Configuring Site to Site VPN policies using Enterprise Command Line Interface E CLI

KNOWLEDGE DATABASE

SONICWALL
Knowledge Database

Configuring Site to Site VPN policies using Enterprise Command Line Interface (E-CLI)

Global System Commands

The following system commands are global and can be executed from anywhere in the **config** module.

NSA 220 Configuration	NSA 4500 Configuration
Create an address object for the remote networks	
config address-object ipv4 "NSA 4500 LAN" network 172.27.24.0 /24 zone VPN	config address-object ipv4 "NSA 220 LAN" network 10.10.10.0 /24 zone VPN
• Make sure there is a space after the network address and before the slash notation. Also the "/" & the bit notation must not have a space. • These address objects will be referenced, as an example, throughout this article. • Address objects can also be created "on the fly" while creating the VPN policy. For example, network remote network 172.27.24.0 /24 would create an address object by the name of "172.27.24.0/24".	
Site to Site VPN Configuration - IKEv2 Mode	
vpn policy site-to-site "To Remote Site" enable gateway primary 192.168.170.51 auth-method shared-secret shared-secret "1234" exit network local name "X0 Subnet" network remote name "NSA 4500 LAN" proposal ike authentication sha256 proposal ike dh-group 2 proposal ike encryption triple-des proposal ike exchange ikev2 proposal ike lifetime 28800 keep-alive management https ssh bound-to zone WAN commit exit	vpn policy site-to-site "To Central Site" enable gateway primary 192.168.170.31 auth-method shared-secret shared-secret "1234" exit network local name "X0 Subnet" network remote name "NSA 220 LAN" proposal ike authentication sha256 proposal ike dh-group 2 proposal ike encryption triple-des proposal ike exchange ikev2 proposal ike lifetime 28800 management https ssh bound-to zone WAN commit exit

Other (optional) commands	
netbios	//Enable Windows Networking (NetBIOS) Broadcast
multicast	//Enable Multicast
management snmp	//Enable SNMP via this SA
user-login http	//Enable user login via this SA over HTTP
user-login https	//Enable user login via this SA over HTTPS
default-lan-gateway	//Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA.
	//Enable suppression of IKEv2 trigger packets
suppress-trigger-packet	//Enable acceleration
tcp-acceleration	//Enable suppression of auto-added rules.
suppress-auto-add-rule	//Enable NAT over VPN.
apply-nat	//Enable management of SonicPoint over VPN
allow-sonicpointn-layer3	

Site to Site VPN Configuration - Main Mode	
vpn policy site-to-site "To Remote Site" enable gateway primary 192.168.170.51 network local name "X0 Subnet" network remote name "NSA 4500 LAN" auth-method shared-secret shared-secret "1234" exit proposal ike authentication sha256 proposal ike dh-group 2 proposal ike encryption triple-des proposal ike exchange main proposal ike lifetime 28800 keep-alive management https ssh bound-to zone WAN commit exit	vpn policy site-to-site "To Central Site" enable gateway primary 192.168.170.31 network local name "X0 Subnet" network remote name "NSA 220 LAN" auth-method shared-secret shared-secret "1234" exit proposal ike authentication sha256 proposal ike dh-group 2 proposal ike encryption triple-des proposal ike exchange main proposal ike lifetime 28800 management https ssh bound-to zone WAN commit exit

Site to Site VPN Configuration - Aggressive Mode

vpn policy site-to-site "To Remote Site"	vpn policy site-to-site "To Central Site"
enable	enable
auth-method shared-secret	gateway primary 192.168.170.31
shared-secret "1234"	auth-method shared-secret
ike-id local sonicwall-id "Branch Office"	shared-secret "1234"
ike-id peer sonicwall-id "HQ"	ike-id local sonicwall-id "HQ"
exit	ike-id peer sonicwall-id "Branch Office"
network local name "X0 Subnet"	exit
network remote name "NSA 4500 LAN"	network local name "X0 Subnet"
proposal ike authentication sha256	network remote name "NSA 220 LAN"
proposal ike dh-group 2	proposal ike authentication sha256
proposal ike encryption triple-des	proposal ike dh-group 2
proposal ike exchange main	proposal ike encryption triple-des
proposal ike lifetime 28800	proposal ike exchange main
keep-alive	proposal ike lifetime 28800
management https ssh	management https ssh
bound-to zone WAN	bound-to zone WAN
commit	commit
exit	exit

Edit VPN policies

To edit and change a VPN policy, follow these steps:

//as already mentioned, at each command, pressing "?" would list usage with example/s; pressing the Tab key would either auto-complete half-way through a command or list suggestions of next commands or values to type. For example:

- pressing the Tab key at **vpn policy** would list the following options:
  enable group-vpn site-to-site tunnel-interface
- pressing the Tab key at **vpn policy sit** would auto-complete site-to-site
- pressing the Tab key at **vpn policy site-to-site** would either list multiple VPN policies, if multiple policies are configured. If there is only one site-to-site VPN policy, this auto-complete the command by filling the name of the VPN policy in this way: **vpn policy site-to-site To Remote Site**

config vpn policy site-to-site "To Remote Site"
Pressing the "?" or the Tab key would list the commands available within this module.

auth-method	Authentication Method.
bound-to	Configure VPN Policy Bound To.
enable	Enable Policy.
gateway	IPsec Gateway Name or Address.
management	Enable Management for VPN Policy.
multicast	Enable VPN Policy Multicast.
name	Policy name.
netbios	Enable VPN Policy NetBIOS.
proposal	Policy proposal.
tcp-acceleration	Enable Permit TCP Acceleration.
transport-mode	Enable Transport Mode.
user-login	Enable VPN Policy for User Login.

(edit-site-to-site[To Remote Site])# no enable	disable the VPN
(edit-site-to-site[To Remote Site])# no management https	disable HTTPS management over VPN
(edit-site-to-site[To Remote Site])# user-login https	enable HTTPS user login over VPN
(edit-site-to-site[To Remote Site])# no netbios	disable NetBios broadcasts over VPN
(edit-site-to-site[To Remote Site])# cancel	exit out of this module without saving changes
(edit-site-to-site[To Remote Site])# commit	save changes

Delete a VPN policy

To delete a VPN policy enter the following command. Must be entered at the config prompt.

```
config
no vpn policy site-to-site "To Remote Site"
```

Display VPN policies and VPN Tunnel information

The show command is global and can be executed from any module.

Enter this command to show a specific site-to-site VPN policy by name

```
show vpn policy "To Remote Site"
```

Enter this command to show all VPN policies :

```
show vpn policies
```

To display information on an active VPN tunnel, enter this command:

```
show vpn tunnel "To Remote Site"
```

To display information on all active VPN tunnels, enter this command:

```
show vpn tunnels
```

Display VPN Logs

To display VPN logs, enter the following command:

```
show log view category "VPN"
```

The view can be further filtered using the following options:

priority	Show Log with specified Priority.
source-interface	Show Log with specified Source Interface.
destination-interface	Show Log with specified Destination Interface.
source-ip	Show Log with specified Source-Ip.
source-port	Show Log with specified Source-Port.
destination-ip	Show Log with specified Destination-Ip.
destination-port	Show Log with specified Destination-Port.
ip-protocol	Show Log with specified IP Protocol number.
user-name	Show Log with specified User Name.
application	Show Log with specified Application.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com