School of Cybersecurity

Your Major: Cybersecurity

Your Name: John Peck

Your ID: 01195489

Topic: VPN

Class: WINDOWS SYSTEM MANAGEMENT AND SECURITY

Instructor: Dr. Khan

TOPIC: VPNs

VPN stands for “Virtual Private Network”. A VPN is essentially a private network that carries controlled information. This information is protected by many security tools. VPNs are private virtually, and because the data actually can travel over shared public networks instead of private connections exclusively. The benefit of VPNs is the potential for saving a significant amount of money compared to leasing lines or dial-up networking. These savings can lend a risk to the user when using the public internet as a tool for VPN data. The performance of a VPN line is more unpredictable and slower than a dedicated line due to the traffic of the internet. VPNs may save money in different ways. Companies that lease lines typically pay a very high monthly expense. A problem to solve this is to use a VPN connection to a local ISP. VPNs also support removing access for people who travel. Instead of setting up remote access servers and paying more fees to reach someone. The company can rely on an ISP that is locally based to help access both ends of the connected VPN.

HOW CAN A VPN BE USED

Your real IP is concealed; to bypass the blocks set by the network administrator, or restrictions of the internet provider.

To encrypt the transmitted data;

To access blocked websites from your country

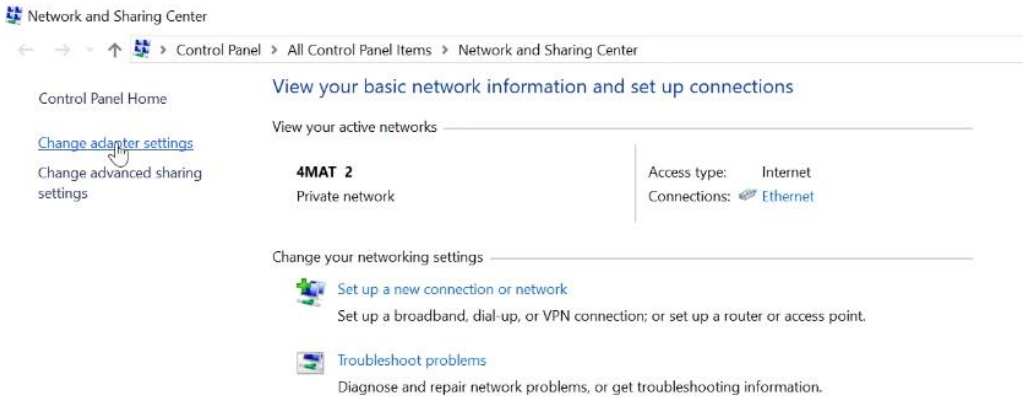
To enable downloading files from a p2p network (such as torrents)

Very importantly to protect your computer when connecting to free wifi

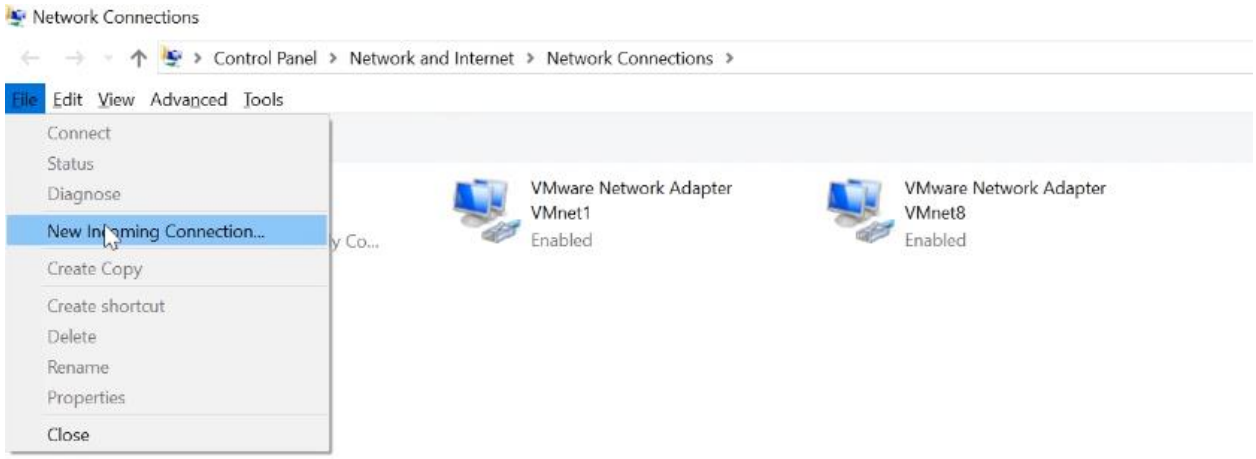
CREATING VPN SERVER ON YOUR COMPUTER

Creating a VPN server on your computer

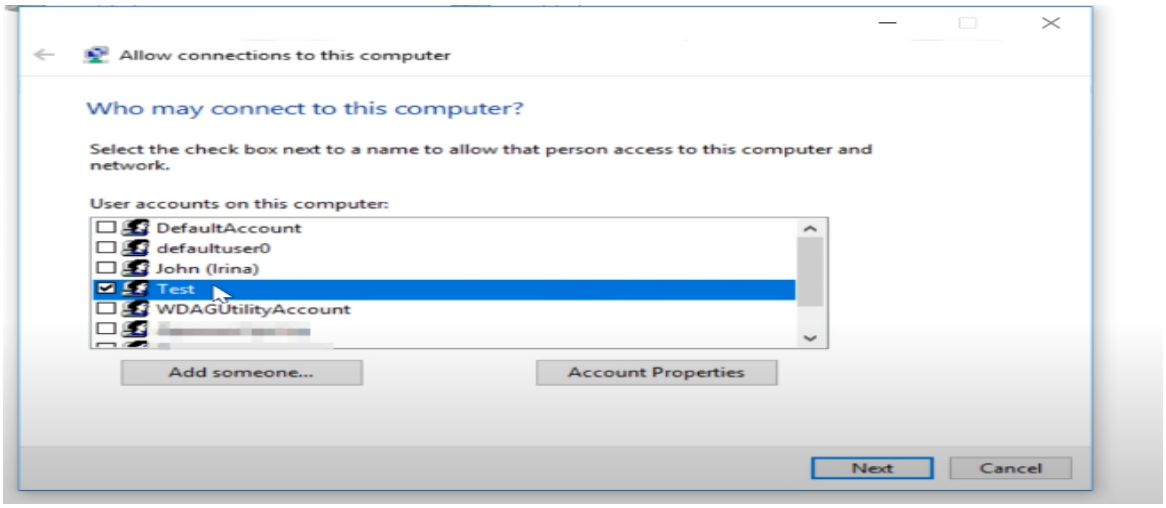
1. Goto network and sharing center then change adapter setting



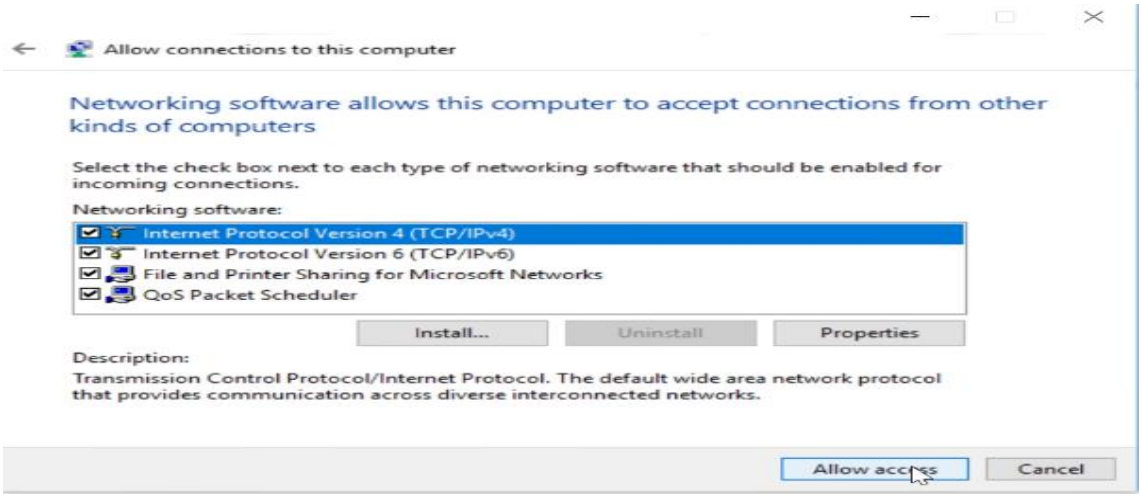
2. In the folder Network, Connections press Alt and select File / New incoming connection



3. Check the box next to the user name to allow this user to access this computer



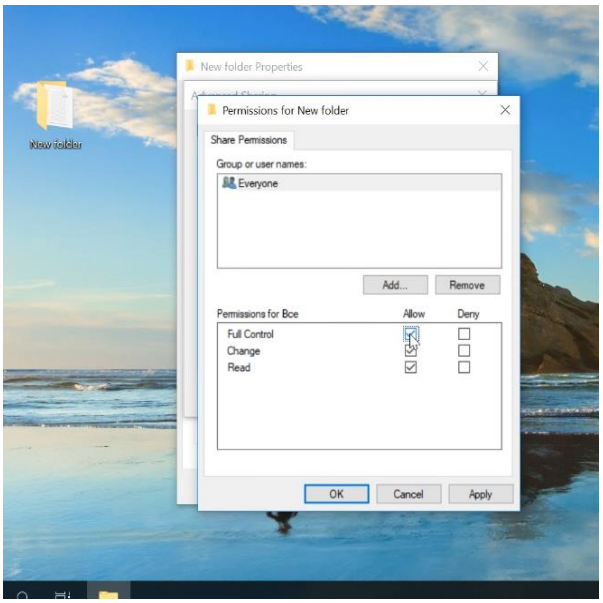
4. Click through the internet then allow access



5. Now the VPN server is created

CREATING A SHARED FOLDER ON VPN

1. Sharing a folder to which other computers will have access through VPN
2. Create a folder with contents,
3. Right-click, go to properties, then sharing
4. Advanced Sharing and check to Share this folder
5. Click permissions and allow full control

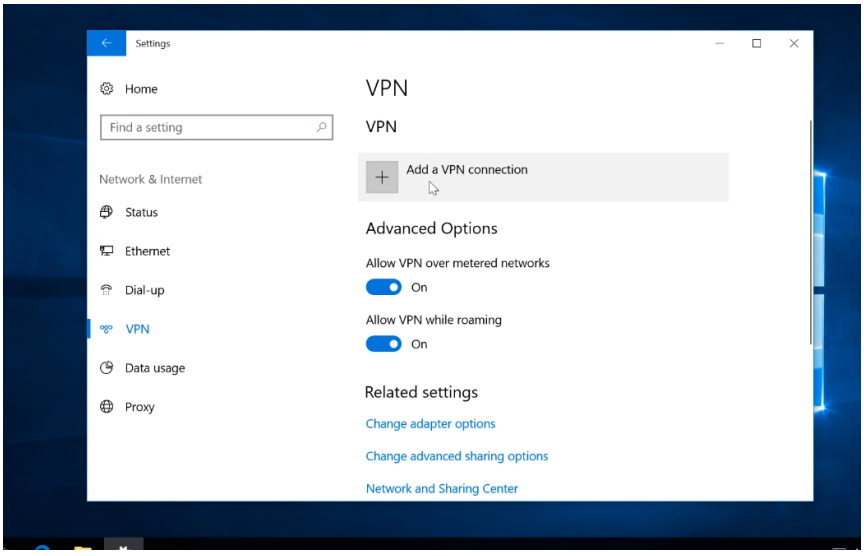


ACQUIRING FULL ACCESS TO FOLDER

Now if the user wants to connect to the VPN server and have access to the folder this is what they must do.

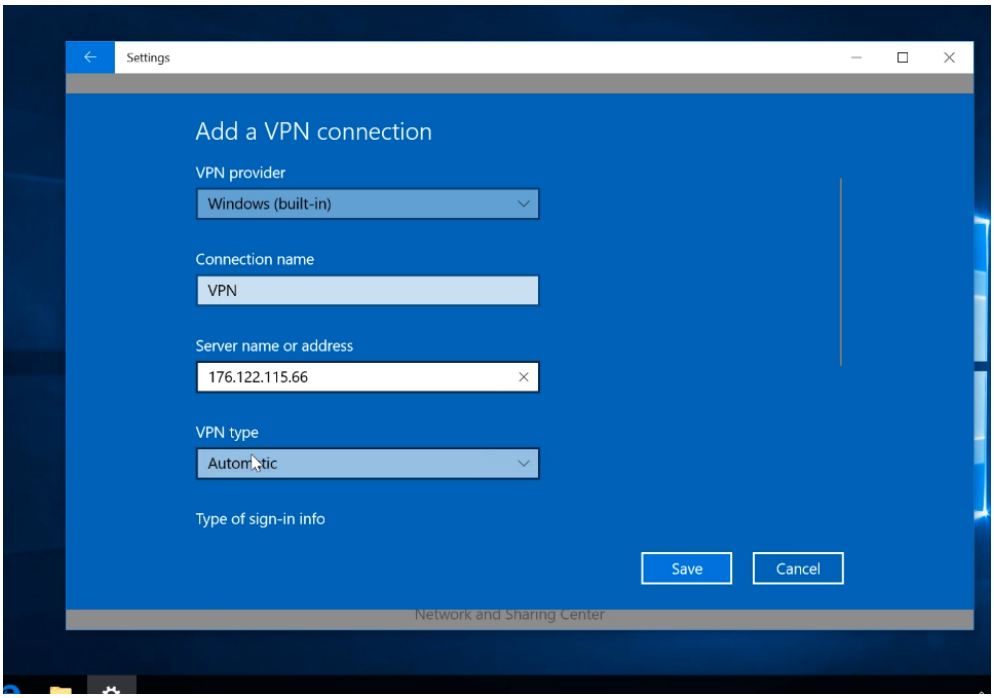
Connecting to VPN server

1. Open settings/Network and Internet/ VPN

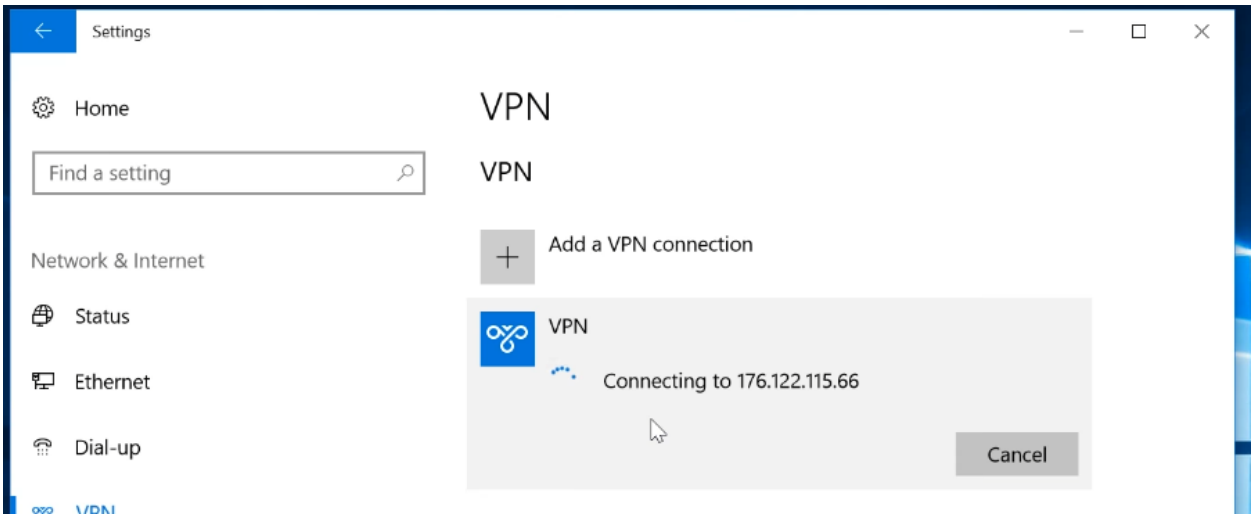


2. Add VPN connection
3. Choose a provider as Windows (built-in)
4. Make a connection name what you want the other connection see
5. Enter the IP address of the computer

6. (To find the IP address of the other computer Open CMD, type ipconfig, and Next to the IPv4 is your IP address)
7. Once you found the IP address enter it into the box.
8. VPN type should be automatic

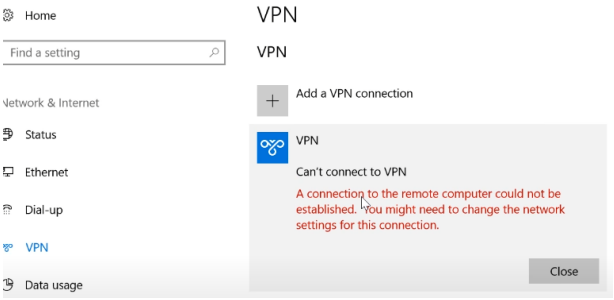


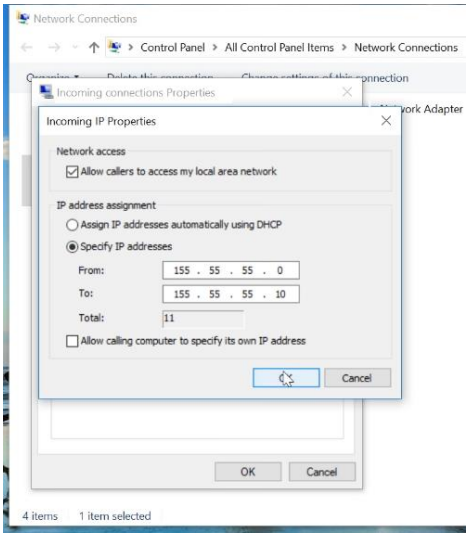
9. Type of sign-in info should be set to Username and password
10. Enter the name and password which is active on the server
11. Click Save and the VPN connection will be displayed
12. Click on the connection and connect to it



TROUBLESHOOTING

If you encounter an error follow these steps

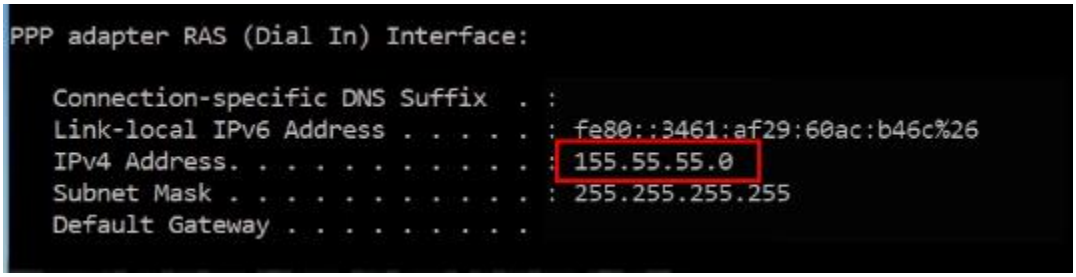


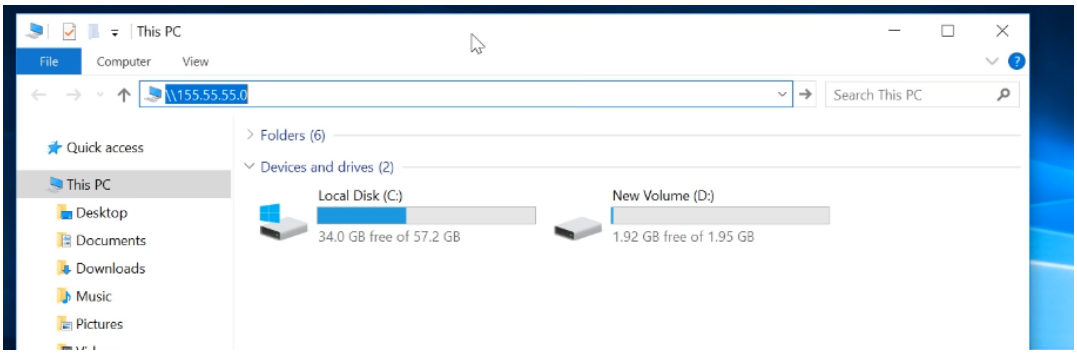
1. Go on the server computer
2. Go to Network and Sharing Center/ Change adapter settings
3. Right-click on incoming connection/ Properties/ Networking/IPv4/Properties
4. Check the box “Specify IP addresses” enter the pool of addresses
5. Connect and try again on another computer
6. 

GAINING ACCESS TO FOLDER

To access the shared folder in the computer which is the VPN server

1. Go to CMD on the VPN server and enter ipconfig
2. Go to the PC connected to VPN and enter the IP address into the address field with 2 backslashes before the address (\\)

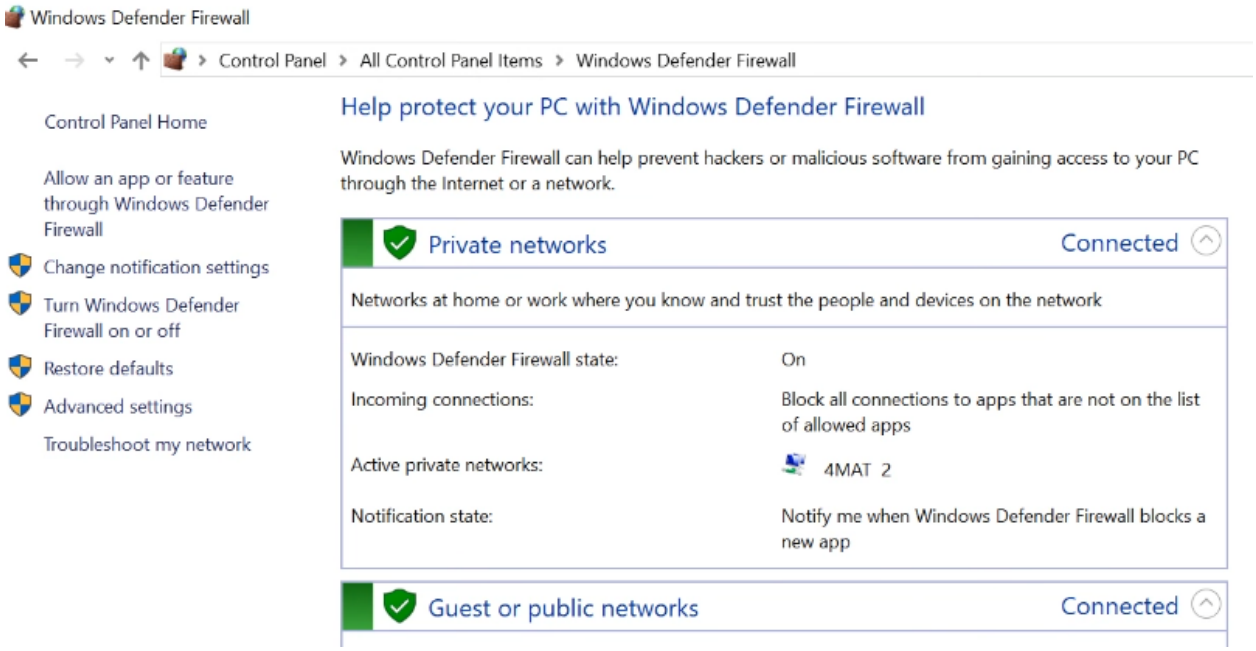




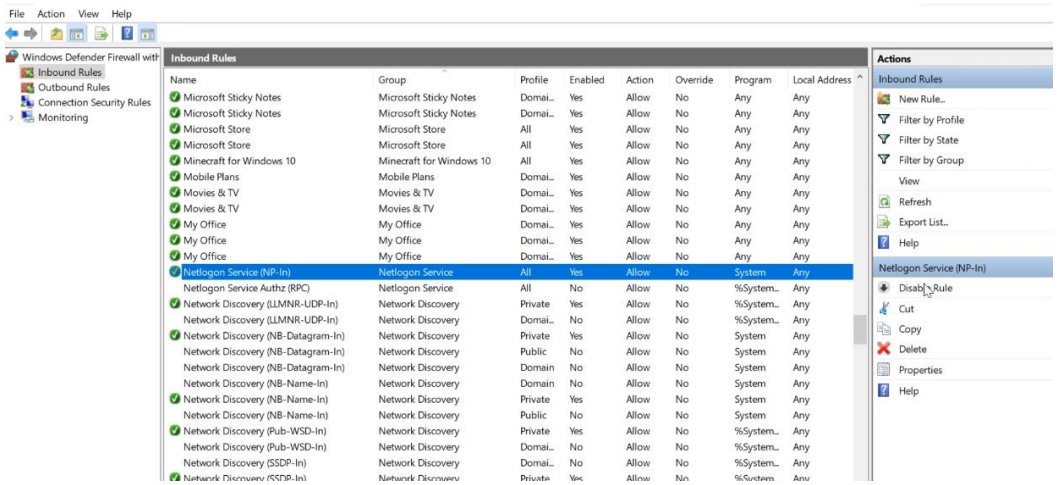
TROUBLESHOOTING

If nothing happens when you press enter follow these steps

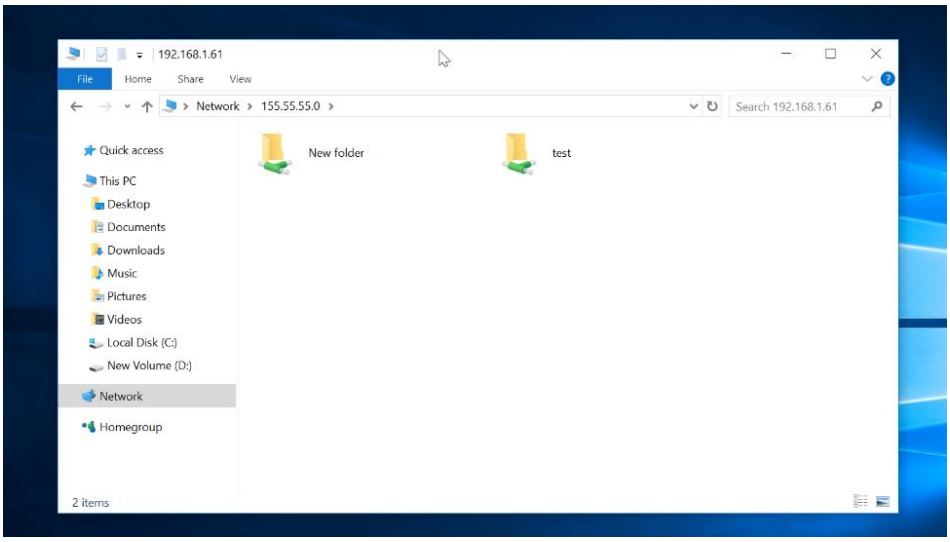
1. Go to the VPN server computer and go to Control Panel/ Windows/ Firewall/ Advanced settings



2. Go to Inbound rules and find the rule named “Net logon Service (NP-in) and enable it



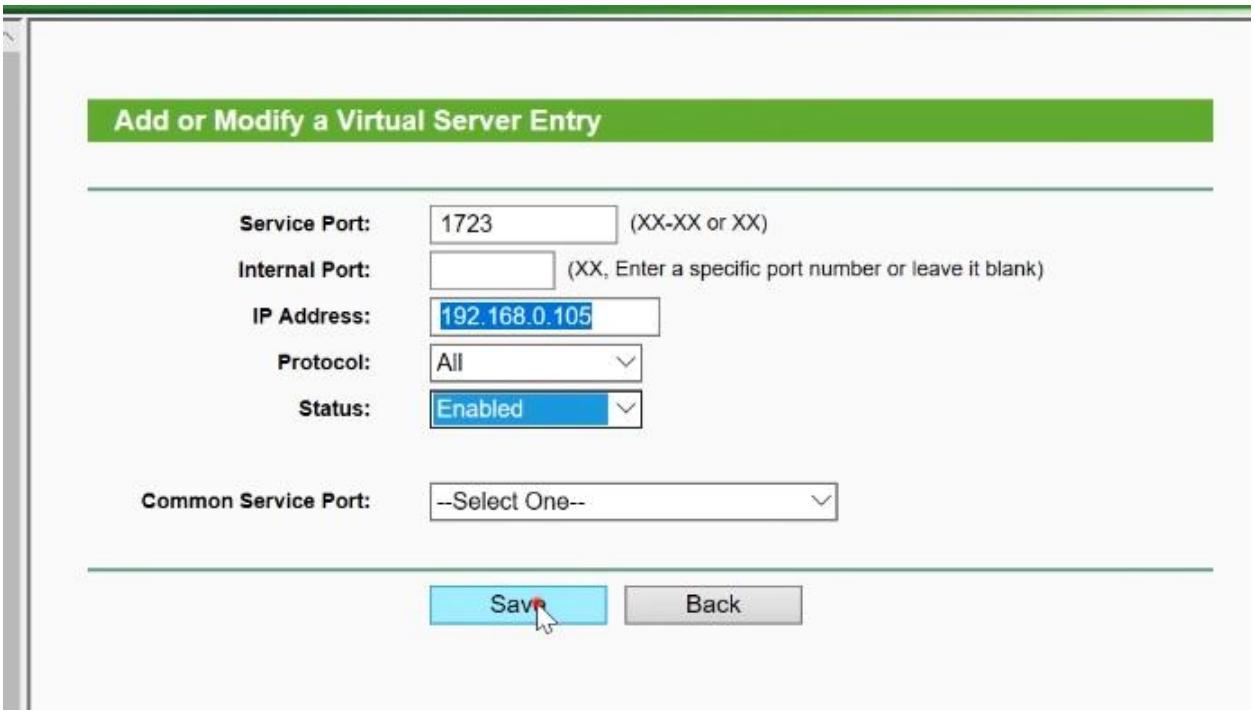
3. Now go back and try to connect to the VPN shared folder

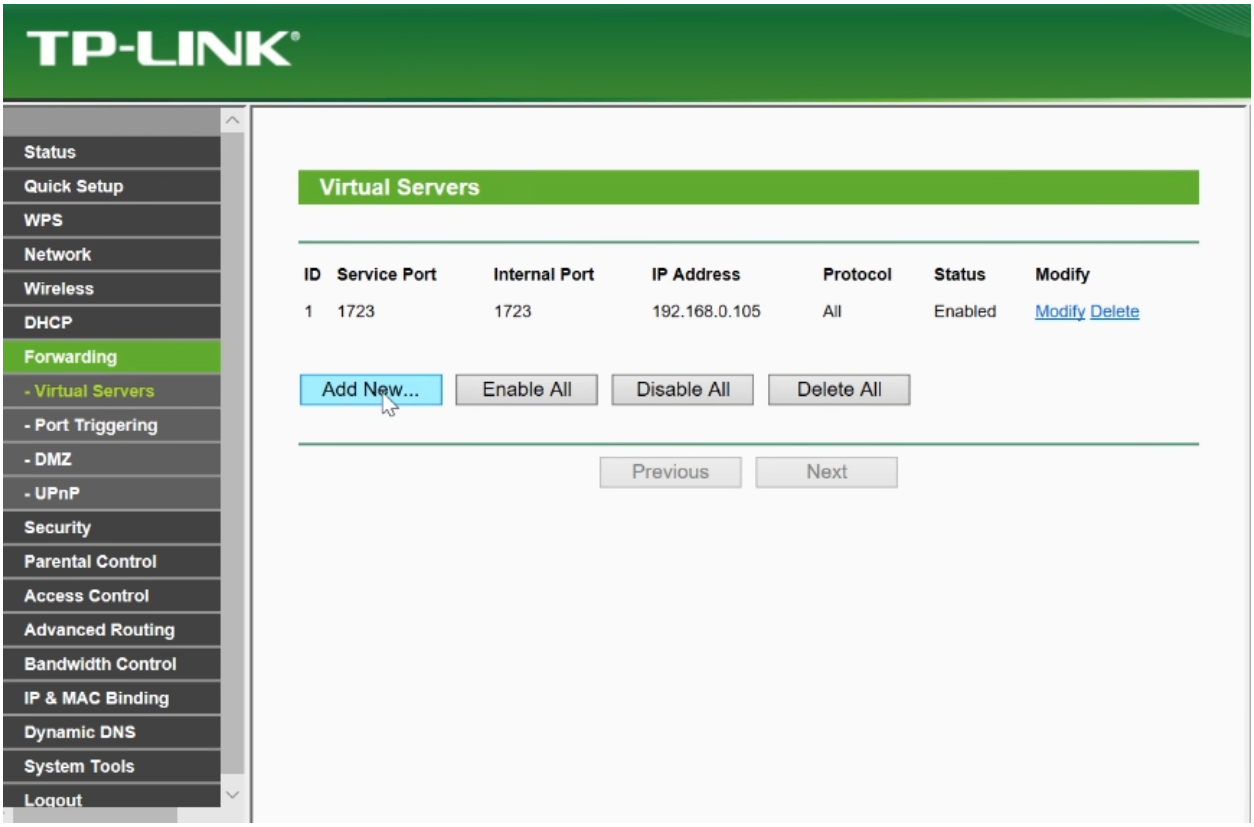


SETTING UP PORT FORWARDING

If you have your server set up on a router you must set up forwarding for port 1723.

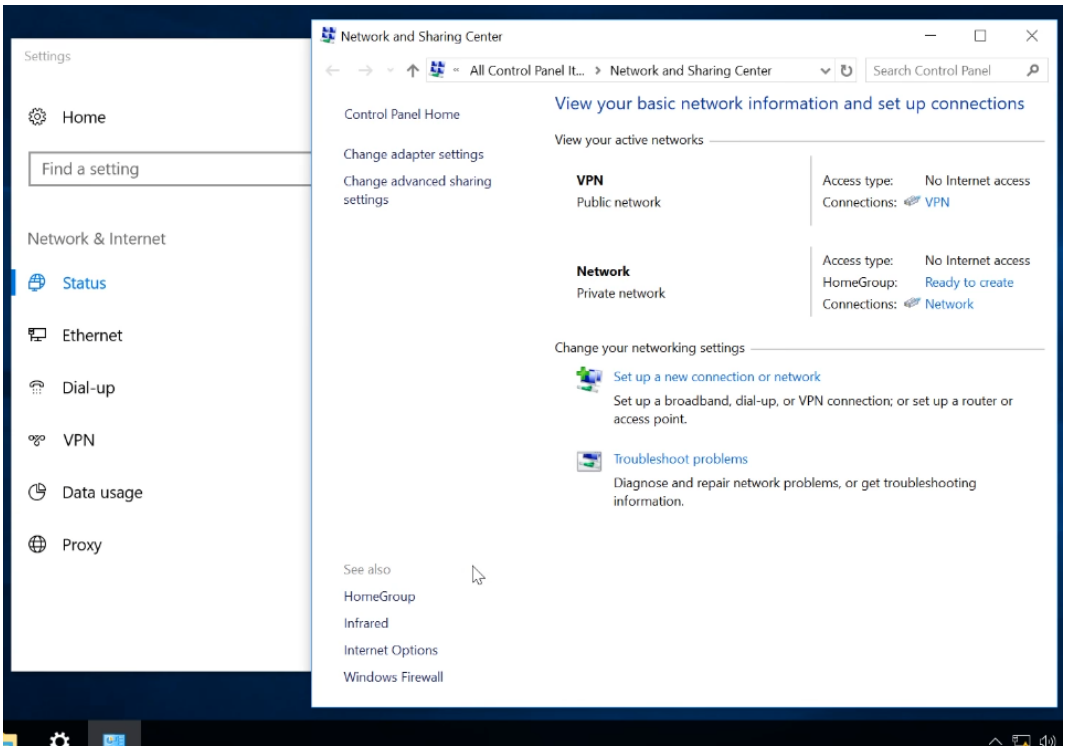
1. Log into Router settings
2. Forwarding/Virtual server
3. Add new/ enter service port 1723
4. Enter the IP address of the computer where the VPN server will be created
5. Protocol All
6. Status Enabled


Add or Modify a Virtual Server Entry
Service Port:
1723
(XX-XX or XX)
Internal Port:
(XX, Enter a specific port number or leave it blank)
IP Address:
192.168.0.105
Protocol:
All
Status:
Enabled
Common Service Port:
--Select One--
Save
Back


TP-LINK
Status
Quick Setup
WPS
Network
Wireless
DHCP
Forwarding
- Virtual Servers
- Port Triggering
- DMZ
- UPnP
Security
Parental Control
Access Control
Advanced Routing
Bandwidth Control
IP & MAC Binding
Dynamic DNS
System Tools
Logout
Virtual Servers
ID Service Port Internal Port IP Address Protocol Status Modify
1 1723 1723 192.168.0.105 All Enabled Modify Delete
Add New...
Enable All
Disable All
Delete All
Previous
Next

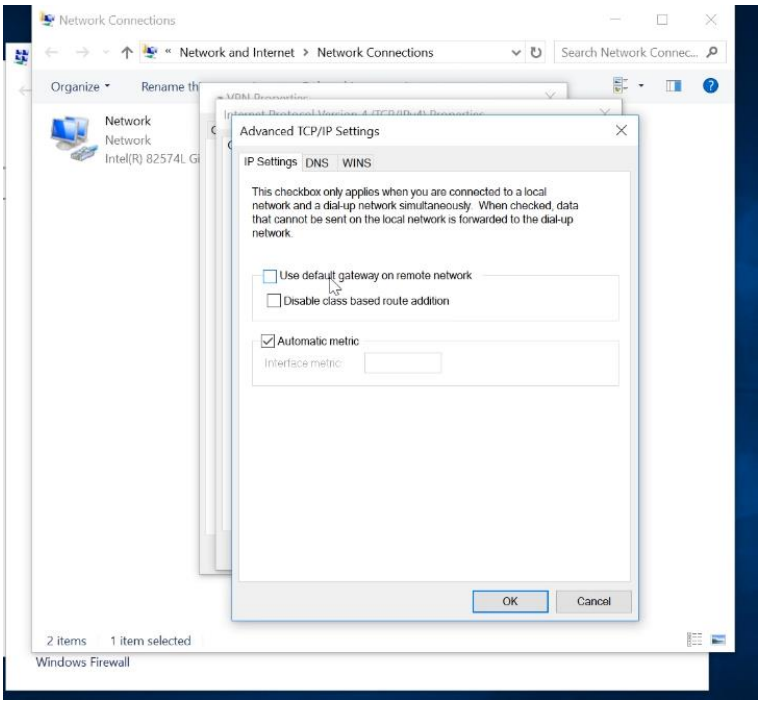
Once that is set up you want to ensure that the VPN connection still has internet access

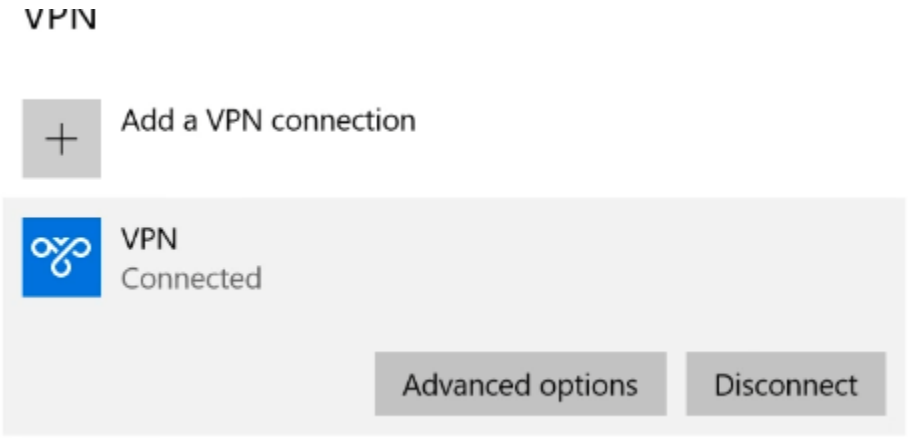
1. When VPN is disconnected go to network and Sharing Center/ Change adapter settings



2. Right-click on the created VPN connection and select properties/Networking/IPv4
3. Click advanced/ In IP settings uncheck the box next to default gateway in the remote.

Now when you connect the internet connection will not drop





CONCLUSION

In conclusion, VPNs are used to have anonymous browsing where your actual IP is concealed. VPN makes your location unknown which can be beneficial. An example would be someone who plays video games. If someone is mad with them online they could find the area you live in and DDOS attack you. Many people use the VPN for travel as there are restrictions in some countries to what website and applications you are using.

References

1. Ndichu, S., Mcoyowo, S., Okoyo, H., & Wekesa, C. (2020). Information Technology and Computer Science. *Information Technology and Computer Science*, *5*, 38–51. https://doi.org/10.5815/ijitcs.2020.05.03

2. *Proper virtual private network (VPN) solution - researchgate*. (n.d.). Retrieved January 16, 2022, from https://www.researchgate.net/profile/Ahmed-Jaha/publication/224373633_Proper_Virtual_Private_Network_VPN_Solution/links/590e41d0458515978185c7b7/Proper-Virtual-Private-Network-VPN-Solution.pdf

3. *The University of Akron ideaexchange@uakron*. (n.d.). Retrieved January 16, 2022, from

https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=2432&context=honors_research_projects

4. *EasyVPN: IPsec Remote Access Made Easy*. Check out the new USENIX Web site. (n.d.). Retrieved January 16, 2022, from https://www.usenix.org/legacy/events/lisa03/tech/full_papers/benvenuto/benvenuto_html/

5. *Attestation-based policy enforcement for remote access*. (n.d.). Retrieved January 16, 2022, from https://courses.cs.vt.edu/~cs5204/fall10-kafura-BB/Papers/TPM/Attestation-based-policy-enforcement.pdf

6. Brad, J. (n.d.). *On the establishment of an access VPN in broadband access ...* Retrieved January 16, 2022, from http://rcohen.cs.technion.ac.il/PAPERS/access-vpn.pdf

7. Ghip, F. (n.d.). *Comparison of machine-learning ... - tandfonline.com*. Retrieved January 16, 2022, from https://www.tandfonline.com/doi/pdf/10.1080/23742917.2017.1321891

8. Fergoson, P. (1998, April 21). Whats a VPN. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.169.7689&rep=rep1&type=pdf

9. *An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps*. (n.d.). Retrieved January 16, 2022, from https://dl.acm.org/doi/pdf/10.1145/2987443.2987448

10. Springer, C. (n.d.). *Customer Management and control of broadband ... - springer*. Retrieved January 16, 2022, from https://link.springer.com/content/pdf/10.1007%2F978-0-387-35180-3_23.pdf