SECU420-A

Network Security

Final Project

Config Firewall Scenario

Fall 2023-2024

Report By:

Ahmad Shaito(1121044)

Report Date:27/12/2023

\*Define and configure the Firewall physical ports (LAN, WAN and DMZ)

***//First we will start the configuration to the HQ Firewall***

***//Configure the interface that connected to the DMZ Area***

config system interface

**//to enter the configuration of the interfaces in firewall**

edit “port 1” (f0/1)

**//to enter the configuration of Port 1**

set ip 10.10.10.254 255.255.255.0

**//set ip address for this port with the subnet**

set monitor-bandwidth enable

**//enable the interface to collect bandwidth information**

set role dmz

**//defining it role within the network architecture. It enables customization of default settings and security policies tailored to the intended use of the interface**

Next

**//exit port 1 configuration mode**

***//Configuration of the interface that connected to the DMZ Area Finished***

***//Configure the interface that connected to the LAN Area***

edit “port 2” (f0/2)

**//to enter the configuration of Port 2**

set ip 192.168.1.254 255.255.255.0

**//set ip address for this port with the subnet**

set role lan

**//defining it role within the network architecture. It enables customization of default settings and security policies tailored to the intended use of the interface**

set monitor-bandwidth enable

**//enable the interface to collect bandwidth information**

Next

**//exit port 2 configuration mode**

***//Configuration of the interface that connected to the LAN Area Finished***

***//Configure the interface that connected to the Wan Area***

edit “port 3” (f0/3)

**//to enter the configuration of Port 2**

set ip 80.81.152.34 255.255.255.0

**//set ip address for this port with the subnet**

set monitor-bandwidth enable

**//enable the interface to collect bandwidth information**

set role wan

**//defining it role within the network architecture. It enables customization of default settings and security policies tailored to the intended use of the interface**

Next

**//exit port 3 configuration mode**

***//Configuration of the interface that connected to the WAN Area Finished***

End

**//exit interfaces configuration mode**

***//Now we will start the configuration to the branch Firewall***

***//Configure the interface that connected to the LAN Area***

edit “port 1” (f0/1)

**//to enter the configuration of Port 1**

set ip 192.168.2.254 255.255.255.0

**//set ip address for this port with the subnet**

set role lan

**//defining it role within the network architecture. It enables customization of default settings and security policies tailored to the intended use of the interface**

set monitor-bandwidth enable

**//enable the interface to collect bandwidth information**

Next

**//exit port 2 configuration mode**

***//Configuration of the interface that connected to the LAN Area Finished***

***//Configure the interface that connected to the Wan Area***

edit “port 2” (f0/2)

**//to enter the configuration of Port 2**

set ip 194.51.52.3 255.255.255.0

**//set ip address for this port with the subnet**

set monitor-bandwidth enable

**//enable the interface to collect bandwidth information**

set role wan

**//defining it role within the network architecture. It enables customization of default settings and security policies tailored to the intended use of the interface**

Next

**//exit port 3 configuration mode**

***//Configuration of the interface that connected to the WAN Area Finished***

End

**//exit interfaces configuration mode**

\*Create the required Firewall objects (IP, subnets...)

***//Create Lan Objects***

***//Create Lan Interface Object***

config firewall address

**//to enter the Addresses in Policy & Objects in Firewall**

edit “Lan Interface”

**//to enter the configuration of this Object**

set subnet 192.168.1.254 255.255.255.255

**//to Set the Ip address of the Lan Interface**

Next

**//to Exit this Object Configuration**

***//Create Lan Subnet Object***

edit “Lan Subnet”

**//to enter the configuration of this Object**

set subnet 192.168.1.0 255.255.255.0

**//to Set the Range of Ip addresses of the Lan Subnet**

Next

**//to Exit this Object Configuration**

***//Create Lan Objects Finished***

***//Create Wan Objects***

***//Create Wan Interface Object***

edit “Wan Interface”

**//to enter the configuration of this Object**

set subnet 80.81.153.34 255.255.255.255

**//to Set the Ip address of the Wan Interface**

Next

**//to Exit this Object Configuration**

edit “Wan Subnet”

**//to enter the configuration of this Object**

set subnet 0.0.0.0 0.0.0.0

**//to Set the Range of Ip addresses of the Wan Subnet**

Next

**//to Exit this Object Configuration**

***//Create Wan Objects Finished***

***//Create DMZ Objects***

***//Create DMZ Interface Object***

edit “DMZ Interface”

**//to enter the configuration of this Object**

set subnet 10.10.10.254 255.255.255.255

**//to Set the Ip address of the DMZ Interface**

Next

**//to Exit this Object Configuration**

edit “DMZ Subnet”

**//to enter the configuration of this Object**

set subnet 10.10.10.0 255.255.255.0

**//to Set the Range of Ip addresses of the DMZ Subnet**

Next

***//Create DMZ Objects Finished***

**//to Exit this Object Configuration**

End

**//to Exit Addresses in Policy & Objects in Firewall**

***Note : Now we Move to the Branch Firewall to add some objects in it***

***Branch FireWall:***

***//Create Lan Objects***

***//Create Branch Interface Object***

config firewall address

**//to enter the Addresses in Policy & Objects in Firewall**

edit “Branch Interface”

**//to enter the configuration of this Object**

set subnet 192.168.2.254 255.255.255.255

**//to Set the Ip address of the Branch Interface**

Next

**//to Exit this Object Configuration**

***//Create Branch Subnet Object***

edit “Branch Subnet”

**//to enter the configuration of this Object**

set subnet 192.168.2.0 255.255.255.0

**//to Set the Range of Ip addresses of the Branch Subnet**

Next

**//to Exit this Object Configuration**

***//Create Wan Objects***

edit “Wan2 Interface”

**//to enter the configuration of this Object**

set subnet 194.51.52.3 255.255.255.255

**//to Set the Ip address of the Wan2 Interface**

Next

**//to Exit this Object Configuration**

***//Create Wan Subnet Object***

edit “Wan2 Subnet”

**//to enter the configuration of this Object**

set subnet 0.0.0.0 0.0.0.0

**//to Set the Range of Ip addresses of the Wan2 Subnet**

Next

**//to Exit this Object Configuration**

End

**//to Exit Addresses in Policy & Objects in Firewall**

\*Create the required routes so internal users in both sites are able to reach the internet

**//Enable the Lan to connect to the Wan in HQ**

config firewall address

**//to enter the Firewall Policy in Policy & Objects in Firewall**

edit 2

**//to enter and configure the Second policy**

set srcintf “Lan Interface”

**//to specify that the “Lan Interface” Object is the source interface**

set dstintf “Wan Interface”

**//to specify that the “Wan Interface” Object is the Destination interface**

set srcaddr “Lan Subnet”

**//to specify that the “Lan Subnet” Object is the source subnet**

set srcaddr “Wan Subnet”

**//to specify that the “Wan Subnet” Object is the destination subnet**

set action accept

**//this command allows the firewall to permit all traffic originating from the source to reach its destination**

set nat enable

**//this command enables the firewall to perform Network Address Translation(Nat), allowing the private IPs of our Lan Network to be translated to Public ones, enabling online connectivity.**

set webfilter-profile “No Social media and Social networking”

**//block access to Social media and Social network sites**

set service “ALL”

**//allow all the protocols**

Next

**//to Exit the configuration of the first policy**

**//Enable the Wan to connect to the DMZ**

edit 3

**//to enter and configure the Third policy**

set srcintf “Wan Interface”

**//to specify that the “Wan Interface” Object is the source Interface**

set dstintf “DMZ Interface”

**//to specify that the “DMZ Interface” Object is the destination Interface**

set srcaddr “Wan Subnet”

**//to specify that the “Wan Subnet” Object is the source subnet**

set dstaddr “DMZ Subnet”

**//to specify that the “DMZ Subnet” Object is the destination subnet**

set action accept

**//this command enables the firewall to permit all traffic originating from the source to reach its destination, provided it also passes the other rules**

set service HTTPS

**//it will allow only HTTPS traffic to pass through, while denying all other types of traffic**

set nat enable

**//this command enables the firewall to perform Network Address Translation(Nat), allowing the private IPs of our Lan Network to be translated to Public ones, enabling online connectivity.**

Next

**//to Exit the configuration of the Second policy**

**//Enable the Lan in HQ to connect to the DMZ**

edit 4

**//to enter and configure the Forth policy**

set srcintf “Lan Interface”

**//to specify that the “Lan Interface” Object is the source Interface**

set dstintf “DMZ Interface”

**//to specify that the “DMZ Interface” Object is the destination Interface**

set srcaddr “Lan Subnet”

**//to specify that the “Lan Subnet” Object is the source subnet**

set dstaddr “DMZ Subnet”

**//to specify that the “DMZ Subnet” Object is the destination subnet**

set action accept

**//this command enables the firewall to permit all traffic originating from the source to reach its destination, provided it also passes the other rules**

set service SMTP

**//it will allow only SMTP traffic to pass through, while denying all other types of traffic**

edit 5

**//Enable the Lan in Branch to connect to the DMZ**

**//to enter and configure the Fifth policy**

set srcintf “VPNBH Interface”

**//to specify that the “VPNBH Interface” Object is the source Interface**

set dstintf “DMZ Interface”

**//to specify that the “DMZ Interface” Object is the destination Interface**

set srcaddr “VPNBH Subnet”

**//to specify that the “VPNBH Subnet” Object is the source subnet**

set dstaddr “DMZ Subnet”

**//to specify that the “DMZ Subnet” Object is the destination subnet**

set action accept

**//this command enables the firewall to permit all traffic originating from the source to reach its destination, provided it also passes the other rules**

set service SMTP

**//it will allow only SMTP traffic to pass through, while denying all other types of traffic**

**//if the traffic didn’t pass through any rules so deny this connection**

edit 1

**//to enter and configure the First policy**

set srcintf any

**//any source ip**

set dstintf any

**//any destination ip**

set srcaddr 0.0.0.0

**//any source subnet**

set dstaddr 0.0.0.0

**//any destination subnet**

set action deny

**//connection deny**

Next

**//to Exit the configuration of the Second policy**

***//Enable the Lan to connect to the Wan in Branch:***

**//if the traffic didn’t pass through any rules so deny this connection**

edit 1

**//to enter and configure the First policy**

set srcintf any

**//any source ip**

set dstintf any

**//any destination ip**

set srcaddr 0.0.0.0

**//any source subnet**

set dstaddr 0.0.0.0

**//any destination subnet**

set action deny

**//connection deny**

Next

**//Enable the Lan to connect to the Wan in Branch**

edit 2

**//to enter and configure the Second policy**

set srcintf “branch Interface”

**//to specify that the “Lan Interface” Object is the source interface**

set dstintf “Wan2 Interface”

**//to specify that the “Wan Interface” Object is the Destination interface**

set srcaddr “branch Subnet”

**//to specify that the “Lan Subnet” Object is the source subnet**

set srcaddr “Wan2 Subnet”

**//to specify that the “Wan Subnet” Object is the destination subnet**

set action accept

**//this command allows the firewall to permit all traffic originating from the source to reach its destination**

set nat enable

**//this command enables the firewall to perform Network Address Translation(Nat), allowing the private IPs of our Lan Network to be translated to Public ones, enabling online connectivity.**

set webfilter-profile “No Social media and Social networking”

**//block access to Social media and Social network sites**

set service “ALL”

**//allow all the protocols**

**//Add the gateway route in HQ and in Branch**

/\*In The HQ Firewall :\*/

config router static

**//Enters the routing configuration mode**

edit 1

**//Enter the configuration for the first rule**

set gateway 80.81.152.34

**//Set the gateway of this Firewall**

set device “port 3”

**//Specify the port of the gateway in this Firewall**

next

**//Exit the configuration mode for the first rule**

End

**//Exit the routing configuration mode**

/\*In The Branch Firewall :\*/

config router static

**//Enters the routing configuration mode**

edit 1

**//Enter the configuration for the first rule**

set gateway 194.51.52.3

**//Set the gateway of this Firewall**

set device “port 2”

**//Specify the port of the gateway in this Firewall**

next

**//Exit the configuration mode for the first rule**

End

**//Exit the routing configuration mode**

\*Add the appropriate security profiles (IPS / AV ..)

For Anti Virus:(config for HQ and Branch FW)

config antivirus profile

**// to enter the configuration of the antivirus in firewall**

edit "AV-Monitor"

**//select the AntiVirus Profile that named “**AV-Monitor**” for configuration**

config http

**//its specifies that the following settings apply to http traffic specifically.**

set av-scan monitor

**// it will enable the antivirus to scan the http traffic for viruses and threats (static scan {search for any known IOCs})**

set fortisandbox monitor

**//provide advanced threat detection and analysis (dynamic analysis) by examining suspicious files or content in a separate, isolated environment {Sandbox}**

End

**// it will end the config for http**

config pop3

**//its specifies that the following settings apply to pop3 traffic specifically.**

set av-scan monitor

**// it will enable the antivirus to scan the pop3 traffic for viruses and threats (static scan {search for any known IOCs})**

set fortisandbox monitor

**//provide advanced threat detection and analysis (dynamic analysis) by examining suspicious files or content in a separate, isolated environment {Sandbox}**

set executables virus

**//treat any executable like .exe files or scripts as viruses**

End

**//end the config of pop3**

config smtp

**//its specifies that the following settings apply to smtp traffic specifically.**

set av-scan monitor

**// it will enable the antivirus to scan the smtp traffic for viruses and threats (static scan {search for any known IOC})**

set fortisandbox monitor

**//provide advanced threat detection and analysis (dynamic analysis) by examining suspicious files or content in a separate, isolated environment {Sandbox}**

set executables virus

**//treat any executable like .exe files or scripts as viruses directly**

End

**//end the config of smtp**

set outbreak-prevention-archive-scan enable

**//it will active scanning of the contents of any archive files like .zip .rar and the other ones that have been compressed**

**//Note : If the archive contains nested archives and the antivirus is configured to handle nested archives so it might continue to unpack and scan these nested archives up to a certain configured depth**

set external-blocklist-enable-all enable

**//enables the utilization of external blocklists within the firewall’s security policies to block or restrict traffic associated with know malicious IP addresses ,domain or URLs listed in these external sources**

Next

**//It will end the edit of the "AV-Monitor"**

End

**//it will end the config antivirus profile**

For IPS:(config for HQ and Branch FW)

config ips sensor

**//Enters the IPS sensor configuration mode**

edit “IPS url block”

**//select the IPS sensor named “IPS url block” for configuration**

set comment "Prevent critical attacks."

**//Add comments to this profile for clarity on its intended purpose, eliminating the need to analyze all the commands below for understanding**

config entries

**//Enter the configurations for the IPS URL block profile**

edit 1

**//In this command, we choose the first element in our table to establish a rule. If we wish to select the second row in this table, we would then enter “edit 2”**

set severity medium high critical

**//In this command, we specify that when the IPS detects any threat with a severity classified as medium, high, or critical, it will execute a default action. This means it won’t immediately block or allow all traffic but will refer back to its predefined table to determine the action for this specific severity. Additionally, it will generate alerts for any occurrence, even if the traffic is allowed**

Next

**// exit the selected row**

End

**Exit the configuration mode**

next

end

For WebFilter:(config for HQ and Branch FW)

config webfilter profile

**//Enters the WebFiltering configuration mode**

edit "No Social media and Social networking”

**//Enter or Create profile name : "No Social media and Social networking”**

set comment “Block Social Media and Social Networking”

**//Add comments to this profile for clarity on its intended purpose, eliminating the need to analyze all the commands below for understanding**

config ftgd-wf

**//Enter the (FortiGuard web filtering) configuration mode for this profile**

config filters

**//Enter to configurate the filters**

edit 1

**//Enter The First Filter**

set category 22(if 22 is for Social Media)

**//Select Social Media Category**

set action block

**//Block the selected Category**

Next

**//Exit the first Rule**

End

**//Exit the filters configuration mode**

End

**//Exit the configuration mode for this profile**

Next

**//Exit the profile**

end

**//Exit WebFiltering configuration mode**

\*Create an IPSec VPN tunnel between HQ and Branch and allow local subnets in each site to reach each others and branch users to reach DMZ servers

**//We suppose that we are using built in forinet\_Factory certificate and the Fortinet\_CA. CA certificate are used for authentication**

**Note : because we are using Forinet\_CA for authentication so the peer user must be configured based on Fortinet\_Ca so :**

**Configure Fw in HQ:**

config user peer

**//to enter vpn configuration mode**

edit "peer1”

**//to enter the configuration mode for the first peer**

set ca “Fortinet\_Ca”

**//to set the Certificate Authority that will we use to verify our certificate in our vpn connection**

Next

**//Exit the configuration mode for the first peer**

End

**//Exit the configuration mode of the vpn**

**Configure Fw in branch:**

config user peer

**//to enter vpn configuration mode**

edit "peer2”

**//to enter the configuration mode for the first peer**

set ca “Fortinet\_Ca”

**//to set the Certificate Authority that will we use to verify our certificate in our vpn connection**

Next

**//Exit the configuration mode for the first peer**

End

**//Exit the configuration mode of the vpn**

**Now we should Configure the IPsec Phase1-interface:**

**In this phase the establishment will be getting ready to enable IPsec VPN tunnel**

**Configure Fw in HQ:**

config vpn ipsec phase1-interface

**//Enter the configuration of the ipsec vpn phase 1**

edit "to\_Branch”

**//Enter or Create the interface named “to\_Branch”**

set interface “port3”

**//set the interface to the port 3**

set authmethod signature

**//set the authentication method used as a signature**

set net-device enable

**//it enables the vpn tunnel to communicate or interact with specified network devices, allowing traffic to pass through these devices as part of the vpn connectivity setup**

set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1

**//it proposed algorithms dictate the negotiation process between VPN peers to establish a secure phase 1 connection**

set remote-gw “Wan2 Interface”

**//it will set the remote gateway interface the one In the other site**

set certificate “test1”

**// the certificate used in this connection**

set peer “peer1”

**// we define a remote vpn peer named peer 1**

Next

**// it will exit the configuration of the interface named “to\_Branch”**

End

**//Exit the configuration of the ipsec vpn phase 1**

**Configure Fw in branch:**

config vpn ipsec phase1-interface

**//Enter the configuration of the ipsec vpn phase 1**

edit "to\_HQ”

**//Enter or Create the interface named “to\_HQ”**

set interface “port2”

**//set the interface to the port 2**

set authmethod signature

**//set the authentication method used as a signature**

set net-device enable

**//it enables the vpn tunnel to communicate or interact with specified network devices, allowing traffic to pass through these devices as part of the vpn connectivity setup**

set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1

**//it proposed algorithms dictate the negotiation process between VPN peers to establish a secure phase 1 connection**

set remote-gw “Wan Interface”

**//it will set the remote gateway interface the one In the other site**

set certificate “test2”

**// the certificate used in this connection**

set peer “peer2”

**// we define another remote vpn peer named peer 2**

next

**// it will exit the configuration of the interface named “to\_Branch”**

End

**//Exit the configuration of the ipsec vpn phase 1**

**Now we should Configure the IPsec Phase2-interface:**

**In this phase the primarily focus is securing and encrypting the actual data transmission within the established tunnel**

**Configure Fw in HQ:**

Config vpn ipsec phase2-interface

**//Enter the configuration of the ipsec vpn phase 2**

edit "to\_Branch”

**//Enter or Create the interface named “to\_Branch”**

set phase1name “to\_Branch”

**//to assigns a specific identifier to the Phase 1 settings**

set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305

**//it proposed algorithms dictate the negotiation process between VPN peers to establish a secure phase 1 connection**

set auto-negotiate enable

**//it enable automatic negotiation of VPN parameters or settings between VPN peers during the initiation of the VPN tunnel**

Next

**// it will exit the configuration of the interface named “to\_Branch”**

End

**//Exit the configuration of the ipsec vpn phase 1**

**Configure Fw in Branch:**

Config vpn ipsec phase2-interface

**//Enter the configuration of the ipsec vpn phase 2**

edit "to\_HQ”

**//Enter or Create the interface named “to\_HQ”**

set phase1name “to\_HQ”

**//to assigns a specific identifier to the Phase 1 settings**

set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305

**//it proposed algorithms dictate the negotiation process between VPN peers to establish a secure phase 1 connection**

set auto-negotiate enable

**//it enable automatic negotiation of VPN parameters or settings between VPN peers during the initiation of the VPN tunnel**

Next

**// it will exit the configuration of the interface named “to\_Branch”**

End

**//Exit the configuration of the ipsec vpn phase 1**

**Now we will configure two static routes to be able to reach the remote protected subnet**

**Configure Fw in HQ:**

Config router static

**//Enter the configuration of the routing table**

edit 2

**//Enter the second row to configuration in routing table**

set dst 192.168.2.0 255.255.255.0

**//destination subnet for the subnet in the other site**

set device “to\_Branch”

**//name of this configuration**

Next

**//Exit the configuration mode of the second in routing table**

End

**//Exit the configuration of the routing table**

**The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down**

set dst 192.168.2.0 255.255.255.0

set blackhole enable

set distance 254

next

**//Exit the configuration mode of the second in routing table**

End

**//Exit the configuration of the routing table**

**Configure Fw in Branch:**

Config router static

**//Enter the configuration of the routing table**

edit 2

**//Enter the second row to configuration in routing table**

set dst 192.168.1.0 255.255.255.0

**//destination subnet for the subnet in the other site**

set device “to\_HQ”

**//name of this configuration**

Next

**//Exit the configuration mode of the second in routing table**

End

**The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down**

set dst 192.168.1.0 255.255.255.0

set blackhole enable

set distance 254

next

end

**Now we will configure two firewall policies to allow bidirectional IPsec traffic flow over the IPsec VPN tunnel**

**Configure Fw in HQ:**

Config firewall policy

**//Enter the configuration of the firewall Policies**

edit 1

**//Edit the first policy**

set name “inbound”

**//Set the name of this policy to “Inbound”**

set srcintf “to\_Branch”

**//Set the source interface to the object name to\_Branch**

set dstintf “Lan Interface”

**//Set the destination interface to the object name “Lan Interface”**

set srcaddr “192.168.2.0 255.255.255.0”

**//Set the source subnet to this subnet Ip**

set dstaddr “Lan Subnet”

**//Set the destination subnet to this subnet Object named “Lan Subnet”**

set action accept

**//Enable all the traffic that pass other rules**

set service “ALL”

**//there is no restrictions in any protocol all the protocols are allowed if they pass other rules**

Next

**//Exit the configuration mode of the first policy**

edit 2

**//Edit the Second policy**

set name “outbound”

**//Set the name of this policy to “outbound”**

set srcintf “Lan Interface”

**//Set the source interface to the object name “Lan Interface”**

set dstintf “to\_Branch”

**//Set the destination interface to the object name to\_Branch**

set srcaddr “Lan Subnet”

**//Set the source subnet to this subnet Object named “Lan Subnet”**

set dstaddr “192.168.2.0”

**//Set the destination subnet to this subnet**

set action accept

**//Enable all the traffic that pass other rules**

set service “ALL”

**//there is no restrictions in any protocol all the protocols are allowed if they pass other rules**

Next

**//Exit the configuration mode of the Second policy**

end

**//Exit the configuration mode of the Policies in the Firewall**

**Configure Fw in Branch:**

Config firewall policy

**//Enter the configuration of the firewall Policies**

edit 1

**//Edit the first policy**

set name “inbound”

**//Set the name of this policy to “Inbound”**

set srcintf “to\_HQ”

**//Set the source interface to the object name to\_HQ**

set dstintf “Branch Interface”

**//Set the destination interface to the object name “Branch Interface”**

set srcaddr “192.168.1.0 255.255.255.0”

**//Set the source subnet to this subnet Ip**

set dstaddr “Branch Subnet”

**//Set the destination subnet to this subnet Object named “Branch Subnet”**

set action accept

**//Enable all the traffic that pass other rules**

set service “ALL”

**//there is no restrictions in any protocol all the protocols are allowed if they pass other rules**

Next

**//Exit the configuration mode of the first policy**

edit 2

**//Edit the Second policy**

set name “outbound”

**//Set the name of this policy to “outbound”**

set srcintf “Branch Interface”

**//Set the source interface to the object name “Branch Interface”**

set dstintf “to\_HQ”

**//Set the destination interface to the object name to\_HQ**

set srcaddr “Branch Subnet”

**//Set the source subnet to this subnet Object named “Branch Subnet”**

set dstaddr “192.168.1.0”

**//Set the destination subnet to this subnet**

set action accept

**//Enable all the traffic that pass other rules**

set service “ALL”

**//there is no restrictions in any protocol all the protocols are allowed if they pass other rules**

Next

**//Exit the configuration mode of the Second policy**

end

**//Exit the configuration mode of the Policies in the Firewall**

\*Company users in both sites should be able to reach IT systems and servers remotely using SSL VPN

**Enable SSL VPN feature:**

Config system settings

**//Enter the configuration of the system settings**

Set gui-sslvpn enable

**//enable ssl vpn feature visibility**

End

**//Exit the configure**

**Configure user and user group:**

Config user local

**//Enter the configuration of the users**

edit “sslvpnuser1”

**//Edit the first user named “sslvpnuser1”**

set type password

**//to enable password for the user**

set passwd sslUSAL

**//to set the password as sslUSAL**

next

End

Config user group

**//Enter the configuration of the groups**

edit “sslvpngroup”

**//edit|create this group named sslvpngroup and enter its configuration mode**

set member “sslvpnuser1”

**//add the first user named “sslvpnuser1” to this group**

next

End

**Configure SSL VPN web Portal:**

Config vpn ssl web portal

**//Enter the configuration of the vpn ssl web portal**

Edit “my-split-tunnel-portal”

**//Edit the config that named my-split-tunnel-portal**

set tunnel-mode enable

set split-tunneling enable

set split-tunneling-routing-address 192.168.1.0

set ip-pools “SSLVPN\_TUNNEL\_ADDR1”

next

end

**Configure SSL VPN settings:**

Config vpn ssl settings

**//Enter the configuration of the vpn ssl settings**

Set servercert “Fortinet\_Factory”

Set tunnel-ip-pools “SSLVPN\_TUNNEL\_IPV6\_ADDR1”

Set tunnel-ipv6-pools “SSLVPN\_TUNNEL\_IPV6\_ADDR1”

Set source-interface “Wan Interface’

Set source-address “all”

Set source-address “all”

Set default-portal “full-access”

Config authentication-rule

edit 1

set groups “sslvpngroup”

set portal “my-split-tunnel-portal”

next

next

end

**Configure one SSL VPN firewall policy to allow the remote user to access the internal network.**

Config firewall policy

**//Enter the configuration of the vpn ssl web portal**

Edit 1

**//Edit the config that named my-split-tunnel-portal**

Set name “sslvpn split tunnel access”

Set srcintf “ssl.root”

Set dstintf “Lan Interface”

Set srcaddr “all”

Set dstaddr “Lan Subnet”

Set groups “sslvpngroup”

Set action accept

Set service “ALL”

next

end