

## SSL VPN Split tunnelling and route to specific websites using IPs or FQDNs.

- This document is created based on 6.5 firmware & ( 6.5.4 onwards - 7.0 firmware for the FQDNs as previous version didn't include the Dynamic Network Address Object Group - DEAG option) but the procedures are the same with previous versions of SonicOS for the IP method.
- In certain scenarios you may need to have certain public IP addresses routed through the SonicWall SSL VPN due to access to the sites / applications being restricted to your business' public IP address. This would mean that any remote user would not be able to access the service or application unless it was routed through the SSL VPN tunnel. Though you could use Tunnel All mode, this isn't necessary for all other web traffic, it would cause additional overhead on the SonicWall and possibly throughput issues for remote workers.
- Note : If you only need to access a host which has a static IP that does not change, then use the IP address method only below. For hosts which may change IP addresses, you will still need to perform the steps on Page 2 in addition to Pages 4 onwards for the FQDN method.

### Setting up the SonicWall for IP Addresses only

1. Add the Address objects for the required remote IP addresses as below, making sure the objects are in the SSLVPN Zone. You can then add to a Group. (Classic GUI - Network/Address Objects, Gen 7 GUI - Objects/Addresses)

The first screenshot shows the 'Address Object' configuration window. The 'Name' field is 'Netthreat.co.uk test IP', 'Zone Assignment' is 'SSLVPN', 'Type' is 'Host', and 'IP Address' is '89.200.141.183'. The status is 'Ready'. The second screenshot shows a similar window with 'Name' as 'Test DNS IP Ping IP 9.9.9.9', 'Zone Assignment' as 'SSLVPN', 'Type' as 'Host', and 'IP Address' as '9.9.9.9'. The status is also 'Ready'. Both windows have 'OK' and 'CANCEL' buttons at the bottom.

2. Add the individual objects (not the group) to the SSL VPN Client Routes. In this example I also have the Internal networks added to the routes as we will need access to those via the SSL VPN tunnel. (Classic GUI - SSL VPN Client Settings/Default Profile/Client Routes, Gen7 GUI - Network/SSLVPN/Client Settings/Default Profile/Client Routes)

The screenshot shows the 'Client Routes' configuration page. At the top, there are tabs for 'Settings', 'Client Routes' (selected), and 'Client Settings'. Below the tabs, 'Tunnel All Mode' is set to 'Disabled'. Under 'Networks', a list of internal networks is shown: 'All Rogue Access Points', 'All Rogue Devices', 'All WAN IP', 'All X0 Management IP', 'All X1 Management IP', and 'All X2 Management IP'. Under 'Client Routes', a list of external addresses is shown: 'Netthreat.co.uk test IP', 'Test DNS IP Ping IP 9.9.9.9', 'X0 Subnet', and 'X2 Subnet'. Navigation buttons '<-' and '->' are between the lists, and a 'REMOVE ALL' button is at the bottom right.

3. Add the Firewall rule from SSLVPN to WAN. In this instance I am using the group for the [www.netthreat.co.uk](http://www.netthreat.co.uk) IP (this is an example please use one of your own domains) and the Ping to 9.9.9.9 IP. (Classic GUI - Firewall/Access Rules, Gen7 GUI - Policy/Access Rules)
4. We now need to add the IP addresses to the **SSL VPN Services Group** VPN Access networks like in the image below on the right. (Classic GUI - Users/Local Users & Groups/Local User Groups, Gen 7 GUI - Device/Users/Local Users & Groups/Local User Groups)

**SONICWALL™** Network Security Appliance

**General** Advanced QoS BWM GeoIP

**Settings**

Policy Name:

Action: ☒ Allow ☐ Deny ☐ Discard

From:

To:

Source Port:

Service:

Source:

Destination:

Users Included:  ... these users will be allowed if not ex

Users Excluded:  ... these users will be denied

Schedule:

Priority:  ... previously set as **Auto Priority**

Comment:

**SONICWALL™** Network Security Appliance

Settings **Members** **VPN Access** Bookmarks

**VPN Client Access Networks**

Networks:

Enter text to filter the list...

- All Rogue Access Points
- All Rogue Devices
- All U0 Management IP
- All U1 Management IP
- All X0 Management IP
- All X2 Management IP
- All X3 Management IP
- All X4 Management IP
- All X5 Management IP
- All X6 Management IP
- All X7 Management IP
- bobo Interface IP
- bobo Interface IPv6 Addresses
- hoho.IPv6 Subnets

Access List:

Enter text to filter the list...

- Netthreat.co.uk test IP
- Test DNS IP Ping IP 9.9.9.9
- X0 Subnet
- X2 Subnet

5. There should already be a NAT policy auto created to translate the traffic out of the WAN IP from the SSL VPN Network. If not, create one like below. (Classic GUI - Network/NAT Policies, Gen 7 GUI - Policy/NAT Rules)

**SONICWALL™** Network Security Appliance

**General** Advanced

**NAT Policy Settings**

Name:

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

**IP Version:** ☒ IPv4 Only ☐ IPv6 Only ☐ NAT64 Only

☒ Enable NAT Policy

6. As we can see when we connect to the SSL VPN, the traffic to the networks is being translated correctly.

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
79	02/05/2019 13:12:33.288	X1*()	X1	172.16.36.1	89.200.	IP	TCP	51444,80	FORWARDED	66[66]
80	02/05/2019 13:12:33.288	X1*()	X1	172.16.36.1	89.200.	IP	TCP	51445,80	FORWARDED	66[66]
81	02/05/2019 13:12:33.288	--	X1*	192.168.10.100	89.200.	IP	TCP	24432,80	FORWARDED	66[66]
82	02/05/2019 13:12:33.288	--	X1*	192.168.10.100	89.200.	IP	TCP	14031,80	FORWARDED	66[66]
83	02/05/2019 13:12:33.304	X1*()	--	89.200.	192.168.10.100	IP	TCP	80,24432	Received	66[66]
84	02/05/2019 13:12:33.304	X1*()	--	89.200.	192.168.10.100	IP	TCP	80,14031	Received	66[66]

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	02/05/2019 13:12:07.096	X1*()	X1	172.16.36.1	9.9.9.9	IP	ICMP	--	FORWARDED	74[74]
2	02/05/2019 13:12:07.096	--	X1*	192.168.10.100	9.9.9.9	IP	ICMP	--	FORWARDED	74[74]
3	02/05/2019 13:12:07.144	X1*()	--	9.9.9.9	192.168.10.100	IP	ICMP	--	Received	74[74]
4	02/05/2019 13:12:08.112	X1*()	X1	172.16.36.1	9.9.9.9	IP	ICMP	--	FORWARDED	74[74]

7. NetExtender shows all the Routes:

SONICWALL NetExtender	
User: preston Connected: 0 Days 00:00:07	
Status	Routes
Destination	Netmask
172.16.32.0	255.255.255.0
192.168.2.0	255.255.255.0
9.9.9.9	255.255.255.255
89.200.	255.255.255.255

8. Also, on the Route Print from the Remote PC you can see the routes created in the route table which will be removed when NetExtender disconnects.

Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.2.1	192.168.2.230	266
	9.9.9.9	255.255.255.255	On-link	172.16.36.2	10
	89.200.	255.255.255.255	On-link	172.16.36.2	10
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	306

## Setting up the FQDN method

If you need to route to an application where the IP addresses change often, then you will need to use the DEAG method as the SSL VPN routing and the Windows route table cannot work with FQDNs therefore we need to convert them in to IP addresses.

1. To get the SonicWall SSLVPN to work with FQDNs we need to utilise the **DEAG** (Dynamic External Address Object Groups)
2. To do this we need to first save the Powershell script included called **Host2IPs.txt** edit this with notepad and save the file as **Host2IPs.ps1**
3. On the Server / PC (minimum Server 2012R2 or Windows 8.1) that you will be hosting this on, you will need to enable scripts. To do this, load PowerShell as an administrator and run the following commands: (we have set this up with a server which is only allowed out to the Internet)

***Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force;***

Also in PowerShell run the command : ***Import-Module DnsClient***

To verify this has been successful enter ***Get-Command -Module DnsClient*** you should see the available DNS modules.

4. This Script does the following things:
  - a. resolves the hostnames from the **Hostnames.txt** file to IP addresses IPV4 only as the SonicWall DEAG only supports IPV4 currently.
  - b. saves the IP addresses to a text file called **ipaddresses.txt** (encoded as ANSI/Ascii as this is the format needed for the SonicWall DEAG)
  - c. adds or removes IPs if any are different from the last scan, removes any duplicates and sorts the order each time the script is run, if changes are found then the file is updated and an email notification is sent to users.
  - d. it will send the users in the AD group or Local Users used for VPN users a notification email to restart the NetExtender / Mobile Connect client if the IP addresses change so they can pick up the new IP routes.

The example script file is included in separate text file which you will need to change the extension to .ps1, there are also three separate text files to be used for the email parameters depending on which method you require, one file for AD or two files needed for Local Users

The script file includes both the email methods, to use one or the other you will need to comment out the section not required like in the example below, or if needed to you can leave both uncommented and email both AD Users and Local Users at the same time if you have a mix of users on the SonicWall i.e.(some AD Users and some Local Users), by default the script has the Local Users email section commented out.

5. **Local Users** refers to users created in the SonicWall Local Users Database using a 3<sup>rd</sup> party Email Server like Google mail rather than users synced via LDAP.

For **Local users** you will need to create a list of all email addresses as shown in the example **local-email-users.txt** file this will be used in the Bcc list, you also need to provide a **To** email address normally this would be the IT admin email address, this is entered in the **3rdpartyemail-params.txt** file. (example below but without the details in the brackets - these are just descriptions for you) the email files in my example are save to the C:/ root directory, but you can save these elsewhere just amend the IP2Hosts.ps1 with the location.

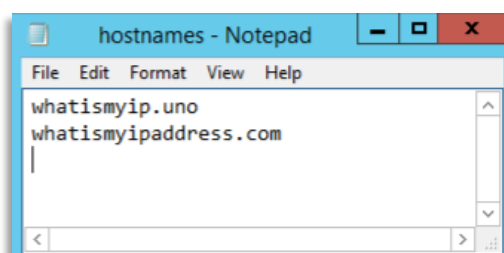
Smtg.gmail.com	(SMTP Server)
587	(Server Port)
bob@gmail.com	(Email Username)
fgdgdgdgdee	(Password)
<a href="mailto:itadmin@domain.co.uk">itadmin@domain.co.uk</a>	(Email From Address)
NetExtender Restart Required	(Email Subject)
Please restart your NetExtender SSL VPN Client - Any issues Please contact Support (Email Body)	

6. For **AD User Groups** you will also need to edit the example file called **email-params.txt** and put it in a separate folder. In this example, it is in the Root folder C:\. This will need to include the email parameters as below, substituting these values for those of your mail server, account credentials and desired text (but without the details in the brackets - these are just descriptions for you).

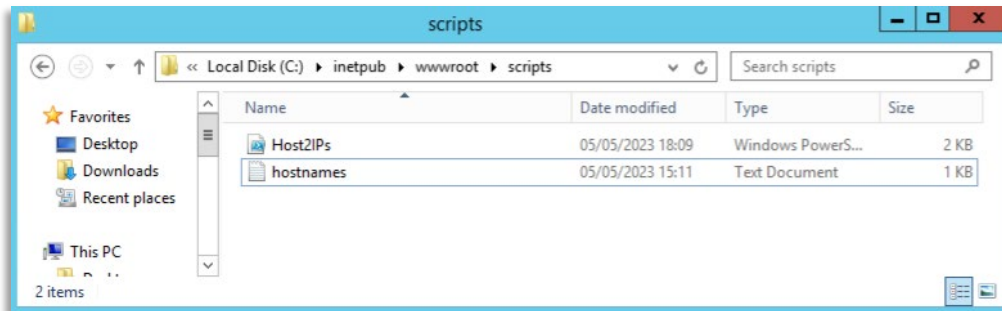
172.16.35.211	(Server IP)
25	(Server Port)
Admintest	(AD User)
pa55W0rd	(AD Password)
<a href="mailto:itadmin@domain.co.uk">itadmin@domain.co.uk</a>	(Email From Address)
NetExtender Restart Required	(Email Subject)
Please restart your NetExtender SSL VPN Client - Any issues Please contact Support (Email Body)	
SSL VPN Users	(AD User Group)

7. We also need to edit the text file with the FQDN entries to be used called **hostnames.txt**.

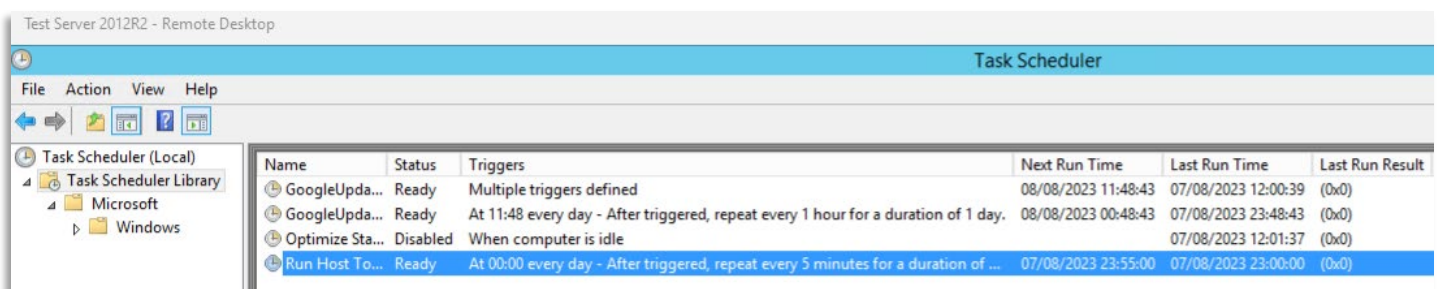
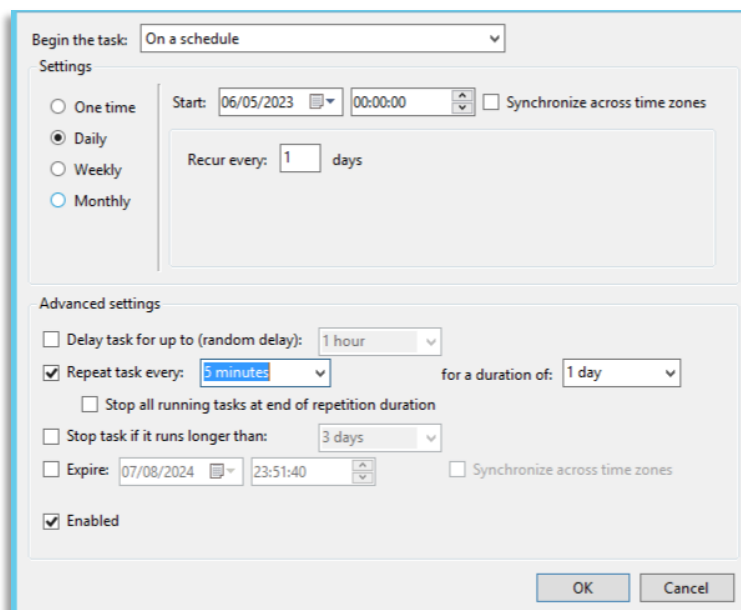
In my example I've just added two but you can add whichever FQDNs you require.



8. Make sure both files are saved in to the same folder as the script is set to run. (as this is hosted via HTTPS I have saved in a new folder called scripts in the wwwroot.) If you are using FTP you can put in another folder if you wish.



9. I would recommend using the Task Scheduler to run the Host2IP.ps1 script on the server to run daily every 5 minutes to be in sync with the DEAG refresh time to get the latest resolved IP addresses. Make sure also add the folder path to the file in the **Start-in** section under the Actions tab.



## Setting up the DEAG (Dynamic External Address Object Groups) on the SonicWall

1. To use HTTPS, ensure your website is set to enable Directory browsing and is bound to port 443 for HTTPS.
2. To Set up the DEAG object in the ( Classic GUI - Firewall/Dynamic External Objects, Gen7 GUI -Object/Dynamic Group), select Add and enter the details. I am using an internally hosted website so in this case it is pointing to <https://172.16.32.181/ipaddresses.txt>
3. If using FTP method, if the file is in the FTP Root folder then in the **Directory Path** just enter \

The screenshot shows the 'Add Dynamic External Object' configuration window. The fields are as follows:

- Name: DEAG\_ IPAddresses
- Type: Address Group
- Zone Assignment: WAN
- FQDN: ☐
- Enable Periodic Download: ☒
- Download Interval: 5 minutes
- protocol: HTTPS
- URL: https://172.16.32.181/ipad

Buttons: Cancel, Save

4. Next select Download. If there is an error check the URL is correct.

The screenshot shows the list of Dynamic External Objects. The table has two columns: URL and CONFIGURE. The first row shows the URL 'https://172.16.32.181/ipadde' and a 'Download' button. Below the table are icons for Add, Delete, Refresh, Edit, View, and Delete.

URL	CONFIGURE
https://172.16.32.181/ipadde	Download

5. If you expand, you will see the List of IP addresses from the text file has imported correctly.



Search...				
<input type="checkbox"/>	#	NAME	FQDN	TYPE
<input type="checkbox"/>	▼ 1	DEAG_IPAddresses	No	Address Group
1	104.16.154.36			
2	104.16.155.36			
3	104.21.56.242			
4	172.67.138.114			

6. Once this has completed you need to go to ( Classic GUI - Network/Address Objects/Address Groups, Gen7 GUI - Object/Addresses/Address Groups). Create a new Address Object Group and add the DEAG group in to the new group. Here I called mine SSL VPN 2 Group. The reason for doing this is that you cannot select the DEAG group from the SSL VPN Routes menu but you can select a group of which the DEAG group is a member.

<input type="checkbox"/>	#	GROUP NAME
<input type="checkbox"/>	▼ 1	SSL VPN 2 Group
		DEAG_IPAddresses

7. You can now go to Classic GUI - SSL VPN/Client Settings/Default Policy/Client RoutesGen, 7 GUI - Network/SSL VPN/Client Settings/Default Policy/Client Routes, and edit the policy and add the Group we create earlier in to it, as in the image below:

CLIENT ROUTES

Tunnel All Mode ☐ ⓘ

Networks 320 items

Search

Client Routes 3 items

Search

- SSL VPN 2 Group
- X0 Subnet
- X2 Subnet

8. Ensure you also update the User Group settings in (Classic GUI - Users/Local Users & Groups/Local User Groups/SSL VPN Services, Gen 7GUI - Device/Users/Local Users & Group/Local User Groups/SSL VPN Services) as below:



## Local Group Settings

Settings Members **VPN Access**

VPN CLIENT ACCESS NETWORKS

Available Networks 568 items

Search

Selected Networks 3 items

Search

SSL VPN 2 Group

X0 Subnet

X2 Subnet

Cancel Save


9. Before we connect with NetExtender I will go to the website (<https://whatismyip.uno/>) to show my real local Public address. I've omitted the last two numbers for privacy.




10. To Test the FQDN to IP is working correctly, we can connect using NetExtender. As you can see the routes for the FQDNs have been added to the routes in NetExtender.

Status	Routes	DNS
Destination	Netmask	
192.168.2.0	255.255.255.0	
172.16.32.0	255.255.255.0	
0.0.0.0	255.255.255.255	
104.16.154.36	255.255.255.255	
104.16.155.36	255.255.255.255	
104.21.56.242	255.255.255.255	
172.67.138.114	255.255.255.255	

11. If we now go to the same website we can see that is showing as the public IP address through the SSLVPN tunnel.

 What Is My IP

My IP Address Is: 193.248.150.1

My IP Location: Boulogne-Billancourt, France   
ISP: Orange

12. When using this method, be aware that if the FQDNs update on the IPAddresses.txt file then the user will need to reconnect to NetExtender to pull through the new routes. The script example in this guide will email the AD user group with the sample notification below:

### NetExtender Restart Required

itadmin@ .co.uk [itadmin@ .co.uk]

**Sent:** 10 May 2023 15:03

**To:** preston

Please restart your NetExtender SSL VPN Client - Any issues Please contact Support

**Note :** The maximum number of DEAGs, including both IP address and FQDN types, is 25% of the total number of address groups supported by the device.

If the accompanying script files are not in the location where you obtained this PDF please contact us at the details below.

## Need help?

Here at NetThreat we offer a full range of professional services so if you would like assistance with setting this up, need to customise it for your environment, or any assistance with your SonicWall device configuration, please do give us a call on 0121 270 1800 or email [enquire@netthreat.co.uk](mailto:enquire@netthreat.co.uk) and we'll be happy to discuss how we can help.