Implementing VPNs

Eli Chang

MSSA Cohort #2

Lab Summary

2/24/2020

Implementing VPNs

After the DirectAccess Deployment, some computers could not connect to the internal network so that the administrators have to deploy a VPN solution. Some users do not have compatible operating systems; others are not members of the domain. The Virtual Private Network provides secure access to the internal network for external clients using the Internet. In the lab, after implementing the VPN solution, the admins validate and troubleshoot the deployment.

Types of VPNs

There are different types of site-to-site VPNs: PPTP, L2TP, IKEv2, and SSTP. The Point-to-Point Tunneling Protocol enables to encrypt and encapsulate traffic in an IP header. It uses TCP port 1723 and provides data confidentiality but does not have data integrity and authentication. This type is the least secure option for a VPN. The Layer-2 Tunneling Protocol encrypts multiprotocol traffic using a combination of PPTP and Layer 2 Forwarding. Unlike PPTP, L2TP uses IPsec to encrypt datagrams. Sometimes, it can be blocked by firewalls. The Secure Socket Tunneling Protocol uses HTTPS protocol over TCP port 443. It encapsulates PPP traffic with the SSL channel. Lastly, IKEv2 supports the latest IPsec encryption algorithm and uses the UDP port 500, unlike the other types. In the lab, the last two options are used because the two types are more stable than the different two types. Since it is the company-level network, the admins should reduce the possibilities against threats.

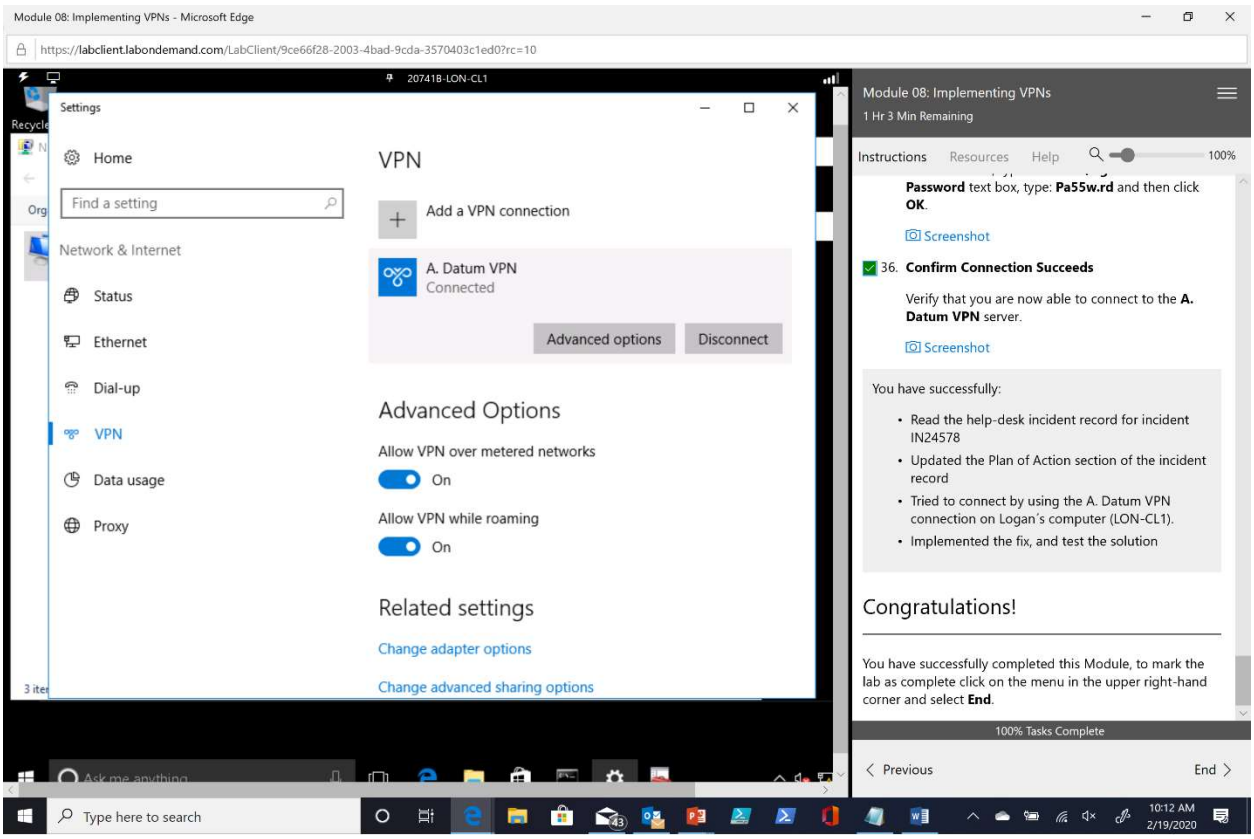
Authentication Protocol

Mainly, Extensible Authentication Protocol (EAP) is chosen in the lab along with the Microsoft Challenge Handshake Authentication Protocol version 2. The options are Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), MS-

CHAPv2, and EAP. As the name refers, PAP uses plaintext passwords so that it has the least secure authentication protocol. CHAP is more reliable than PAP by challenging responses over the passwords. MS-CHAPv2 is the upgrade version of CHAP and provides two-way authentication so that it can establish stronger security. EAP offers the most reliable security by the arbitrary authentication mechanism, which means it provides authentication variations. Since EAP and MS-CHAPv2 provide the strongest security, the admins in the lab decided to use these two authentication options.

Configure a VPN Connection

On the client computer, LON-CL1, the VPN connection is established as PPTP even though the connection to the VPN server is using more secure connections, such as L2TP, IKEv2, or SSTP. Unfortunately, the client computer did not have the certificate so that the L2TP and IKEv2 could not be used. If the capability issues arise, then it should use MS-CHAPv2 and PEAP. Even the least secure option, PPTP, is chosen, it is with the CHAPv2 authentication.


Module 08: Implementing VPNs - Microsoft Edge
https://labclient.labondemand.com/LabClient/9ce66f28-2003-4bad-9cda-3570403c1ed0?rc=10
20741B-LON-CL1
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Data usage
Proxy
VPN
Add a VPN connection
A. Datum VPN
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
Module 08: Implementing VPNs
1 Hr 3 Min Remaining
Instructions
Resources
Help
100%
Password text box, type: Pa55w.rd and then click OK.
Screenshot
36. Confirm Connection Succeeds
Verify that you are now able to connect to the A. Datum VPN server.
Screenshot
You have successfully:
Read the help-desk incident record for incident IN24578
Updated the Plan of Action section of the incident record
Tried to connect by using the A. Datum VPN connection on Logan's computer (LON-CL1).
Implemented the fix, and test the solution
Congratulations!
You have successfully completed this Module, to mark the lab as complete click on the menu in the upper right-hand corner and select End.
100% Tasks Complete
Previous
End
Type here to search
10:12 AM
2/19/2020