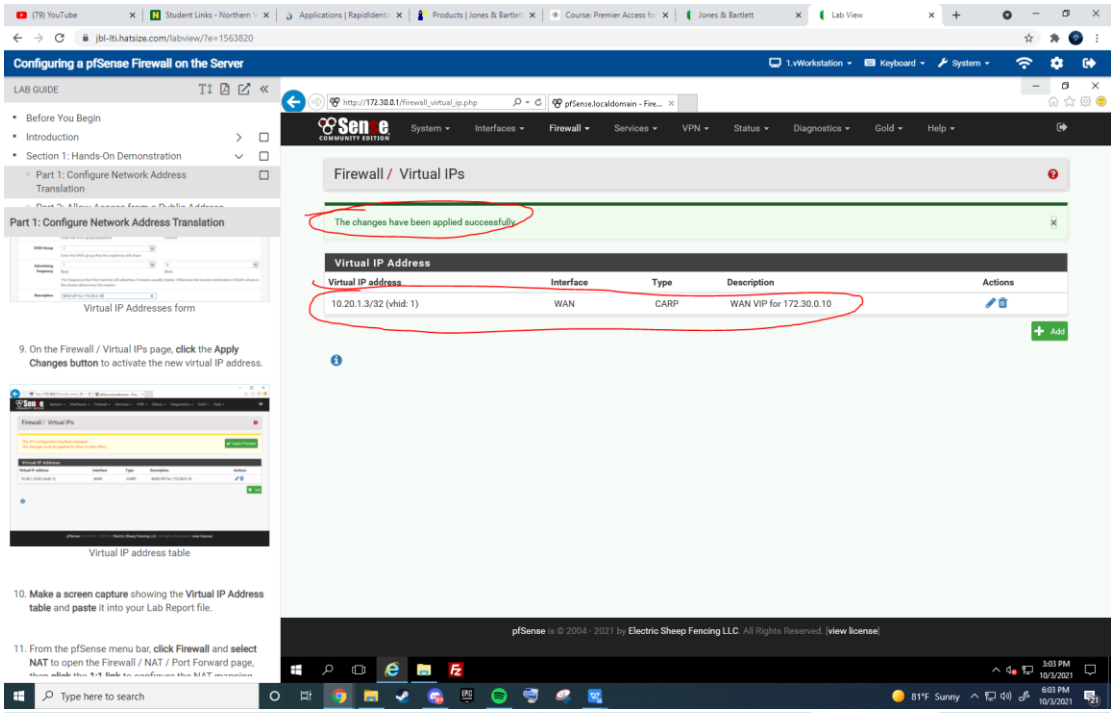
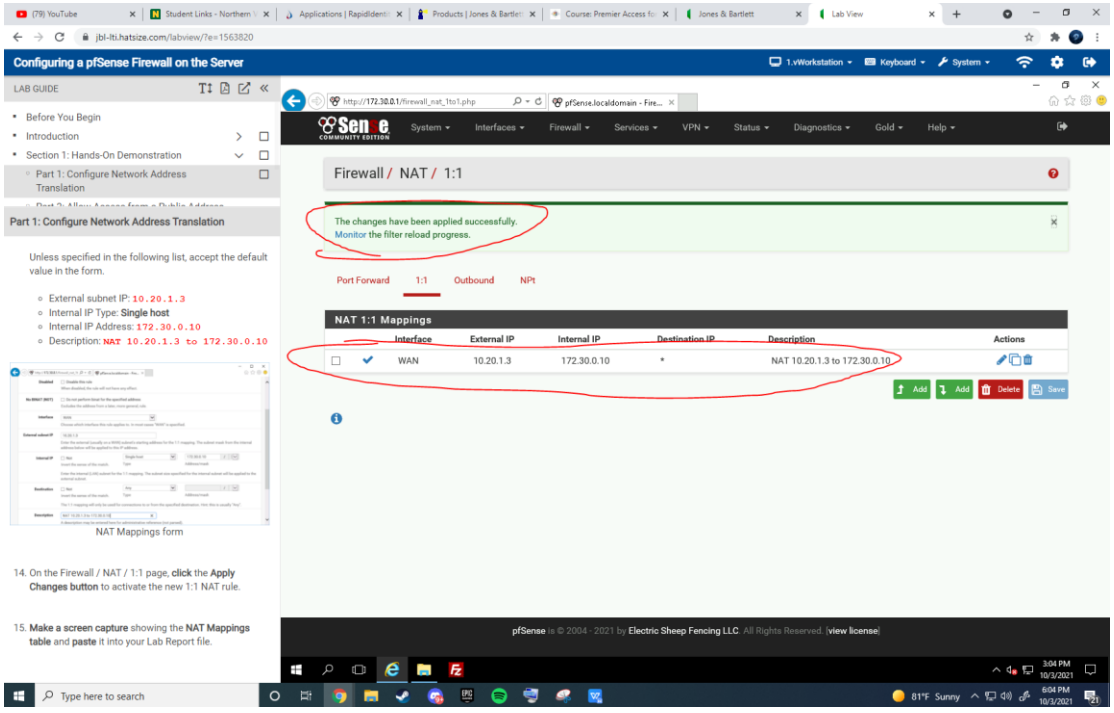
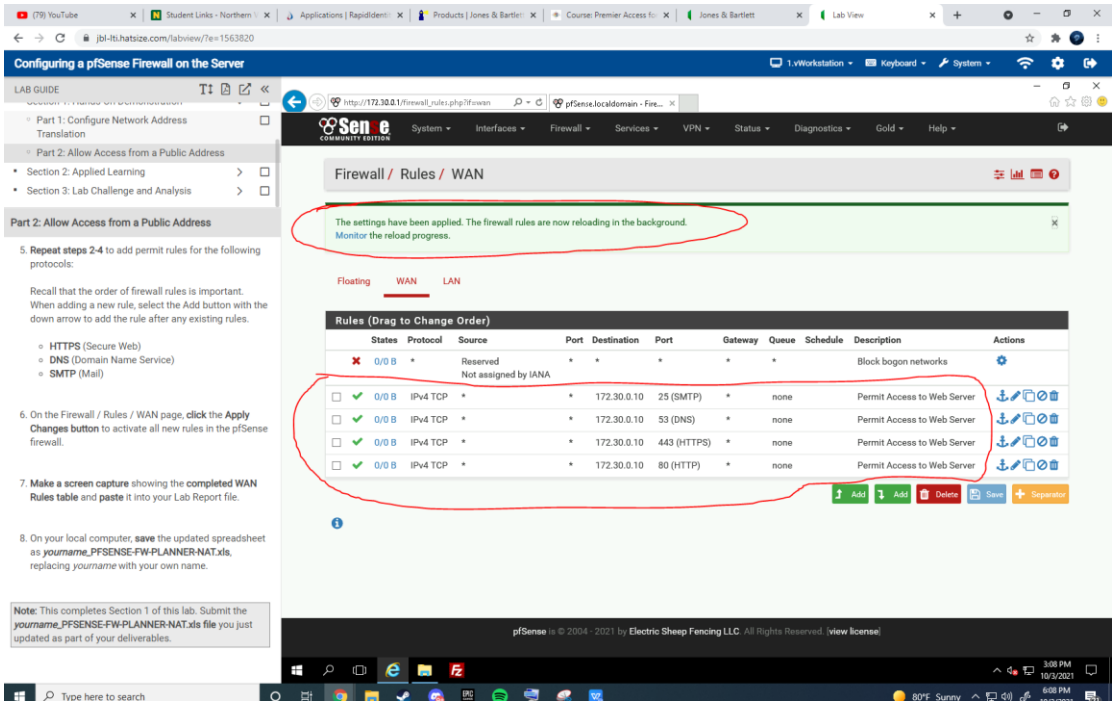
JBL Labs Ch 12 and 13
Michael Dawson

Chapter 12 Configuring a pfSense Firewall on the Server.

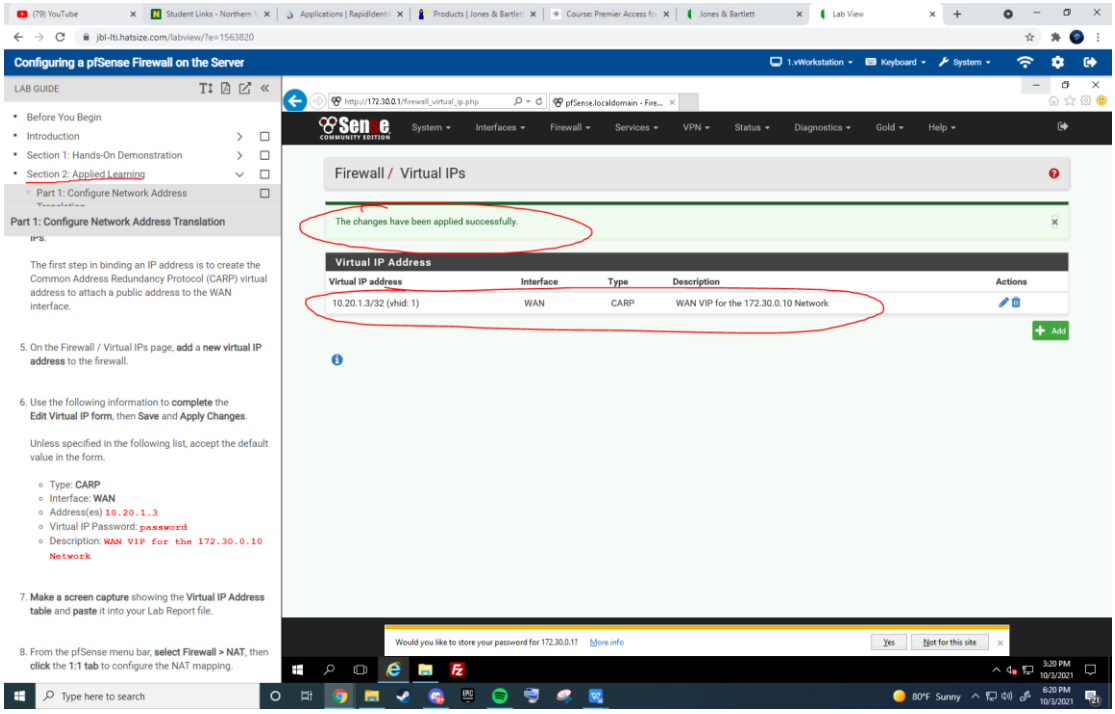
Section 1

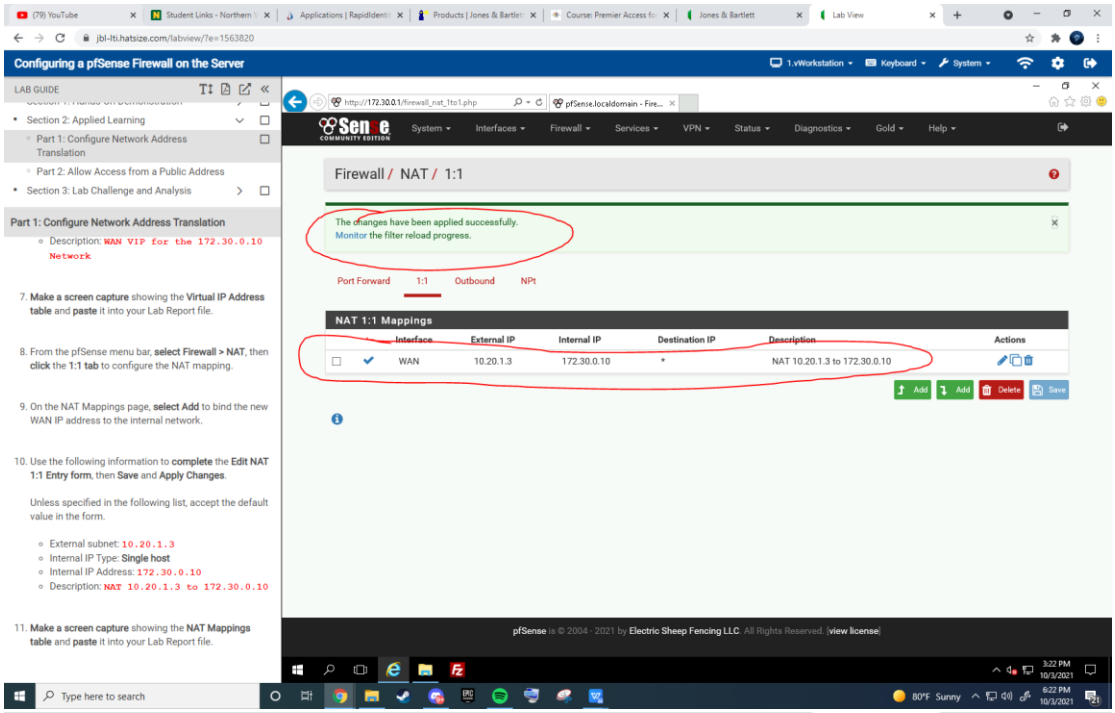


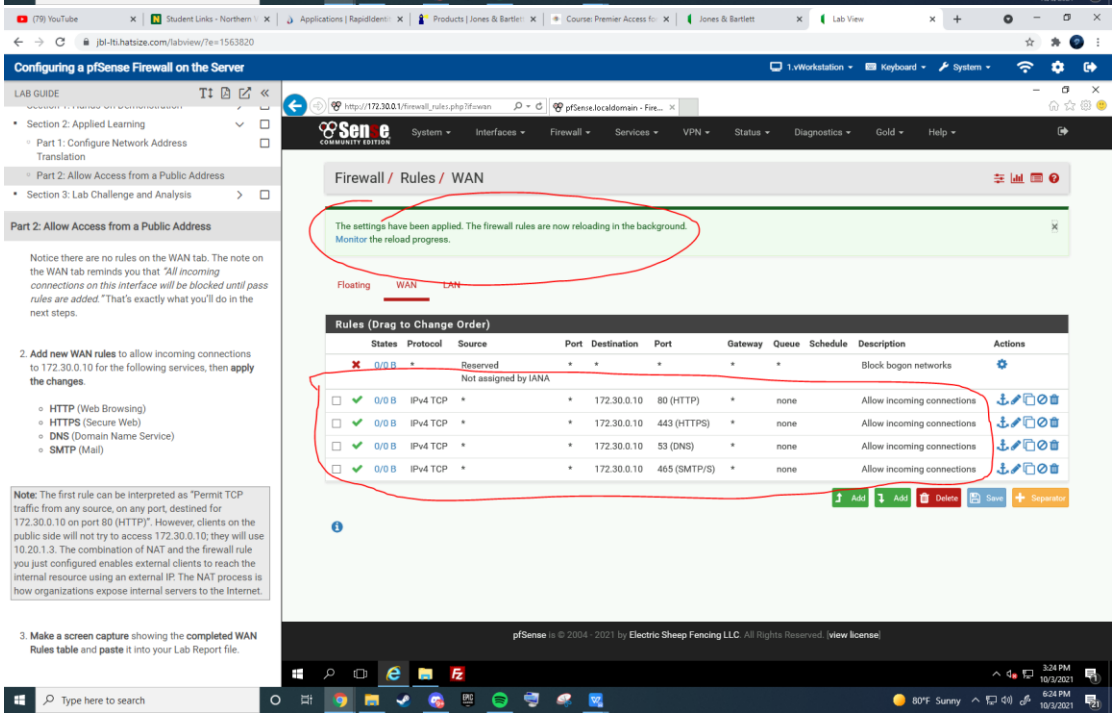


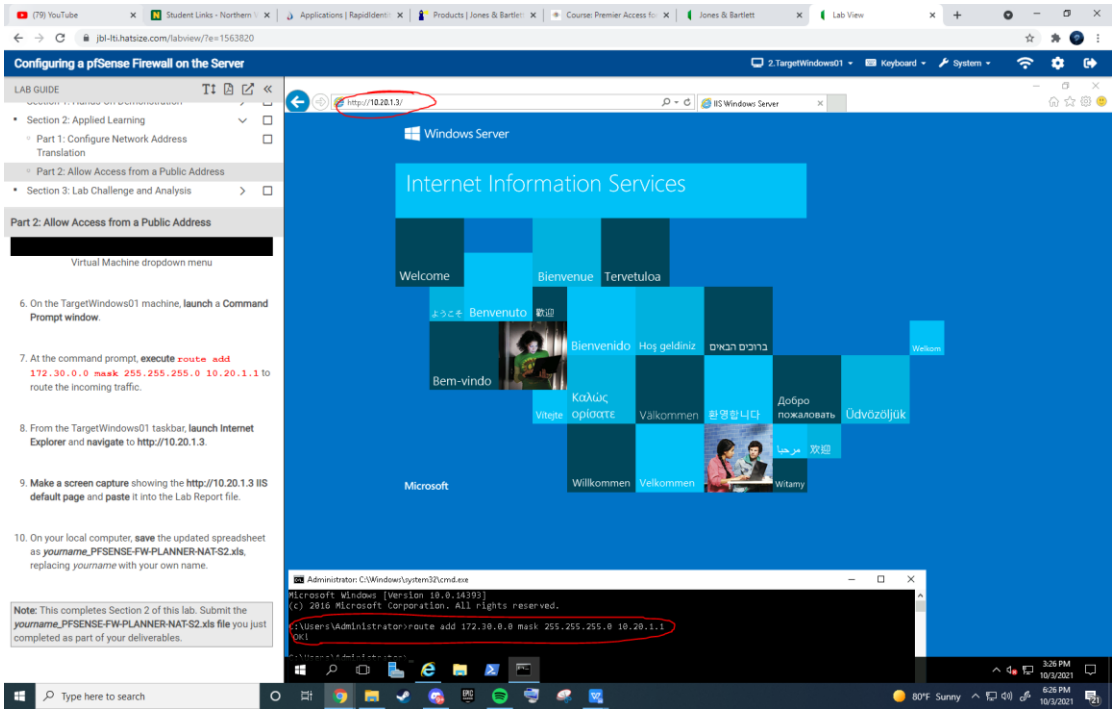


Section 2: Applied Learning




Configuring a pfSense Firewall on the Server
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure Network Address Translation
Part 2: Allow Access from a Public Address
Section 3: Lab Challenge and Analysis
Part 1: Configure Network Address Translation
Description: WAN VIP for the 172.30.0.10 Network
7. Make a screen capture showing the Virtual IP Address table and paste it into your Lab Report file.
8. From the pfSense menu bar, select Firewall > NAT, then click the 1:1 tab to configure the NAT mapping.
9. On the NAT Mappings page, select Add to bind the new WAN IP address to the internal network.
10. Use the following information to complete the Edit NAT 1:1 Entry form, then Save and Apply Changes.
Unless specified in the following list, accept the default value in the form.
External subnet: 10.20.1.3
Internal IP Type: Single host
Internal IP Address: 172.30.0.10
Description: NAT 10.20.1.3 to 172.30.0.10
11. Make a screen capture showing the NAT Mappings table and paste it into your Lab Report file.
Firewall / NAT / 1:1
The changes have been applied successfully.
Monitor the filter reload progress.
Port Forward
1:1
Outbound
NPt
NAT 1:1 Mappings
Interface
External IP
Internal IP
Destination IP
Description
Actions
WAN
10.20.1.3
172.30.0.10
*
NAT 10.20.1.3 to 172.30.0.10
Add
Add
Delete
Save
pfSense is © 2004 - 2021 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]


Configuring a pfSense Firewall on the Server
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure Network Address Translation
Part 2: Allow Access from a Public Address
Section 3: Lab Challenge and Analysis
Part 2: Allow Access from a Public Address
Notice there are no rules on the WAN tab. The note on the WAN tab reminds you that "All incoming connections on this interface will be blocked until pass rules are added." That's exactly what you'll do in the next steps.
2. Add new WAN rules to allow incoming connections to 172.30.0.10 for the following services, then apply the changes.
HTTP (Web Browsing)
HTTPS (Secure Web)
DNS (Domain Name Service)
SMTP (Mail)
Note: The first rule can be interpreted as "Permit TCP traffic from any source, on any port, destined for 172.30.0.10 on port 80 (HTTP)". However, clients on the public side will not try to access 172.30.0.10; they will use 10.20.1.3. The combination of NAT and the firewall rule you just configured enables external clients to reach the internal resource using an external IP. The NAT process is how organizations expose internal servers to the Internet.
3. Make a screen capture showing the completed WAN Rules table and paste it into your Lab Report file.
Firewall / Rules / WAN
The settings have been applied. The firewall rules are now reloading in the background.
Monitor the reload progress.
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
Reserved
Not assigned by IANA
Block bogon networks
IPv4 TCP
172.30.0.10
80 (HTTP)
Allow incoming connections
443 (HTTPS)
53 (DNS)
465 (SMTP/S)
Add
Add
Delete
Save
Separator
pfSense is © 2004 - 2021 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

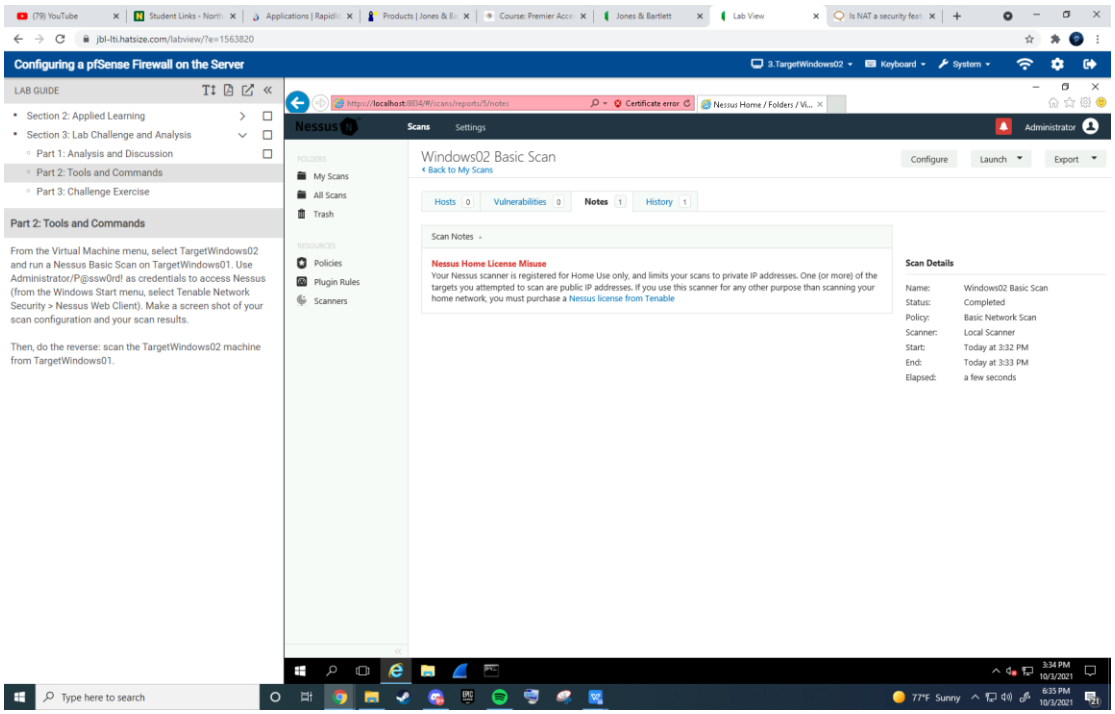


Sections 3:

1. Security through obscurity is enforcing secrecy and confidentiality of a system's architecture. NAT is not truly secure, if a user were to do any web based work that require the IP address can have problems. Basic NAT provides no security.

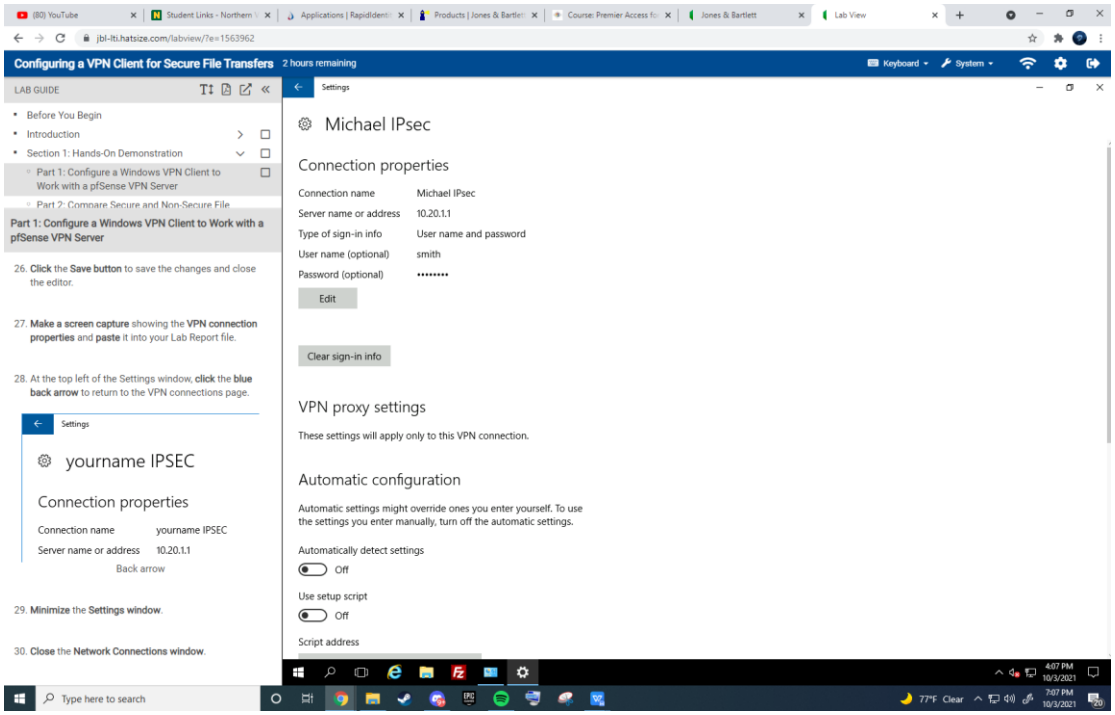
https://blog.ipspace.net/2011/12/is-nat-security-feature.html#:~:text=Summary%3A%20Basic%20NAT%20provides%20no%20security.

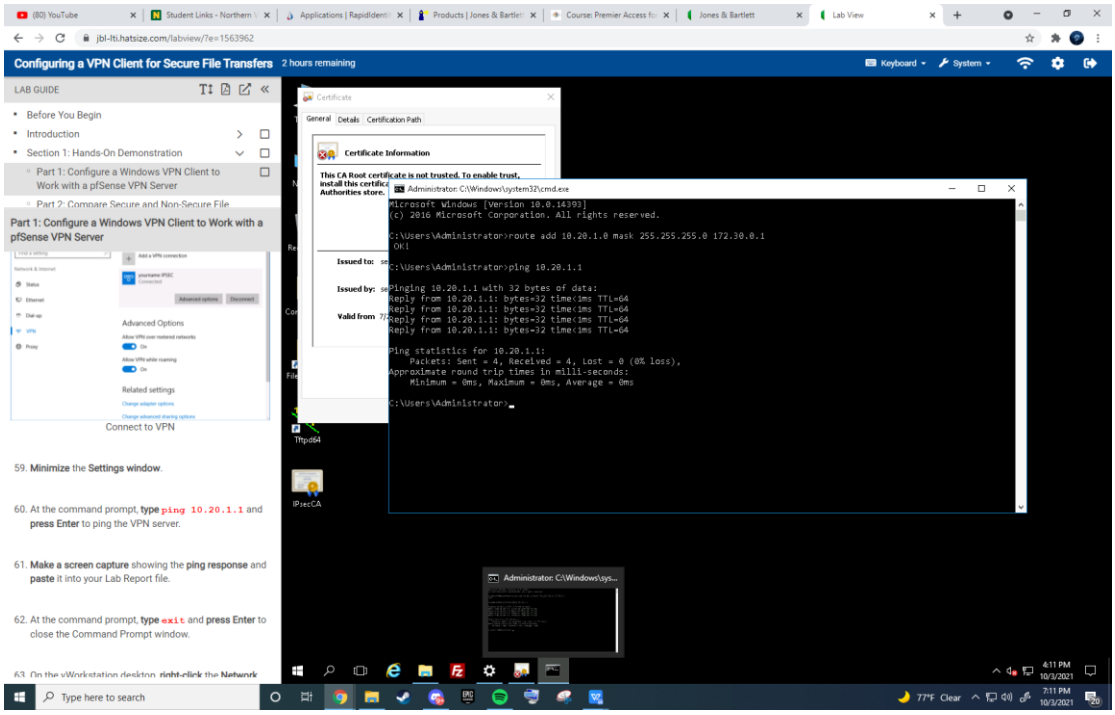
2. Nessus Scan

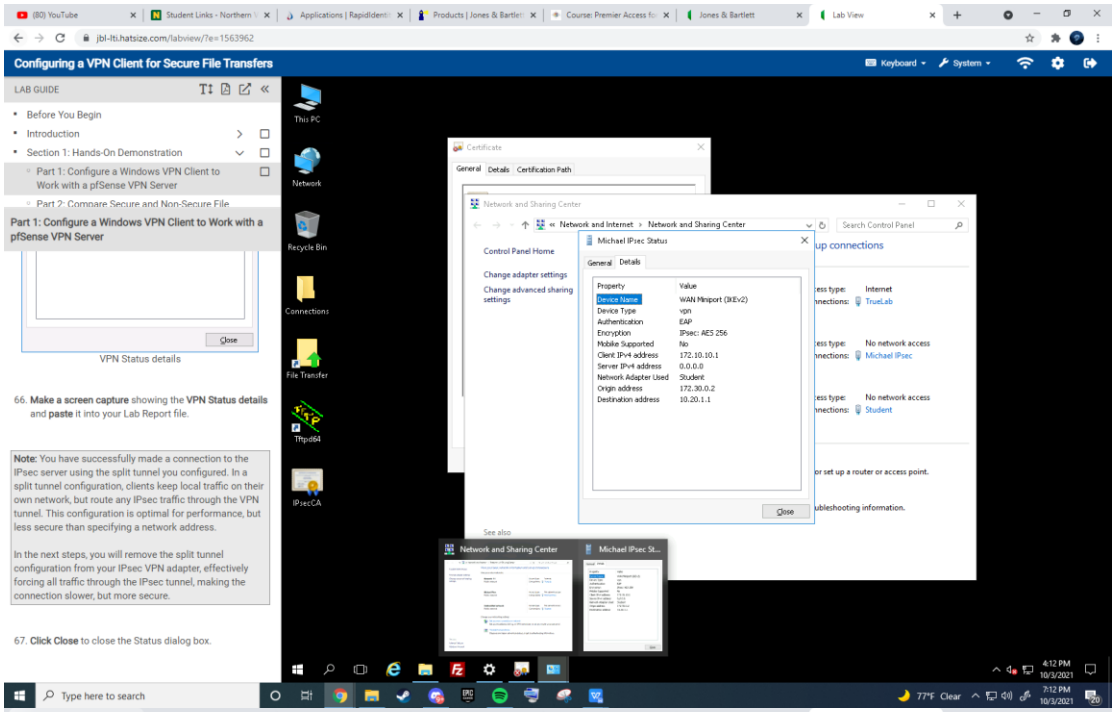


Chapter 13 Configuring a VPN for Secure File Transfers

Section 1







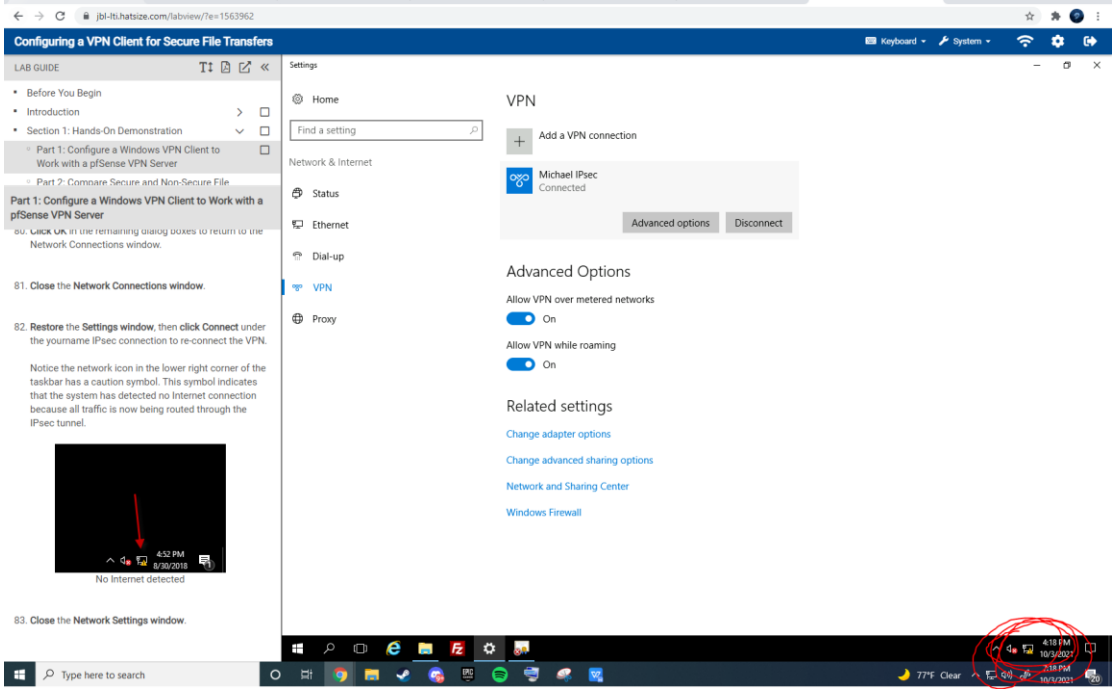
VPN Status details

66. **Make a screen capture** showing the **VPN Status details** and **paste** it into your Lab Report file.

Note: You have successfully made a connection to the IPsec server using the split tunnel you configured. In a split tunnel configuration, clients keep local traffic on their own network, but route any IPsec traffic through the VPN tunnel. This configuration is optimal for performance, but less secure than specifying a network address.

In the next steps, you will remove the split tunnel configuration from your IPsec VPN adapter, effectively forcing all traffic through the IPsec tunnel, making the connection slower, but more secure.

67. **Click Close** to close the Status dialog box.



80. **Click OK** in the remaining dialog boxes to return to the Network Connections window.

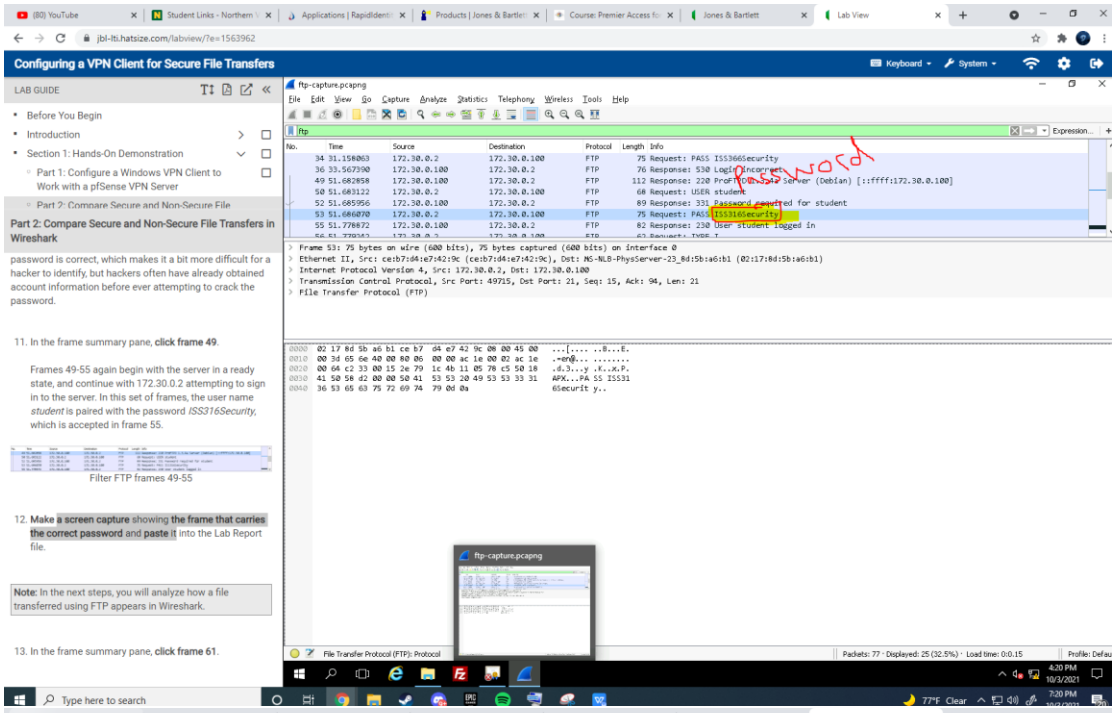
81. **Close** the **Network Connections window**.

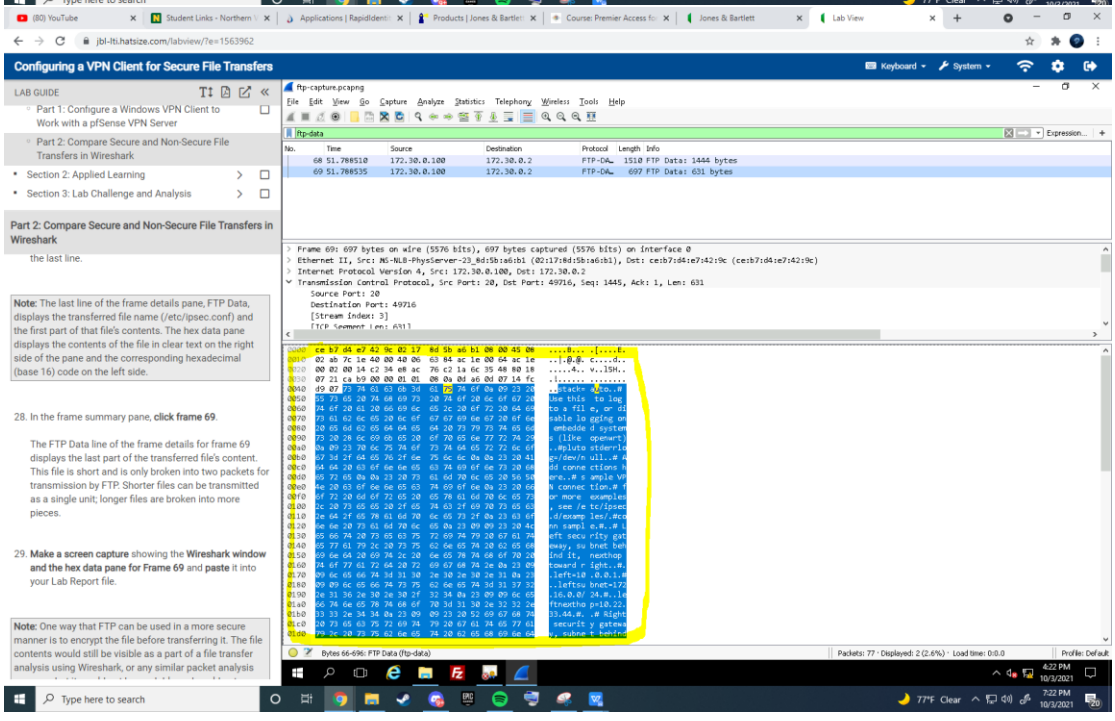
82. **Restore** the **Settings window**, then **click Connect** under the yourname IPsec connection to re-connect the VPN.

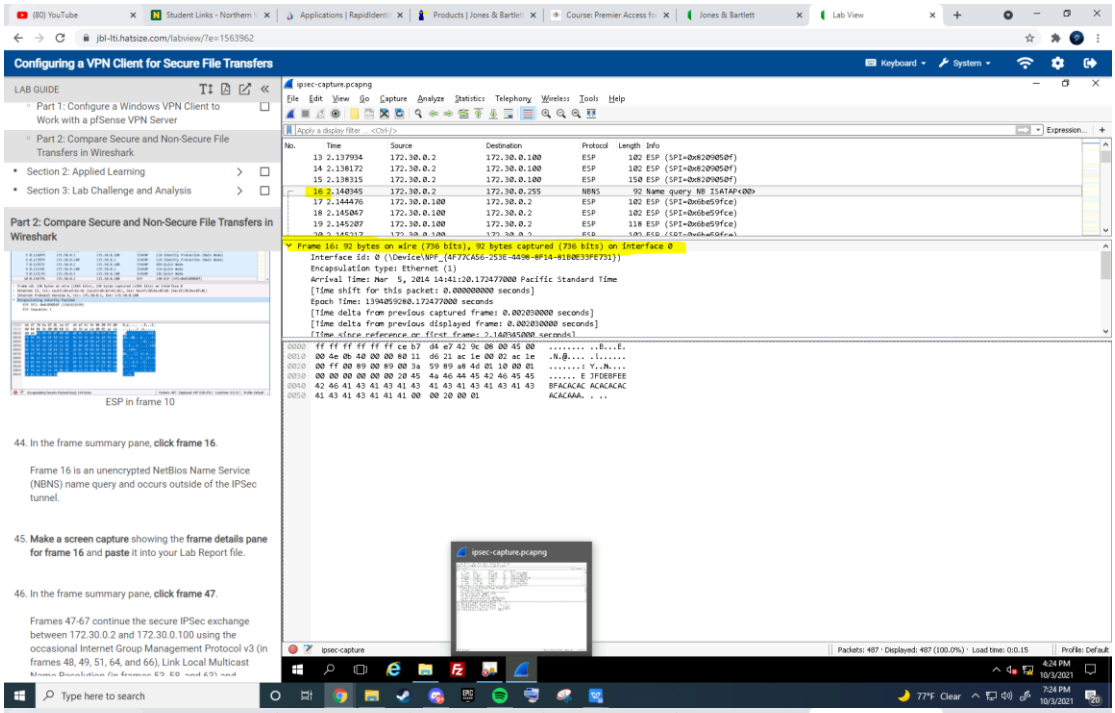
Notice the network icon in the lower right corner of the taskbar has a caution symbol. This symbol indicates that the system has detected no Internet connection because all traffic is now being routed through the IPsec tunnel.

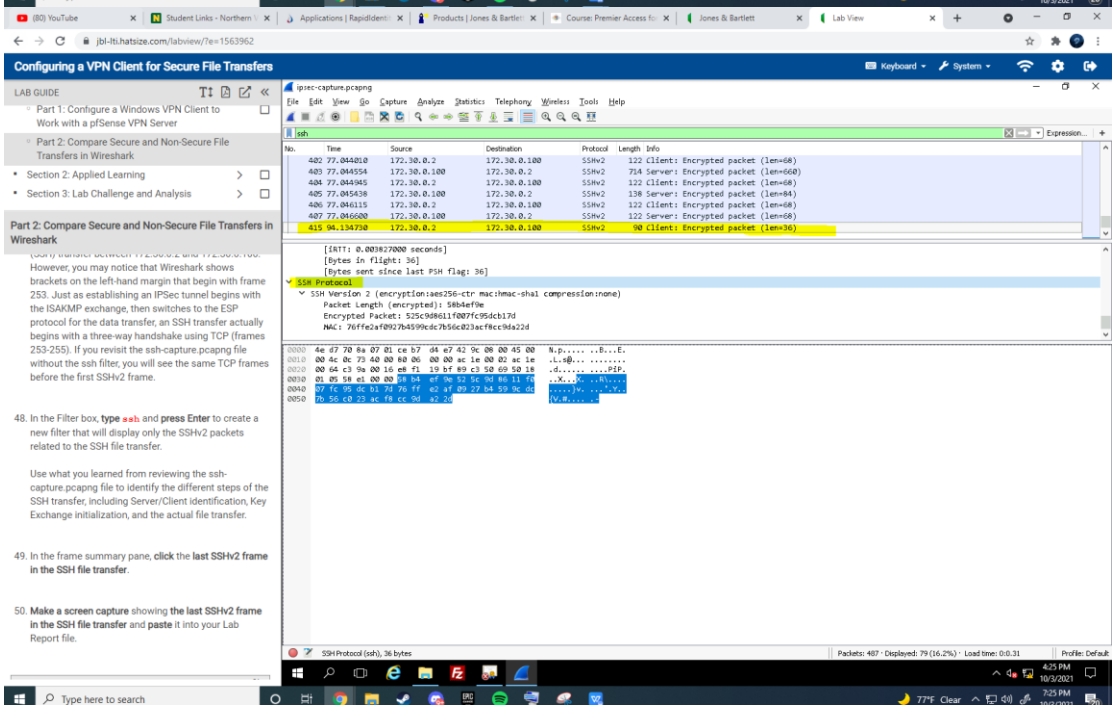
No Internet detected

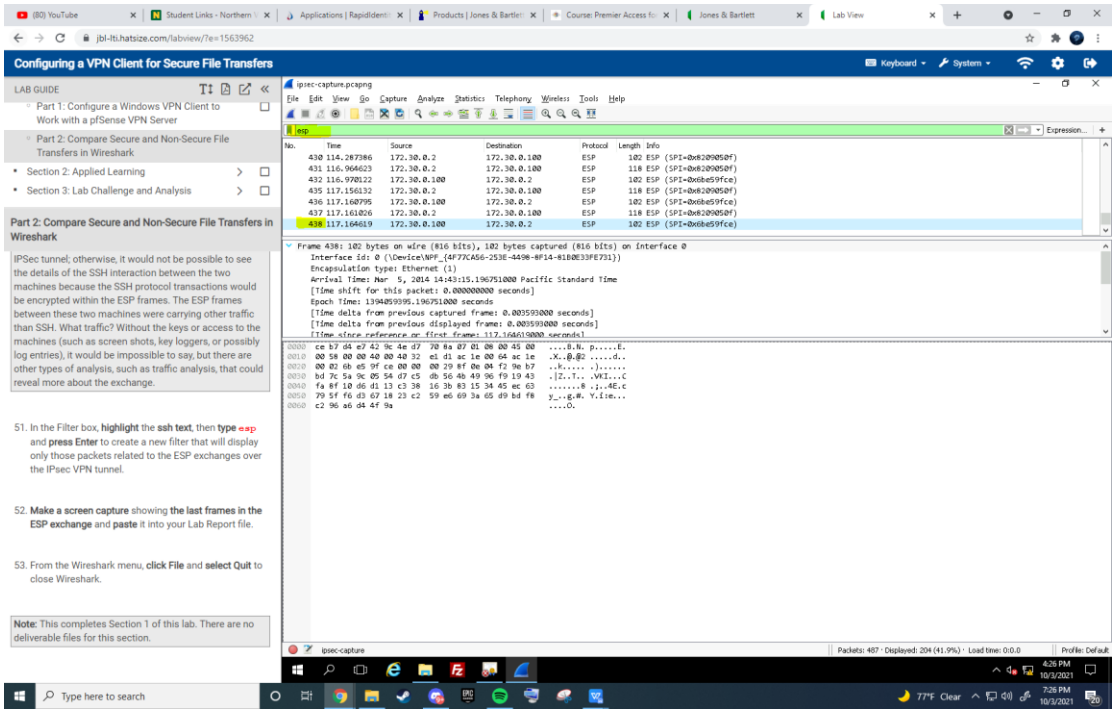
83. **Close** the **Network Settings window**.


Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Before You Begin
Introduction
Section 1: Hands-On Demonstration
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
password is correct, which makes it a bit more difficult for a hacker to identify, but hackers often have already obtained account information before ever attempting to crack the password.
11. In the frame summary pane, click frame 49.
Frames 49-55 again begin with the server in a ready state, and continue with 172.30.0.2 attempting to sign in to the server. In this set of frames, the user name student is paired with the password ISS316Security, which is accepted in frame 55.
Filter FTP frames 49-55
12. Make a screen capture showing the frame that carries the correct password and paste it into the Lab Report file.
Note: In the next steps, you will analyze how a file transferred using FTP appears in Wireshark.
13. In the frame summary pane, click frame 61.
ftp-capture.pcapng
Password

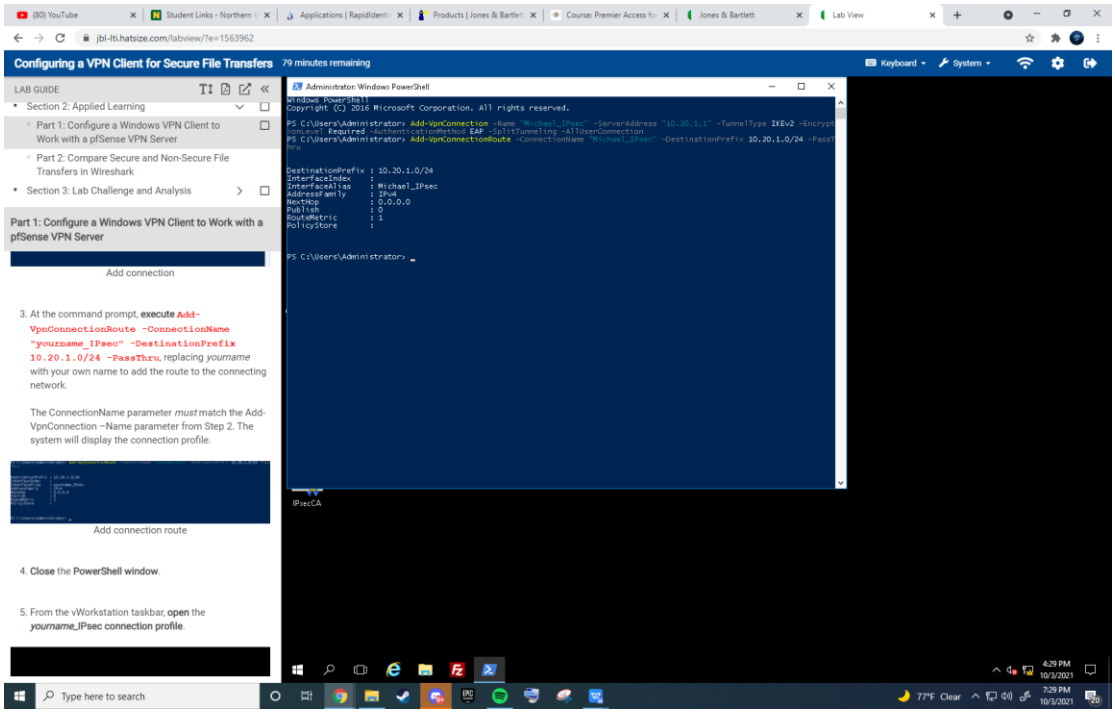

Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 2: Applied Learning
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
the last line.
Note: The last line of the frame details pane, FTP Data, displays the transferred file name (/etc/ipsec.conf) and the first part of that file's contents. The hex data pane displays the contents of the file in clear text on the right side of the pane and the corresponding hexadecimal (base 16) code on the left side.
28. In the frame summary pane, click frame 69.
The FTP Data line of the frame details for frame 69 displays the last part of the transferred file's content. This file is short and is only broken into two packets for transmission by FTP. Shorter files can be transmitted as a single unit; longer files are broken into more pieces.
29. Make a screen capture showing the Wireshark window and the hex data pane for Frame 69 and paste it into your Lab Report file.
Note: One way that FTP can be used in a more secure manner is to encrypt the file before transferring it. The file contents would still be visible as a part of a file transfer analysis using Wireshark, or any similar packet analysis

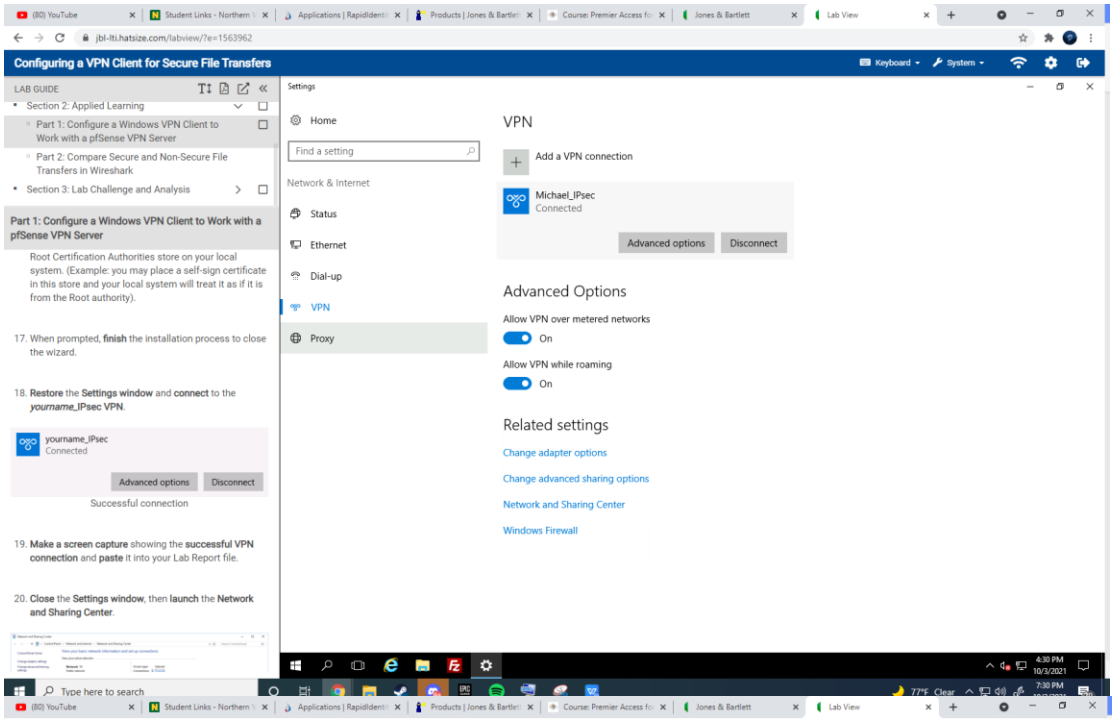

Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 2: Applied Learning
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
ESP in frame 10
44. In the frame summary pane, click frame 16.
Frame 16 is an unencrypted NetBios Name Service (NBNS) name query and occurs outside of the IPSec tunnel.
45. Make a screen capture showing the frame details pane for frame 16 and paste it into your Lab Report file.
46. In the frame summary pane, click frame 47.
Frames 47-67 continue the secure IPSec exchange between 172.30.0.2 and 172.30.0.100 using the occasional Internet Group Management Protocol v3 (in frames 48, 49, 51, 64, and 66), Link Local Multicast
ipsec-capture.pcapng
Frame 16: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Encapsulation type: Ethernet (1)
Arrival Time: Mar 5, 2014 14:41:20.172477000 Pacific Standard Time
Epoch Time: 1394059280.172477000 seconds
Type here to search

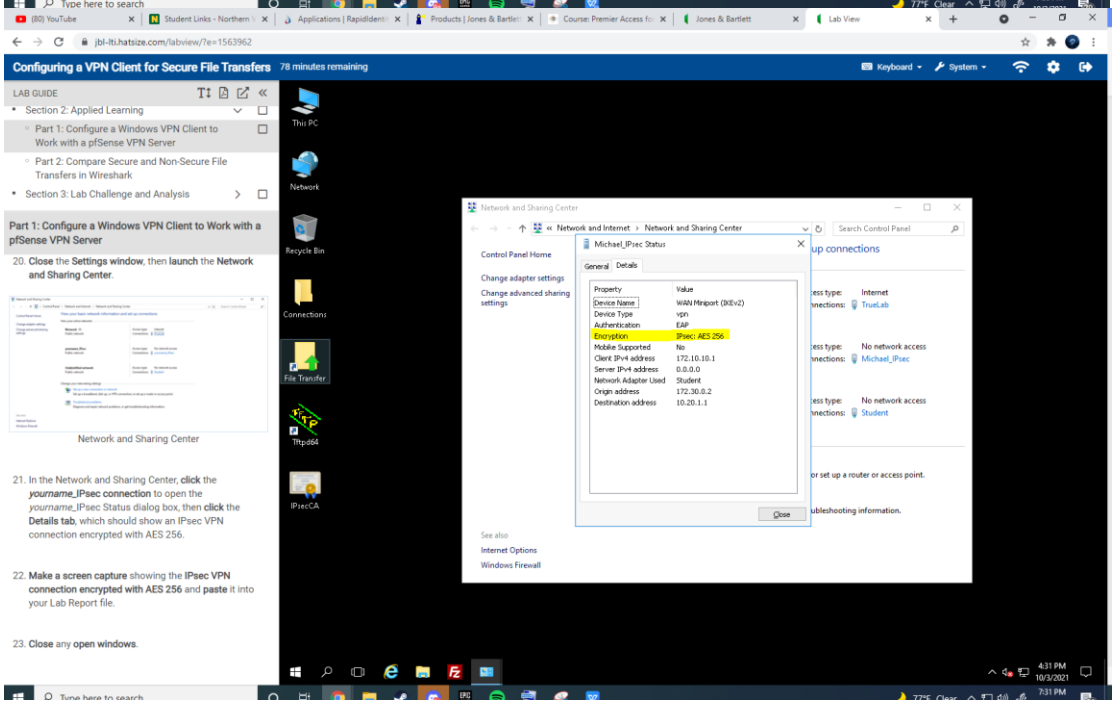

Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 2: Applied Learning
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
However, you may notice that Wireshark shows brackets on the left-hand margin that begin with frame 253. Just as establishing an IPSec tunnel begins with the ISAKMP exchange, then switches to the ESP protocol for the data transfer, an SSH transfer actually begins with a three-way handshake using TCP (frames 253-255). If you revisit the ssh-capture.pcapng file without the ssh filter, you will see the same TCP frames before the first SSHv2 frame.
48. In the Filter box, type ssh and press Enter to create a new filter that will display only the SSHv2 packets related to the SSH file transfer.
Use what you learned from reviewing the ssh-capture.pcapng file to identify the different steps of the SSH transfer, including Server/Client identification, Key Exchange initialization, and the actual file transfer.
49. In the frame summary pane, click the last SSHv2 frame in the SSH file transfer.
50. Make a screen capture showing the last SSHv2 frame in the SSH file transfer and paste it into your Lab Report file.
ipsec-capture.pcapng
SSH Protocol
SSH Version 2 (encryption:aes256-ctr mac:hmac-sha1 compression:none)
Type here to search

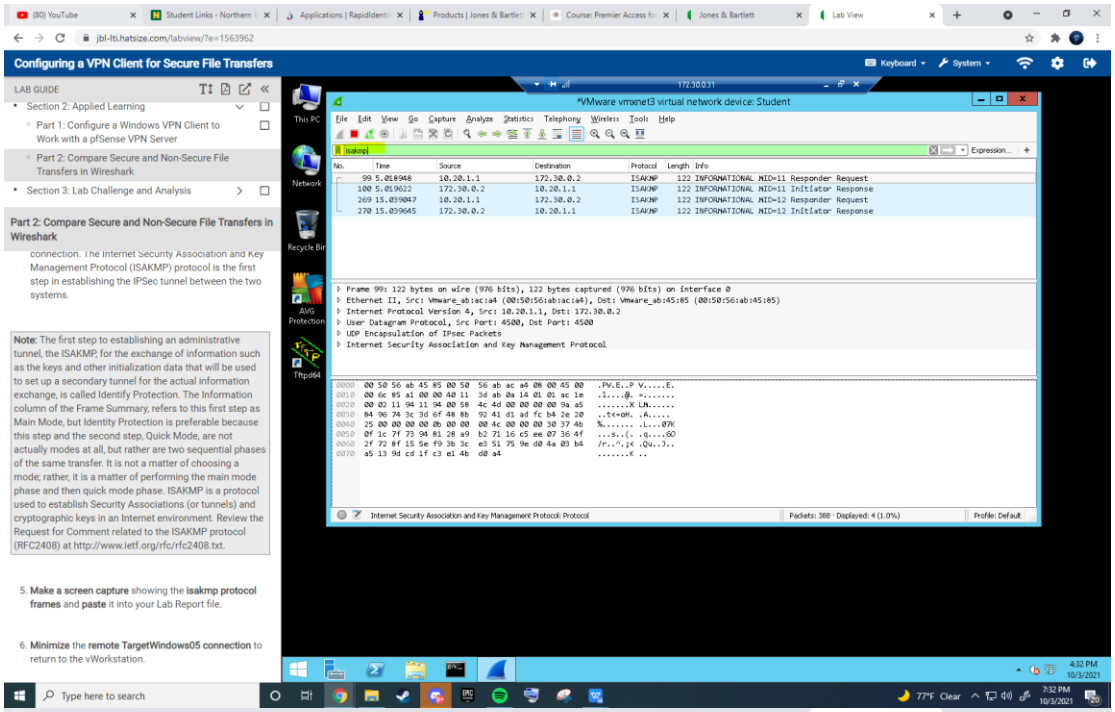

Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 2: Applied Learning
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
IPSec tunnel; otherwise, it would not be possible to see the details of the SSH interaction between the two machines because the SSH protocol transactions would be encrypted within the ESP frames. The ESP frames between these two machines were carrying other traffic than SSH. What traffic? Without the keys or access to the machines (such as screen shots, key loggers, or possibly log entries), it would be impossible to say, but there are other types of analysis, such as traffic analysis, that could reveal more about the exchange.
51. In the Filter box, highlight the ssh text, then type esp and press Enter to create a new filter that will display only those packets related to the ESP exchanges over the IPsec VPN tunnel.
52. Make a screen capture showing the last frames in the ESP exchange and paste it into your Lab Report file.
53. From the Wireshark menu, click File and select Quit to close Wireshark.
Note: This completes Section 1 of this lab. There are no deliverable files for this section.
ipsec-capture.pcapng
Type here to search

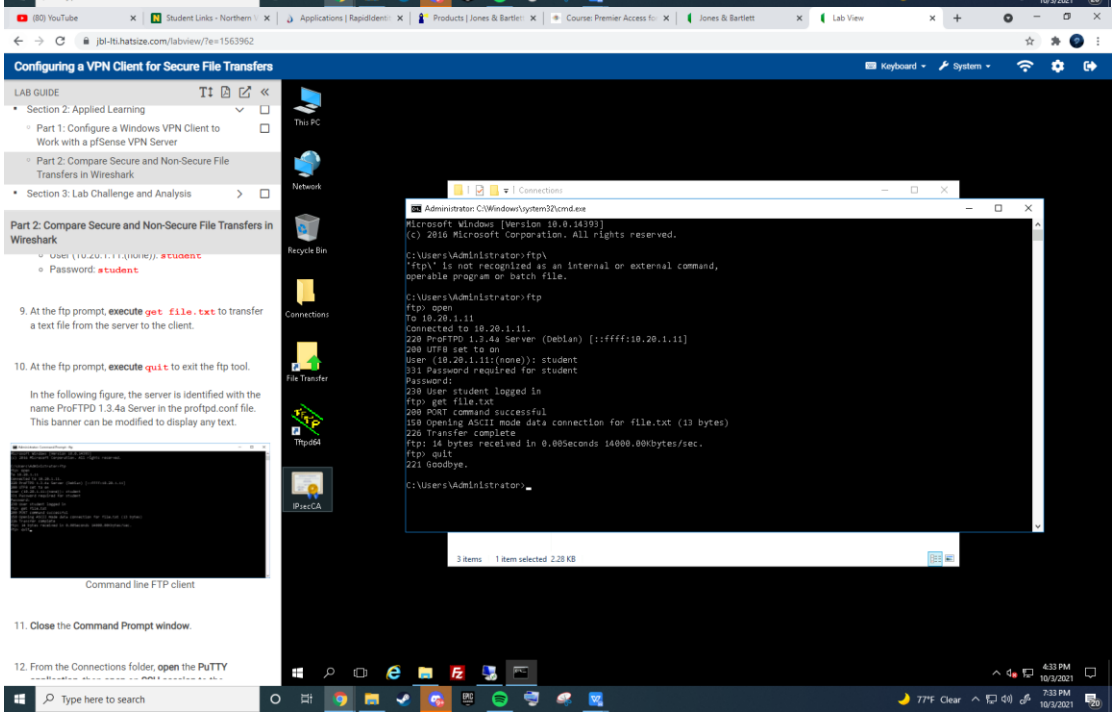
Section 2

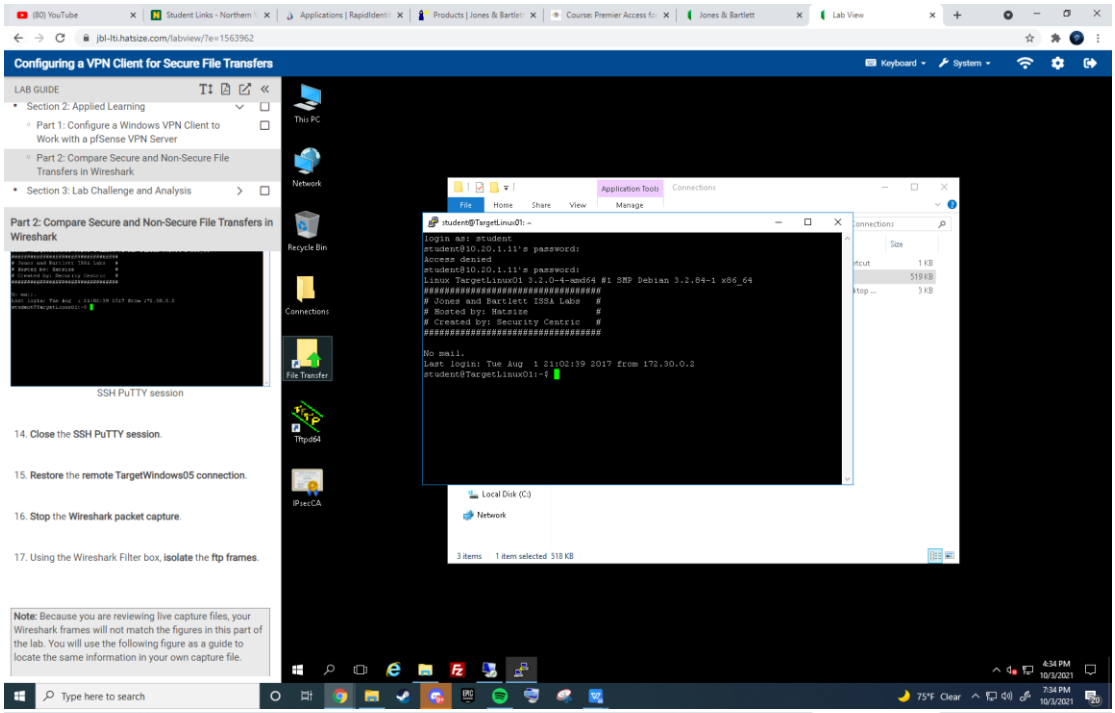

Configuring a VPN Client for Secure File Transfers
79 minutes remaining
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Add connection
3. At the command prompt, execute Add-VpnConnectionRoute -ConnectionName "yourname_IPsec" -DestinationPrefix 10.20.1.0/24 -PassThru, replacing yourname with your own name to add the route to the connecting network.
The ConnectionName parameter must match the Add-VpnConnection –Name parameter from Step 2. The system will display the connection profile.
Add connection route
4. Close the PowerShell window.
5. From the vWorkstation taskbar, open the yourname_IPsec connection profile.
Administrator: Windows PowerShell
IPsecCA
Type here to search

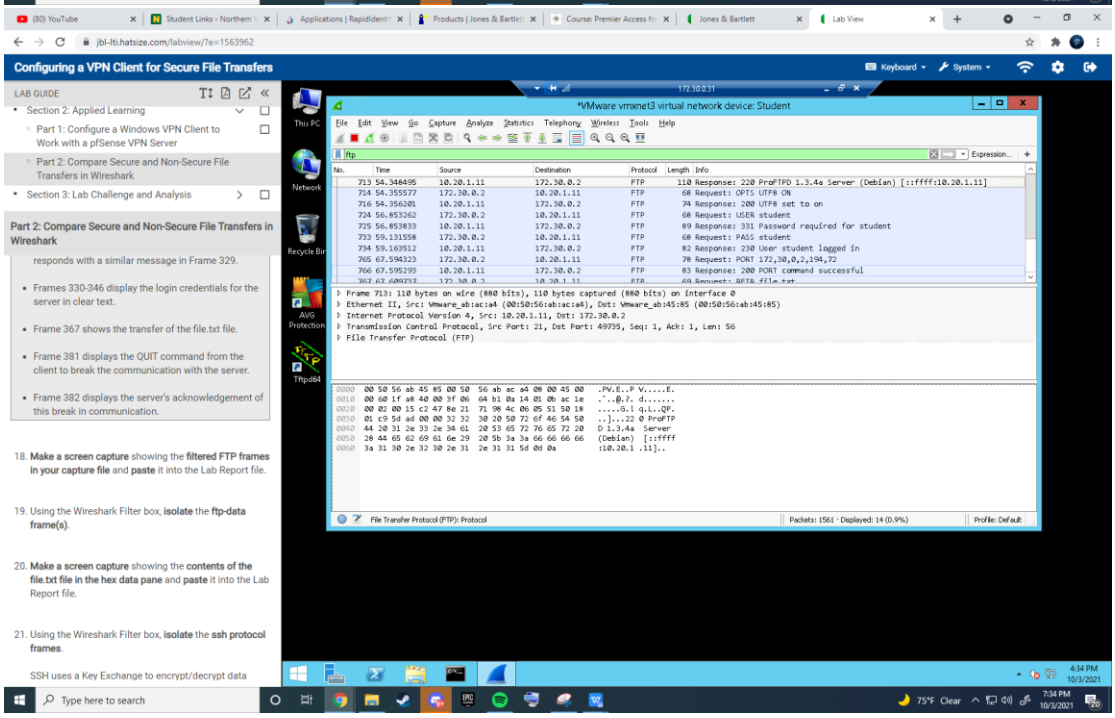

Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Root Certification Authorities store on your local system. (Example: you may place a self-sign certificate in this store and your local system will treat it as if it is from the Root authority).
17. When prompted, finish the installation process to close the wizard.
18. Restore the Settings window and connect to the yourname_IPsec VPN.
yourname_IPsec
Connected
Advanced options
Disconnect
Successful connection
19. Make a screen capture showing the successful VPN connection and paste it into your Lab Report file.
20. Close the Settings window, then launch the Network and Sharing Center.
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
Add a VPN connection
Michael_IPsec
Connected
Advanced options
Disconnect
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings
Change adapter options
Change advanced sharing options
Network and Sharing Center
Windows Firewall

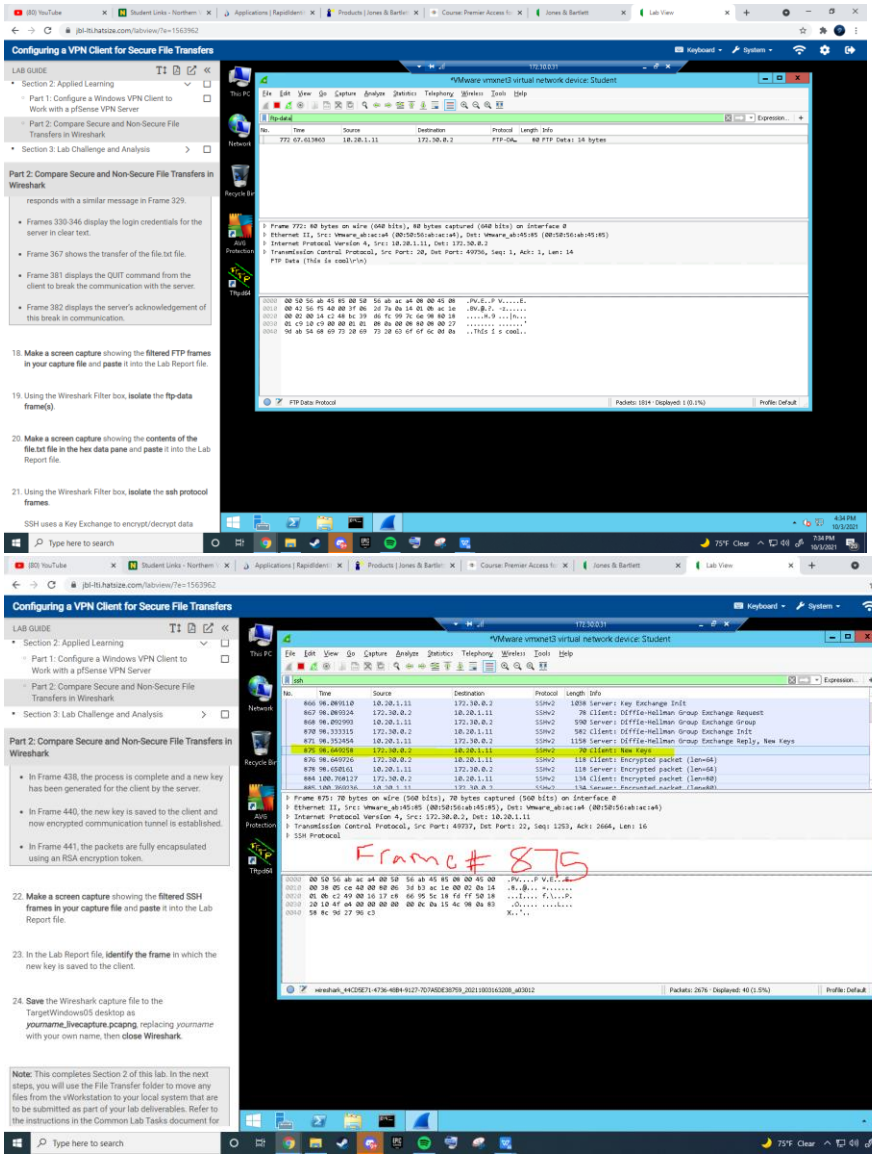

Configuring a VPN Client for Secure File Transfers
78 minutes remaining
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
20. Close the Settings window, then launch the Network and Sharing Center.
Network and Sharing Center
21. In the Network and Sharing Center, click the yourname_IPsec connection to open the yourname_IPsec Status dialog box, then click the Details tab, which should show an IPsec VPN connection encrypted with AES 256.
22. Make a screen capture showing the IPsec VPN connection encrypted with AES 256 and paste it into your Lab Report file.
23. Close any open windows.
This PC
Network
Recycle Bin
Connections
File Transfer
Tftpd64
IPsecCA
Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Michael_IPsec Status
General
Details
Property
Value
Device Name
WAN Miniport (IKEv2)
Device Type
vpn
Authentication
EAP
Encryption
IPsec: AES 256
Mobile Supported
No
Client IPv4 address
172.10.10.1
Server IPv4 address
0.0.0.0
Network Adapter Used
Student
Origin address
172.30.0.2
Destination address
10.20.1.1
Close
See also
Internet Options
Windows Firewall


Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
*VMware vmxnet3 virtual network device: Student
isakmp
No. Time Source Destination Protocol Length Info
99 5.016948 10.20.1.1 172.30.0.2 ISAKMP 122 INFORMATIONAL MID=11 Responder Request
100 5.019622 172.30.0.2 10.20.1.1 ISAKMP 122 INFORMATIONAL MID=11 Initiator Response
269 15.039047 10.20.1.1 172.30.0.2 ISAKMP 122 INFORMATIONAL MID=12 Responder Request
270 15.039645 172.30.0.2 10.20.1.1 ISAKMP 122 INFORMATIONAL MID=12 Initiator Response
Frame 99: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
Ethernet II, Src: Vmware_ab:ac:a4 (00:50:56:ab:ac:a4), Dst: Vmware_ab:45:85 (00:50:56:ab:45:85)
Internet Protocol Version 4, Src: 10.20.1.1, Dst: 172.30.0.2
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Internet Security Association and Key Management Protocol
Internet Security Association and Key Management Protocol: Protocol
Packets: 388 · Displayed: 4 (1.0%)
Profile: Default
connection. The Internet Security Association and Key Management Protocol (ISAKMP) protocol is the first step in establishing the IPSec tunnel between the two systems.
Note: The first step to establishing an administrative tunnel, the ISAKMP, for the exchange of information such as the keys and other initialization data that will be used to set up a secondary tunnel for the actual information exchange, is called Identify Protection. The Information column of the Frame Summary, refers to this first step as Main Mode, but Identity Protection is preferable because this step and the second step, Quick Mode, are not actually modes at all, but rather are two sequential phases of the same transfer. It is not a matter of choosing a mode; rather, it is a matter of performing the main mode phase and then quick mode phase. ISAKMP is a protocol used to establish Security Associations (or tunnels) and cryptographic keys in an Internet environment. Review the Request for Comment related to the ISAKMP protocol (RFC2408) at http://www.ietf.org/rfc/rfc2408.txt.
5. Make a screen capture showing the isakmp protocol frames and paste it into your Lab Report file.
6. Minimize the remote TargetWindows05 connection to return to the vWorkstation.


Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Password: student
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ftp\
'ftp\' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>ftp
ftp> open
To 10.20.1.11
Connected to 10.20.1.11.
220 ProFTPD 1.3.4a Server (Debian) [::ffff:10.20.1.11]
200 UTF8 set to on
User (10.20.1.11:(none)): student
331 Password required for student
Password:
230 User student logged in
ftp> get file.txt
200 PORT command successful
150 Opening ASCII mode data connection for file.txt (13 bytes)
226 Transfer complete
ftp: 14 bytes received in 0.00Seconds 14000.00Kbytes/sec.
ftp> quit
221 Goodbye.
C:\Users\Administrator>
3 items 1 item selected 2.28 KB
9. At the ftp prompt, execute get file.txt to transfer a text file from the server to the client.
10. At the ftp prompt, execute quit to exit the ftp tool.
In the following figure, the server is identified with the name ProFTPD 1.3.4a Server in the proftpd.conf file. This banner can be modified to display any text.
Command line FTP client
11. Close the Command Prompt window.
12. From the Connections folder, open the PuTTY


Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
SSH PuTTY session
14. Close the SSH PuTTY session.
15. Restore the remote TargetWindows05 connection.
16. Stop the Wireshark packet capture.
17. Using the Wireshark Filter box, isolate the ftp frames.
Note: Because you are reviewing live capture files, your Wireshark frames will not match the figures in this part of the lab. You will use the following figure as a guide to locate the same information in your own capture file.
student@TargetLinux01: ~
login as: student
student@10.20.1.11's password:
Access denied
student@10.20.1.11's password:
Linux TargetLinux01 3.2.0-4-amd64 #1 SMP Debian 3.2.84-1 x86_64
Jones and Bartlett ISSA Labs
Hosted by: Hatsize
Created by: Security Centric
No mail.
Last login: Tue Aug 1 21:02:39 2017 from 172.30.0.2
student@TargetLinux01:~$
Type here to search


Configuring a VPN Client for Secure File Transfers
LAB GUIDE
Section 2: Applied Learning
Part 1: Configure a Windows VPN Client to Work with a pfSense VPN Server
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
Section 3: Lab Challenge and Analysis
Part 2: Compare Secure and Non-Secure File Transfers in Wireshark
responds with a similar message in Frame 329.
Frames 330-346 display the login credentials for the server in clear text.
Frame 367 shows the transfer of the file.txt file.
Frame 381 displays the QUIT command from the client to break the communication with the server.
Frame 382 displays the server's acknowledgement of this break in communication.
18. Make a screen capture showing the filtered FTP frames in your capture file and paste it into the Lab Report file.
19. Using the Wireshark Filter box, isolate the ftp-data frame(s).
20. Make a screen capture showing the contents of the file.txt file in the hex data pane and paste it into the Lab Report file.
21. Using the Wireshark Filter box, isolate the ssh protocol frames.
SSH uses a Key Exchange to encrypt/decrypt data
*VMware vmxnet3 virtual network device: Student
ftp
Frame 713: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Vmware_ab:ac:a4 (00:50:56:ab:ac:a4), Dst: Vmware_ab:45:85 (00:50:56:ab:45:85)
Internet Protocol Version 4, Src: 10.20.1.11, Dst: 172.30.0.2
Transmission Control Protocol, Src Port: 21, Dst Port: 49735, Seq: 1, Ack: 1, Len: 56
File Transfer Protocol (FTP)
Type here to search



1. Some benefits of deploying a VPN would be to have a secure connection, and overall just to be safe. Also another benefit, you can access another network from home.\

2.