

# SecureFirst

How to create a mesh VPN network using Tunnel Interfaces and OSPF

KNOWLEDGE DATABASE



# How to create a mesh VPN network using Tunnel Interfaces and OSPF

## **DESCRIPTION:**

It is quite easy to implement a Hub and Spoke VPN network using both Tunnel Interface and OSPF but the transition to a mesh network can be troublesome if you want to redistribute the SonicWall's firewalled subnets.

### **RESOLUTION:**

If you simply use the option "Redistribute Connected Network" in your OSPF configuration, it will perfectly work in hub and spoke environment but will prevent transition to a mesh environment as a tunnel interface is considered a connected interface by the SonicWall, hence the "spoke to spoke" VPN tunnel will fail to be created as both spokes will try to contact each other via the already existing VPN tunnel to the Hub.

🕨 📮 s	System		(4 (N/A)	RIP Disabled		Ø	OSPF Disabled		Ø				
- 👱 N	Network	÷ )	(5 (N/A)	RIP Disabled		Ø	OSPF Disabled		Ø				
	Interfaces	<b>•</b> :	216 (VPN)	RIP Disabled			OSPF Enabled						
	Failover & LB								-		-		
	Zones												
	DNS												
	Address Objects	Apply the following metric to default routes received from Advanced Routing protocols: 110 Change											
	Services	Route Poly	Route Policies										
	Routing	Routeron											
	NAT Policies	View Style:	All Policies	C Custom Policies C Default Poli	des								
	ARP	E.c.	Source	Dectination	Carries	Cataway	Interface	Matrix	Drianity	Drohe	Comment	Configure	
	MAC-IP Anti-spoof	-	Source	Deschaton	Service	Gaterray	Dite lace	Medic	Priority	Probe	Comment	Conigare	
	DHCP Server	1	Any	255.255.255.255/32	Any	0.0.0.0	XO	20	1		2	00	
	IP Helper	III 2	Any	X1Default Gateway	Any	0.0.0.0	×1	20	2		Ø	0	
	Web Proxy Dynamic DNS	П з	Any	X0 Subnet	Any	0.0.0.0	xo	20	3		ø	0	
	Network Monitor	<b>4</b>	Any	X1 Subnet	Any	0.0.0.0	X1	20	4		ø	0	
3 🕑 ۱	3G/Modem	<b>5</b>	Any	X2 Subnet	Any	0.0.0.0	X2	20	5		ø	0	
🕨 📥 s	SonicPoint	-									2	00	
- F 🎼 E	Firewall	6	Any	1.1.212.0/24	Any	0.0.0.0	216	110	0		2	0	
• 🔞 •	OPI-SSL	7	Any	10.10.212.0/24	Any	0.0.0.0	216	110	7		Ø	0	
► <b>6</b> ∂ ∨	/oIP	8	Any	10.10.216.0/24	Any	0.0.0.0	216	110	8		Ø	0	
► 💎 A	Application Firewall	9	Any	10.71.10.0/24	Any	0.0.0.0	216	110	9		ø	0	
- 6 v	/PN	<b>I</b> 10	Any	10.71.216.0/24	Any	0.0.0.0	216	110	10		ø	0	
▶ 🔣 s	SSL VPN	11	X1 IP	Any	Any	X1 Default Gateway	X1	20	11		ø	0 0	
→ 🔮 v → 🚑 u	Jsers	<b>1</b> 2	Any	0.0.0/0	Any	1.1.211.1	X1	20	12		ø	0	

Figure 1





• 💻	System		(5 (N/A)	RIP Disabled		Ø	OSPF Disabled		Ø				•		
- 👱	Network	<b>•</b> 3	216 (VPN)	RIP Disabled		Ø	OSPF Enabled		Ø						
	Interfaces Failover & LB														
	Zones DNS	Apply the fo	lowing metric to	o default routes received from Advanc	ed Routing pro	tocols: 110 Change									
	Address Objects Services	Address Objects Route Policies I to 12 (of 12) (													
	Routing	View Style:	Al Policies	C Custom Policies C Default Policie	5										
	NAT Policies	Γ :	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure			
	MAC-IP Anti-spoof	Π 1	Any	255.255.255.255/32	Any	0.0.0.0	xo	20	1		ø	0			
	DHCP Server	III 2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2		ø	0			
	IP Helper Web Proxy	П з	Any	X0 Subnet	Any	0.0.0.0	x0	20	3		ø	0			
	Dynamic DNS	<b>I</b> 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	4		ø	0			
0	Network Monitor	5	Any	X2 Subnet	Any	0.0.0.0	X2	20	5		Ø	0			
	3G/Modem SonicPoint	<b>F</b> 6	Any	1.1.211.0/24	Any	0.0.0.0	216	110	6		ø	0			
٠ 🏟	Firewall	<b>7</b>	Any	10.10.216.0/24	Any	0.0.0.0	216	110	7		Ø	0			
• 6	DPI-SSL	<b>■</b> 8	Any	10.71.216.0/24	Any	0.0.0.0	216	110	8		ø	0			
<u>}</u>	VoIP	9	Any	10.10.211.0/24	Any	0.0.0.0	216	110	9		ø	0			
• 🖓	Anti-Spam	<b>I</b> 10	Any	10.71.211.0/24	Any	0.0.0.0	216	110	10		ø	0			
ه ا	VPN	П 11	X1 IP	Any	Any	X1 Default Gateway	X1	20	11		ø	0			
	SSL VPN	II 12	Any	0.0.0.0/0	Any	1.1.212.1	X1	20	12		ø	0			
Status: F	Users	Add		Delete								Delete All	•		

### Figure 2

In figure 1, you can see that a route exist to the second spoke (#6). In Figure 2, it should the equivalent on Spoke 2 (route #6).

The solution in to create a fully mesh environment is to use the OSPF "Passive" mode on the connected interface of all the mesh network's nodes.

When OSPF passive mode is enabled on an interface, neither OSPF packets are sent nor any received on this interface. It only results in that interface's network being advertised by OSPF to other OSPF peers as LSA 1 (Router) instead of LSA5 (External) when using "Redistribute Connected Networks".

To Activate the Passive mode on your SonicWall's internal networks, simply go to Network, Routing.

Then configure an internal network.

Routing	- nis								
Routing Mode: Advanced Routing									
Ŧ	Interface (Zone)	RIP	Configure RIP	OSPEv2	Configure OSPF				
*	X0 (LAN)	RIP Disabled	Ø	OSPF Disabled	$\oslash$				
*	XI (WAN)	RIP Disabled	Ø	OSPF Disabled	Ø				





# Then simply choose the mode "Passive"

2 Configuration				
Passive 🖌		OSPF Area:	0	
40		OSPFv2 Area Type:	Normal	¥
10		Interface Cost (1 - 65535):		🗹 Auto
Disabled	~	Router Priority: (0 - 255):	1	
	2 Configuration Passive 40 10 Disabled	2 Configuration Passive V 40 10 Disabled V	2 Configuration         Passive       OSPF Area:         40       OSPFv2 Area Type:         10       Interface Cost (1 - 65535):         Disabled       Router Priority: (0 - 255):	2 Configuration         Passive       OSPF Area:         40       OSPFv2 Area Type:         10       Interface Cost (1 - 65535):         Disabled       Router Priority: (0 - 255):

