

SecureFirst

VPN: Port Forwarding overa Site to Site VPN Tunnel (SonicOS Enhanced)

KNOWLEDGE DATABASE



Route traffic to certain website(s) through site to site VPN without Route All Traffic VPN

Considering an existing site to site vpn tunnel is created and functional, following are the steps for additional configuration/modification that needs to be done to achieve the above setup.

In this knowledge article we will use google.com website ip address which is randomly taken. So in this example, we will route traffic from Remote Office for google.com website through Head Office firewall ISP.

Configuration in Remote Office Firewall:

Step 1: Create an address object for the website public ip as shown in the screenshot below. The address object will need to be in zone VPN.

SONI	CWA	LL	Net
------	-----	----	-----

twork Security Appliance

Name:	Google	
Zone Assignment:	VPN	۲
Туре:	Host	•
IP Address:	64.89.45.11	
Ready		

Step 2: Create a new Address Group, include the address object we created in step 1 and also add the existing address object for the Head Office network(s). So this address group will consist remote network and the website(s) ip address.

SONIC WALL	Networ	k Security Appliance				Alert Wizinds	Help Logout
						Ho	de: Configuration +
 Cabboard Suttern Interfaces Fallower & L5 Zones DVS Antimal Oktische 	Address Grow View Style:	e Deserver) Default Address Objects Weer B	Version: 8 24019 🗿 246019	0 PvtadPv6	erra Tota I	iof 2) (n) + (+) (H) domes Objects (C) Delete All
Services	1.1	New	Address Detail	Tipe	Ime	Configure	Converta
NAT Policies	0.01	Remote Site		Grad	- 09	Øð	ø
ARP		VPN N/W	192.168.1.0/255.255.255.8	Network	VPN	08	17
Neighbor Discovery		Google	64.89.45.11/255.255.255.255	Host	VPN	08	ø
NAC-D Anti-speed DHCP Server	Add Grou	PDem				5	Delete All

Step 3: In the existing vpn policy to the Head Office, in the Network tab, for the Remote Network, select the Address Group created in Step 2.

Configuration in Head Office Firewall:

Step 1: Create an address object for the website(s)' public ip address as shown in the screenshot below. The address object will need to be in zone WAN.

Name:	Google	
Zone Assignment:	WAN	•
Type:	Host	▼
IP Address:	64.89.45.11	
Deed		

Step 2: Create a new Address Group, include the address object we created in step 1 and also add the existing address object for the Remote Office network(s). So this address group will consist remote network and the website(s) ip address.

SONICWALL	Network	k Security Appli	ance					Alert Wizar
Cookboard System System Network Interfaces Falorer 5.15 Zones DNS Address Objects	Address Address Grow View Style:	es Objects	Custom Address Objects	Default Address Objects	View IP Version:	* P404 0	Pri Ofy © Pri ac	Dems 1 to 1946 Go t
Routing		Name		Address Detail		Тури	Zone	Configure
NAT Policies	II + 1	Local Site				Group		N N
ARP		LAN Subnets				Group		6
Neighbor Discovery		Google		64.09.45.11/255.255.255.255		Heat	WAN	Ø
MAC-IP Anti-spool	Add Grou	Delate]						

Step 3: In the existing vpn policy to the Remote Office, in the Network tab, for the Local Network, select the Address Group created in Step 2.

Step 4.: Configure NAT policy in the Head Office firewall to translate traffic coming from the Remote office network to WAN IP going to the website(s).



AT F	olicies											Iteris 1	to 4 (of 4) (+ +
/iew	Style:	© All Po	icies 🖲 Cus	tom Policies	O Default P	olicies	View IP Version:	 IPv 	4 Only	IPv6 Only	IPv4 and IPv6		Hide Disabled Po
	Add.		elete										Delete 4
		Source		Destination	-	Service		Interface		Priority	Comment	Enable	Configure
		Original				Original							
8	1	Remote Ste	X1 IP	Google	Original	Any	Original	Any	×1	19 🔃			(d) (2) (8)
0	2	Any	X1.1P	Any	Original	Any	Original	X4	XL	20 10	ø	8	<i>.</i>
13	3	Any	X1 IP	Any	Original	Any	Original	XS	XL	21 80	ø		
8	-4	Any	X1 IP	Any	Original	Any	Original	xo	×1	22 ÛQ	ø		
	Add.	De	eletai										Delete -

Once the above setup is done, from the Remote Office site visit the website added in the vpn configuration. If running packet capture in Remote Office firewall and Head Office firewall, you will notice the traffic getting routed through the Head Office firewall to the website ip address.

RESOLUTION FOR SONICOS 6.5 AND LATER

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

Feature/Application:

In existing site to site vpn tunnel setup between Head Office and Remote Office, there would be requirement that traffic to certain website from remote office might need to be routed through head office internet connection through the existing site to site vpn tunnel. However the requirement would not be to configure the site to site vpn tunnel in Route All Traffic through the vpn tunnel.

We can achieve the setup in few configuration modifications in existing vpn policy in the head office and remote office firewall.

Procedure:

Considering an existing site to site vpn tunnel is created and functional, following are the steps for additional configuration/modification that needs to be done to achieve the above setup.

In this knowledge article we will use google.com website ip address which is randomly taken. So in this example, we will route traffic from Remote Office for google.com website through Head Office firewall ISP.

Configuration in Remote Office Firewall:

Step 1: Go to Manage in the top navigation menu

Select Objects | Address Objects and add

SONICWALL	Network Secur	ty Appliance MONITOR		N
> VPN	Address	Objects Address Groups		
3G/4G/Modem	① Ad	Delete • Search	Show IPv4 & IPv6 - View All Types -	0 91
Policies		Name	Details	Туре
Rules Objects	0 1	192.168.168.254	192.168.168.254/255.255.255.255	Host
Match Objects	8 2	3600lan	192.168.136.0/255.255.255.0	Network
Action Objects Address Objects	0 3	400w_lan	192.168.41.0/255.255.255.0	Network
Service Objects	0.4	7b7a6c Radio n 2.4G BSSID	18:b1:69:7b:7a:76	MAC Address
Bandwidth Objects Email Address Objects	0.5	7b7a6c Radio n 5G BSSID	18:b1:69:7b:7a:6e	MAC Address
Content Filter Objects	0.6	Default Active WAN IP	192.168.0.152/255.255.255.255	Host

Create an address object for the website public ip as shown in the screenshot below. The address object will need to be in zone VPN.

🦟 Add Address Objec	t - Google Chrome	
A Not secure	https://192.168.198.1/addNetObjDlg.l	ntml Q
SONIC	Network Security Appliance	
Name:	Google	
Zone Assignment:	VPN T	
Туре:	Host	
IP Address:	64.89.45.11	
Death		
Reduy		
	ADD	CLOSE

Step 2: Create a new Address Group. Go to Manage > Objects > address objects > address group and Add

	SONICWALL'	Networ	k Security	Appliance	MONITOR	INVESTIGATE
,	VPN	•				
۲	SSL VPN	19	Address O	bjects Add	ress Groups	
	Access Points					
•	3G/4G/Modem		Add	O Delete	· Search	
	Policies	1.1		Name		
	Rules		and 11.097			
	Objects	1.1	1 +	All Authorized A	ccess Points	
	Match Objects		2 .	All Interface IP		
	Action Objects					
	Address Objects	1	3 .	All Interface IPV	6 Addresses	

Calle 140 #11-45. Bogotá D.C. Colombia +57 13680290 / +57 3184914652 sales@itclatam.com/tss@itclatam.com REV 1.01



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



Step 3: Include the address object we created in step 1 and also add the existing address object for the Head Office network(s). So this address group will consist remote network and the website(s) ip address.

	NAMES OF TAXABLE PARTY OF TAXABLE AND ADDRESS OF TAXABLE ADDRESS OF TA	Contraction in the second s		000000000			1993
A Not s	ecure bttps://192.168	.198.1/addNetObjGro	upDlg.h	tml			Q
SONI Name: FG It If	irewalled Subnets suest Authentication Servers phPolicyDstAuto_0 Pv6 Link-Local Subnet aspersky Client AV Enforcem AN Interface IP	Security Appliance	I <mark>N</mark> /W ogle			*	
	AN Interface IPv6 Addresses AN IPv6 Subnets AN Subnets IcAfee Client AV Enforcement	<-				*	
кеабу							
	Network Security Appliance MONITOR DIVES	TIGATE NAMAGE QUICK CONFIGURAT	C	к		CANCE	Help 1
	Network Security Appliance MONITOR IDVES	TIGATE MANAGE QUICK CONFIGURAT		к	3	CANCE	Help Mode: Confg.
Ready DNICWALL WPN ss Points GG/Modem	Network Socuth Applance MONITOR INVES	TIGATE MANAGE QUICK CONFIGURAT	C ION C O Ress	K he• ≡ Purpe•		CANCE	Help Mode: Corlig.
INICWALL INICWALL INICWALL INICWALL INICWALL	Network Sourch Applance MONITION INVES	IIGATE NWWAZ QUECK CONFIGURAT Ston IPv1 & IPv5 • Ven All Types • Deals	C ION C C C Ress Type II	K Ne • ≓ Parge *	Class	CANCE	Help Mode: Confg.
NICWALL [®] NICWALL [®] N Points //Hodem 5	Network Security Appliance MONITOR INVES Address Objects Monitories © Add © Dalate • Sanch • Sanch • Sanch • Sanch • Sanch • Sanch	TIGATE NAVAGE QUICK CONFIGURAT	C ION Type II Grag	K le • ≓ Purgi • Version Zone	Class custom	CANCE	Help Help Mode: Corlig Configure () () () () () () () () () () () () ()
NICWALL NICWALL NiPototo 5 0 Objecto s ochore	Metwork Security Appliance MCAILTOR INVES Address Objects Address Organs © Add © Diskets • Search © Finance © G • Search International © G • Search International	TIGATE NWWCZ QUICK CONFIGURAT Show TIP4 & TIP4 • View All Types • Deals extends	C ION C O Rest Units Rest Rest Rest Rest Rest Rest Rest Re	Ke Na • ≓ Purge Vension Zone Na Vita	Class custom Custom		Help Help Mode: Corlig Configure 2 (8)
PN PN P Dette Diffedam El Diffedam El Diffeda	Methods (Socially Appliance MONITOR INVES Address Objects Address Group @ Add @ Delets • Search @ I in • Revent Invite to Invite I if • Revent Invite To Invite To Invite I if • Revent Invite To Invite To Invite To Invite I if • Revent Invite To Invite T	IIGATE WWWCE QUICK CONFIGURAT Show IPv4 & IPv6 • Vew All Types • Details 6488-614(2012)121212212212	C O Reso Type B Once Nat B Network 3	K Ne • # Purge • Version Zone Ne Vin Version Zone	Class custom Custom Custom	Connect	Help Help Mode: Corig

Step 3: In the existing vpn policy to the Head Office, in the Network tab, for the Remote Network, select the Address Group created in Step 2.

Go to **Manage > VPN > Base settings**, edit the VPN in question on the pencil option

	121						Moder Confi
icenses	<u>^</u>						
rniware & Backups	VPN G	ilobal Settings					
estart		and the second					
	M Ensi Unique F	ble VPN Vreweil Identifier (18816970060)	1				
innectivity	Outor .	100109/00/0	62 <u>A</u>		9	View IP Versi	on: # 1Pv4 ©
M .							
IN Dase Settings		alleles					
PN Base Settings Advanced Settings DECE-over VEN	VPN P	olicies		(ii) 🍙 Refresh In	terval (secs) 10 Items per page 50	Items 1	to 5 (of 5) 🛞
N Base Settings Advanced Settings DHCP over VPN L2TP Server	VPN P	olicies Name	Gateway	(ii) 🍺 Refresh In Destinations	nterval (secs) 10 Rems per page 50	Items 1	to 5 (of 5)
N Base Settings Advanced Settings DRCP over VIPI LETP Server E. VPN rease Projects		Name WATH Groups (PH	Gateway	(i) (iii) Refresh In Destinations	tterval (secs) 10 Items per page 50 Crypto Sette ESP: 20ES/HMVC SH41 (IKE)	Items 1	to 5 (of 5)
N Base Settings Advanced Settings DHCP over VPN L2TP Server 8. VPN cess Points 5/46/Hodem	VPN P	Name Name WAN Group/PN WLAN Group/PN	Gateway	(ii) (iii) Refresh In Destinations	terval (secs) 10 Terms per page 50 Crypto Suite ESP 2055/HMC SH1 (X6) ESP 2055/HMC SH1 (X6)	Items 1	to 5 (of 5)
N Bisse Settings Advaced Settings DHCP over VPN L2TP Server L2TP Server L2TP Server L2TP Server L2TP Server L2TP Server L2TP Settings	VPN P	Name Wares WAN Group/IPN WLAN Group/IPN VEN to INSA 2850 Sta	Gateway 3.3.3	(ii) (iii) Refresh In Destinations 10:10.00.0 - 50.10.10.255	terval (secs) 10 Terms per page 50 Crypto Sume ESH 2055/HMC DHU (XK) ESH 2055/HMC DHU (XK) ESH 455-156/HMC DHU2(XK) ESH 455-156/HMC DHU2(XK)	Items 1	to 5 (of 5)
N Base Settings Advanced Settings DIKP over VRI LLTP Server BL VPN zcess Points 3/46/Modem	VPN P	VICIES Name WAN Group/IPN WLAN Group/IPN WAN Droup/IPN URN IN ICSA 2850 Ste To_400e	Gateway 2.2.2.2 10.193.20.200	ii) 🔊 Refresh In Destinations	terval (secs) 10 Items per page 50 Crypto Sette 50 50 50 ESH 2055/HMC DH1 (DK2) 50 50 50	Items 1	to 5 (of 5) (c) Configure (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)

Select **Network Tab** and on the **Remote Network** select the **Address Group** created in Step 2 as shown below:

VPN Policy - Google Chrome			2 0 0
Not secure bttp5://192.168.198.1/vpnConfig	1_5_0.html#		Q
SONICWALL Network Security Appliance			
Local Networks			
Choose local network from list	Select Local Network	۲	
Any address			
Remote Networks			
Use this VPN Tunnel as default route for all Internet trail	effic		
Choose destination network from list	Remote Site	•	
Use IKEV2 IP Pool	Select IP Pool Network	Ŧ	
Ready			
	ок	CANCEL	HELP

Configuration in Head Office Firewall:

Step 1: Create an address object for the website(s)' public ip address as shown in the screenshot below. The address object will need to be in zone WAN.

A Not secure bttps://192.168.198.1/addNetObjDlg.html			Q
SONICWA	LL Network Secur	ity Appliance	
Name:	Google		
Zone Assignment	WAN	•	
Туре:	Host	•	
IP Address:	64.89.45.11		
12000			
Ready			
		ADD	CLOSE

Step 2: Create a new Address Group, include the address object we created in step 1 and also add the existing address object for the Remote Office network(s). So this address group will consist remote network and the website(s) ip address.





Step 3: In the existing vpn policy to the Remote Office, in the Network tab, for the Local Network, select the Address Group created in Step 2.

VPN Policy - Google Chrome			COLU
A Not secure bttp5://192.168.198.1/vpn/	Config_4_0.html		
SONICWALL Network Security Appli	ance		
General Network Proposals Adv	anced		
Local Networks			
Choose local network from list	Local Site	۲	
Any address			
Remote Networks			
O Use this VPN Tunnel as default route for all inte	ernet traffic		
Choose destination network from list	Remote Site	•	
Use IKEv2 IP Pool [*]	Select IP Pool Network	٣	
Roady			
neauy			(
	OK	CANCEL.	HELP



5

Once the above setup is done, from the Remote Office site visit the website added in the vpn configuration. If running packet capture in Remote Office firewall and Head Office firewall, you will notice the traffic getting routed through the Head Office firewall to the website ip address.

Step 4.: Configure NAT policy in the Head Office firewall to translate traffic coming from the Remote office network to WAN IP going to the website(s).

Goto Manage>Rules>NAT Policies and add a new NAT polocy as shown below:

