CLIENTLESS SSL VPN CONFIGURATION

Configuring SSL (Secure Sockets Layer) virtual private network (VPN). The purpose is for some employee to have access to organization data remotely without the appearance on premises. Configuring SSL VPN will give them secure access to access the organization server. SSL will verify and encrypt the data between the clients and the servers, it is use to have provide high security communication between web brewers, server and the client.

This LAB will be done using two department server, a firewall, two switches and two employee devices to connect remotely. The firewall (5505) will be placed between the two switches (2960), one switch will connect to the server and the second switch will connect to the remote users. The switch that will connect between firewall and server will be the incoming switch while the second switch will be the outgoing and will connect the employee devices to the firewall. IP will be given to the servers and devices statically.

Starting the configuration: (FIREWALL)

en

IT will ask password, just double click

conf t

int vlan 1

ip add 192.168.1.1 255.255.255.0

no shutdown

exit

int vlan 2

ip add 192.168.2.1 255.255.255.0

#no shutdown

exit

When need to do a bookmark manager for the two dep servers, click on config at the top and click bookmark manager on the left side

UAT dep URL: https://192.168.1.10

Production dep URL: https://192.168.1.20

Go back to CLI interface to create login and pass for the two employee. You can use any username and password of your choice

username qa1 password qa123

username dev1 password dev123

exit

We have to add the employees to USER MANAGER, go to config and click user manager

“Select the user name dev1, bookmark prod, profile name (Vpnpro1) and policy group (Vpnp1) you can put anything of your choice then click on set”

“Do the same for qa1” bookmark UAT, profile name (Vpnpro1) and policy group (Vpnp2) you can put anything of your choice then click on set”

Go back to CLI interface to enable the VPN

webvpn

enable outside

exit

TO Check VPN Status

sh run

On each devices, go to web browser, put in the firewall port link https://192.168.2.1

QA Engineer

Username: qa1

Password: qa123

Developer

Username: dev1

Password: dev123

The username and password will be the ones you used when you configured the firewall.

NOTE: Port numbers in this Lab are the numbers of port we connected our cables, this can be different in your situation if you connect your cables to a different port. Therefore you have to use the port numbers during the configuration.