JW4158-INFO8580-22S-Portfolio-1

John White

6714158

INFO8580

Table of Contents

Lab 1 - A Basic Firewall

Description

The purpose of this lab is to teach us how to configure pfSense to provide DHCP and DNS to devices on the network. We did this by creating 2 VMs in VSphere and configuring one to be our pfSense router and the other to be a Windows Desktop.

Preparation

Create a new virtual machine in VSphere. It should have 2 network cards (network 1 and network 2). The operating system should be FreeBSD 12 and the .ISO boot file used should be pfSense 2.5.2. Boot up the VM and install pfSense.

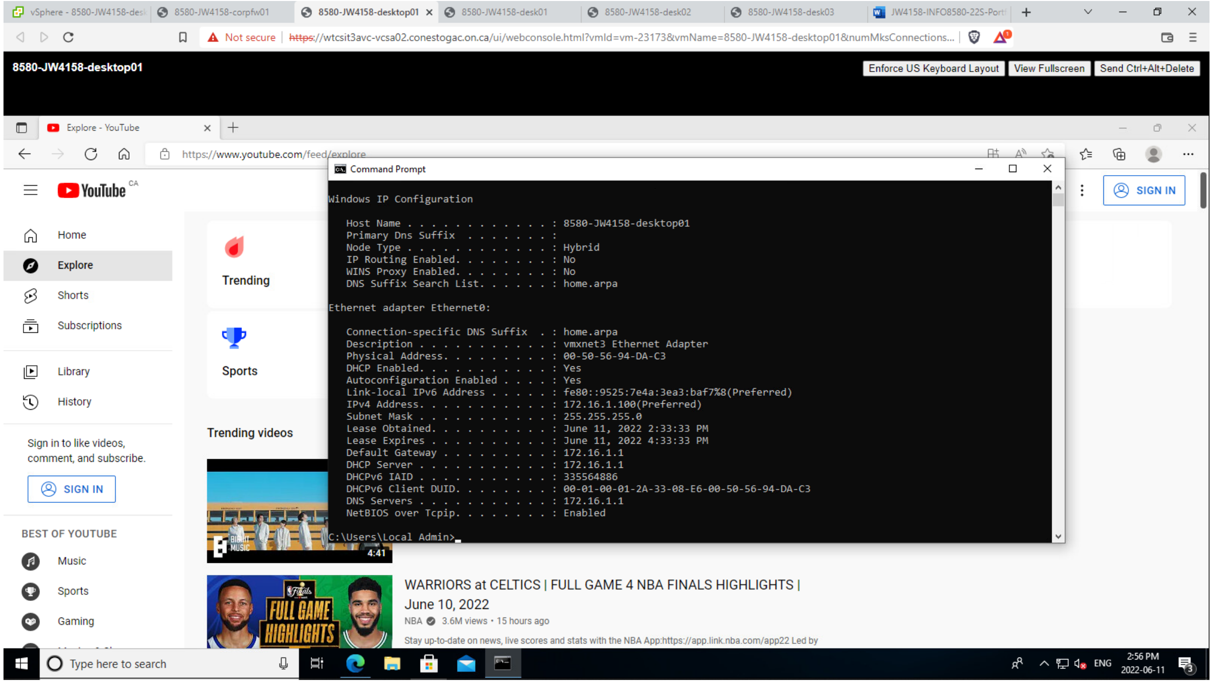
Create a 2nd virtual machine from a template and select the Windows Education edition. Customize its hardware and make sure it is using the '02' network card. Power on the new VM and we should be ready to start the lab.

Observations

On the firewall VM, configure the WAN address to be 10.175.68.254/24 and set the upstream LAN address to 10.175.68.1. Next, set the LAN address to 172.16.1.1/24. When you are asked about enabling the DHCP server, say yes. Set the client start range to 172.16.1.100 and the end address to 172.16.1.254. The rest of the firewall configuration will be done from the desktop VM.

From the desktop VM, open a web browser and navigate to 172.16.1.1. Log in with username: admin and password: pfSense. Go to System > General Setup and set 8.8.8.8 as the DNS server. Save/apply then go to Services > DNS Forwarder. Enable the DNS Forwarder, DHCP Registration, and Static DHCP. Save/apply then restart both VMS. The desktop should be able to connect to the internet now.

Screenshots



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : 8580-JW4158-desktop01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home.arpa

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : home.arpa
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-DA-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9525:7e4a:3ea3:baf7%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : June 11, 2022 2:33:33 PM
   Lease Expires . . . . . . . . . . : June 11, 2022 4:33:33 PM
   Default Gateway . . . . . . . . . : 172.16.1.1
   DHCP Server . . . . . . . . . . . : 172.16.1.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-33-08-E6-00-50-56-94-DA-C3
   DNS Servers . . . . . . . . . . . : 172.16.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Local Admin>
```

Figure 1.1 - pfsense has assigned desktop01 an IP starting with 172 using DHCP and is also providing DNS so desktop01 can connect to the internet.

Reflection

One issue that I had at the start of this lab was that I had never used DHCP before and was not familiar with using CIDR range 8. Overall, it was not much different from configuring pfSense without DHCP but there were some additional DHCP options that needed to be turned on in the DNS Forwarder settings as well a different range of private addresses. I also helped a friend troubleshoot his lab and we found that setting the preferred DHCP client start address incorrectly in the initial pfSense LAN setup can cause some issues with the clients, allowing them to connect to the firewall but not the internet, even if DNS is configured correctly.

NAT allows the computers inside of our network to connect to computers outside of our network. Our firewall uses NAT to translate our private IP addresses so that they these computers can access the public internet without having a public IP address.

I chose 10.175.68.254 as my WAN address because it is the last available address on my assigned subnet, as .255 is the broadcast address and cannot be used. For this same reason, I set my DHCP client end range to .254 as well. I set the DHCP client start range to 172.16.1.100 as I understand it to be a common practice in enterprise environments.

Lab 2 - Port Forwarding and Firewalls

Part 1

Description

The purpose of this lab is for us to demonstrate our knowledge of port forwarding. We did this by setting up a pair of computers on our domain from the last lab, then creating port forwarding rules so that outside traffic is redirected to a different domain computer depending on which port they connect to.

Preparation

To prepare for this lab, follow the instructions from the previous lab. After this, duplicate the desktop VM twice (or deploy 2 new Windows desktops). Boot up the new VMS and we are now ready to start the lab and configure our machines.

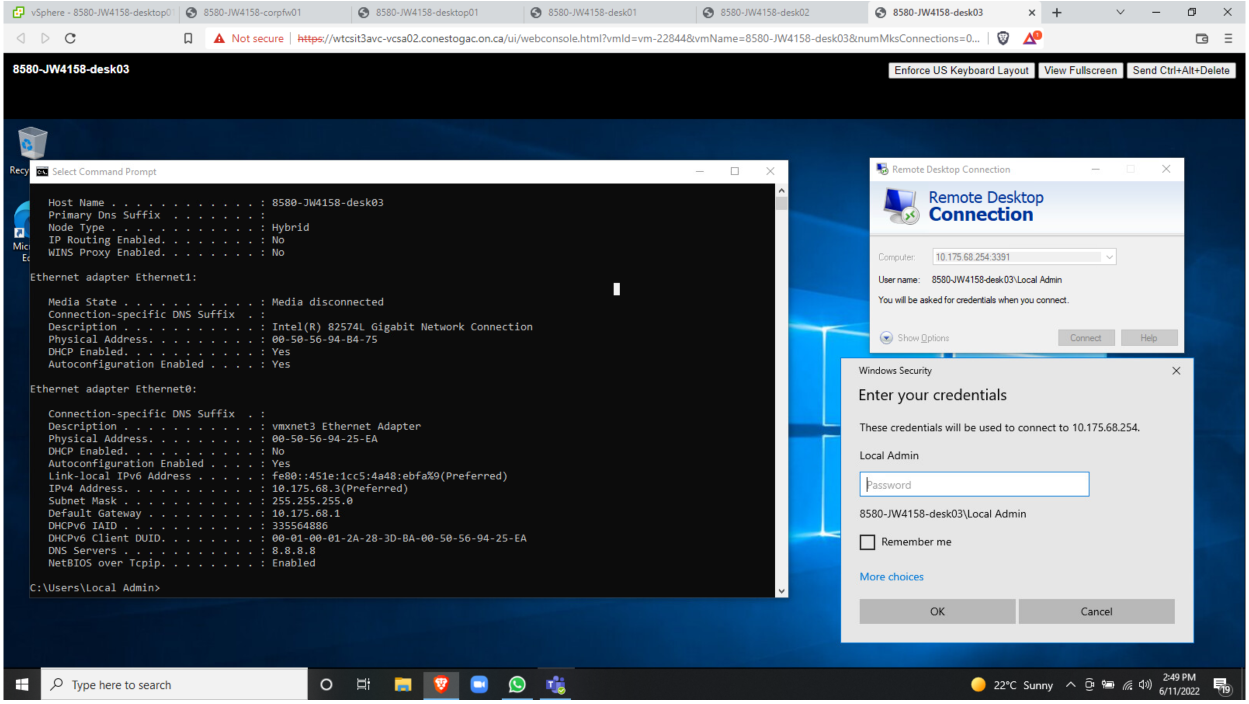
Observations

First, we'll configure the static IP addresses on our desktop VMS. On desk01, in the Windows Search bar, navigate to Network Status. The go to Adapter Settings > Ethernet0 > Properties > Internet Protocol Version 4. Set 172.16.1.11 for the IP, 255.255.255.0 for the subnet mask, 172.16.1.1 for the default gateway, and 8.8.8.8 for the DNS Server. Do the same for desk02 but set the IP to 172.16.1.12. We are now ready to configure our pfSense router to allow port forwarding.

Connect to pfSense via web browser on one of the desktop VMS. Go to Interfaces > WAN and make sure "Block private networks and loopback addresses" is unchecked. Next go to Firewall > NAT and add a new port forward rule. Set the Interface to WAN, the Address Family to IPv4, and the Protocol to TCP. The Destination IP should be set to WAN address and the Destination port should be 3391. The redirect target will be 172.16.1.11 and the port will be 3389 (MS RDP). Save the port forward rule. For the other rule, use the same settings except change the destination port to 3392 and the redirect IP to 172.16.1.12.

Since my home computer uses Windows 10 Home Edition and cannot use Remote Desktop Connection, I configured a third Windows VM that has it's IP statically configured as shown in Figure 2.1.

Screenshots



```
   Host Name . . . . . . . . . . . . : 8580-JW4158-desk03
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-94-B4-75
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-25-EA
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::451e:1cc5:4a48:ebfa%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.175.68.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.175.68.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-28-3D-BA-00-50-56-94-25-EA
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Local Admin>
```

Remote Desktop Connection

Computer: 10.175.68.254:3391

User name: 8580-JW4158-desk03\Local Admin

You will be asked for credentials when you connect.

Windows Security

Enter your credentials

These credentials will be used to connect to 10.175.68.254.

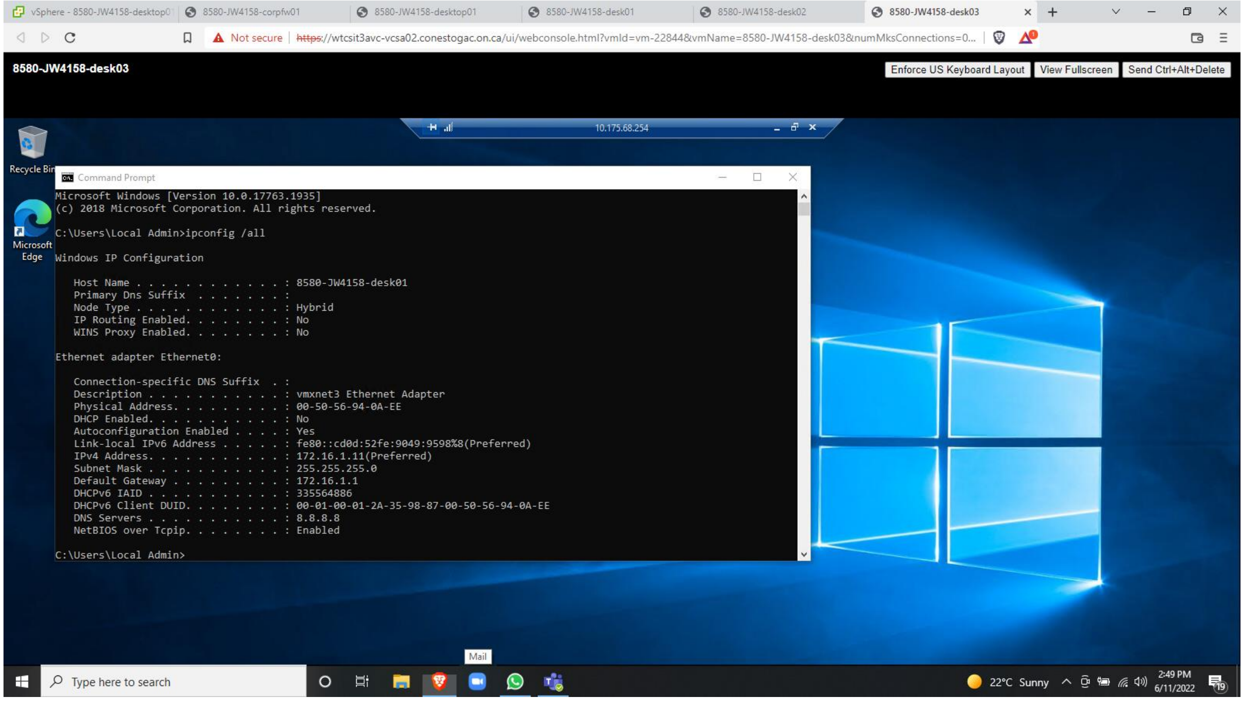
Local Admin

Password

8580-JW4158-desk03\Local Admin

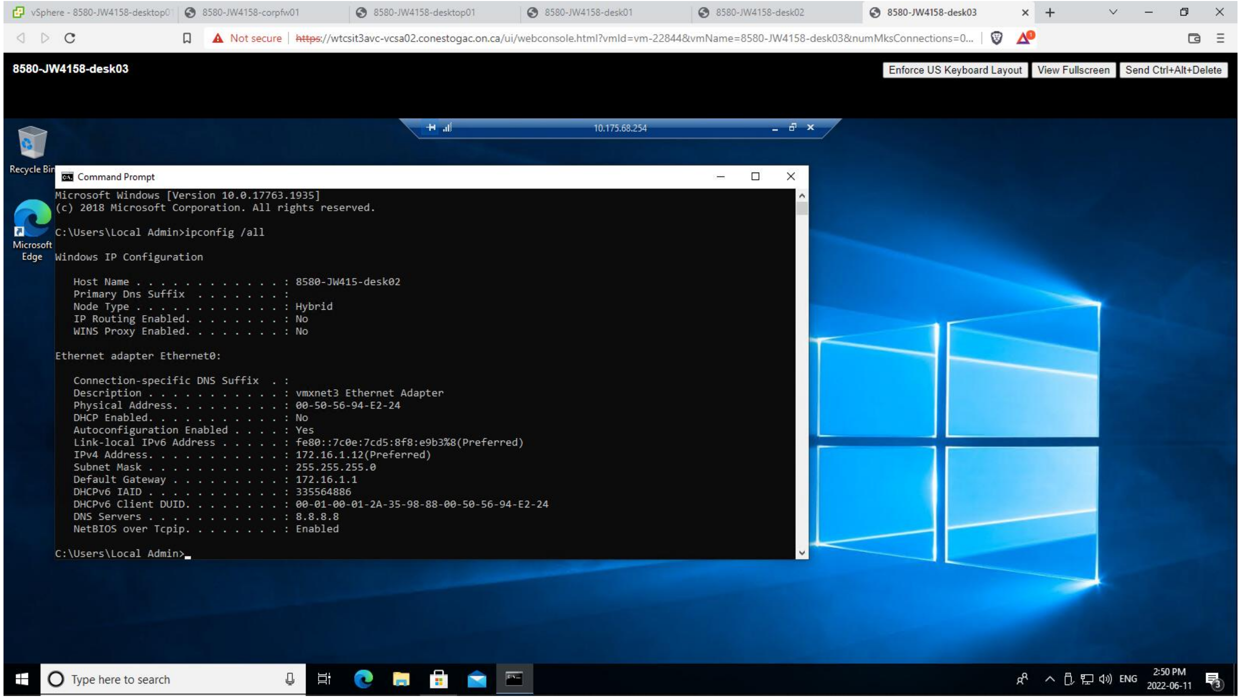
□ Remember me

Figure 2.1 - A third desktop is configured in front of the firewall to test the port forward rules.



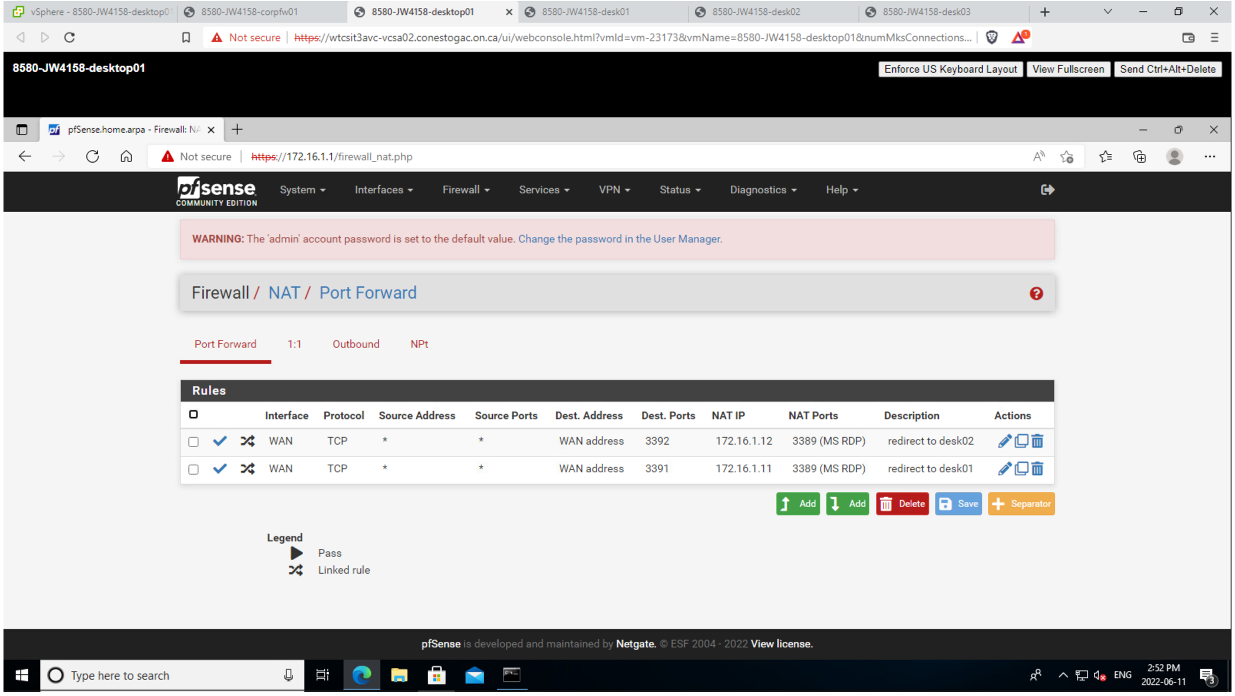
```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Local Admin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 8580-JW4158-desk01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-0A-EE
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cd0d:52fe:9049:9598%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-35-98-87-00-50-56-94-0A-EE
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Local Admin>
```

Figure 2.2 - Connecting to 10.175.68.254:3391 redirects the traffic to 172.10.68.11



```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Local Admin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 8580-JW415-desk02
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-E2-24
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::7c0e:7cd5:8f8:e9b3%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.1.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-35-98-88-00-50-56-94-E2-24
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Local Admin>
```

Figure 2.3 - Connecting to 10.175.68.254:3392 redirects the traffic to 172.10.68.12



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

Firewall / NAT / Port Forward

Port Forward | 1:1 | Outbound | NPt

Rules

□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	WAN address	3392	172.16.1.12	3389 (MS RDP)	redirect to desk02	
□	✓	⤮	WAN	TCP	*	*	WAN address	3391	172.16.1.11	3389 (MS RDP)	redirect to desk01	

Legend
▶ Pass
⤮ Linked rule

pfSense is developed and maintained by Netgate. © ESF 2004 - 2022 View license.

Figure 2.4 - The 2 port forward rules that we have specified.

Reflection

Overall, setting up the port forward rules wasn't too complicated and mostly worked as expected. The thing that really held me up was that I had "Block private networks and loopback addresses" checked. This would block my RDP connections from reaching the target computers and it took well over an hour for me to figure out that was the problem. I chose 172.16.1.11 and 172.16.1.12 as my IP addresses so that I could easily remember which desktops had which ip (11 for 01, 12 for 02).

In order to keep the computers on our network safe, we generally refrain from giving them a public address. Instead, we give them a private address on our router's network and give the router a public address. Then, network traffic that comes through the router can easily be filtered via firewall. However, this gives no way for computers outside of our network to refer directly to desk01 or desk02. To get around this, the router uses port forwarding rules to redirect outside traffic depending on which port is connected to.

The benefit of our current setup is that it is very easy to create and use as we don't need to change the default configuration much and our computers will allow connections from anywhere. However, this is not very secure, and it may be better to specify which sources we want to allow network traffic from. This can be done in the port forwarding rules if we want to restrict traffic from outside the network, or on host-based firewalls if we are concerned with local traffic.

Lab 3 - Fundamental Windows Security

Part 1

Description

The purpose of this lab is to teach us the basic Windows security tools that are given to us right out of the box. By becoming familiar with these tools, we can make our PCs much safer without investing much time or spending any money.

Preparation

To prepare for this lab, the instructions for the previous 2 labs should be followed. For our desktop deliverable, we will be reusing desktop01 as well as corpfw01 for our router. We will be using desk01 and desk02 as well but only to test our ability to ping desktop01 later. The exact IP and DNS configuration for desktop01 is shown in Figure 1.1 from Lab 1.

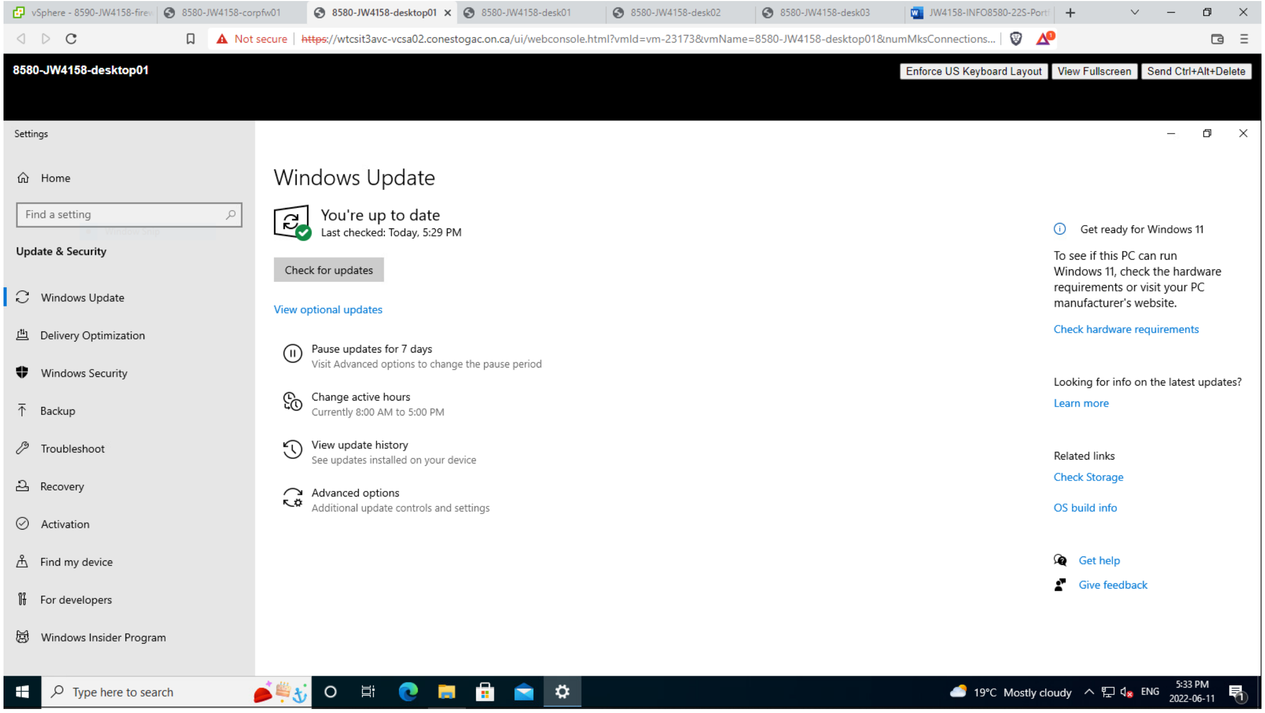
Observations

First, we will make sure all Windows updates are installed. Type “update” in the Windows search bar to find the appropriate update screen. Keeping checking for/installing all new updates and restarting the computer as needed. This could take up to an hour.

Next, go to Windows Security > Virus & threat protection, then update the virus and malware signatures. Once these are up to date, scan desktop01 for any threats. After this, go down to ransomware protection and turn on Protected folders. The protected folders will include all Windows default folders. I have also included a custom folder called Code.

To allow desktop01 to be pinged by other computers on the network, navigate to Windows Defender Firewall. Under inbound rules, find the rule that is named “File and Printer Sharing (Echo Request – ICMP4-In)” and is under the “Domain” profile. Enable this rule and other computers on the network should be able to ping desktop01.

Screenshots



Windows Update

You're up to date
Last checked: Today, 5:29 PM

Check for updates

View optional updates

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Get ready for Windows 11

To see if this PC can run Windows 11, check the hardware requirements or visit your PC manufacturer's website.

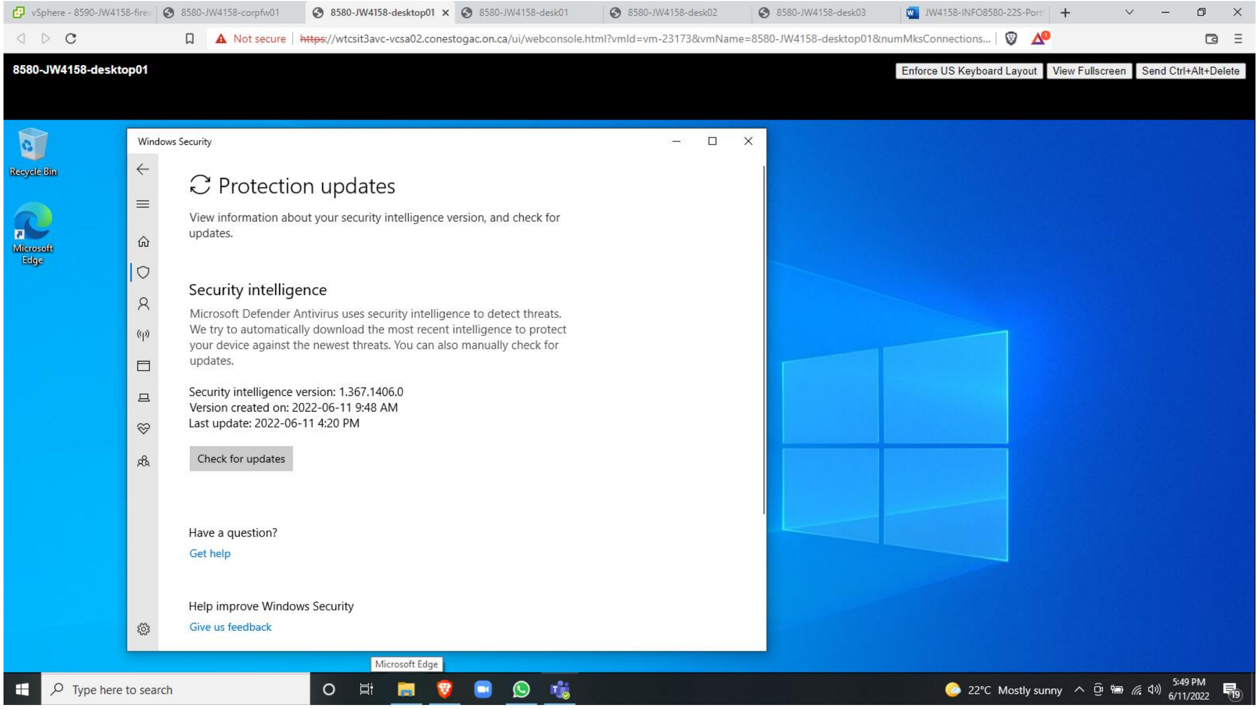
Check hardware requirements

Looking for info on the latest updates?
Learn more

Related links
Check Storage
OS build info

Get help
Give feedback

Figure 3.1 - All Windows updates have been applied to desktop01.



Protection updates

View information about your security intelligence version, and check for updates.

Security intelligence

Microsoft Defender Antivirus uses security intelligence to detect threats. We try to automatically download the most recent intelligence to protect your device against the newest threats. You can also manually check for updates.

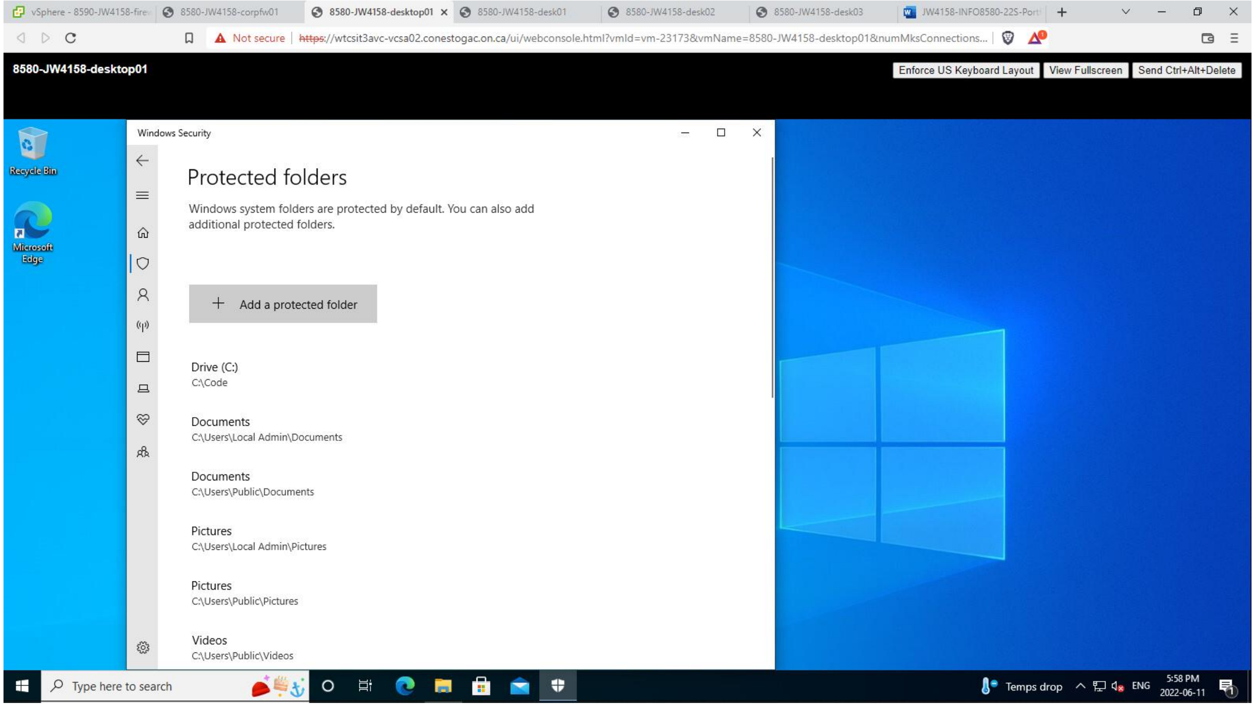
Security intelligence version: 1.367.1406.0
Version created on: 2022-06-11 9:48 AM
Last update: 2022-06-11 4:20 PM

Check for updates

Have a question?
Get help

Help improve Windows Security
Give us feedback

Figure 3.2 - Virus and Malware signatures have been updated on desktop01.



Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

+ Add a protected folder

Drive (C:)
C:\Code

Documents
C:\Users\Local Admin\Documents

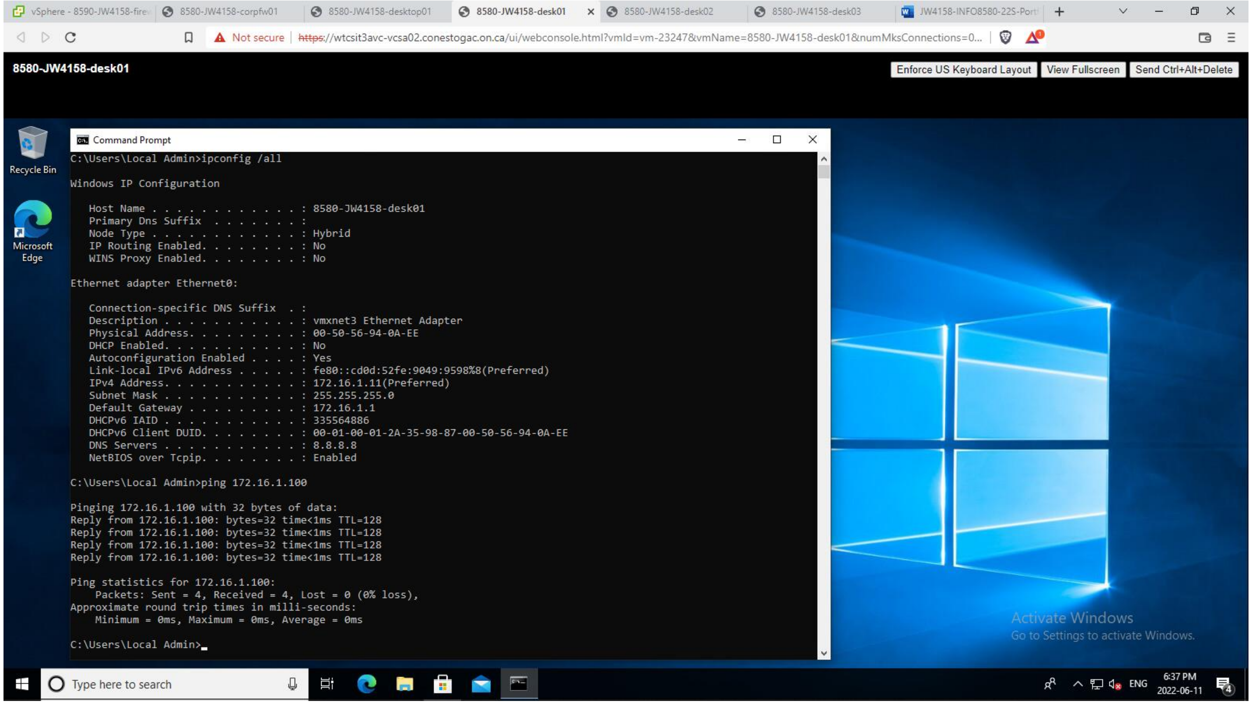
Documents
C:\Users\Public\Documents

Pictures
C:\Users\Local Admin\Pictures

Pictures
C:\Users\Public\Pictures

Videos
C:\Users\Public\Videos

Figure 3.3 - Protected folders have been turned on and a new folder has been added.



```
C:\Users\Local Admin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 8580-JW4158-desk01
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-0A-EE
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cd0d:52fe:9049:9598%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-35-98-87-00-50-56-94-0A-EE
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Local Admin>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time<1ms TTL=128
Reply from 172.16.1.100: bytes=32 time<1ms TTL=128
Reply from 172.16.1.100: bytes=32 time<1ms TTL=128
Reply from 172.16.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Local Admin>_
```

Figure 3.4 - desk01 is able to ping desktop01 after the firewall rule was enabled.

Reflection

This lab was the easiest of the 3. Most of the time required was just waiting for updates to download/install. The Protected folders feature seems like a very useful and easy-to-use tool that can help you keep your information safe on a default Windows machine. Though using it on one's home computer might make the data difficult to recover in the event of a hard disk failure. This should be kept in mind if backup drives are not kept. Keeping backups of your data is also another way to limit damage done by ransomware or file-encrypting viruses. Keeping backups may not keep your private info safe, but it will allow you to effectively restore your hard drive to a previous point in time. This can be done via physical backup or by using OneDrive as is recommended in Windows Ransomware Protection.

References

VSphere - https://wtcsit3avc-vcsa02.conestogac.on.ca/