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

Fundamentals of Information Systems Security, Fourth Edition - Lab 01

Student:	Email:
Andrew Sweeney	asweene8@depaul.edu

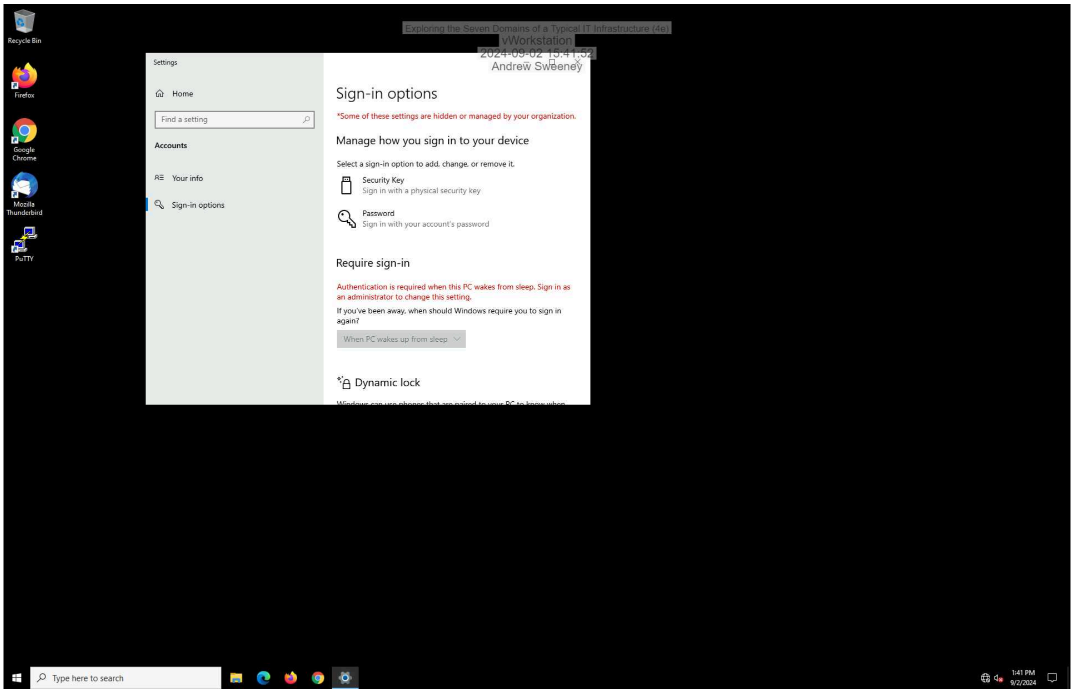
Time on Task:	Progress:
4 hours, 27 minutes	100%

Report Generated: Saturday, September 7, 2024 at 12:38 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)
vWorkstation
2024-09-02 15:41:52
Andrew Sweeney

Settings

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

Require sign-in

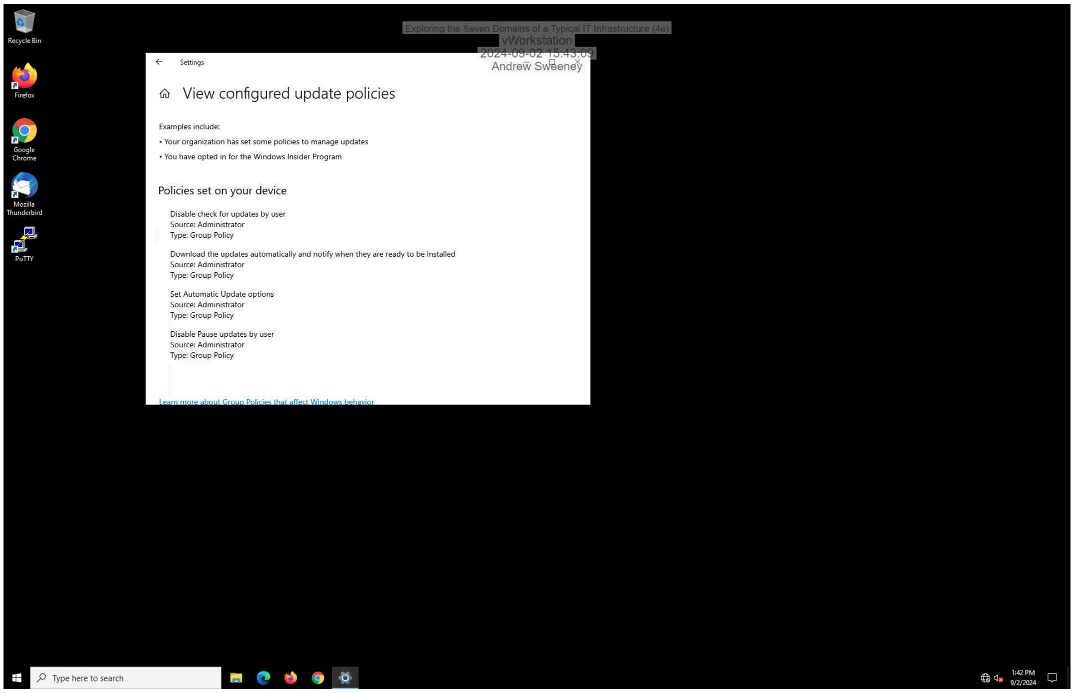
Authentication is required when this PC wakes from sleep. Sign in as an administrator to change this setting.

If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

Dynamic lock

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:43:09
Andrew Sweeney

Settings

View configured update policies

Examples include:

- Your organization has set some policies to manage updates
- You have opted in for the Windows Insider Program

Policies set on your device

Disable check for updates by user
Source: Administrator
Type: Group Policy

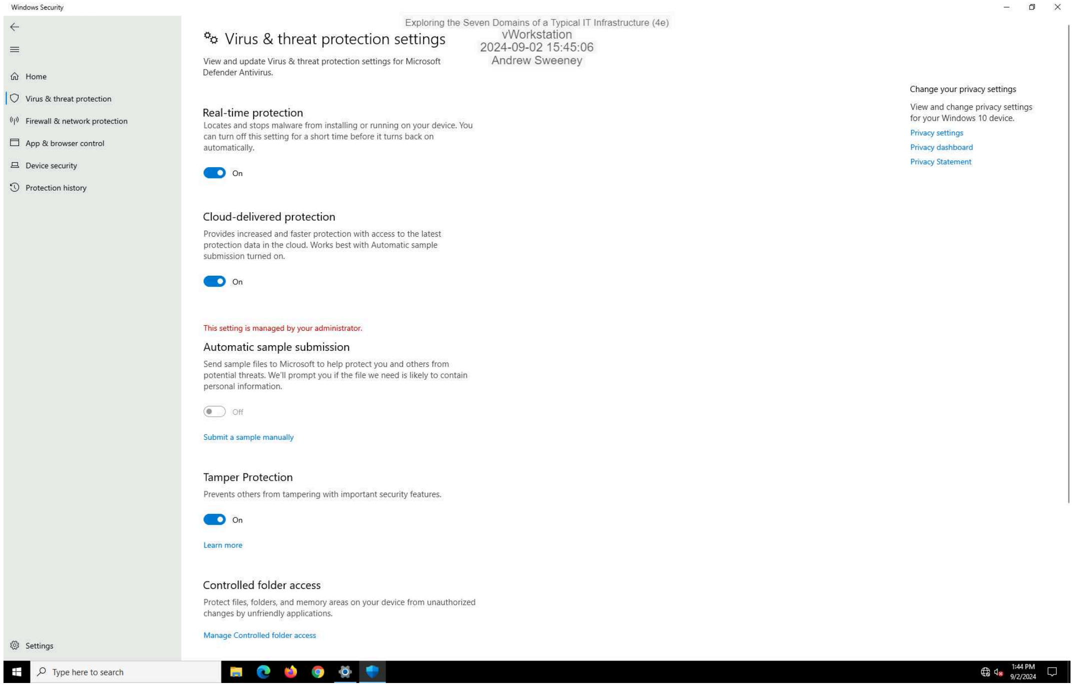
Download the updates automatically and notify when they are ready to be installed
Source: Administrator
Type: Group Policy

Set Automatic Update options
Source: Administrator
Type: Group Policy

Disable Pause updates by user
Source: Administrator
Type: Group Policy

Learn more about Group Policies that affect Windows behavior

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



Windows Security

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:45:06
Andrew Sweeney

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

This setting is managed by your administrator.

Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Off

Submit a sample manually

Tamper Protection
Prevents others from tampering with important security features.

On

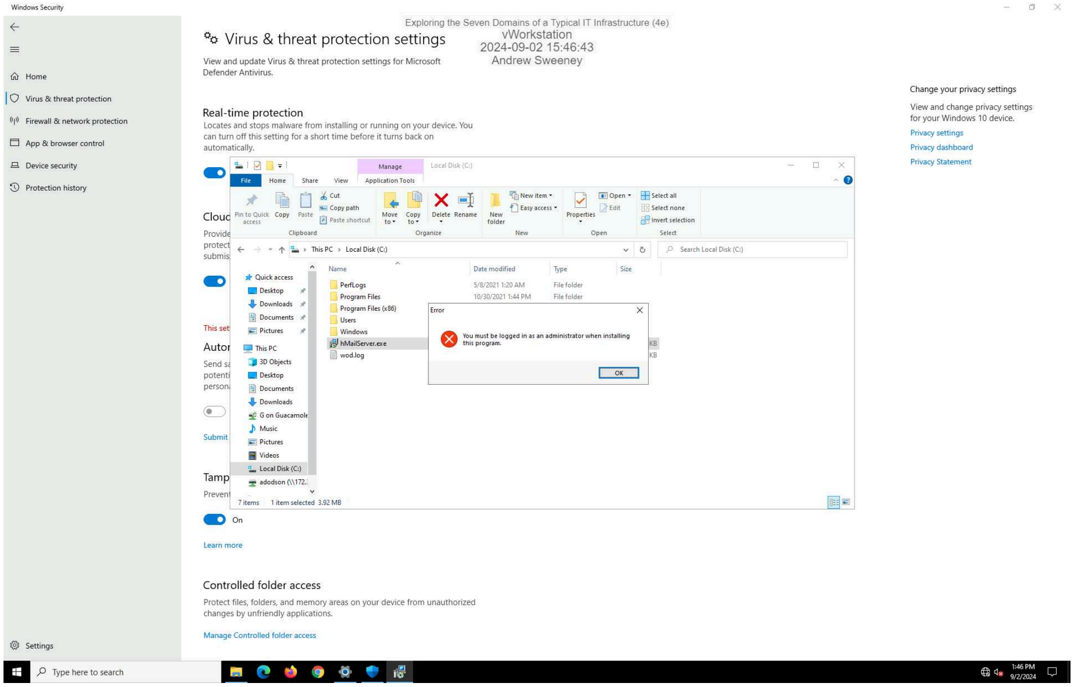
Learn more

Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Manage Controlled folder access

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:46:43
Andrew Sweeney

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Controlled folder access

Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Name	Date modified	Type	Size
PerfLogs	5/8/2021 1:20 AM	File folder	
Program Files	10/30/2021 1:44 PM	File folder	
Program Files (x86)			
Users			
Windows			
hMailServer.exe			KB
wod.log			KB

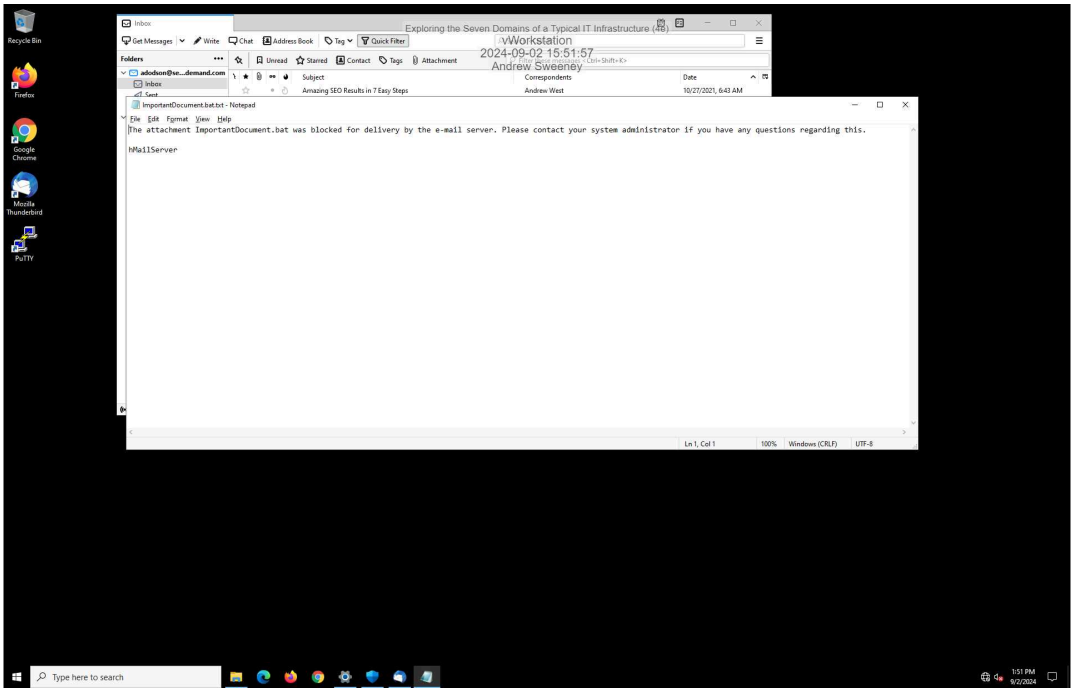
7 items 1 item selected 3.92 MB

Error

You must be logged in as an administrator when installing this program.

OK

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



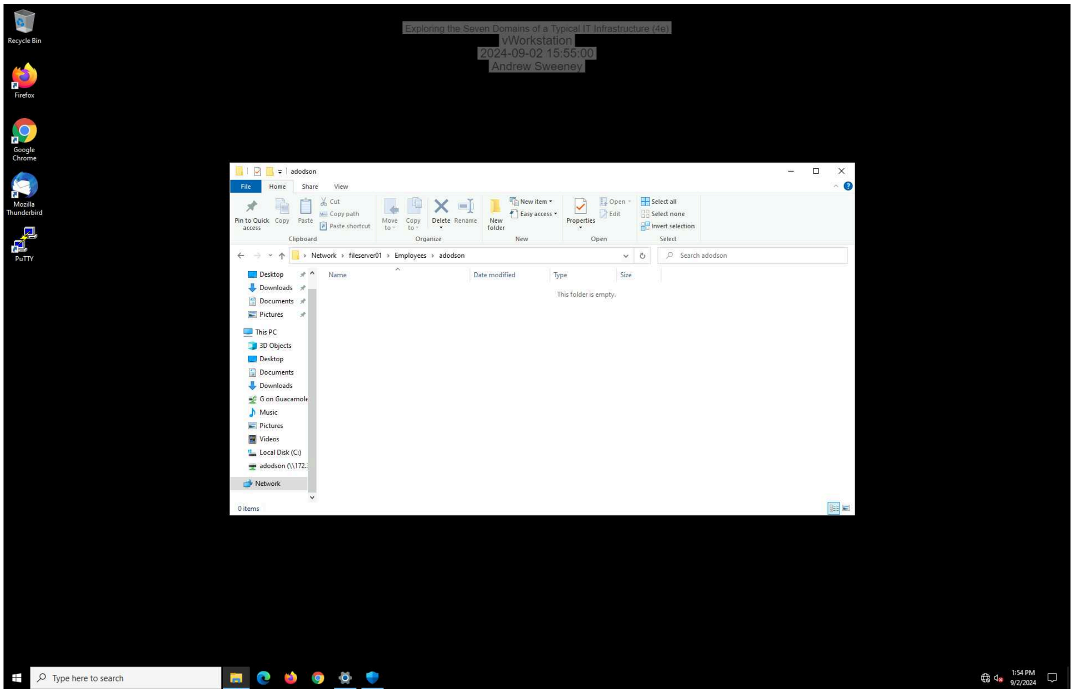
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:51:57
Andrew Sweeney

Subject	Correspondents	Date
Amazing SEO Results in 7 Easy Steps	Andrew West	10/27/2021, 6:43 AM

ImportantDocument.bat.txt - Notepad

```
The attachment ImportantDocument.bat was blocked for delivery by the e-mail server. Please contact your system administrator if you have any questions regarding this.

hMailServer
```

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



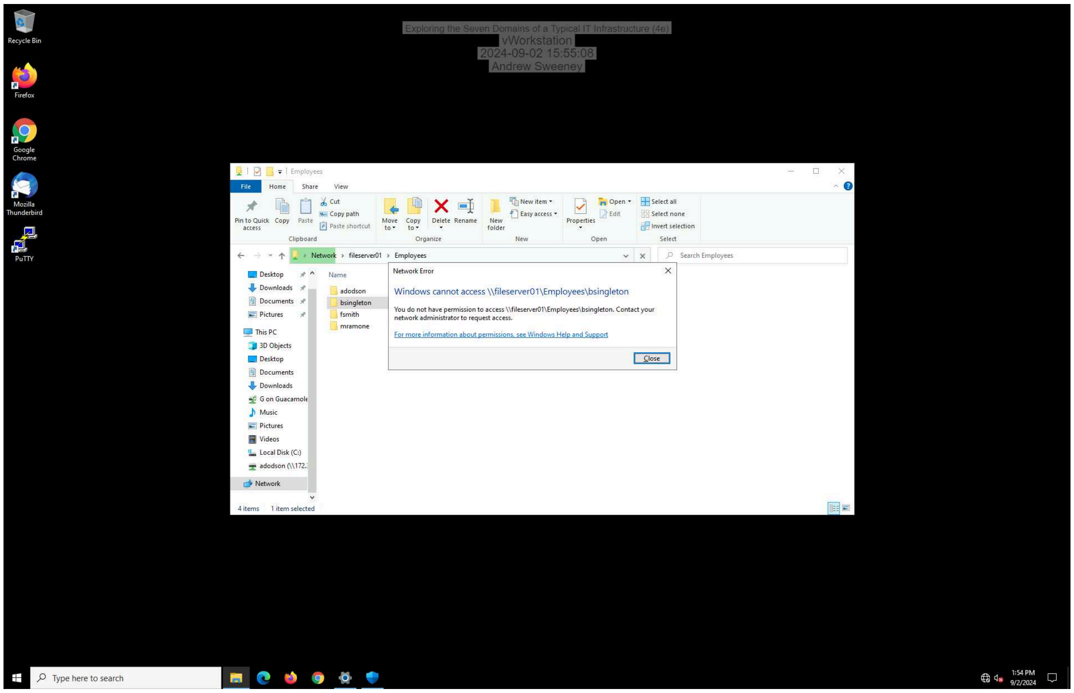
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:55:00
Andrew Sweeney

Network › fileserver01 › Employees › adodson

This folder is empty.

0 items

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:55:08
Andrew Sweeney

Network Error

Windows cannot access \\fileserver01\Employees\bsingleton

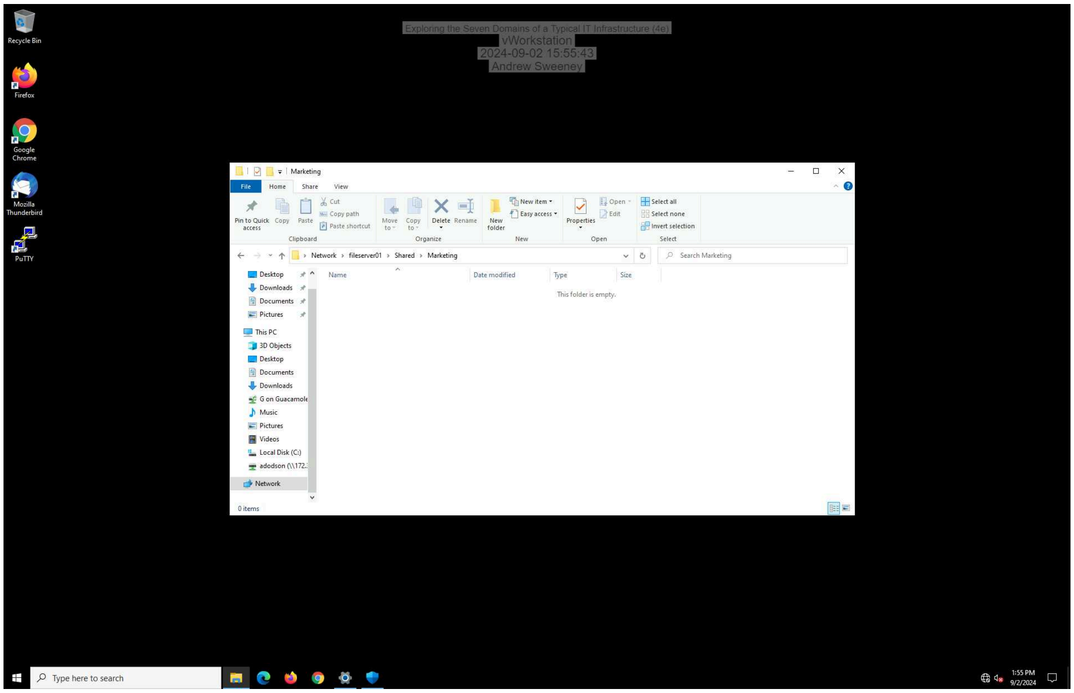
You do not have permission to access \\fileserver01\Employees\bsingleton. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

Close

4 items 1 item selected

31. **Make a screen capture** showing a **successful connection to the Marketing shared folder**.



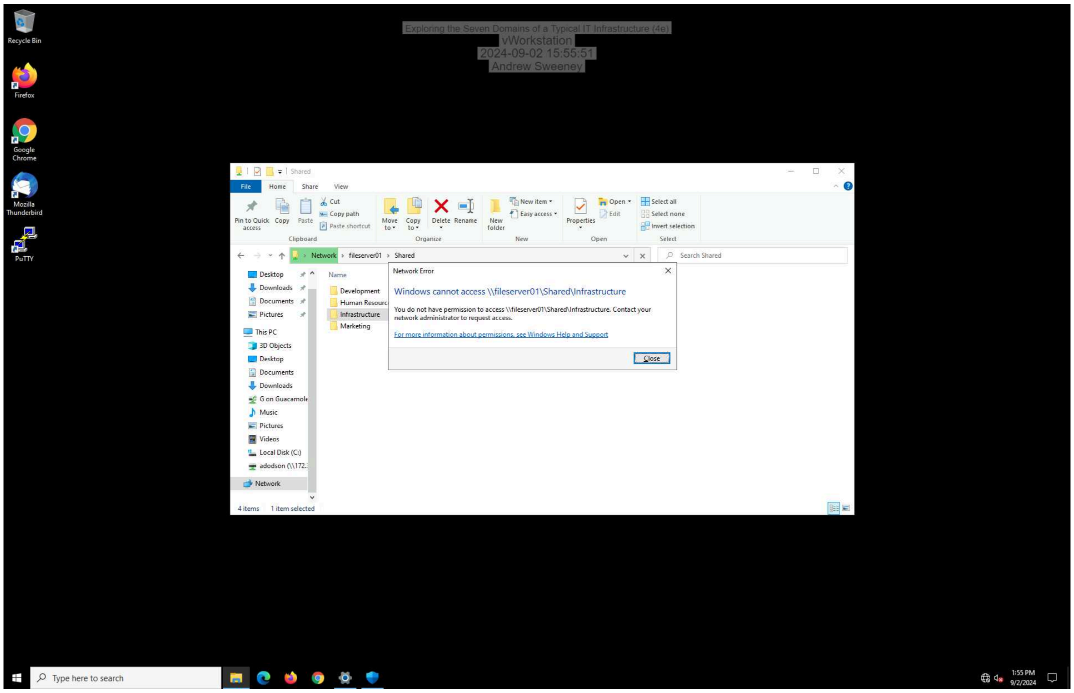
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:55:43
Andrew Sweeney

Network › fileserver01 › Shared › Marketing

This folder is empty.

0 items

32. **Make a screen capture** showing a **failed connection to another shared folder**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-02 15:55:51
Andrew Sweeney

Network › fileserver01 › Shared

Network Error

Windows cannot access \\fileserver01\Shared\Infrastructure

You do not have permission to access \\fileserver01\Shared\Infrastructure. Contact your network administrator to request access.

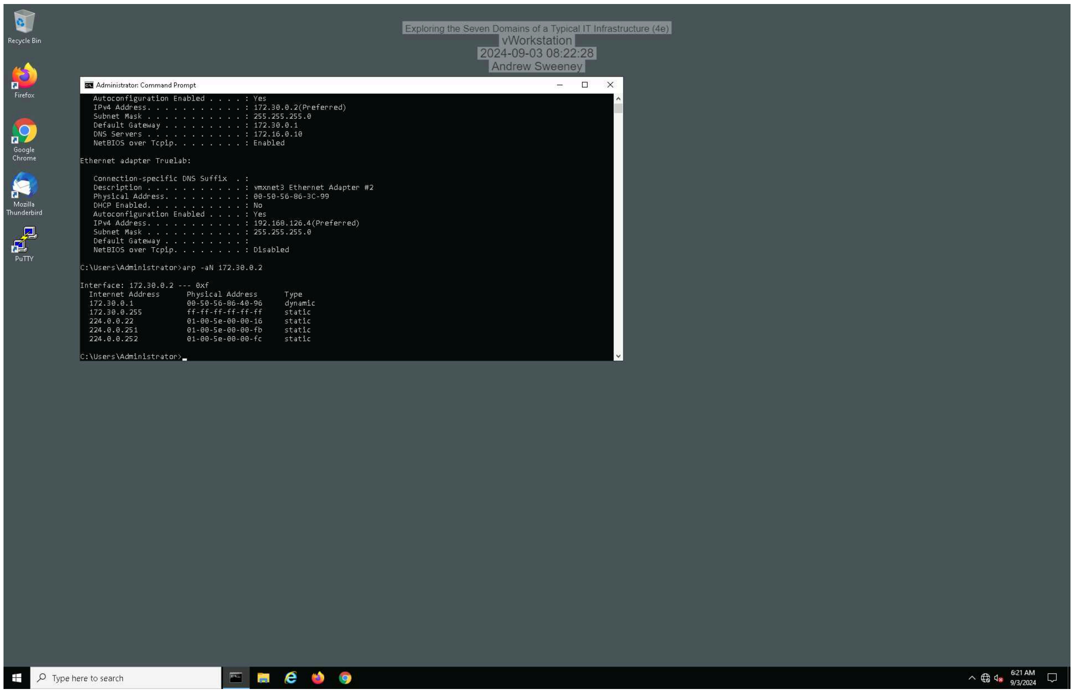
For more information about permissions, see Windows Help and Support

Close

4 items   1 item selected

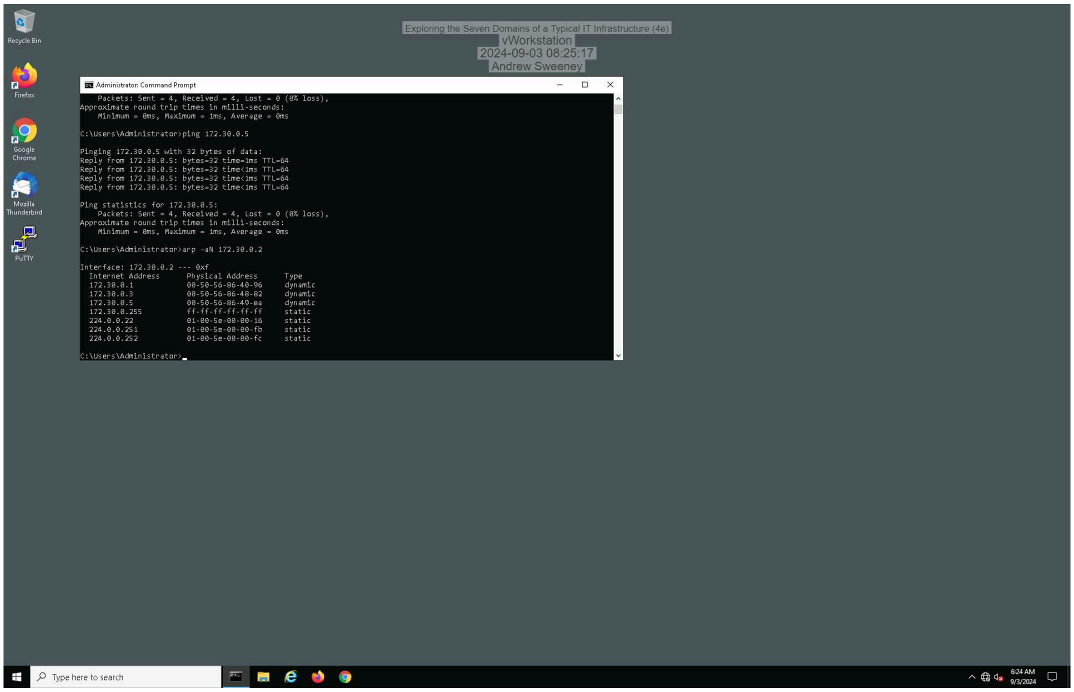
Part 2: Explore the LAN Domain

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



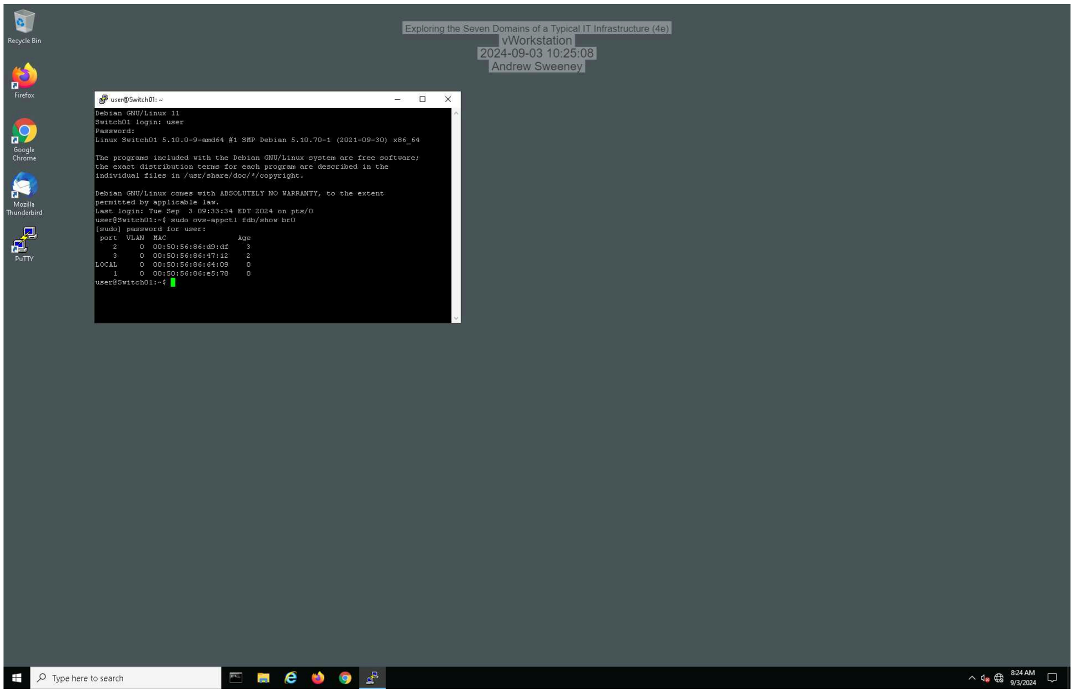
```
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.30.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.0.1
   DNS Servers . . . . . . . . . . . : 172.16.0.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Truelab:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter #2
   Physical Address. . . . . . . . . : 00-50-56-86-3C-99
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.126.4(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Disabled

C:\Users\Administrator>arp -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-86-40-96     dynamic
  172.30.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\Users\Administrator>
```

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



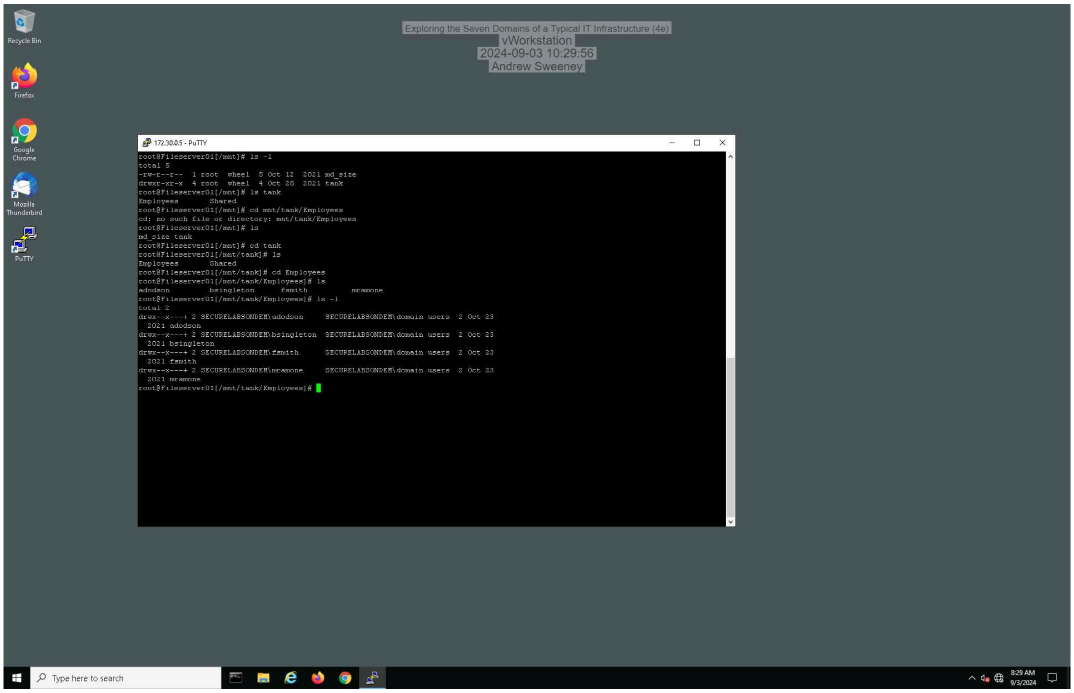
```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 172.30.0.5

Pinging 172.30.0.5 with 32 bytes of data:
Reply from 172.30.0.5: bytes=32 time=1ms TTL=64
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64
Reply from 172.30.0.5: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.0.5:
    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>arp -aN 172.30.0.2

Interface: 172.30.0.2 --- 0xf
  Internet Address      Physical Address      Type
  172.30.0.1            00-50-56-86-40-96     dynamic
  172.30.0.3            00-50-56-86-48-82     dynamic
  172.30.0.5            00-50-56-86-49-ea     dynamic
  172.30.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\Users\Administrator>
```

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



```
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: Tue Sep  3 09:33:34 EDT 2024 on pts/0
user@Switch01:~$ sudo ovs-appctl fdb/show br0
[sudo] password for user:
 port  VLAN  MAC                Age
    2     0  00:50:56:86:d9:df    3
    3     0  00:50:56:86:47:12    2
LOCAL     0  00:50:56:86:64:09    0
    1     0  00:50:56:86:e5:78    0
user@Switch01:~$ 
```

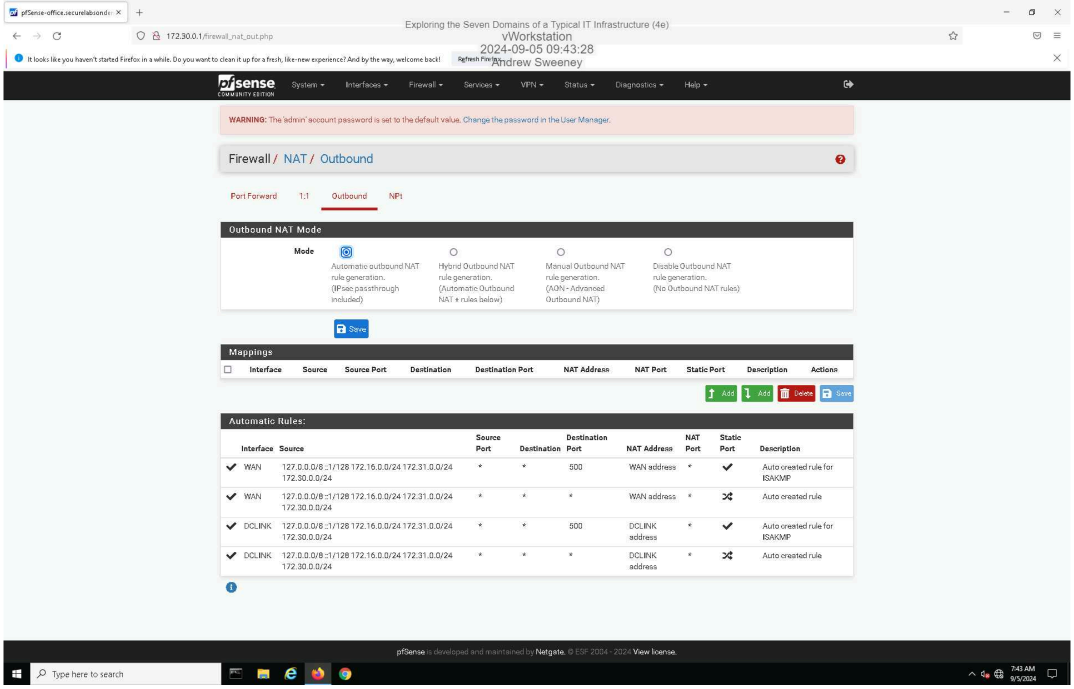
30. **Make a screen capture** showing the **contents of the Employees directory**.



```
root@Fileserver01[/mnt]# ls -l
total 5
-rw-r--r--  1 root  wheel  5 Oct 12  2021 md_size
drwxr-xr-x  4 root  wheel  4 Oct 28  2021 tank
root@Fileserver01[/mnt]# ls tank
Employees       Shared
root@Fileserver01[/mnt]# cd mnt/tank/Employees
cd: no such file or directory: mnt/tank/Employees
root@Fileserver01[/mnt]# ls
md_size tank
root@Fileserver01[/mnt]# cd tank
root@Fileserver01[/mnt/tank]# ls
Employees       Shared
root@Fileserver01[/mnt/tank]# cd Employees
root@Fileserver01[/mnt/tank/Employees]# ls
adodson         bsingleton      fsmith          mramone
root@Fileserver01[/mnt/tank/Employees]# ls -l
total 2
drwx--x---+ 2 SECURELABSONDEM\adodson     SECURELABSONDEM\domain users  2 Oct 23
  2021 adodson
drwx--x---+ 2 SECURELABSONDEM\bsingleton  SECURELABSONDEM\domain users  2 Oct 23
  2021 bsingleton
drwx--x---+ 2 SECURELABSONDEM\fsmith      SECURELABSONDEM\domain users  2 Oct 23
  2021 fsmith
drwx--x---+ 2 SECURELABSONDEM\mramone     SECURELABSONDEM\domain users  2 Oct 23
  2021 mramone
root@Fileserver01[/mnt/tank/Employees]# 
```

Part 3: Explore the LAN-to-WAN Domain

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 09:43:28
Andrew Sweeney

172.30.0.1/firewall_nat_out.php

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Outbound

Outbound NAT Mode

Mode
● Automatic outbound NAT rule generation. (IPsec passthrough included)
○ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Mappings

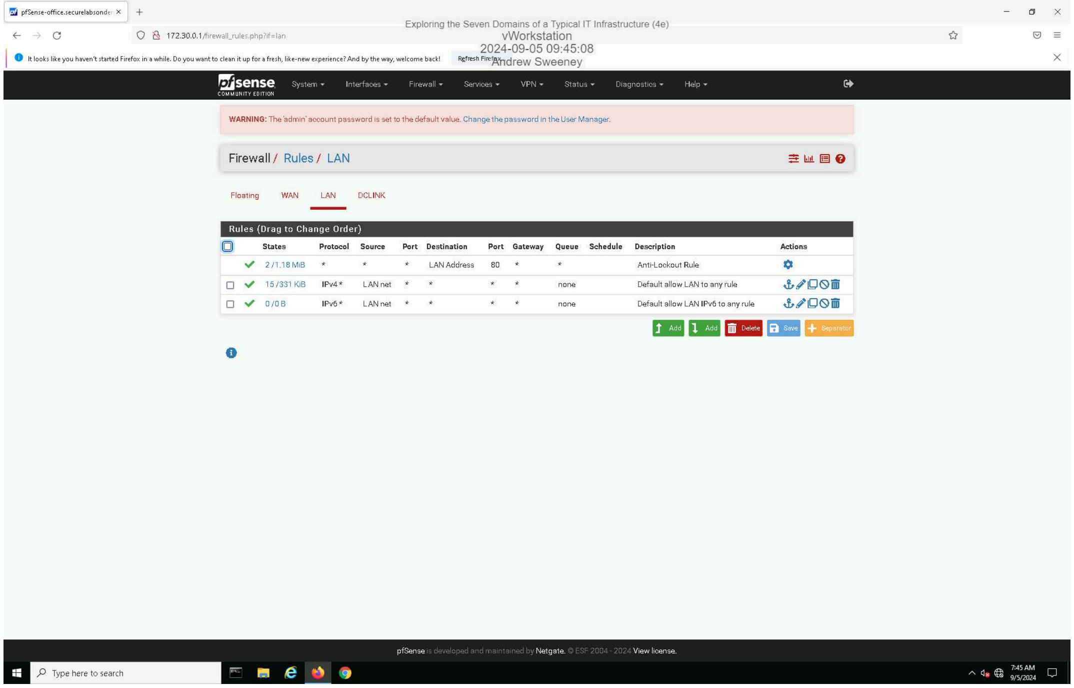
□	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	*	WAN address	*	⤮	Auto created rule
✓	DCLINK	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	500	DCLINK address	*	✓	Auto created rule for ISAKMP
✓	DCLINK	127.0.0.0/8 ::1/128 172.16.0.0/24 172.31.0.0/24 172.30.0.0/24	*	*	*	DCLINK address	*	⤮	Auto created rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 09:45:08
Andrew Sweeney

172.30.0.1/firewall_rules.php?if=lan

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

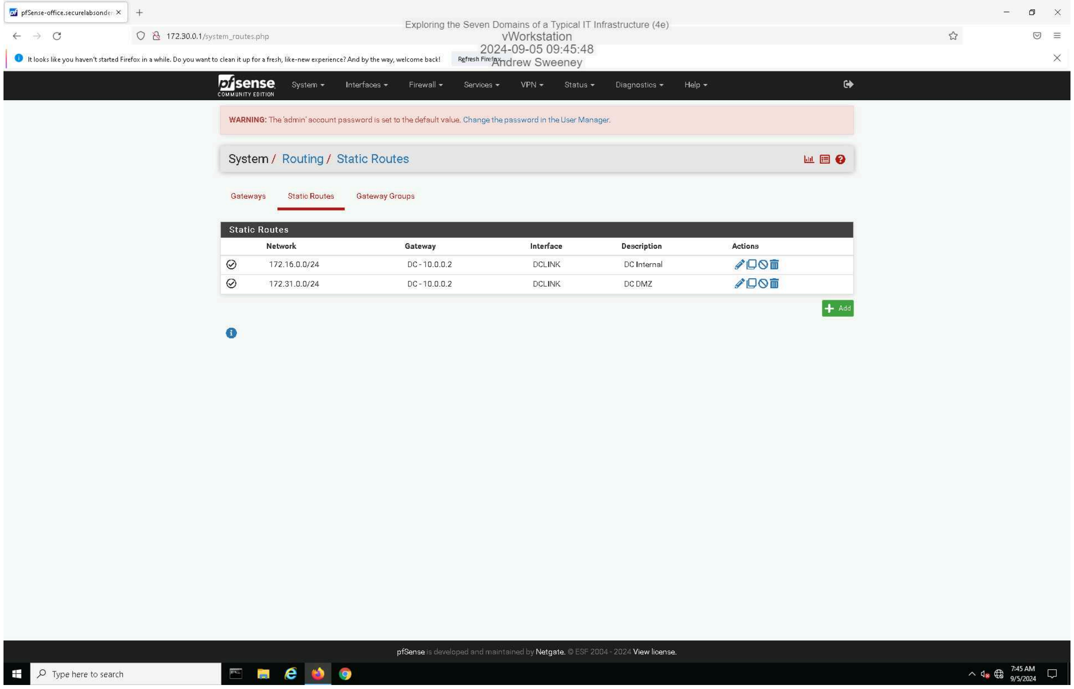
Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	2 /1.18 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✓	15 /331 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓✎❐⊘🗑
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓✎❐⊘🗑

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 09:45:48
Andrew Sweeney

172.30.0.1/system_routes.php

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

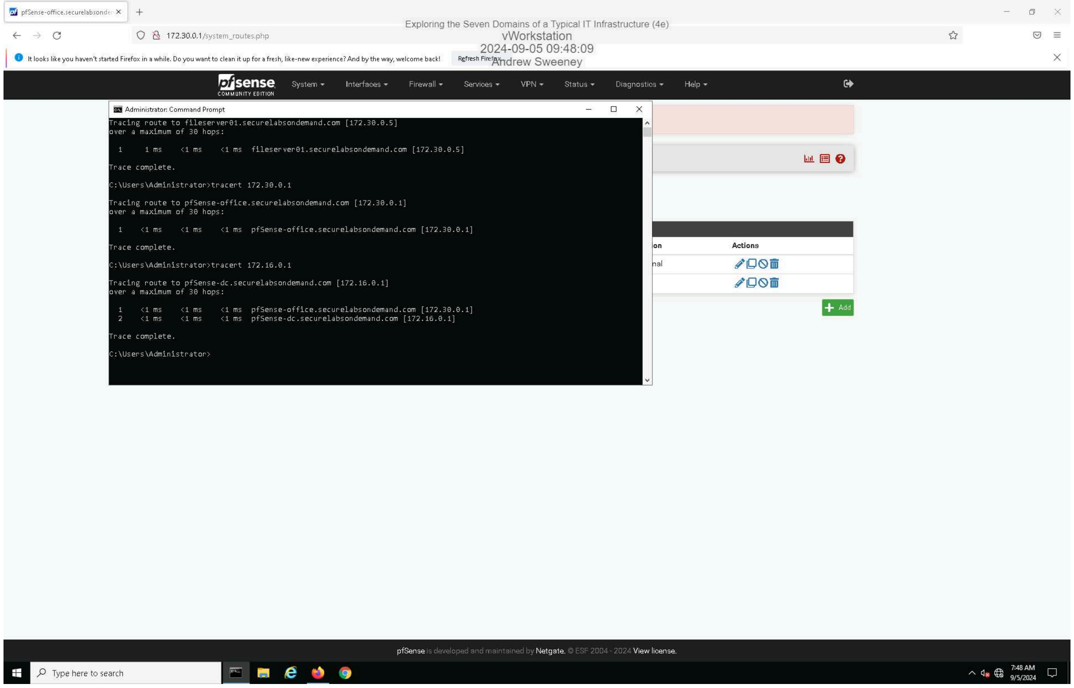
System / Routing / Static Routes

Static Routes

	Network	Gateway	Interface	Description	Actions
✓	172.16.0.0/24	DC - 10.0.0.2	DCLINK	DC Internal	
✓	172.31.0.0/24	DC - 10.0.0.2	DCLINK	DC DMZ	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 09:48:09
Andrew Sweeney

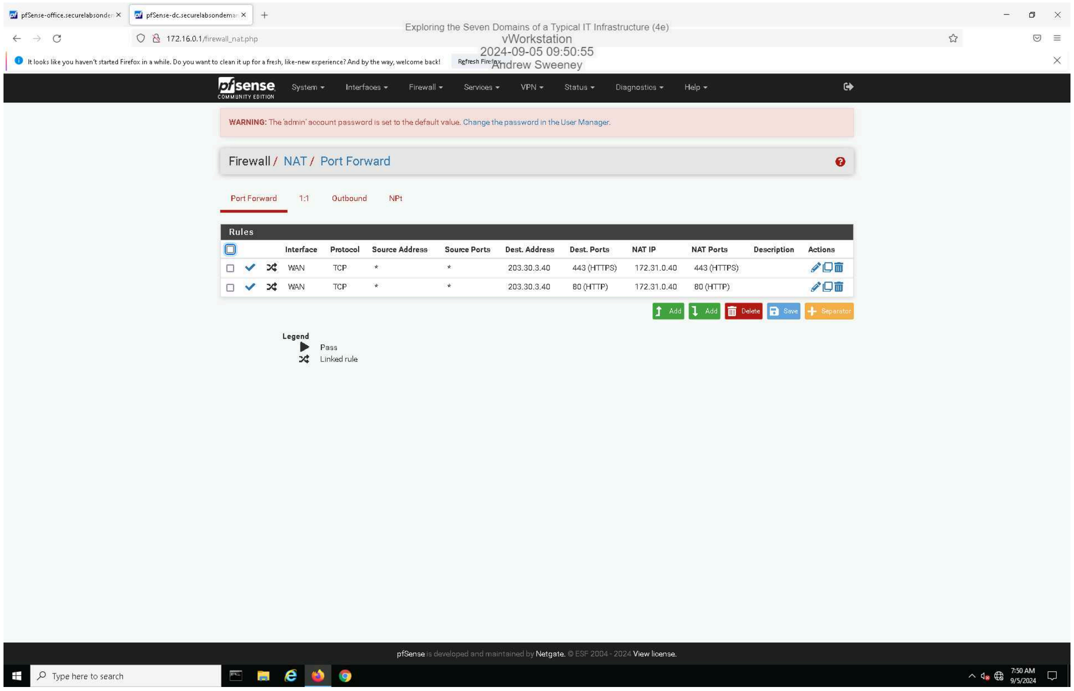
172.30.0.1/system_routes.php

Administrator: Command Prompt

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

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

Trace complete.

C:\Users\Administrator>tracert 172.30.0.1

Tracing route to pfSense-office.securelabsondemand.com [172.30.0.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  pfSense-office.securelabsondemand.com [172.30.0.1]

Trace complete.

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.

C:\Users\Administrator>
```

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



172.16.0.1/firewall_nat.php

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 09:50:55
Andrew Sweeney

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Port Forward

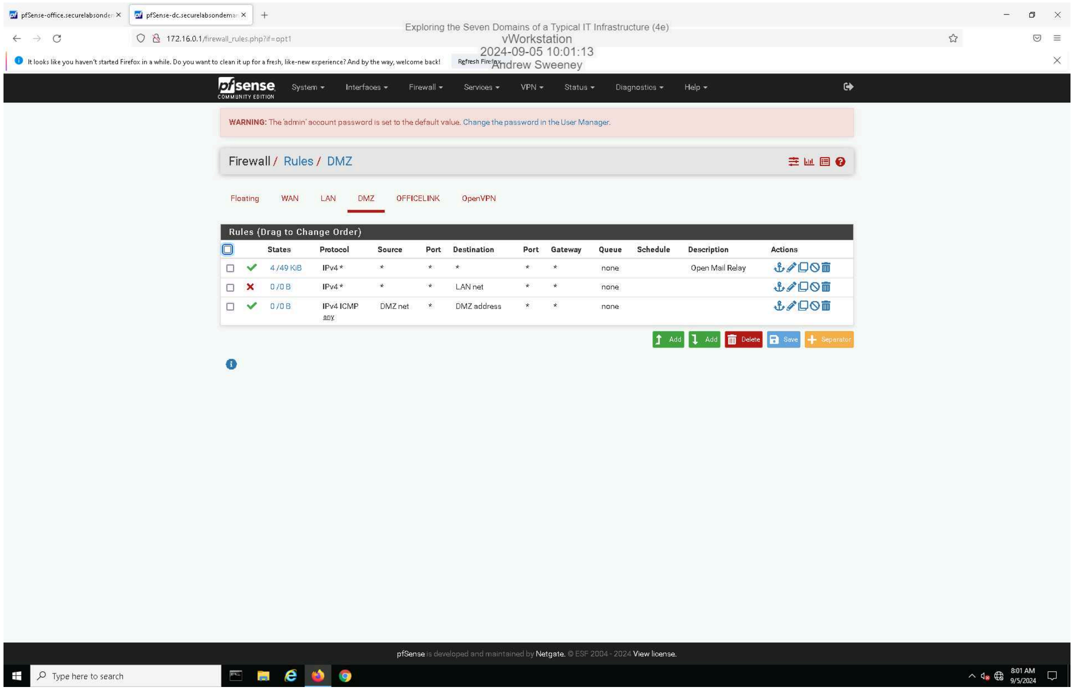
Rules

☐			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	✓	⤮	WAN	TCP	*	*	203.30.3.40	443 (HTTPS)	172.31.0.40	443 (HTTPS)		
☐	✓	⤮	WAN	TCP	*	*	203.30.3.40	80 (HTTP)	172.31.0.40	80 (HTTP)		

Legend
▶ Pass
⤮ Linked rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



172.16.0.1/firewall_rules.php?if=opt1

Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 10:01:13
Andrew Sweeney

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / DMZ

Rules (Drag to Change Order)

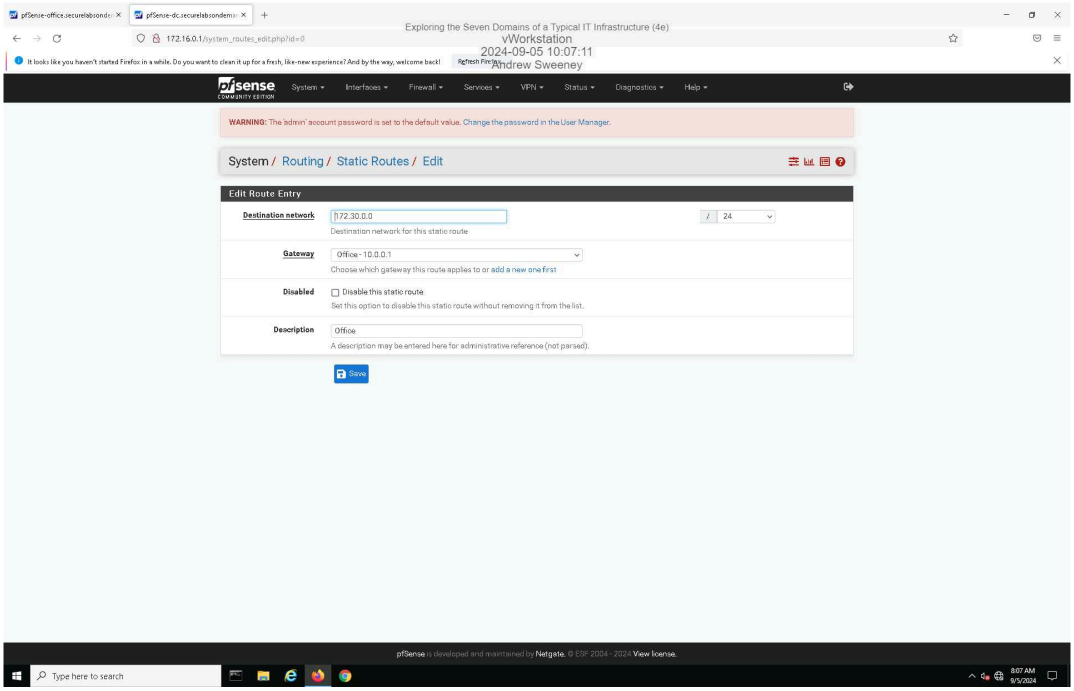
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	4 /49 KiB	IPv4 *	*	*	*	*	*	none		Open Mail Relay	
☐	✗	0 /0 B	IPv4 *	*	*	LAN net	*	*	none			
☐	✓	0 /0 B	IPv4 ICMP any	DMZ net	*	DMZ address	*	*	none			

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 10:07:11
Andrew Sweeney

172.16.0.1/system_routes_edit.php?id=0

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Routing / Static Routes / Edit

Edit Route Entry

Destination network: 172.30.0.0 / 24
Destination network for this static route

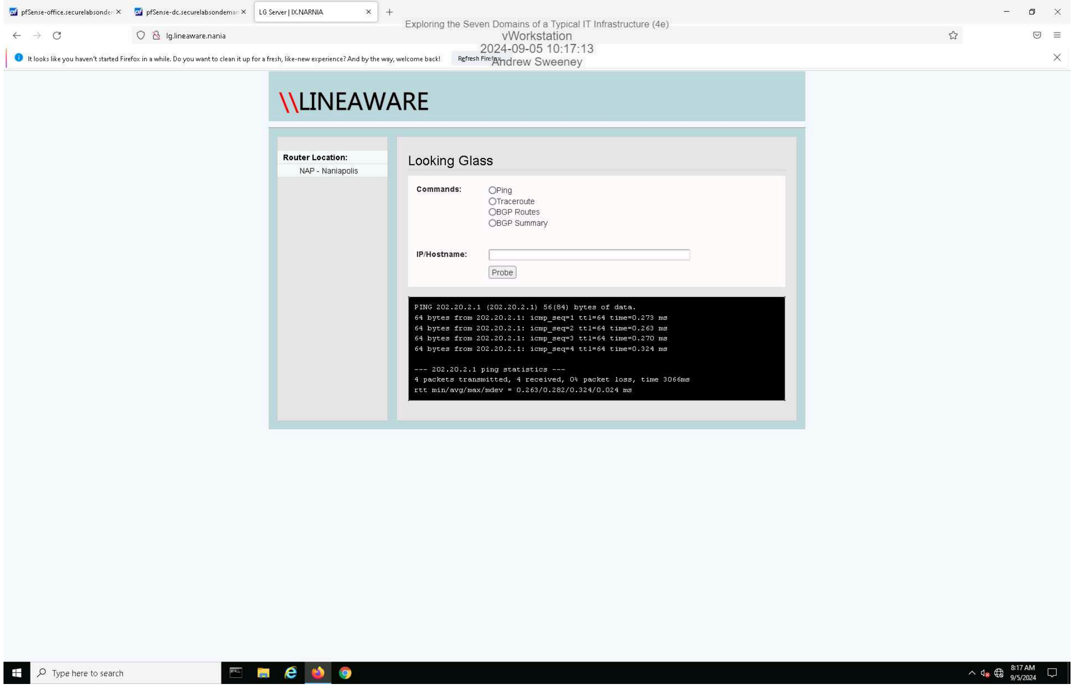
Gateway: Office - 10.0.0.1
Choose which gateway this route applies to or add a new one first

Disabled: □ Disable this static route
Set this option to disable this static route without removing it from the list.

Description: Office
A description may be entered here for administrative reference (not parsed).

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 10:17:13
Andrew Sweeney

lg.lineaware.nania

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Router Location:
NAP - Naniapolis

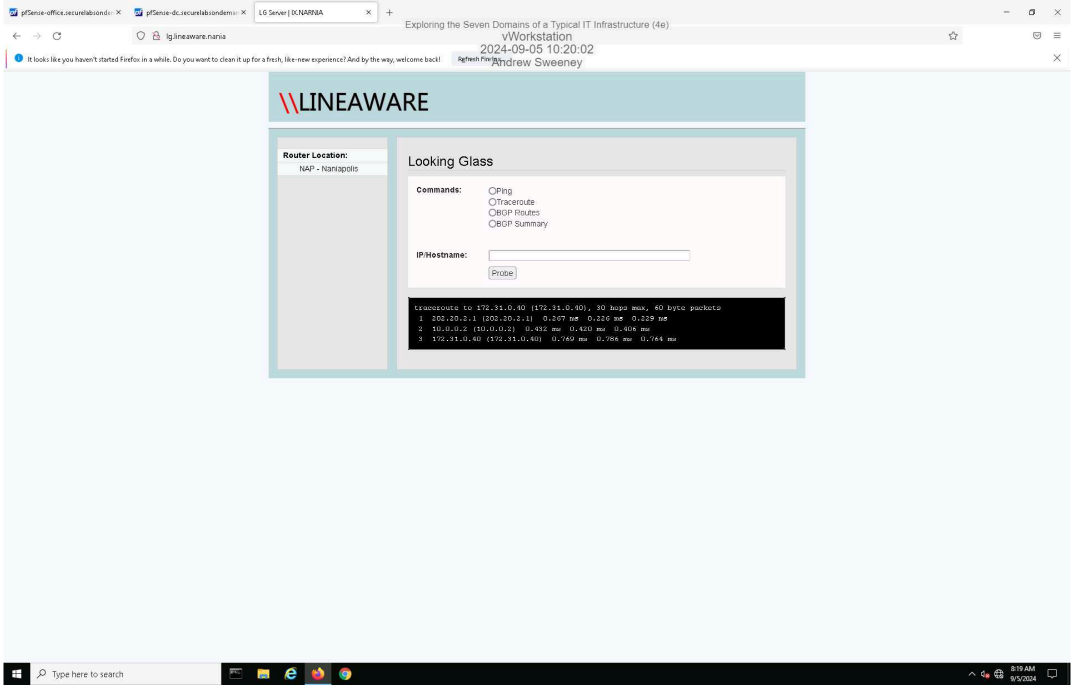
Looking Glass

Commands: ○Ping ○Traceroute ○BGP Routes ○BGP Summary

IP/Hostname:

```
PING 202.20.2.1 (202.20.2.1) 56(84) bytes of data.
64 bytes from 202.20.2.1: icmp_seq=1 ttl=64 time=0.273 ms
64 bytes from 202.20.2.1: icmp_seq=2 ttl=64 time=0.263 ms
64 bytes from 202.20.2.1: icmp_seq=3 ttl=64 time=0.270 ms
64 bytes from 202.20.2.1: icmp_seq=4 ttl=64 time=0.324 ms

--- 202.20.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.263/0.282/0.324/0.024 ms
```

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-05 10:20:02
Andrew Sweeney

lg.lineaware.nania

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

\\LINEAWARE

Router Location: NAP - Naniapolis

Looking Glass

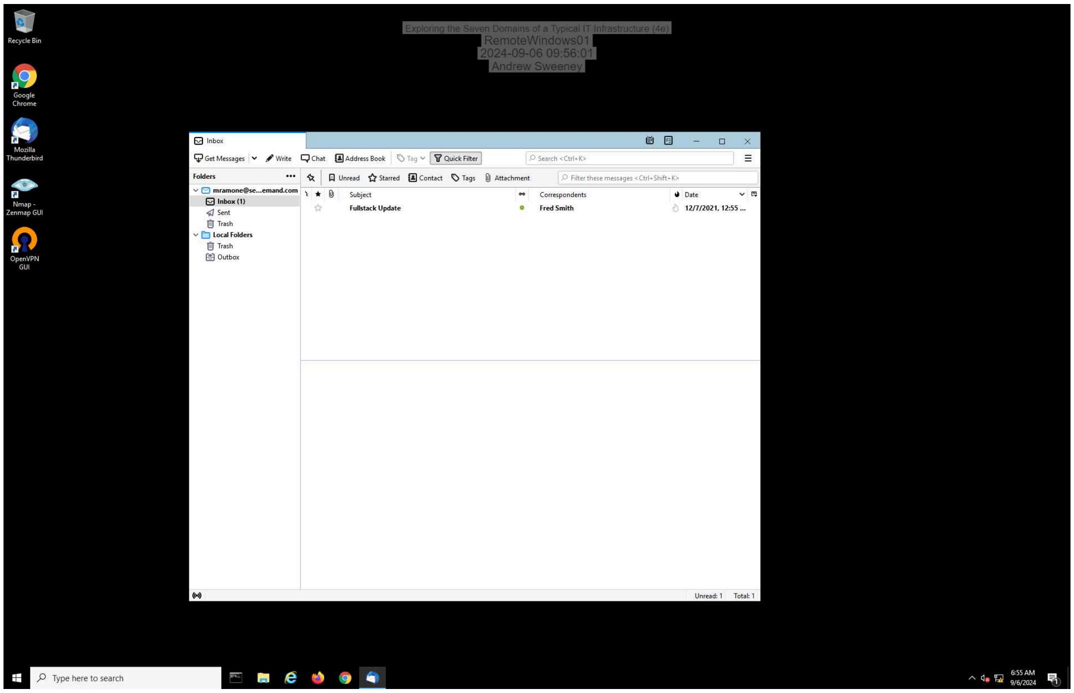
Commands: ○Ping ○Traceroute ○BGP Routes ○BGP Summary

IP/Hostname:

```
traceroute to 172.31.0.40 (172.31.0.40), 30 hops max, 60 byte packets
 1  202.20.2.1 (202.20.2.1)  0.267 ms  0.226 ms  0.229 ms
 2  10.0.0.2 (10.0.0.2)  0.432 ms  0.420 ms  0.406 ms
 3  172.31.0.40 (172.31.0.40)  0.769 ms  0.786 ms  0.764 ms
```

Part 2: Explore the Remote Access Domain

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



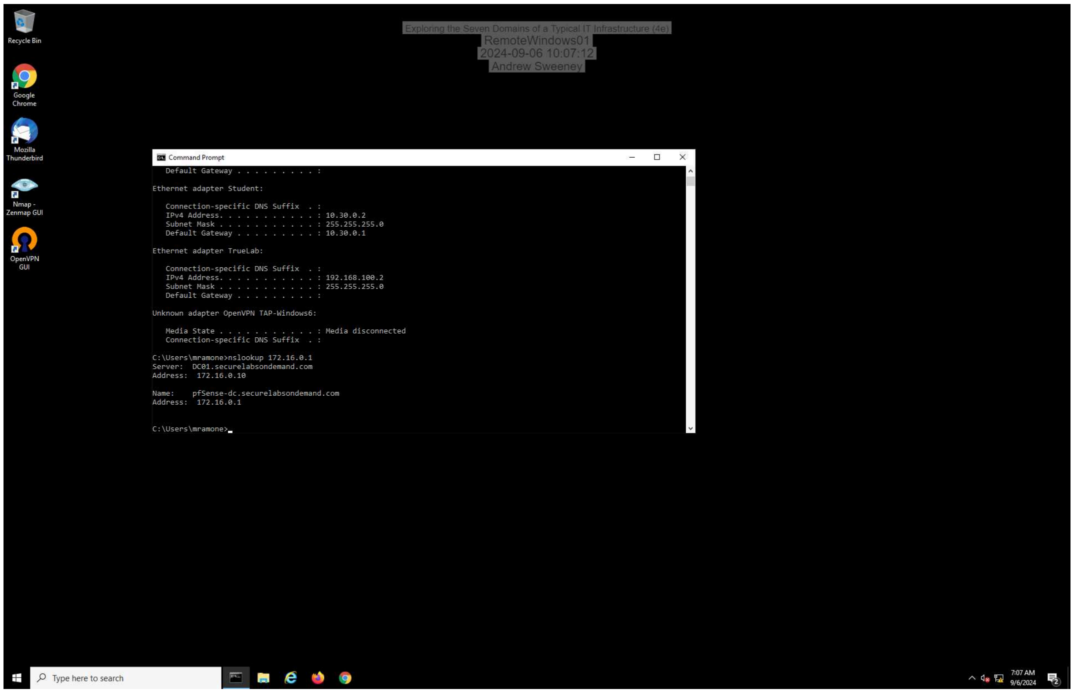
Exploring the Seven Domains of a Typical IT Infrastructure (4e)
RemoteWindows01
2024-09-06 09:56:01
Andrew Sweeney

Subject	Correspondents	Date
Fullstack Update	Fred Smith	12/7/2021, 12:55 ...

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

It is a split tunnel because our first hop was to the Default Gateway

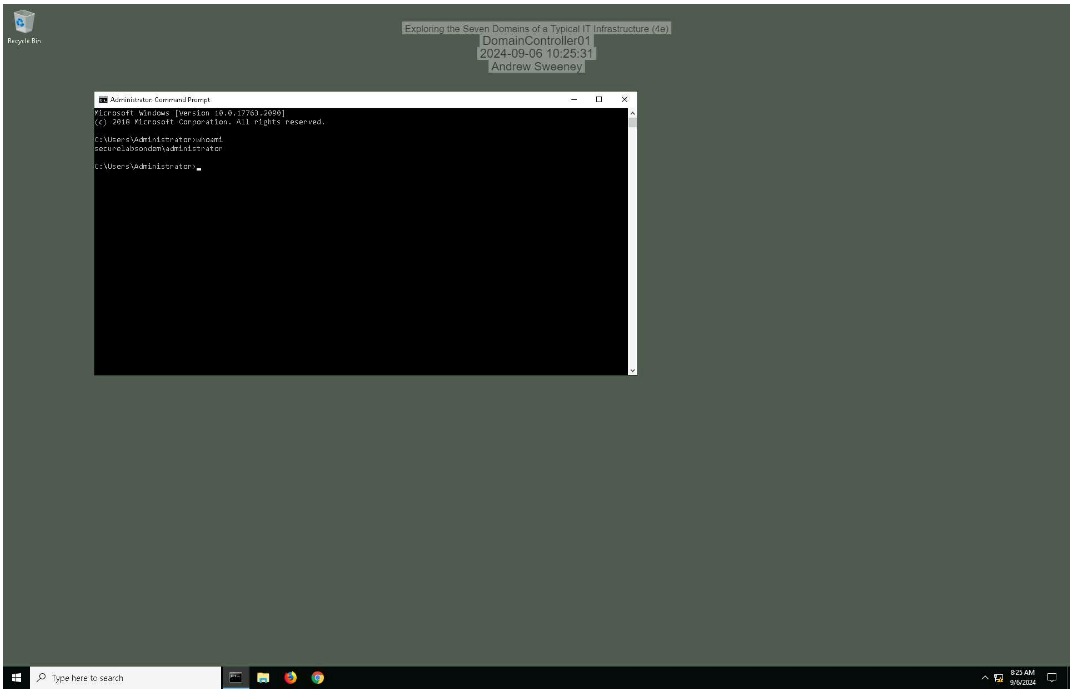
16. **Make a screen capture** showing the **successful reverse DNS lookup for the internal host**.



```
   Default Gateway . . . . . . . . . :

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.30.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.30.0.1

Ethernet adapter TrueLab:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Unknown adapter OpenVPN TAP-Windows6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

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>
```

Part 3: Explore the System/Application Domain

4. **Make a screen capture** showing the **whoami results**.

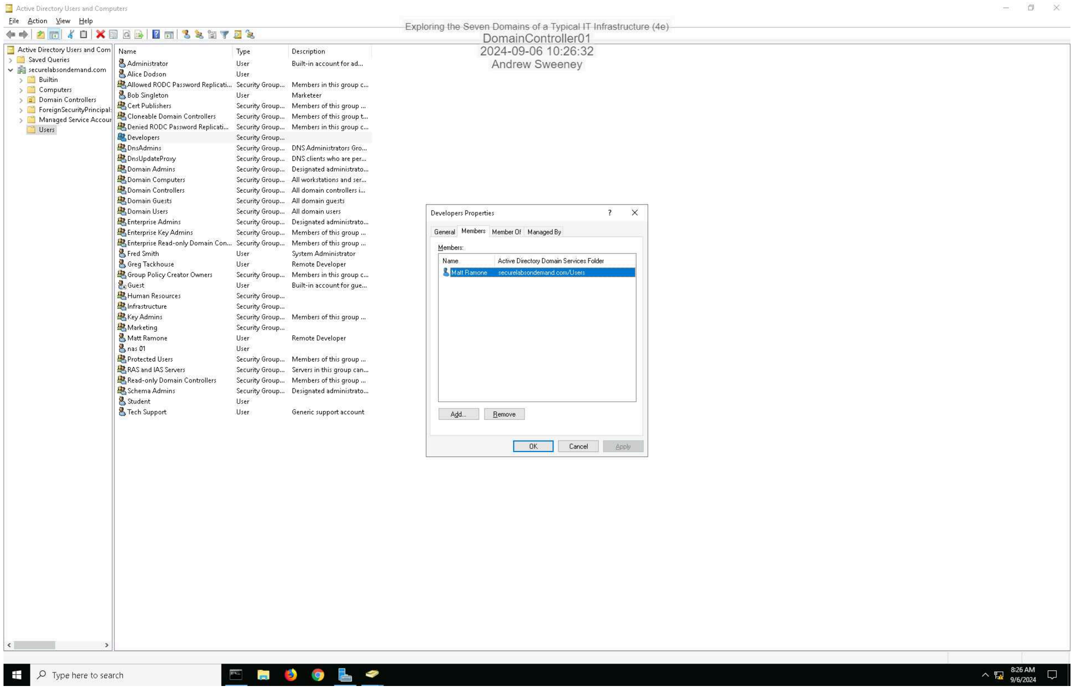


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-09-06 10:25:31
Andrew Sweeney

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.2090]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
securelabsondem\administrator

C:\Users\Administrator>_
```

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-09-06 10:26:32
Andrew Sweeney

Active Directory Users and Computers

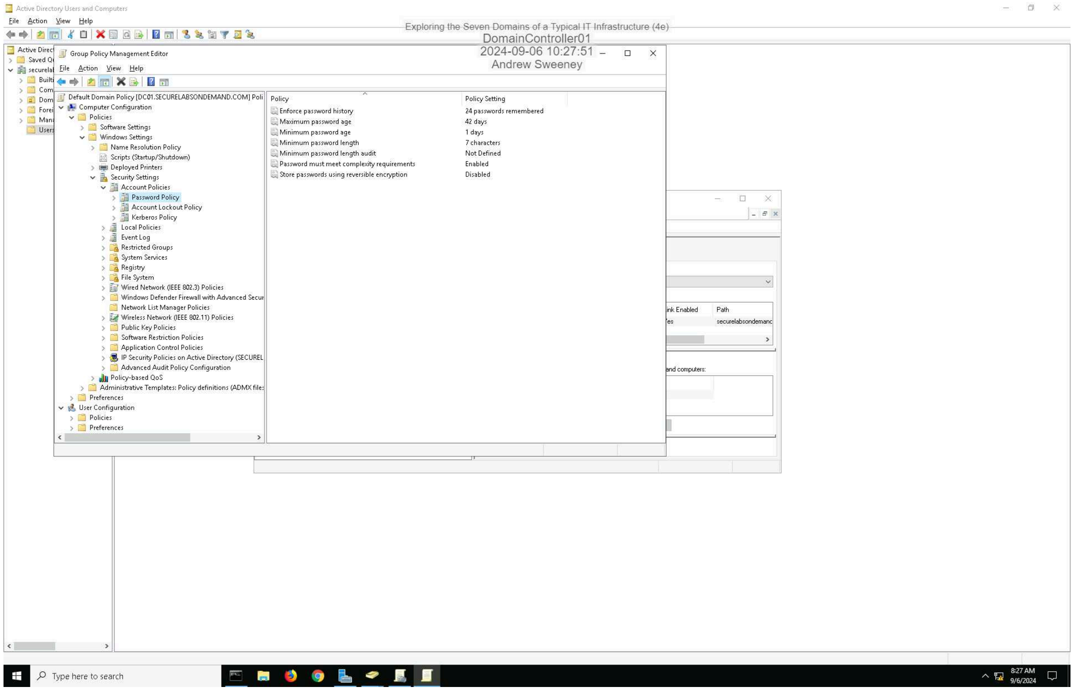
Name	Type	Description
Administrator	User	Built-in account for ad...
Alice Dodson	User	
Allowed RODC Password Replicati...	Security Group...	Members in this group c...
Bob Singleton	User	Marketeer
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replicati...	Security Group...	Members in this group c...
Developers	Security Group...	
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Con...	Security Group...	Members of this group ...
Fred Smith	User	System Administrator
Greg Tackhouse	User	Remote Developer
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Human Resources	Security Group...	
Infrastructure	Security Group...	
Key Admins	Security Group...	Members of this group ...
Marketing	Security Group...	
Matt Ramone	User	Remote Developer
nas 01	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
Student	User	
Tech Support	User	Generic support account

Developers Properties

Members:

Name	Active Directory Domain Services Folder
Matt Ramone	securelabsondemand.com/Users

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)
DomainController01
2024-09-06 10:27:51
Andrew Sweeney

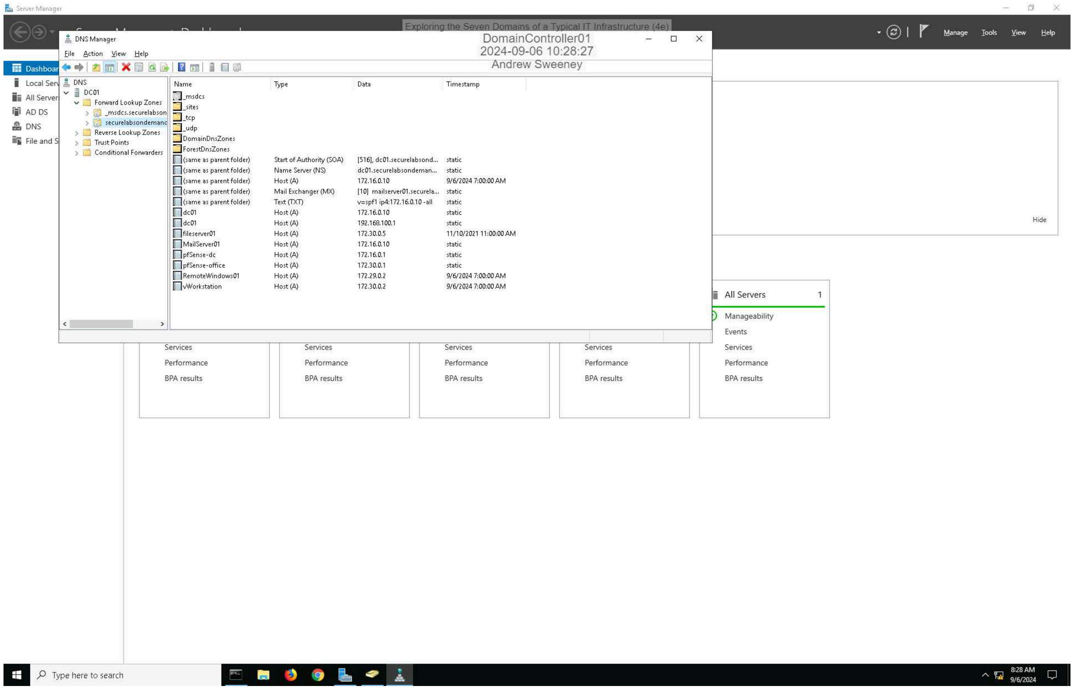
Group Policy Management Editor

Default Domain Policy [DC01.SECURELABSONDEMAND.COM] Poli

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Active Directory Users and Computers
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Secur
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECUREL
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files
Preferences
User Configuration
Policies
Preferences
Type here to search
8:27 AM
9/6/2024

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

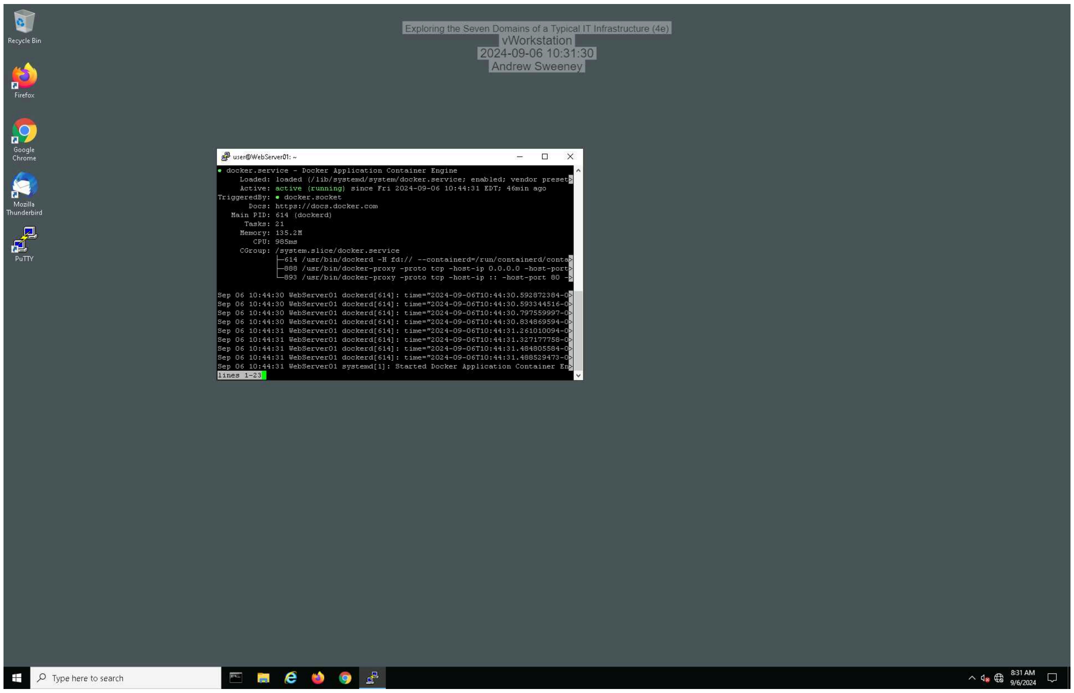


Exploring the Seven Domains of a Typical IT Infrastructure (4e)
DomainController01
2024-09-06 10:28:27
Andrew Sweeney

DNS Manager

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[516], dc01.securelabsond...	static
(same as parent folder)	Name Server (NS)	dc01.securelabsondeman...	static
(same as parent folder)	Host (A)	172.16.0.10	9/6/2024 7:00:00 AM
(same as parent folder)	Mail Exchanger (MX)	[10] mailserver01.securela...	static
(same as parent folder)	Text (TXT)	v=spf1 ip4:172.16.0.10 -all	static
dc01	Host (A)	172.16.0.10	static
dc01	Host (A)	192.168.100.1	static
fileserver01	Host (A)	172.30.0.5	11/10/2021 11:00:00 AM
MailServer01	Host (A)	172.16.0.10	static
pfSense-dc	Host (A)	172.16.0.1	static
pfSense-office	Host (A)	172.30.0.1	static
RemoteWindows01	Host (A)	172.29.0.2	9/6/2024 7:00:00 AM
vWorkstation	Host (A)	172.30.0.2	9/6/2024 7:00:00 AM

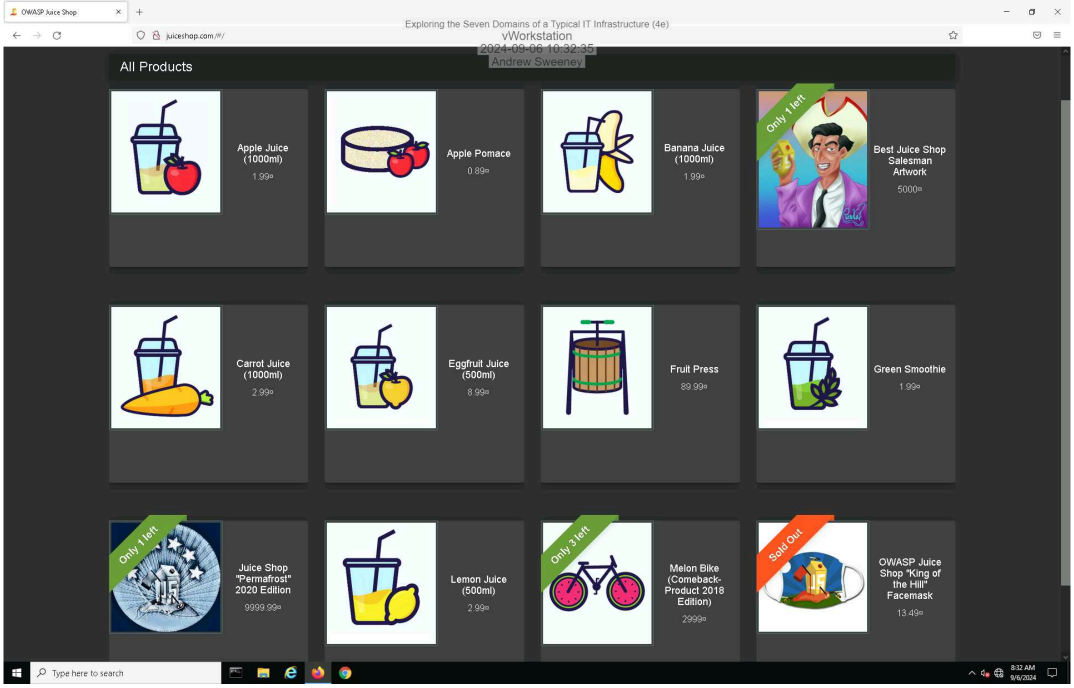
28. **Make a screen capture** showing the **Docker service status**.



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-06 10:31:30
Andrew Sweeney

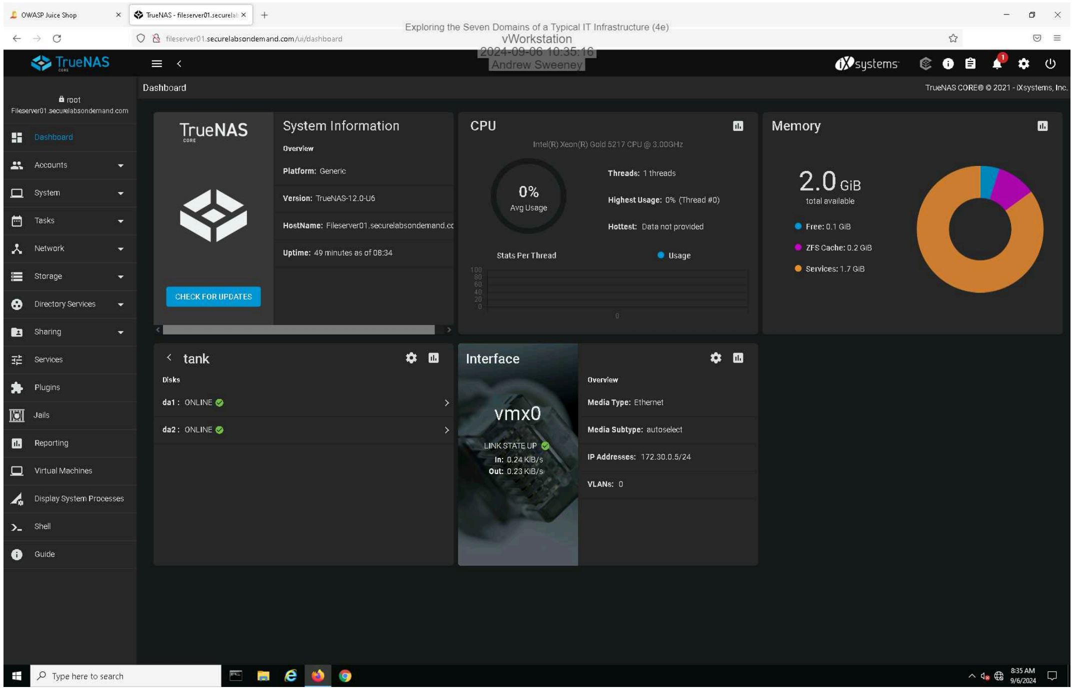
```
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset>
     Active: active (running) since Fri 2024-09-06 10:44:31 EDT; 46min ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 614 (dockerd)
      Tasks: 21
     Memory: 135.2M
        CPU: 985ms
     CGroup: /system.slice/docker.service
             ├─614 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/conta>
             ├─888 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port>
             └─893 /usr/bin/docker-proxy -proto tcp -host-ip :: -host-port 80 ->

Sep 06 10:44:30 WebServer01 dockerd[614]: time="2024-09-06T10:44:30.592872384-0>
Sep 06 10:44:30 WebServer01 dockerd[614]: time="2024-09-06T10:44:30.593344516-0>
Sep 06 10:44:30 WebServer01 dockerd[614]: time="2024-09-06T10:44:30.797559997-0>
Sep 06 10:44:30 WebServer01 dockerd[614]: time="2024-09-06T10:44:30.834869594-0>
Sep 06 10:44:31 WebServer01 dockerd[614]: time="2024-09-06T10:44:31.261010094-0>
Sep 06 10:44:31 WebServer01 dockerd[614]: time="2024-09-06T10:44:31.327177758-0>
Sep 06 10:44:31 WebServer01 dockerd[614]: time="2024-09-06T10:44:31.484805584-0>
Sep 06 10:44:31 WebServer01 dockerd[614]: time="2024-09-06T10:44:31.488529473-0>
Sep 06 10:44:31 WebServer01 systemd[1]: Started Docker Application Container En>
lines 1-23
```

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-06 10:32:35
Andrew Sweeney

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



Exploring the Seven Domains of a Typical IT Infrastructure (4e)
vWorkstation
2024-09-06 10:35:16
Andrew Sweeney

fileserver01.securelabsondemand.com/ui/dashboard

root
Fileserver01.securelabsondemand.com

TrueNAS CORE® © 2021 - iXsystems, Inc.

System Information

Overview

Platform: Generic

Version: TrueNAS-12.0-U6

HostName: Fileserver01.securelabsondemand.cc

Uptime: 49 minutes as of 08:34

CPU

Intel(R) Xeon(R) Gold 5217 CPU @ 3.00GHz

0% Avg Usage

Threads: 1 threads

Highest Usage: 0% (Thread #0)

Hottest: Data not provided

Memory

2.0 GiB total available

Free: 0.1 GiB

ZFS Cache: 0.2 GiB

Services: 1.7 GiB

tank

Disks

da1 : ONLINE ✓

da2 : ONLINE ✓

Interface

vmx0

LINK STATE UP ✓

In: 0.24 KiB/s

Out: 0.23 KiB/s

Overview

Media Type: Ethernet

Media Subtype: autoselect

IP Addresses: 172.30.0.5/24

VLANs: 0

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.

My first thought here was phishing attacks as it is one of the most popular methods used today. Like many of todays breaches this partly relies on human error whether that be clicking a malicious link or giving credentials to the wrong person. MFA is a great counter to this issue as it adds an additional wall to the simple password and username. If attacker can get the password and username often they will get stopped by the MFA.

An insider threat whether or not it be on purpose or accident is another security concern. Often those with high level access in companies have knowledge and access to sensitive information. They may send an email revealing to much and accidently cause a security breach. A good counter to this is employee awareness trainings where everyone can learn and be educated on sensitive information.

Part 2: Research Additional Security Controls

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.

Workstation: the best for workstations is an EDR solution where it monitors patterns of activity on the station and can alert us if something is different. This works great for detecting sus activity and is crucial for protection against higher level threats.

LAN: Splitting up the network or network seg is a great way to secure this. Even if one part of the network is breached they cannot move laterally to more critical areas and are stuck in the seg that they breached. This minimizes widespread damage.

LAN-to-WAN: I researched and found SWGs which was pretty cool. The solution sits between the users workstation and the internet and filters web traffic at the app level. Sounds similar to a firewall but is different SWGs can be configured at every level to block specific or alike traffic
WAN: Similar to and EDR, an IPS monitors patterns and sus network activity. It will block sus stuff and alert admins. I find often these return false pos but better safe then sorry. I wish I had one of these about 10 years ago to block incoming DDOS.

Remote Access: the best way to secure remote access is with a VPN that requires MFA. Often times a hacker can get the username and password so when paired with MFA it makes the VPN a viable option. However, I imagine within the next 5-10 years the VPN may be obsolete for newer better remote access security.

System/Application: Application whitelisting is the best security practice for this I currently know. In my home setup I have implemented this. Lets say you have a linux system that is designed to only run 1 single application you can put in rules that tell the system that it is only allowed to run that single application and blacklist all other applications this way nothing else can run except what is known to the system on the whitelist. This protects against unapproved software that someone may try to run.

My sources:
https://expertinsights.com/insights/the-top-secure-web-gateway-swg-solutions/
https://www.akamai.com/blog/security/understanding-the-differences-between-edr-and-segmentationhttps://www.ninjaone.com/it-hub/endpoint-security/what-is-application-whitelisting/