

SecureFirst

Dynamic Route Based VPN in SonicOS 5.9.0 - Basic Config KNOWLEDGE DATABASE



Dynamic Route Based VPN in SonicOS 5.9.0 - Basic Config

Beginning with SonicOS 5.9.0, configuring dynamic route based VPN has changed from previous versions. In the new configuration method, a Tunnel Interface must be configured under **Network | Interfaces** page and OSPF configured on the Tunnel Interface under **Network | Routing | Advanced Routing** page.

This articles describes the basic method to perform this task.

- The first step involves creating a Tunnel Interface VPN policy. The crypto suites used to secure the traffic between two end-points are defined in the policy.
- The second step is to create a new Tunnel Interface under **Network** | **Interfaces**.

•	The third ste	p involves configur	ing OSPF
for	the	Tunnel	Interface
unc	ler	Network	Routing.

• The fourth step involves creating access rules from LAN/DMZ to VPN and from VPN to LAN/DMZ to allow traffic over the VPN.

In this scenario a Dynamic Route-based VPN is configured between an NSA 2400 (Site A) and an NSA 220 (Site B). For this article, we'll be using the following IP addresses as examples to demonstrate the VPN configuration. You can use these examples to create VPN policies for your network, substituting your IP addresses for the examples shown here:

Site A - NSA 2400

WAN (X1): 1.1.1.1 LAN (X0) Subnet: 10.10.10.0/24 Tunnel Interface IP: 192.168.1.1/24

Corporation®

/isit our Website: www.itclatam.com

Site B - NSA 220

WAN (X1): 2.2.2.2 LAN (X0) Subnet: 192.168.168.0/24 Tunnel Interface IP: 192.168.1.2/24

Site A (NSA 2400) Configuration

- 1. Adding a Tunnel Interface VPN policy
- 2. <u>Create and configure a tunnel interface</u>
- 3. Configuring OSPF for a Tunnel Interface
- 4. Adding rules to allow traffic over the VPN

Adding a Tunnel Interface VPN policy

- 01. Login to the SonicWall management interface.
- 02. Navigate to the **VPN** | **Settings** page.

03. Click on the **Add** button to create a tunnel interface VPN as per the screen shots.

General	Proposals	Advanced			
Security Policy					
Policy Type:			Tunnel Ir	nterface	
Authentication Method:			IKE using	g Preshared Se	ecret
Name:			To Site B	}	
IPsec Primary Gateway	Name or Address		2.2.2.2		
IKE Authenticatio	n				
Shared Secret:	••••				
Confirm Shared Secret:				Mask Sh	ared Secret
Local IKE ID:	IPv4 A	ddress	•		
Peer IKE ID:	IPv4 A	ddress	•		
	Network Se	OK ecurity Appliance	e	Cancel	Help
dy DNIC WALL	Network Se Propos	OK ecurity Applianc als Adv	e anced	Cancel	Help
dy DNICWALL General	Network Se Propos	OK ecurity Applianc als Adv	e	Cancel	Help
dy ONICWALL General IKE (Phase 1)	Network Se Propos Proposal	OK als Adv	e anced Mode	Cancel	Help
dy ONICWALL General IKE (Phase 1) Exchange: DH Group:	Network Se Propos Proposal	OK acurity Applianc als Adv IKEv2 Group	e anced Mode	Cancel	Help
dy ONICWALL General IKE (Phase 1) Exchange: DH Group: Encryption:	Network Se Propos Proposal	OK als Adv IKEv2 Group 3DES	e anced Mode	Cancel	Help
dy ONICWALL General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication:	Network Se Propos Proposal	OK als Adv IKEv2 Group 3DES SHA1	e anced Mode	Cancel	Help
dy ONICWALL General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication: Life Time (seconds)	Network Se Proposal Proposal	OK acurity Applianc als Adv IKEv2 Group 3DES SHA1 28800	e anced Mode	Cancel	Help
dy Control Control Co	Network Se Proposal Proposal): 2) Proposa	OK ecurity Applianc als Adv IKEv2 Group 3DES SHA1 28800	Mode	Cancel	Help
dy General General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication: Life Time (seconds) IPsec (Phase Protocol:	Network Se Proposal): 2) Proposa	OK als Adv IKEv2 Group 3DES SHA1 28800 al	e anced Mode	Cancel	Help
dy ONICWALL General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication: Life Time (seconds) IPsec (Phase Protocol: Encryption:	Network Se Proposal Proposal	oK als Adv IKEv2 Group 3DES SHA1 28800 al ESP 3DES	Mode	Cancel	Help
dy General General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication: IPsec (Phase Protocol: Encryption: Authentication:	Network Se Proposal Proposal	OK als Adv IKE 2 Group 3DES SHA1 28800 al ESP 3DES SHA1	Mode	Cancel	Help
dy General General IKE (Phase 1) Exchange: DH Group: Encryption: Authentication: Life Time (seconds) IPsec (Phase Protocol: Encryption: Authentication: Chapter Perfect	Network Se Proposal Proposal): 2) Proposa	OK als Adv IKEv2 Group 3DES SHA1 28800 al ESP 3DES SHA1 recy	e Mode 0 2	Cancel	Help
Ady Control Co	Network Se Proposal): 2) Proposa t Forward Sec):	oK ecurity Applianc als Adv IKEv2 Group 3DES SHA1 28800 al ESP 3DES SHA1 28800 al	e anced Mode	Cancel	Help

Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290 / +57 318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01

Sonic wall	Network Security A	Appliance	
General	Proposals	Advanced	
Advanced Set	tings		
🗹 Enable Keep A	live		
🗖 Enable Windo	ws Networking (NetBI	OS) Broadcast	
🗖 Enable Multica	ast		
🗖 Permit Acceler	ration		
Management via th	iis SA: 🗖 HTTPS	🗆 SSH 🗖 SNMP	· 🚣
User login via this S	БА: 🗖 НТТР	🗆 нттрз	-2-
VPN Policy bound t	o: Interface X	1	•
IKEv2 Setting	5		

- Do not send trigger packet during IKE SA negotiation
- Accept Hash & URL Certificate Type
- 🗖 Send Hash & URL Certificate Type

Ready

Create and configure a Tunnel Interface

- 01. Navigate to the Network | Interfaces page.
 - 02. Select **Tunnel Interface** from the **Add** Interface drop-down menuto open the **Add Tunnel Interface** window.

SONICWALL Network Security Appliance

Dashboard System Network	Network / Interfaces		
Interfaces PortShield Groups	Accept		
Fallover & LB	Interface Settings		
DN5	🕳 Name	Zone	Group
Address Objects	XD	LAN	
Services	XI	WAN	Default LB Group
Routing	¥2	Unarright	
NAT Policies	· · · ·	onassigned	
ARP	X3	Unassigned	
Neighbor Discovery	X4	Unassigned	
MAC-IP Anti-spoof	X5	Unassigned	
DHCP Server	X6	Unassigned	
Dynamic DNS Network Monitor 3G/4G/Modem SonicPoint	Add Interface: -Sele -Sele Display All Tunne WLAP	ect Interface Type- ect Interface Type I Interface I Interface V Tunnel Interface	ortShield Wizard
- Incolor	Interface Traffic Sta	atistics	



03The **Zone** will be pre-selected with VPN.

04. Under VPN Policy, select the VPN policy created earlier.
05. Mode / IP Assignment will be preselected with Static IP Mode.
06. Under IP Address and Subnet Mask, enter an IP address and subnet mask. The remote site must be in the same subnet as this IP address.
07. Click on OK to save.

SONICWALL Network Security Appliance

General Advanced

Interface Settings



Configuring OSPF for a Tunnel Interface

01. Navigate to the Network | Routing Page.
02. Click on the drop-down under Routing Mode and select Advanced Routing.
03. Click on OK on the warning window.
04. The tunnel interface created earlier will be visible now.





								Mode:
• 🗠	Dashboard	Rout	ting Mode: Advanc	ed Routing	▼ View IP V	ersion: © IPv4	C IPV6 BGP	The Expanded License is r
• 💻	System	*	Interface (Zone)	RIP	Configure RJP	OSPFv2	Configure OSI	*F OSPF Neighbor Status
-	Interfaces	-	X0 (LAN)	RIP Disabled	Ø	OSPF Disabled	Ø	
	PortShield Groups	-	X1 (WAN)	RIP Disabled	Ø	OSPF Disabled	Ø	
	Failover & LB	-	TI2 (VPN)	RIP Disabled	Ø	OSPF Disabled	0 🗲	-
	Zones	*	X2 (N/A)	RIP Disabled	Ø	OSPF Disabled	Ø	
	Address Objects		X3 (N/A)	RIP Disabled	Ø	OSPF Disabled	Ø	
	Services		X4 (N/A)	RIP Disabled	0	OSPF Disabled	Ø	
	Routing		X5 (N/A)	RIP Disabled	0	OSPF Disabled	Ø	
	NAT Policies ARP	-	X6 (N/A)	RIP Disabled	Ø	OSPF Disabled	Ø	

05. Click on the Configure OSPF button on the Tunnel Interface to open the OSPF configuration window.
06. Enter information as per the screenshot in the OSPFv2 Configuration window
07. The OSPF Router ID must be a unique IP address in your network.
08. Click on OK to save the settings.

Interface TI2 (VPN) OSPFv	2 Configuration				
OSPFv2:	Enabled -	OSPF Area		0	
Dead Interval (1 - 65535):	40	OSPEv2 An	ea Type:	Normal	-
Hello Interval (1 - 65535):	10	Interface C	ost (1 - 65535):		iuto
Authentication:	Disabled	Router Prio	rity: (0 - 255):	1	
Password:					
Global OSPFv2 Configurati	on				
OSPF Router-ID (n.n.n.n):	10.0.0.1	Default Me	tric (1 - 16777214);	Undefined	
ABR Type:	Cisco	Auto-Cost	Reference BW (Mb/s	s): 100	
Originate Default Route: Ner	ver	-			
Metric (1 - 16777214): 10		Metric Type:	External Type	2 -	
Redistribute Static Route	5	Tag (0 - 4294967295):	Undefined	1	
Metric (1 - 16777214): De	efault	Metric Type:	External Type	2 💌	
Redistribute Connected N	letworks	Tag (0 - 4294967295):	Undefined	1	
Metric (1 - 16777214): De	efault	Metric Type:	External Type	2 💌	
C Redistribute RIP Routes		Tag (0 - 4294967295):	Undefined	L	
Metric (1 - 16777214);	əfault	Metric Type:	External Type	2 -	
Redistribute Remote VPN	Networks	Tag (0 - 4294967295):	Undefined	1	
Metric (1 - 16777214): De	efault	Metric Type:	External Type	2 -	

Adding rules to allow traffic over the VPN

Although the tunnel will be up and OSPF will be able to detect neighbors, traffic will be blocked to the other side of the tunnel until access rules are created from the local zones to the VPN zone. **01.** Navigate to **Network** Address Objects 02. Click on Add to create an address object for the destination network (see screenshot below)

General	Advanced	QoS
Settings		
Action:	● Allow C Deny C Discard	
From :	LAN	•
To :	VPN	•
Source Port:	Any	•
Service:	Any	•
Source:	Any	•
Destination:	Site B Network	•
Users Included:	All	 these users will be allowed if not exclude
Users Excluded:	None	 these users will be denied.
Schedule:	Always on	•
Comment:		
🗹 Enable Logging	3	Enable Geo-IP Filter
Allow Fragmen	ited Packets	Enable Botnet Filter
Enable flow re	porting	
🗆 Enable packet	monitor	
🗖 Enable Manage	ement "	
ady		

03. Navigate to **Firewall | Access Rules 04.** Go to **LAN** to **VPN** 05. Create an access rule as per the screenshot.

General	Advanced	QOS	
Settings			
Action:	● Allow C Deny C Discard		
From :	VPN	•	
To :	LAN	-	
Source Port:	Any	▼	
Service:	Any	-	
Source:	Site B Network	•	
Destination:	Any	•	
Users Induded:	All	💌 these use	rs will be allowed if not exclude
Users Excluded:	None	▼ these use	rs will be denied.
Schedule:	Always on	*	
Comment:			
🗹 Enable Loggin	9	🗹 Enable Geo-II	PFilter
🗹 Allow Fragmer	nted Packets	🗹 Enable Botne	t Filter
Enable flow re	porting		
🗆 Enable packet	monitor		
🗆 Enable Manag	ement		
eady			
		Add	Close Help





06. Navigate to VPN to LAN07. Create an access rule as per the screenshot.

General	Proposals	Advanced			
Security Polic	y				
Policy Type:			Tunnel I	nterface	*
Authentication Me	thod:		IKE usin	g Preshared Secret	*
lame:			To Site A	\	
Psec Primary Gab	eway Name or Addres	15:	1.1.1.1		
IKE Authentic	ation				
ihared Secret:	••••				
Confirm Shared Se	icret:			Mask Shared Secret	
ocal IKE ID:	IPv47	Address	•		
eer IKE ID:	IPv47	Address	•		
Site E	3 (NSA 2) . <u>Addinc</u>	20) Confi	iguratio	Cancel H DN face Tunnel Interf	elp
Site E	3 (NSA 2) . <u>Adding</u> 2. <u>Create</u> 3. <u>Config</u> 4. <u>Adding</u>	20) Confi g a Tunn and confi uring OSF g rules to	guration el Inter gure a PF for a allow	Cancel Interf Tunnel Interf Traffic over t	ace ace he VPN
Site E 1 2 3 4 Addir	3 (NSA 2) . <u>Adding</u> 2. <u>Create</u> 3. <u>Config</u> 4. <u>Adding</u> 1g a Tun	20) Confi g a Tunn and confi uring OSF g rules to nel Interf	guration el Inter gure a PF for a allow f ace VF	Cancel Interf Tunnel Interf Tunnel Interf Traffic over t 'N policy	ace ace he VPN
Site E 1 2 3 4 Addir 01	3 (NSA 2 . <u>Adding</u> . <u>Create</u> . <u>Config</u> . <u>Adding</u> ng a Tun I. Login t	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son	guration el Inter gure a PF for a allow ace VP icWall	Cancel H face Tunnel Interf Tunnel Interf traffic over t 'N policy management	ace ace ace he VPN
Site E 1 2 3 4 Addir 01	B (NSA 2) <u>Adding</u> <u>Create</u> <u>Configu</u> <u>Adding</u> <u>Adding</u> <u>a Tun</u> <u>Login</u> t interfa	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce.	guration el Inter gure a PF for a allow ace VP icWall i	Cancel H Face Tunnel Interf Tunnel Interf traffic over t PN policy management	ace ace he VPN
Site E 1 2 3 3 4 4 Addir 01	3 (NSA 2) . <u>Addino</u> 2. <u>Create</u> 3. <u>Configu</u> 4. <u>Addino</u> 1. Addino 1. Login t interfa 02. Nav	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce. vigate to	iguration el Inter gure a PF for a allow f ace VF icWall f the VP	Cancel Interf face Tunnel Interf Tunnel Interf Traffic over t PN policy management N Settings	ace ace he VPN
Site E	B (NSA 2: Adding Create Configu Adding Adding Adding D a Tun L Login t interfa 02. Nav 03. Clic	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce. vigate to ck on the s	guration el Inter gure a PF for a allow ace VF icWall the VP Add bu	Cancel H face <u>Tunnel Interf</u> <u>Tunnel Interf</u> traffic over t 'N policy management N Settings tton to creat	ace ace he VPN : page. e a
Site E 1 2 3 4 Addir 01	3 (NSA 2) <u>Adding</u> <u>Create</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Config</u> <u>Co</u>	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce. vigate to ck on the interface	iguration el Inter gure a PF for a allow f ace VF icWall f the VP Add bu	Cancel H face Tunnel Interf Tunnel Interf traffic over t PN policy management N Settings tton to creat sperthe scre	<u>ace</u> Face he VPN tea ea en
Site E 1 2 3 4 Addir 01	3 (NSA 2) Adding Create Configu Adding Adding a Tun Login t interfa 02. Nav 03. Clic tunnel shots.	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce. vigate to ck on the interface	iguration el Inter gure a PF for a allow f ace VF icWall f the VP Add bu VPN as	Carcel H Face Tunnel Interf Tunnel Interf traffic over t PN policy management N Settings tton to creat sperthe scre	ace ace he VPN c page. e a en
Site E	 Adding <u>Adding</u> <u>Create</u> <u>Configu</u> <u>Adding</u> <u>Adi</u>	20) Confi g a Tunn and confi uring OSF g rules to nel Interf o the Son ce. vigate to ck on the interface	iguration el Inter gure a PF for a allow f ace VF icWall f the VP Add bu	Cancel Interf <u>face</u> <u>Tunnel Interf</u> <u>Tunnel Interf</u> <u>traffic over t</u> 'N policy management N Settings tton to creat sperthe scre	ace ace he VPN c page. e a en

Policy Type:		Tunne	Interface
Authentication Method:		IKE us	ing Preshared Secret
Name:		To Site	A
IPsec Primary Gateway Nar	ne or Address:	1.1.1.1	
IKE Authentication			
Charact Canada			
Shared Secrec;			
Confirm Shared Secret:	••••		Mask Shared Secret
Confirm Shared Secret: Local IKE ID:	•••• IPv4 Address	•	Mask Shared Secret
Confirm Shared Secret: Local IKE ID: Peer IKE ID:	IPv4 Address	•	Mask Shared Secret

NICWALL No	twork Security	Appliance			
General	Proposals	Advar	nced		
IKE (Phase 1) Pro	oposal				
Exchange:		IKEV2 N	lode		ŀ
OH Group:		Group 2			-
Encryption:		3DES			ŀ
Authentication:		SHA1			ŀ
life Time (seconds):		28800			
IPsec (Phase 2)	Proposal				
Protocol:		ESP			
Encryption:		3DES			•
Authentication:		SHA1			-
Enable Perfect For	rward Secrecy				
life Time (seconds):		28800			
lfe Time (KBytes):		0			
dy					
DNICWALL	OK Network S	ecurity Aş	Ca opliance	ncel	Help
General	Propo	sals	Adv	anced	
	ttings				
Advanced Se					
Advanced Se	Alive				
Advanced Se	Alive lows Network	ng (Net81	05) Broa	lcast	
Advanced Se	Alive lows Network cast	ng (NetBl	05) Broa	icast	
Advanced Se Enable Keep Enable Wind Enable Multi- Permit Accel	Alive lows Network cast eration	ng (Net81)	05) Broa	lcast	

IKEv2 Settings

VPN Policy bound to:

User login via this SA:

☑ Do not send trigger packet during IKE SA negotiation *

Interface X1

HTTP HTTPS

- C Accept Hash & URL Certificate Type
- Send Hash & URL Certificate Type

Ready

0K

Help

-

Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290 / +57 318 4914652 sales@itclatam.com / tss@itclatam.com REV 1.01

Cancel



SONIC WALL[®] Knowledge Database

6

Create and configure a Tunnel Interface

01. Navigate to the **Network** | **Interfaces** page. 02. Select Tunnel Interface from the Add Interface drop-down menu to open the Add Tunnel Interface window.

SONICWALL Network Security Appliance

Dashboard System	Interfaces		
Interfaces	Accept		
PortShield Groups Failover & LB Zonor	Interface Settings		
DNS	🕳 Name	Zone	Group
Address Objects	XD	LAN	
Services	×1	WAN	Default LB Group
Routing	×2	Unassigned	
ARP	Х3	Unassigned	
Neighbor Discovery	X4	Unassigned	
MAC-IP Anti-spoof	Х5	Unassigned	
DHCP Server IP Helper	×6	Unassigned	
Dynamic DNS Network Monitor 3G/4G/Modem	Add Interface: -Sele -Sele Display All T	ct Interface Type- 💽 🛛 F ct Interface Type- Interface	atShield Wizard
SonicPoint Firewall	WLAN	I Tunnel Interface	_
Frewall Settings	Interface Traffic Sta	tistics	

03. In the Add Tunnel Interface window, the Zone will be pre-selected with VPN.

04. Under **VPN Policy**, select the VPN policy created earlier.

05. Mode/IP Assignment will be pre-selected with Static IP Mode.

06. Under IP Address and Subnet Mask, enter an IP address and subnet mask. The remote site must be in the same subnet as this IP address.

07. Click on **OK** to save.

General	Advanced	
Interface Settings		
Zone:	VPN	
VPN Policy: 💛	To Site A	
Mode / IP Assignment:	Static IP Mode	
IP Address:	192.168.1.2	
Subnet Mask:	255.255.255.0	
Comment:		
dy		
OK	Cancel	Help

Configuring OSPF for a Tunnel Interface

01. Navigate to the **Network** | **Routing** Page.

02. Click on the drop-down under **Routing** Mode and select Advanced Routing.

03. Click on **OK** on the warning window.

04. The Tunnel Interface created earlier will be visible now.

05. Click on the **Configure OSPF** button on the **Tunnel Interface** to open the OSPF configuration window.

06. Enter information as per the screenshot in the OSPFv2 Configuration window

07. The OSPF Router ID must be a unique IP address in your network.

08. Click on **OK** to save the settings.



OSPFy2:	Enabled 💌	OSPF Area:	0
Dead Interval (1 - 65535):	40	OSPEv2 Area Type:	Normal
Hello Interval (1 - 65535):	10	Interface Cost (1 - 68	5535): 🔽 Auto
Authentication:	Disabled	Router Priority: (0 - 2	:55): 1
Password:			
Global OSPEy2 Configura	ation		
OSPF Router-ID (n.n.n.n):	10.0.0.254	Default Metric (1 - 1	6777214): Undefined
ABR Type:	Cisco 💌	Auto-Cost Reference	e BW (Mb/s): 100
Originate Default Route:	lever		
Metric (1 - 16777214):	10	Metric Type:	External Type 2 💌
Redistribute Static Rou	tes	Tag (0 - 4294967295):	Undefined
Mebric (1 - 16777214):	Default	Metric Type:	External Type 2 💌
Redistribute Connecte	d Networks	Tag (0 - 4294967295):	Undefined
Mebric (1 - 16777214):	Default	Mebric Type:	External Type 2 💌
Redistribute RIP Route	5	Tag (0 - 4294967295):	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2
Redistribute Remote V	PN Networks	Tag (0 - 4294967295);	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2 💌
Ready			

Adding rules to allow traffic over the VPN

Although the tunnel will be up and OSPF will be able to detect neighbors, traffic will be blocked to the other side of the tunnel until access rules are created from the local zones to the VPN zone.

01. Navigate to Network | Address Objects

02. Click on **Add** to create an address object for the destination networks and group them (see screenshot below)

SONICWALL	Network Security Appliance	
oon on the		
Name:	Site A Network	
Zone Assignment:	VPN	-
Fype:	Network	
Network:	10.10.10.0	
Netmask/Prefix Length:	255 255 255 0	





03. Navigate to Firewall | Access Rules 04. Go to LAN to VPN

05. Create an access rule as per the screenshot.

SONICWALL Network Security Appliance

General	Advanced	QoS
Settings		
Action:		
From :	LAN	•
To :	VPN	V
Source Port:	Any	•
Service:	Any	×
Source:	Any	
Destination:	Site A Network	
Users Included:	All	these users will be allowed if not exclude
Users Excluded:	None	these users will be derived.
Schedule:	Always on	
Comment:		
🗹 Enable Logging	1	💌 Enable Geo-IP Filter
Allow Fragmen	ted Packets	🔽 Enable Botnet Filter
🗆 Enable flow rep	porting	
Enable packet	monitor	
🗆 Enable Manage	ement "	

Rule action done, please check rule table

06. Navigate to VPN to LAN07. Create an access rule as per the screenshot.

General	Advanced	QoS
Settings		
Action:	€ Allow C Deny C Discard	
From :	VPN	•
To :	LAN	•
Source Port:	Any	•
Service:	Any	•
Source:	Site A Network	•
Destination:	Any	•
Users Included:	All	these users will be allowed if not exclud
Users Excluded:	None	these users will be denied.
Schedule:	Always on	•
Comment:		
🗹 Enable Loggin	0	✓ Enable Geo-IP Filter
🗹 Allow Fragmer	nted Packats	🗹 Enable Botnet Filter
Enable flow re	porting	
🗆 Enable packet	monitor	
🗆 Enable Manag	ement *	
eady		
		Add Clase Help

Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01



OSPF Neighborship, Dynamic Routes

The VPN tunnel status will be green as soon as the the configuration of the VPN Tunnel Interface policies are completed on both sites.

The screenshots below shows the OSPF neighborship status on both sites and also the dynamically learned routes from each other.

Site A

NUU	ting										
Routing	Protocols										
Routing	Mode: A	dvanced Routing	•	View IP Version:	C IPv4 C IPv4	6 BGP: The Expande	d License i	s required	for BGP sup	port. Click h	ere to open the
*	Interface	(Zone)	RIP	Con	ñgure RIP	CSIFv2	Ċ.	nfigure OS	SPF	097 Teich	oor Status
*	X0 (LAN)		RIP Disabled	0	1	OSPF Disabled	G	8			
*	XI (WAN)		RIP Disabled	e		OSPF Decabled	Q	0			
*	TI2 (VPN)	6	RIP Disabled	Ø	E.	OSPF Enabled	G	0		0	
*	X2 (N/A)		RIP Disabled	e	8	OSPF Disabled	G	8			
*	X3 (N/A)		RIP Disabled	e		OSPF Disabled	G	0			
•	::::::::::::::::::::::::::::::::::::::		RIP Disabled	Ø		OSPF Disabled	6	0			
*	x5 (N/A)		RIP Disabled	0		OSPF Disabled	Q	0			
•	X6 (N(A)		RIP Disabled	e)	OSPF Disabled	Q	0			
Apply the Route I	x6 (N(A) he following Policies Style:	metric to default route C All Policies	RIP Disabled s received from	m Advanced Routing	protocols: 110 fault Policies	OSP# Disabled Change View IP Version:	(° IPv	€ 4 Only	Rems 1 C IPró	to 11	of 11) (1 +)
Apply U Route I View S	x6 (N(A) the following Policies Style:	C Al Polices	RIP Disabled s received from Clustom Po	eloies C De	protocols: 110 fault Policies	OSPF Disabled Change View IP Version:	 IP Metric 	4 Only Proday	Rems 1 C IPv64	to 11 1 Only C	of 11) (a) + 1 IPv4 and IPv1
Apply the Route I	x6 (N(A) he following Policies Style: Source Any	Metric to default route	RIP Disabled s received from C Custom Po Ecolor 2 Any	olcies P De No. 105/Mack.	protocols: 110 fault Policies	OSPE Disabled Change View IP Version: Dronface 20	@ IPv Metric 20	4 Ordy Priority 2	Rems 1 C IPv61	to II I Only C Comment	(of 11) (a) + () IPv4 and IPv1 Contigure () (c)
Apply d Route I View S	x6 (It(A) he following Policies Style: Source Any Any	C Al Polices Destination 255-255-255-255/ X1 Default Gateway	RIP Disabled s received from C Custom Pc Sorry IZ Any y Any	a Advanced Routing alcies P De co 1057 Mask. Any Any	protocolis: 110 fault Policies	OSPP Deabled Change View IP Version: Deenfoce 20 20 20 20 20 20 20 20 20 20 20 20 20	G IP- Mistric 20 20	4 Only Priority 2 3	Rems T	to 11 0 Drily C Comment D	(of 11) (a +) (Pv4 and Pvi Controller (2) (0) (2) (0)
Apply th Route I View S	x6 (It(A) he following Policies Style: Source Any Any Any	C Al Polices Destination 295-255-255-255/ XI Default Gateway 30 Subnet	RIP Disabled s received from C Custom Po Sono 2 Any 4	m Advanced Routing okces P De co TOS / Mask Any Any Any	protocols: 110 fault Policies 0.0.0.0 0.0.0.0 0.0.0.0	OSPP Disabled Change View IP Version: Interface X0 X1 X1 X1 X1	 IPv Metric 20 20 20 	4 Ordy Priority 2 3 5	Rems 1 C IPv6 · Probe	to 11 f	lof 11) (n +) IPv4 and IPv Configure (2) (0) (2) (0) (2) (0) (2) (0) (2) (0)
Apply the Route of Strength St	x6 (N(A) he following Policies Style: Style: Any Any Any Any	Metric to default route Al Polices Distination 255.255.255.255.255 XI Default Gatowin 20 Subnet XI Subnet	RIP Disabled s received from C Custom Po C Custom Po C Custom Any Any Any Any Any	akces P Ce acco TOS / Mask Any Any Any Any Any	protocols: 110 fault Policies Gisteway, 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	OSPP Deabled Change View IP Version: 20 20 21 21 20 20 20 20 20 20 20 20 20 20	IPv Metric 20 20 incally	4 Only Protey 2 3 5 6	Rems T C IPv6 / Probe	to 11 f	lof 11) (1+) IPv4 and IPv1 Configure (2) (0) (2) (0) (2) (0) (2) (0) (2) (0) (2) (0)
Apply the Route I	x6 (N(A) he following Policies Style: Source Any Any Any Any Any	metric to default route C Al Polices Destination 255.255.255.255.255/ X1 Default Gatower X0 Subnet X1 Subnet T12 Subnet	RIP Disabled s received from C Custom Pc Econy (2 Any (Any	m Advanced Routing olders P De no 105 / Mack Any Any Any Any Any Any	protocols: 110 fault Policies 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	View IP Version:	Metric 20 20 20 20 20 20 20 20 20	4 Only Priority 2 3 5 6 7	Rems 1 C IPró I	to 11 1 Only C Comment D D D D D D D	[of 11] (1+) IPv4 and IPv1 Configure IP IP

Site B

Routing

outing Protocols

outing Node: Advanced Routing 💽 View IP Version: @ Ipvi C Ipvi6 BGP: The Expanded License is required for BGP support. Click here to

100						
*	300 (LAN)	RIP Disabled	Ø	OSP# Disabled	Ø	
*	XL (WAN)	RIP Disabled	0	OSPF Disabled	Ø	
*	T12 (VPN)	RIP Disabled	Ø	OSPF Enabled	Ø	۲
÷	:12 (LAN)	RIP Disabled	Ø	OSPF Disabled	Ø	
*	303 (LAN)	RIP Disabled	Ø	OSPF Disabled	Ø	
*	X4 (LAN)	RIP Disabled	Ø	OSPF Disabled	Ø	
*	25 (WLAN-1)	RJP Disabled	Ø	OSPF Disabled	Ø	
*	WD (WLAN)	RIP Disabled	0	OSPF Disabled	Ø	

View Style: C All Policies C Custom Policies

sion: @ JPv4 Only C JPv6 Only C JPv4 and JPv6

E.c.	Source	Destination	Service	TOS / Mask	Gatemay	Interface	Metric	Priority	Probe	Comment	Configure
Π1	Апу	258.258.255.255/32	Any	Any	0.0.0.0	300	20	2		ø	O.S.
Π2	Any	XI Default Gateway	Any	Any	0.0.0.0	21	20	3		9	00
Пэ	Any	X3 Subnet	Any	Acty	0.0.0.0	5(3	20	4		9	00
Π.4	Any	X0 Subnet	Any	Any	0.0.0	300	20	6		ø	00
III s	Any	XI Subnet	Any	Any	0.0.0	21	20	7		9	00
■ 6	Any	X4 Subnet	Any	Any	0.0.0.0	204	20	8		ø	60
Π 7	Any	W0 Subnet	Any	Any	0.0.0.0	WD	20	9		ø	00
П в	Any	X5 Subnet	Any	Any	0.0.0.0	15	20	10		ø	00
E 9	Any	X2 Subnet	Any	Any	0.0.0.0	Dynamically	P	11		ø	00
II 10	Απγ	TI2 Subnet	Acty	Arty	0.0.0.0	learned route	10	12		ø	OD
E 11	Atty	10.10.10.0/24	Arty	Any	192.168.1.1	TI2	110	13		9	00
Ein	V0.10	Anu	- Anu	And I	VII Definiti Cate		20	14		d	

Testing

Test by pinging an IP address from one site to another. Only the subnets defined in the access rules will beaccessible.

Troubleshooting

Checkthefollowing when the VPN tunnel is not up:

- 1. Gateway IP address.
- 2. Pre-shared secret
- 3. Proposal mismatch

Check the following when the VPN tunnel is up but the VPN Tunnel Interface is unable to form neighborship:

 Make sure the interface the VPN is bound to is not configured in L2 Bridged Mode.
 Make sure the VPN Tunnel Interfaces are

in the same **OSPF Area**

3. **OSPFv2AreasType**musthavethesame area type on both sites. (Normal, Stub Area, TotallyStubbyArea, Not-So-StubbyArea, Totally StubbyNSSA)

 OSPF Router-ID should not be duplicate.
 The Tunnel Interfaces created should be configured with an IP addresses in the same subnet.

6.

Check the following when the VPN Tunnel Interface has formed neighborship but dynamic routes are not present:

1. Make sure the local and destination

networks are not overlapping.

2. Make sure **Redistribute Connected Networks** is checked in the OSPFv2 Configuration.

Check the following when unable to pass traffic across the tunnel even after neighborship is formed

1. Make sure OSPF has dynamically learnt the routes to the remote networks. Look under **Route Policies** on the **Network | Routing** page.

Calle 146 #7-64. Bogotá D.C. Colombia +57 1 466 0599 / +57 315 786 8258 sales@itclatam.com / tss@itclatam.com REV 1.01

Visit our Website: www.itclatam.com



2. Make sure access rules have been created from local network zones to the VPN zone.

3. Make sure access rules have been created from the VPN zone to local network zones.

4. The zone of local network address objects should match the zone to which that network belongs to. For eg. LAN, DMZ etc
5. The destination network should be

assigned zone VPN.

6. Make sure no conflicting rules with higher priority are present.

7. Make sure no conflicting static routes are present in the routing table. Check under **Route Policies** on the **Network** |**Routing** page.

