

SecureFirst

Adding a subnet to an existing Site to Site VPN Tunnel (SonicOS Enhanced)(KB Article and

KNOWLEDGE DATABASE



Adding a subnet to an existing Site to Site VPN Tunnel (SonicOS Enhanced)(KB Article and

DESCRIPTION:

VPN: Adding a subnet to an existing Site to Site VPN Tunnel (SonicOS Enhanced)(KB Article and Video Tutorial)

RESOLUTION:

Feature/Application:

Adding a subnet or subnets to an existing Site to Site VPN Tunnel (SonicOS Enhanced). This scenario based article illustrates how additional subnet/s can be added to an active Site to Site VPN tunnel between two Sonicwall appliances.

In this scenario we have an active VPN tunnel between a NSA 2400 (Site A) at the central site and a NSA 240 (Site B) at the remote site with the following configuration:

Site A : NSA 2400: X1: WAN - 1.1.1.1 X0: LAN - 192.168.1.0/24

Site B: NSA 240: X1: WAN - 2.2.2.2 X0: LAN - 10.10.10.0/24

The Tunnel is up and both sites are able to access the other site's LAN segment.

Site A has expanded their network to include a DMZ segment to their local network: **X2**: **DMZ - 192.168.2.0/24**. In order to add the new subnets to the site to site VPN tunnel follow these directions:



ICorporation® /isit our Website: www.itclatam.com

Procedure: <u>Central Site Configuration (Site A)</u>

Step 1. Create a group called Central Site Network and add the default Address Objects X0 Subnets and X2 Subnets to it.

	Locarticition	Group		
All Authorized All Interface I All M0 Manas All SonicPoir All U0 Manas All U1 Manas All WAN IP All X0 Manas All X1 Manas All X1 Manas	d Access Points	>> <-	X0 Subnet X2 Subnet]

Step 2. Edit the VPN Policy and select the group Central Site Network from the "Choose local network from list" drop-down list under Local Networks in the Network tab.

General	Network	Proposals	Advanced
cal Networks			
		-	
Choose local ne	etwork from list	Local Net	work Group
 Choose local network of Local network of Local network 	etwork from list obtains IP addresse:	Local Net	work Group
Choose local ne Local network o Any address	etwork from list obtains IP addresse:	Local Net	work Group his VPN Tunnel
Choose local network o Local network o Any address mote Networe	etwork from list obtains IP addresse: *ks	Local Net	work Group hthis VPN Tunnel
Choose local network o Local network o Any address emote Networ Use this VPN To	etwork from list obtains IP addresse: rks unnel as default roui	s using DHCP through	work Group this VPN Tunnel
Choose local network o Any address mote Networ Use this VPN To Destination net	etwork from list obtains IP addresses rks unnel as default rou work obtains IP add	te for all Internet trai	work Group hthis VPN Tunnel ffic wough this VPN T

Step 3. Click on OK to save the settings.

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



Remote Site Configuration (Site B)

Step 1. Create an Address Object called Central Site DMZ with the following settings:

Name: Central Site DMZ

Zone: VPN

Type: Network

Network: 192.168.2.0

Net Mask: 255.255.255.0

Name:	Central Site DMZ
Zone Assignment:	VPN 👤
Type:	Network
Network:	192.168.2.0
Netmask:	255.255.255.0

Step 2. Create a group called Central Site Network and add Address Objects Central Site LAN and Central Site DMZ to it. Here it is assumed that an address object Central Site LAN was created when configuring the Site to Site VPN.

Step 3. Edit the VPN Policy and select the group Central Site Network from the "Choose destination network from list" drop-down list under Desination Networks in the Network tab.



How to Test:

Ping from a workstation on the Remote Site to a workstation in the X2 subnet on the Central Site, for eg. 192.168.2.2. Refresh the VPN > Settings page on both side and you should see a green icon on both LAN and DMZ segments.

L	#	Name	Gab	onay	Destinatio	ons		Crypto S	ute			Enable	Configu
п	1	WAN Group/PN						ESP: 3DE	S/HMAC SHA1 (B	E)		1	00
п	z	WLAN Group/P	N					ESP: 3DE	5/HMAC SHAL (1	E)			00
	з	To Central Site		1.1.1.1	192.16 192.16	8.1.1 - 192.168.1 3.2.1 - 192.168.2	255 255)	ESP: 3DE	S/HMAC SHA1 (D	E)		S	08
												-	
Bite T Droup	Add Fo Site I pVPN F	Dele Policies: 1 Policie Policies: 2 Policie	es Defined, 1 Policies E s Defined, 1 Policies E	Enabled, 10 I inabled, 6 Ma	faximum Policies Allow ximum Policies Allower	red 1							Delete
Bite T Droup urre	Add Fo Site I pVPN F	Policies: 1 Polici Policies: 2 Policie Active VPN Tur	es Defined, 1 Policies E s Defined, 1 Policies E mels	Enabled, 10 I inabled, 6 Ma	faximum Policies Allow ximum Policies Allower Start Tabi	ed 1 = Refresh 🕞	Refresh Interval (se	ecs) 10	Items per page	50 Ren	15 1	to 2 (of 2)	Delete
Bite T Droup urre	Add Fa Site pVPN F ently #	Dee Policies: 1 Polici Policies: 2 Policie Active VPN Tur Created	es Defined, 1 Policies E s Defined, 1 Policies E mels Name	Enabled, 10 I inabled, 6 Ma	faximum Policies Allow ximum Policies Allowe Skart Tabl	red J = Refresh (je) Re	Refresh Interval (se mote	ecs) 10	Items per page Gabewa	50 Iten	15 1	to 2 (of 2)	Delete
Bite T Group	Add Fo Site pVPN F ently # 1	Policies: 1 Polici Policies: 2 Policie Active VPN Tur Created 02/05/2010 23:34:33	es Defined, 1 Policies E s Defined, 1 Policies E nels Name To Central Site	Enabled, 10 I inabled, 6 Ma Lo 10	Maximum Policies Allowe skart Tabé sal 10.10.1 - 10.10.10.255	red 1 Refresh (i) Re	Refresh Interval (se mote 92.168.1.1 - 192.16	ecs) 10 8.1.255	Items per page Gatawa 1.1.1.1	50 Ren	is 1 Renegol	to 2 (of 2)	Delete

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