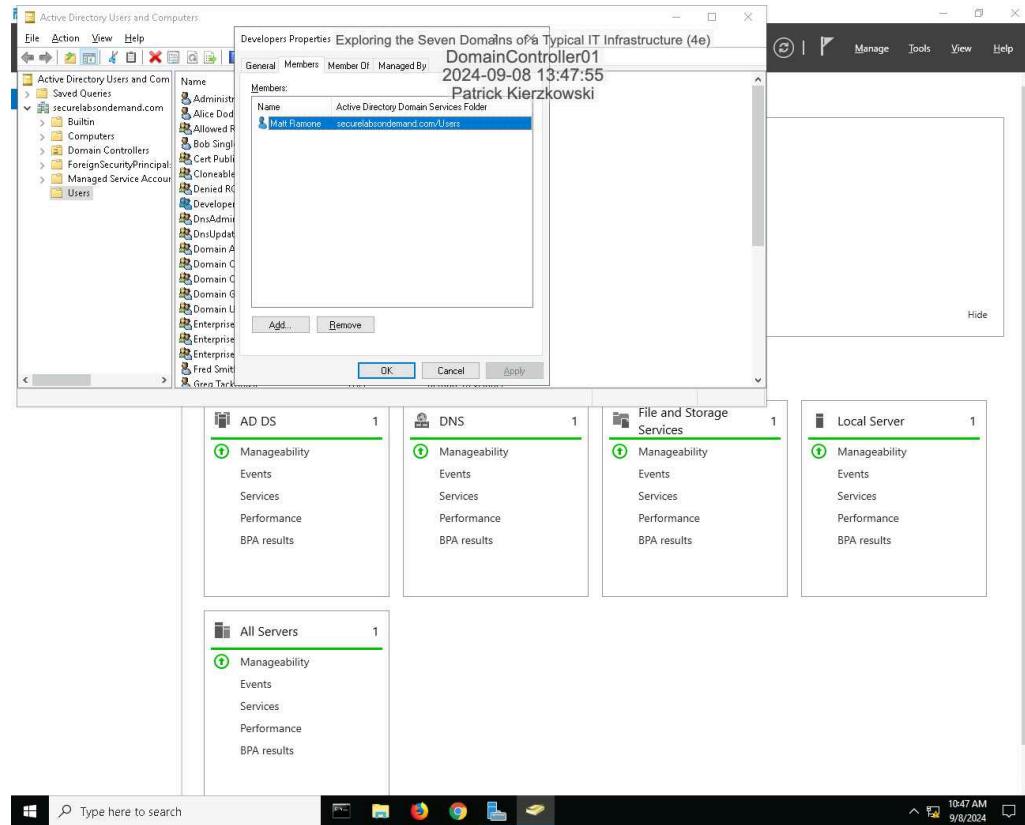
4. Make a screen capture showing the whoami results.



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

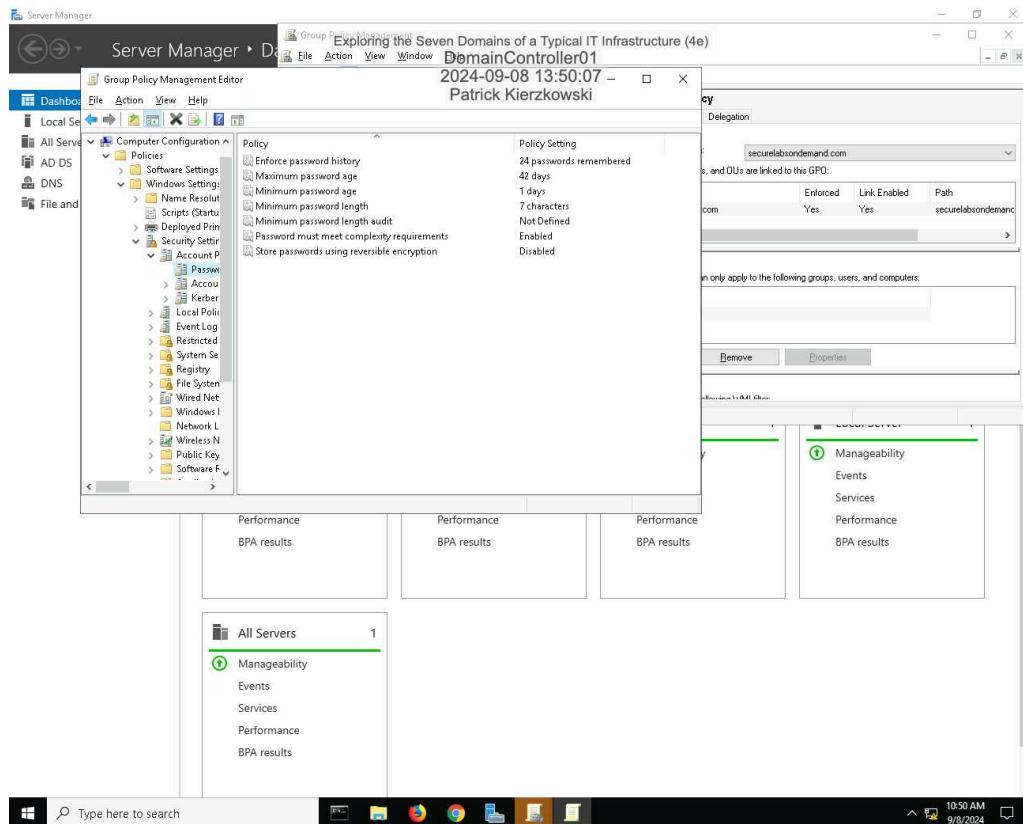
10. Make a screen capture showing the members of the Developers AD group.



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

16. Make a screen capture showing the password policy settings in the Group Policy Management Console.



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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

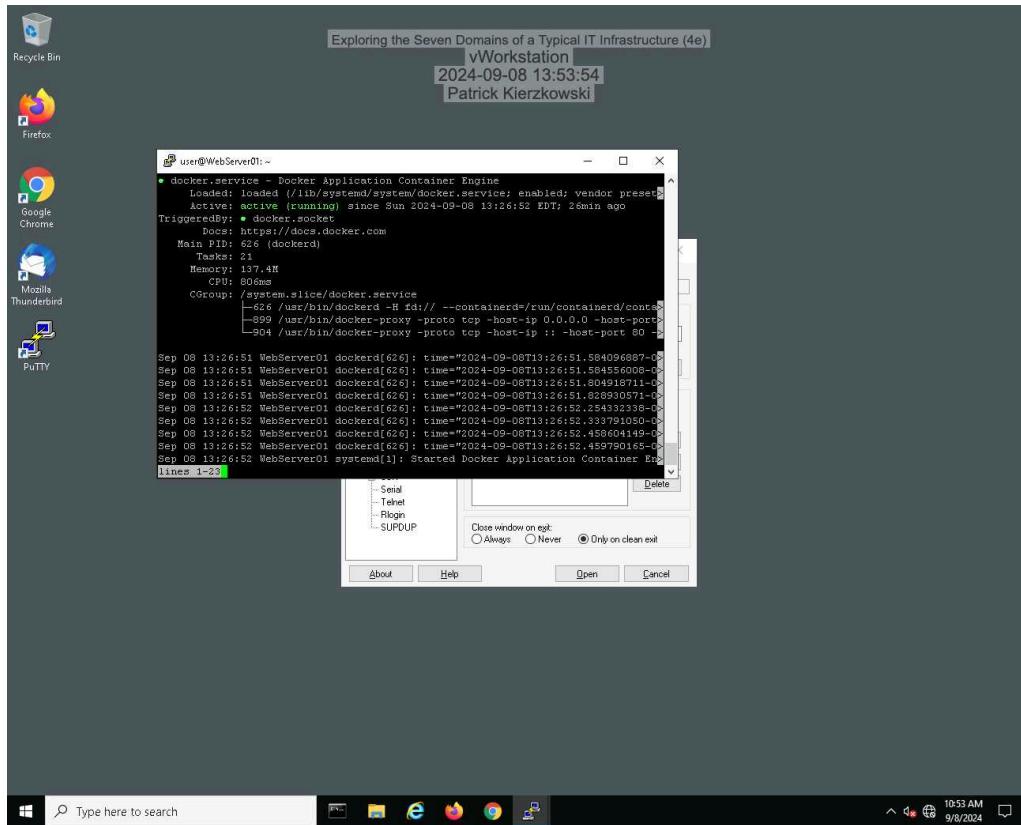
20. Make a screen capture showing the DNS entries.

Name	Type	Data	Timestamp
msdc	Start of Authority (SOA)	[490] dc01.securelabondemand.com	static
sites	Name Server (NS)	dc01.securelabondemand.com	static
_tcp	Host (A)	172.16.0.10	9/8/2024 10:00:00 AM
_udp	Mail Exchanger (MX)	[10] mailserver01.securelab...	static
_DomainDnsZones	Text (TXT)	vs-pf1 ip4:172.16.0.10-all	static
_ForestDnsZones	Host (A)	172.16.0.10	static
_dc01	Host (A)	192.168.1.77.1	static
dc01	Host (A)	172.30.0.5	11/10/2021 11:00:00 AM
fileserver01	Host (A)	172.16.0.10	static
mailserver01	Host (A)	172.16.0.1	static
rsense-dc	Host (A)	172.30.0.1	static
rsense-office	Host (A)	172.29.0.2	9/8/2024 10:00:00 AM
RemoteWindows01	Host (A)	172.30.0.2	9/8/2024 10:00:00 AM
Workstation	Host (A)		

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

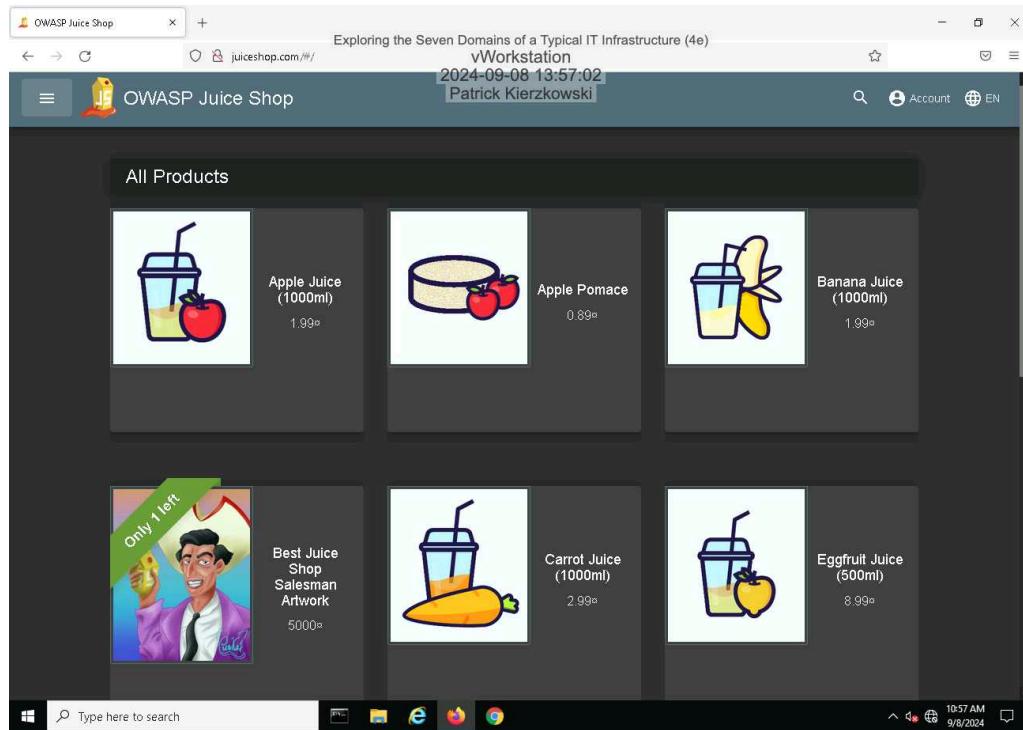
28. Make a screen capture showing the Docker service status.



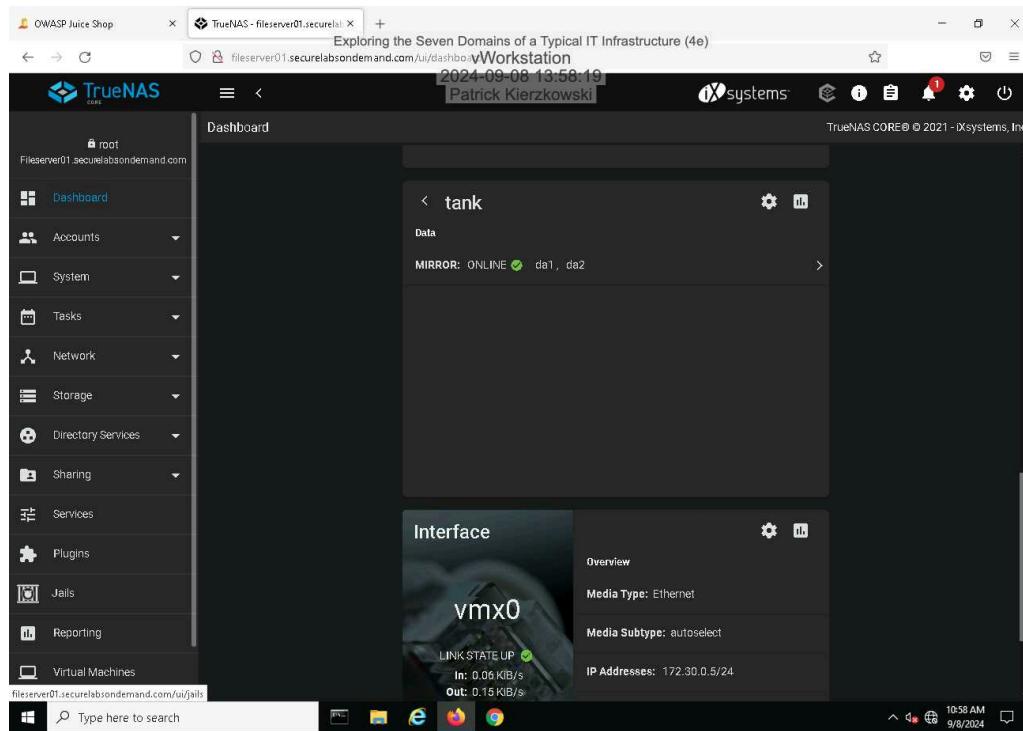
Exploring the Seven Domains of a Typical IT Infrastructure (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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



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



Section 3: Challenge and Analysis

Part 1: Explore the User Domain

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.

Two compelling threats to the User Domain would be phishing attacks and insider threats. Phishing attacks are when people outside of the company try to trick employees into giving away information by pretending to be a trusted source in an email or website. Insider threats on the other hand is when the companies own employees misuse sensitive data, either by accident or for their own gain. These are both serious threats to the User Domain, but they also have security controls that are effective at protecting against it. For example to protect yourself against phishing attacks, you shouldn't respond to spam and make your email uncommon so its hard to guess your email. You should also implement spam filters and anti-phishing software incase spammers do get your email. Then they will get blocked out before they reach your inbox and reduce the chance that they can fall victim to phishing (Kaspersky, n.d.). To protect yourself from insider threats, you should assess access levels, and review how much access everyone has. Then you give everyone the minimum to where they can still complete their tasks, and minimize the amount of data everyone can obtain , so insider threats are less likely to happen (Netwrix, n.d.). You should also pinpoint the areas where the most harm can be done, and use data classification to prioritize and focus your security efforts efficiently (Netwrix, n.d.). Kaspersky. (n.d.). Phishing Prevention Tips. <https://usa.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips> Netwrix. (n.d.). Insider Threat Prevention Best Practices. <https://www.netwrix.com/insider-threat-prevention-best-practices.html>

Part 2: Research Additional Security Controls

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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

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.

There are various security controls that can be added in the Workstation, Lan, LAN-to-WAN, WAN, Remote Access, and System/Application Domains, respectively. For example in the Workstation you can implement a endpoint security software. This essentially enables businesses to protect devices that employees use for work by allowing them to quickly detect malware and other cyber threats (Fortinet, n.d.). A software that could be installed for endpoint security software is ESET Endpoint Security. A security control for LAN is network segmentation. This essentially means that you control how the traffic flows amongst a network by splitting it into subnetworks. By reducing overall traffic, the system will work better for employees that use it and makes it safer (Cisco n.d.). This can be enforced by including internal firewalls, but the less costly resolution would be for technology to group and tag network traffic, then using the traffic tags to enforce segmentation policy directly onto the network equipment (Cisco, n.d.). Firewalls can be used to secure LAN-to-WAN. Firewalls allows traffic flows from the LAN, while blocking it out from the WAN. When a local client initiates a session to the internet, return traffic is allowed, but any traffic initiated from the internet, is blocked (Sandu, n.d.). The traffic from the internet could be an attacker, so its blocked. To protect the WAN and remote access I would recommend using a VPN because a VPN creates a tunnel between two points for data privacy (Paloalto, n.d.). This tunnel encrypts data and protects it from unwanted access, and it keeps all data confidential that travels over the WAN. For remote access the VPN adds in an extra layer of security by using a secure tunnel, allowing them to access the network as if they were at work, which reduces the risk of being exposed to cyber attacks. The security control for System/Application Domains would be patch managements. If a hacker or malware find out about the system vulnerabilities, a patch is sent out to correct it (Essex, 2024). If not it can be exploited, which would be bad for the company

Fortinet. (n.d.). What Is Endpoint Security?. <https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security#:~:text=The%20endpoint%20security%20solution%20enables,face%20of%20a%20security%20threat>. Cisco. (n.d.). What Is Network Segmentation?.

<https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html>

Dimi Sandu. (n.d.). Firewalls - Securing the LAN-WAN border. <https://info.verkada.com/firewalls/#:~:text=In%20simple%20terms%2C%20by%20default,return%20traffic%20is%20not%20blocked>.

Paloalto. (n.d.). SD-WAN vs. VPN: How Do They Compare?. <https://www.paloaltonetworks.com/cyberpedia/sd-wan-vs-vpn#:~:text=It%20can%20adapt%20quickly%20and,network%20as%20the%20VPN%20server>

David Essex (2024, May). What is patch management? Lifecycle, benefits and best practices.<https://www.techtarget.com/searchenterprisedesktop/definition/patch-management>