Implementing VPNs

Eli Chang

MSSA Cohort #2

Diagram Exercise 8

2/24/2020

Implementing VPNs

The three client computers should connect to the private network across the public network because they cannot be connected with the DirectAccess due to the incompatibility of the operating systems. The client computers are in the same organization so that there is one router with the same gateway IP address. SSTP and IKEv2 are the options to choose for stable security. The firewall access is going to be TCP port 443 for SSTP and UDP port 500 for IKEv2. The authentication options are PAP, CHAP, CHAPv2, and EAP. The first option is EAP because it has the strongest security, among other options. Since it uses IKEv2, the VPN Reconnect would provide consistent VPN connectivity. However, it is usually compatible with the newer devices so that PPTP with CHAPv2 could be used for the security issue. Even the IKEv2 option is selected along with SSTP; the SSTP would be usually used in the VPN environment because it is easier and faster to use from the external users.

Legend		
Symbol	Count	Description
	2	Router/ Gateway
	1	DC/NPS
	1	VPN
	2	DHCP/DNS
	1	Database server
	1	Firewall
	3	External users
	6	Internal users

DC/NPS   Database

DHCP   DNS

131.107.0.100

VPN server
SSTP/IKEv2

131.107.0.20

131.107.0.21   131.107.0.22   131.107.0.23