

SecureFirst

How to Configure a Site to Site VPN Policy using Main Mode

KNOWLEDGE DATABASE



Howto Configure a Site to Site VPN Policy using Main Mode

Step 1: Creating <u>Address Objects</u> for VPN subnets:

1. Login to the SonicWall Management Interface

2. Click **Manage** in the top navigation menu

3. Navigate to **Objects | Address Objects,** scroll down to the bottom of the page and click on **Add** button.

On the NSA 2650

•	Rules Objects	Address Objects	Addre	ss Groups				
	Match Objects Action Objects	⊕ Add ⊝	Delete 🔻	Search			show	IPv4 & IPv
	Address Objects	C Add Address Object - G	oogle Chrome			00	23	Ŋ
	Service Objects	A Not secure bitp	5://	/addNet	DbjDlg.htm	-	Q	ype
	Bandwidth Objects	CONTONIALLE INTERACTION						AC Address
	Content Filter Objects	SONIC	LL .	ethork security	Appliance			AC Address
	Guttam Catur	Name:	NSA 26	50 Site				
	System Setup	Zone Assignment:	VPN		٠			lost
;	Users	Type:	Netwo	rk	•			lost
	Network	Network	10 10 1	0.0				lost
•	Switching	Netmask/Prefix	10.10.1					
۲	High Availability	Length:	255.25	5.255.0				lost
	WAN Acceleration	Ready					_	lost
	Virtual Assist	(Ready						Intunde
				ADD	>	CLOSE		VECTION
	Security Configuration				1		_	lost
	VEN SHEWES							

On the NSA 4600



4. Configure the Address Objects as mentioned in the figure above, click **Add** and click **Close** when finished.

Step 2: Configuring a VPN policy on <u>Site A</u> <u>SonicWall</u>

1. Click Manage in the top navigation menu.

2. Navigate to **VPN | Base Settings** page and Click **Add** button. The VPN Policy window is displayed.

2. Click the **General** tab.

• Select **IKE using Preshared Secret** from the **Authentication Method** menu.

• Enter a name for the policy in the **Name** field.

• Enter the WAN IP address of the remote connection in the IPsec Primary Gateway Name or Address field (Enter NSA 240's WAN IP address).

- TIP: If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the IPsec Secondary Gateway Name or Address field.
 - Enter a **Shared Secret** password to be used to setup the Security Association the Shared Secret and Confirm Shared Secret fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.
 - Optionally, you may specify a Local IKE ID (optional) and Peer IKE **ID** (optional) for this Policy. By default, the IP Address (ID IPv4 ADDR) is used for Main Mode negotiations, and the SonicWall Identifier (ID_USER_FQDN) is used for Aggressive Mode.





SONIC WALL	Network Security Appliance	MONITOR	INVEST	GATE	MANAGE	QUICK CONFIG	URATION
	VPN Policy - Google Chrome					l	
	A Not secure bitpS://	/vpnCor	fig_0_0.html				Q
Updates Licenses Firmware & Backups	SONICWALL	Network Securit	y Appliance				
WXA Firmware Restart	General Network	Proposals	Advanced				- 11
Connectivity	Security Policy						- 11
A VPN Base Settings	Policy Type:			Site to S	ite		- 11
Advanced Settings	Authentication Method:			IKE usin	g Preshared Sec	ret •	- 11
DHCP over VPN L2TP Server	Name:			VPN to N	ISA 2650 Site		- 11
SSL VPN	IPsec Primary Gateway N	ame or Address:		2.2.2.2			- 11
SonicPoints 3G/4G/Modem	IPsec Secondary Gatewa	y Name or Addres	5.°				- 11
Policies	IKE Authenticatio	n					- 11
Rules	Shared Secret:						- 13
 Objects 	Confirm Shared Secret:				Mask S	hared Secret	- 11
System Setup	Local IKE ID:	IPv4 Address		٠			
Appliance Users	Peer IKE ID:	IPv4 Address		•			Ξ.

- 3. Click the Network Tab.
 - Under Local Networks, select a local network from Choose local network from list: and select the address object X0 Subnet (LAN Primary Subnet)
 - Under **Destination Networks**, select **Choose destination network from list:** and select the address object **NSA 240 Site** (Site B network).
 - NOTE: DHCP over VPN is not supported with IKEv2.

	VPN Policy - Google Chrome			
	• Not secure bttps://	/vpnConfig_0_0.html	*	G
Licenses	SONICWALL Net	work Security Appliance		
WXA Firmware Restart	General Network	Proposals Advanced		ĺ
Connectivity	Local Networks			
Base Settings	Choose local network from	list	X0 Subnet	•
Advanced Settings DHCP over VPN L2TP Server	Any address*			
SSL VPN SonicPoints	Remote Networks			
3G/4G/Modem	Use this VPN Tunnel as d	efault route for all Internet tra	affic	
Policies	Choose destination netwo	rk from list	NSA 2650 Site	5 • 2
Rules	Use IKEv2 IP Pool		-Select IP Pool Network	
 Objects 				
System Setup				
Appliance				
Users	-			

- 4. Click the **Proposals** Tab.
 - Under IKE (Phase 1) Proposal, select Main Mode from the Exchange menu. Aggressive Mode is generally used when WAN addressing is dynamically assigned. IKEv2 causes all the negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.

• Under **IKE (Phase 1) Proposal**, the default values for DH Group, Encryption, Authentication, and Life Time are acceptable

• for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose AES-128, AES-192, or AES-256 from the Authentication menu instead of 3DES for enhanced authentication security.

NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

• Under **IPsec (Phase 2) Proposal**, the default values for Protocol, Encryption, Authentication, Enable Perfect Forward Secrecy, DH Group, and Lifetime are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

SONICWALL	Network Security Appliance	MONITOR	INVESTI	GATE MANAG	GE QUICK CONFIGUR		
	VPN Policy - Google Chrome						
	A Not secure bttps://	/vpnCo	nfig_0_0.h	tml#			
Updates	SONICWALL M	letwork Security Ap	pliance		Î		
Firmware & Backups WXA Firmware	General Network	Proposals Ac	lvanced				
Connectivity	IKE (Phase 1) Prop	osal					
A VPN	Exchange:			Main Mode	*		
Base Settings	DH Group:			Group 14	•		
Advanced Settings	Encountion			AES-256			
DHCP over VPN	Encryption,			CUADEE			
SSI VPN	Authentication:			584230	A		
SonicPoints	Life Time (seconds):			28800			
3G/4G/Modem	Ipsec (Phase 2) Pr	oposal					
Policies							
Rules	Protocol:			ESP	· · · · · ·		
 Objects 	Encryption:			AES-256	•		
System Setup	Authentication:			SHA256	•		
Appliance	Enable Perfect Forward	d Secrecy					
Users	Life Time (seconds):			28800			
Network							
Switching					*		
h that tout hat the	0						

5. Click the **Advanced** Tab.

• Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

ITCorporation[®] Visit our Website: www.itclatam.com



• Select Enable Windows Networking (NetBIOS) Broadcast to allow access to remote network resources by browsing the Windows® Network Neighborhood.

• To manage the local SonicWall through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

• If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to Use this VPN Tunnel as default route for all Internet traffic, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

• Select an interface or zone from the VPN Policy bound to menu. A Zone WAN is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

• Click **OK** to apply the settings.

	VPN Policy - Google Chrome		00 2
	▲ Not secure bttp5:// /vpnCo	nfig_0_0.html#	
Updates Licenses		pliance	
Firmware & Backups WXA Firmware	General Network Proposals	Vanced	Î
Restart	Enable Keep Alive		- 11
Connectivity	Suppress automatic Access Rules creation	for VPN Policy	
VPN Base Settings	Disable IPsec Anti-Replay*		- 11
Advanced Settings	Require authentication of VPN clients by XA	UTH	
DHCP over VPN	Enable Windows Networking (NetBIOS) Bro	adcast	
SSL VPN	Enable Multicast		
SonicPoints	WXA Group: None •		
3G/4G/Modem	Display Suite B Compliant Algorithms Only		- 11
Policies	Apply NAT Policies		
Rules	Allow SonicPointN Layer 3 Management		- 11
objects	Management via this SA:	IN HTTPS SSH SNMP	
System Setup	User login via this SA:	HTTP HTTPS	
Appliance	Default LAN Gateway (optional):		
Users	VPN Policy bound to:	Zone WAN	
Switching			
High Availability			

Step 3: Configuring a VPN policy on <u>Site B</u> <u>SonicWall</u>

1. Login to the <u>Site B SonicWall</u> appliance and Click **Manage** in the top navigation menu. Click **VPN | Base Settings** page and Click **Add** button. The VPN Policy window is displayed.

2. Click the General Tab.

• Select IKE using Preshared Secret from the Authentication Method menu.

• Enter a name for the policy in the **Name** field.

• Enter the WAN IP address of the remote connection in the IPsec Primary Gateway Name or Address field (Enter NSA 4600's WAN IP address).

• If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.

NOTE: Secondary gateways are not supported with IKEv2.

• Enter a **Shared Secret** password to be used to setup the Security Association the Shared Secret and Confirm Shared Secret fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

• Optionally, you may specify a **Local IKE ID** (optional) and **Peer IKE ID** (optional) for this Policy. By default, the IP Address (ID_IPv4_ADDR) is used for Main Mode negotiations, and the SonicWall Identifier (ID_USER_FQDN) is used for Aggressive Mode.

SONICWALL	Network Security Appliance	MONITOR	INVESTIGATE	MANAGE	QUICK CONFIGURATI
COMPLETENCE CONTRACTORS	💎 VPN Policy - Google Chrome				
	A Not secure bttps://	/vpnCo	nfiq_0_0.html#		
Updates Licenses	SONICWALL	Network Security Ap	opliance		Î
Firmware & Backups WXA Firmware Restart	General	Proposals Ad	lvanced		
Connectivity	Security Policy				
VPN	Policy Type:		Site to S	ilte	•
Base Settings	Authentication Method:	IKE usin	IKE using Preshared Secret		
Advanced Settings	Name:		VPN to N	ISA 4600 Site	
L2TP Server	IPsec Primary Gateway N	ame or Address:	1.1.1.1		
SSL VPN SonicPoints	IPsec Secondary Gatewa	/ Name or Address:			
 3G/4G/Modem 	IKE Authenticatio	n			
Policies	Shared Secret		20		
Objects	Confirm Shared Secret			Mask Shar	ed Secret
Custom Colum	Local IKE ID:	IPv4 Address	٠		10 10 4 M / 10
Appliance	Peer IKE ID:	IPv4 Address	•		
Users		10000			-

- 3. Click the Network Tab.
 - Under Local Networks, select a local network from Choose local network from list: and select the address object X0 Subnet (LAN Primary Subnet)





NOTE: DHCP over VPN is not supported with IKEv2.

 Under Destination Networks, select Choose destination network from list: and select the address object NSA 4600 Site (Site A network)



4. Click the **Proposals** Tab. *N***OTE:** Settings must be same as Site A.

SONICWALL	Network Security Appliance	MONITOR	INVES	TIGATE	MANAGE	QUICK CONFIGU
	VPN Policy - Google Chrome					
	A Not secure bttps://	/vpn0	Config_0_0.	.html#		
Updates Licenses	SONICWALL	Network Security	Appliance			
Firmware & Backups WXA Firmware	General Network	Proposals	Advanced			
Connectivity	IKE (Phase 1) Pro	posal				
VPN	Exchange:			Main Mode		•
Base Settings	DH Group:			Group 14		•
Advanced Settings	Encryption:			AES-256		•
L2TP Server	Authentication			SHA256		•
SSL VPN SonicPoints	Life Time (seconds):			28800		
 3G/4G/Modem 	Ipsec (Phase 2) P	roposal				
Policies	Protocol:			ESP		
> Objects	Encryption:			AES-256		•
	Authentication:			SHA256		۲.
System Setup Appliance	Enable Perfect Forward	d Secrecy				
• Users	Life Time (seconds):			28800		
Network Switching						

- 5. Click the Advanced Tab.
- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keep alives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

• Select Enable Windows Networking (NetBIOS) Broadcast to allow access to remote network resources by browsing the Windows® Network Neighborhood.

• To manage the local SonicWall through the VPN tunnel, select HTTP, HTTPS, or both from Management via this SA. Select HTTP, HTTPS, or both in the User login via this SA to allow users to login using the SA.

• If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to Use this VPN Tunnel as default route for all Internet traffic, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

• - Select an interface or zone from the VPN Policy bound to menu. A Zone WAN is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

Click **OK** to apply the settings.

SONICWALL	Network Security Appliance	MONITOR	INVESTIGATE	MANAGE	UICK CON	FIGUR	
	💎 VPN Policy - Google Chrome						
	A Not secure https://	/vpn0	Config_0_0.html#				
Updates	SONICWALL	Network Security	Appliance			Î	
Firmware & Backups WXA Firmware	General Network	Proposals	Advanced				
Connectivity	Advanced Setting	<u>js</u>					
VPN	Enable Keep Alive	•				- 1	
Base Settings Advanced Settings DHCP over VPR L2TP Server > SSL VPN > Gold/Golds > G/4G/Modem Policies > Rules > Objects	Suppress automatic , Disable IPsec Anti-R Require authenticatic Enable Windows Net Enable Multicast WXA Group: None Display Suite B Com Apply NAT Policies	Access Rules creatio eplay [*] on of VPN clients by : tworking (NetBIOS) E vorking (NetBIOS) E pliant Algorithms Onl	n for VPN Policy KAUTH roadcast y				
System Setup	Allow SonicPointN La	ayer 3 Management					
Appliance	Management via this SA:		🗷 нттр	S SSH SNM	2		
Users Network	User login via this SA: Default LAN Gateway Jon	tional):	П нттр	HTTPS		-	
Switching High Availability	VPN Policy bound to:		Zone W/	AN .		• .	

