

Integration Guide: Site-to-Site VPN Between SonicWall NGFW and Microsoft Azure VPN Gateway

April 2019

This document describes how SonicOS is integrated with Microsoft Azure, a cloud computing platform and infrastructure created by Microsoft. Such integration allows the site-to-site configuration of a Virtual Private Network (VPN) between a next-generation SonicWall firewall and Microsoft Azure.

Topics:

- [Requirements](#)
- [Networks](#)
- [Azure VPN Gateway](#)
- [Azure Configuration](#)
- [SonicWall Configuration](#)

Requirements

You need the following subscriptions and hardware to configure a tunnel interface VPN:

- Azure valid subscription
- SonicWall NGFW running SonicOS 6.2.5 and above
- Valid Public IP Address at on premise side

Networks

The following networks are used for demonstration purposes in this guide. Your networks may be different.

Azure Side Resources

- Gateway subnet: 10.10.1.0/24
- LAN subnet: 10.10.2.0/24

SonicWall Side Resources

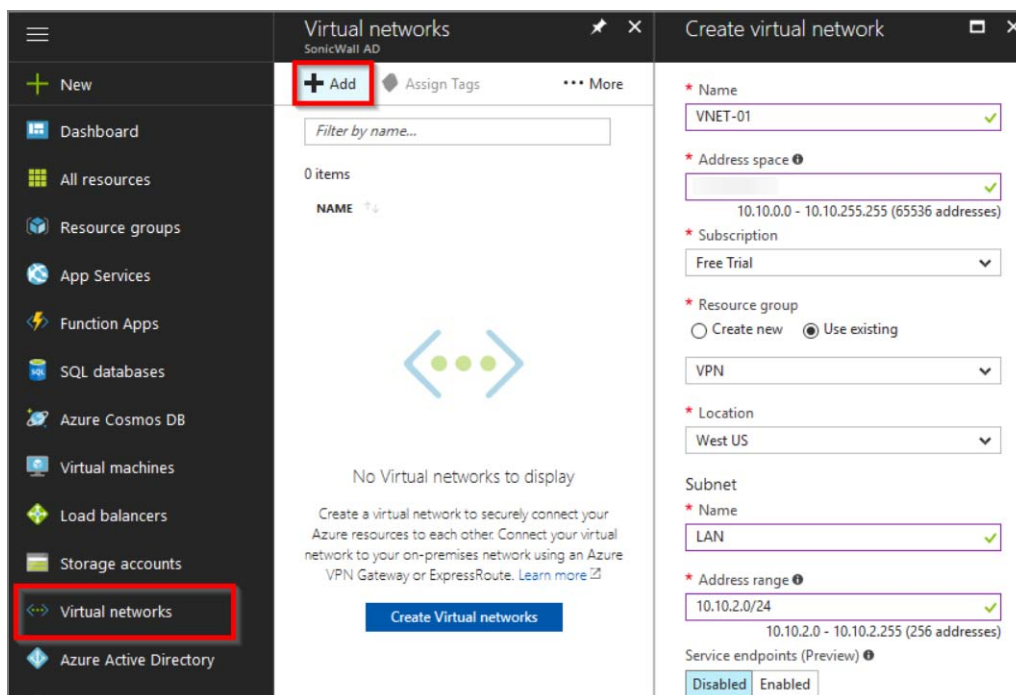
- LAN subnet: 192.168.168.0/24
- Public routable WAN IP address

Azure VPN Gateway

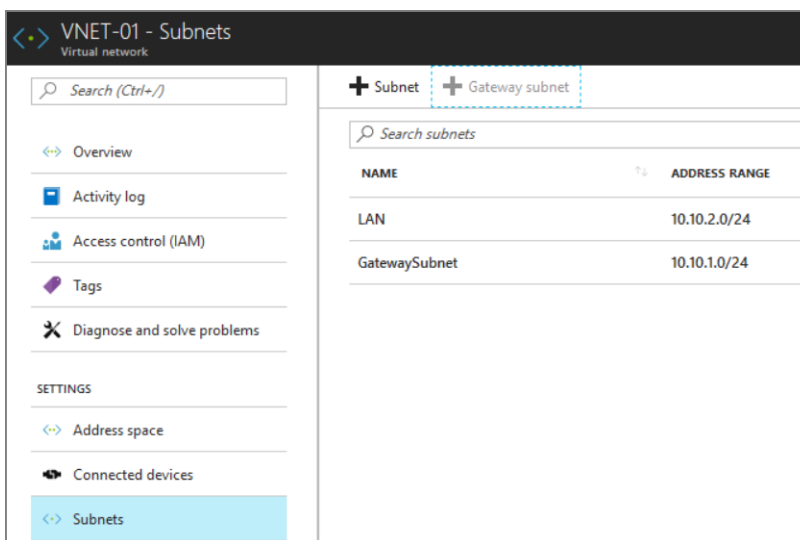
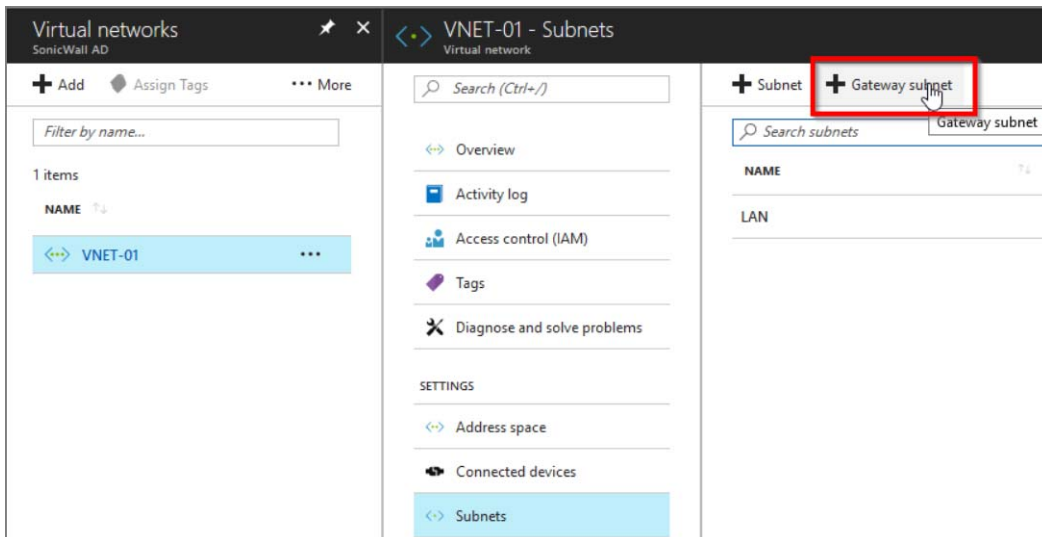
SonicOS on-premises networks can securely connect to Microsoft Azure through the Azure VPN Gateway service. The connection is safe using the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). Refer to this [Microsoft Azure VPN Gateway](#) article to learn more about the product.

Azure Configuration

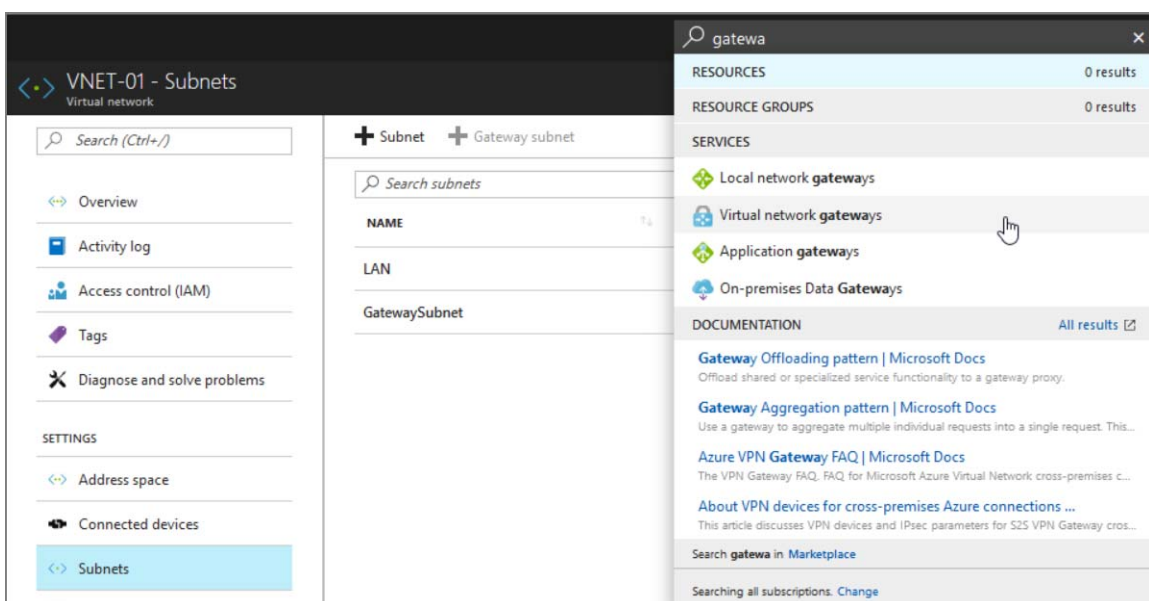
- 1 Log into the **Microsoft Azure** portal at <https://portal.azure.com>.
- 2 Navigate to **Virtual networks** and click **Add** to create a new network scheme.
- 3 In this scenario the following network has been defined. Once filled out, click **Create Virtual network**.
 - **Name:** VNET-01
 - **Address space:** 10.10.0.0/16
 - **Subnet name:** LAN
 - **Subnet address range:** 10.10.2.0/24



- 4 Next, define the gateway network inside of the virtual network created. In this case the virtual network is **VNET-01**. Click VNET-01, select **Subnets | Gateway Subnet**. Define the gateway subnet (in this case 10.10.1.0/24) and click **Create**.



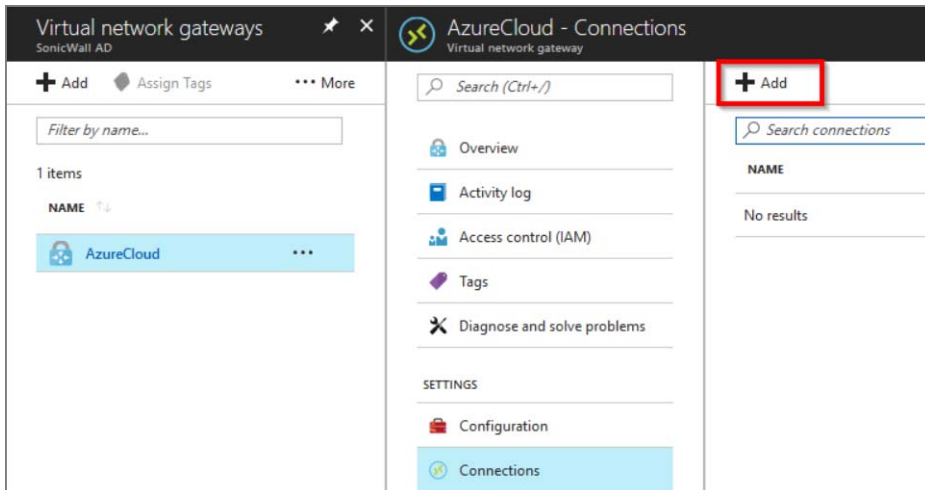
- 5 Create a virtual network gateway. In the search bar at the top of the page type **gateway**. Select **Virtual network gateways**:



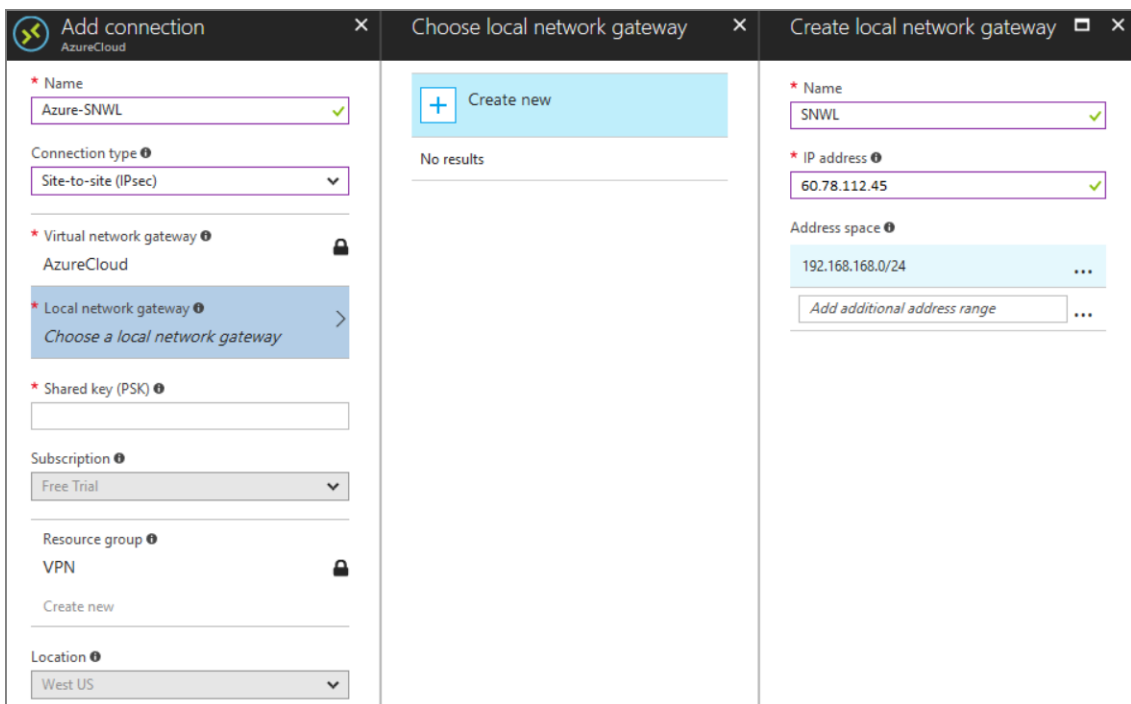
- 6 Create a new virtual network gateway. Give the gateway a name and define the **VPN** type. Select gateway type VPN and VPN type **Route-based**. Select the virtual network VNET-01 and create a new public IP address. Use this public IP address later while configuring the VPN on the SonicWall. Click **Create**.

NOTE: Provisioning a virtual network gateway may take up to 45 minutes.

- 7 Click on the newly created virtual network gateway. Select **Connections | Add**.



- 8 Give the connection a name. Under connection type select **Site-to-site (IPsec)**. Create a new local network gateway. This is the public IP of the SonicWall and the local network. The local network of the SonicWall is the default SonicWall subnet 192.168.168.0/24.



- 9 Provide a secure shared key. This is also used on the SonicWall. Click **OK**.

Add connection
AzureCloud

* Name
Azure-SNWL ✓

Connection type ⓘ
Site-to-site (IPsec) ▼

* Virtual network gateway ⓘ
AzureCloud 🔒

* Local network gateway ⓘ
(new) SNWL >

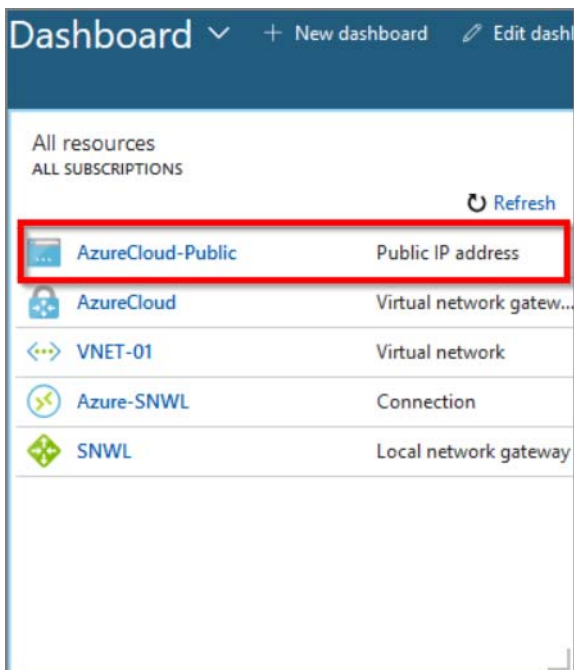
* Shared key (PSK) ⓘ
[Redacted] ✓

Subscription ⓘ
Free Trial ▼

Resource group ⓘ
VPN 🔒
Create new

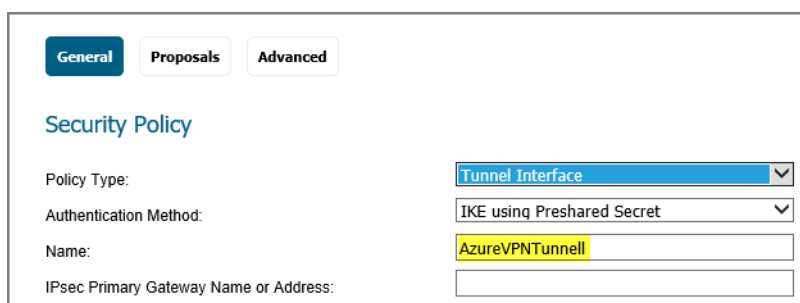
Location ⓘ
West US ▼

10 Grab the public IP of Azure and use it in the SonicWall. Navigate to **Dashboard** and select the **Public IP address** resource. Take a note of the public IP for the next steps.



SonicWall Configuration

- 1 Log into the SonicWall NGFW.
- 2 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.
- 3 Under **VPN Policies**, click **ADD** to create a new VPN policy.
- 4 Give the VPN policy a name. Use the following settings:
 - **Policy Type:** Tunnel Interface
 - **Authentication Method:** IKE using Preshared Secret
 - Next click the **Proposals** tab.



The screenshot shows the 'Security Policy' configuration page in the SonicWall management interface. At the top, there are three tabs: 'General' (selected), 'Proposals', and 'Advanced'. Below the tabs, the 'Security Policy' title is displayed. The configuration fields are as follows:

Policy Type:	Tunnel Interface
Authentication Method:	IKE using Preshared Secret
Name:	AzureVPNTunnell
IPsec Primary Gateway Name or Address:	

- 5 Under Proposals select:
 - Under **IKE (Phase 1) Proposal** select:
 - **Exchange:** IKEv2 Mode
 - **DH Group:** Group 2,
 - **Encryption:** AES-256
 - **Authentication:** SHA1
 - **Life Time (seconds):** 28800
 - Under **Ipsec (Phase 2) Proposal** select:
 - **Protocol:** ESP
 - **Encryption:** 3DES
 - **Authentication:** SHA1
 - **Life Time (seconds):** 27000

General Proposals **Advanced**

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds): 27000

6 Under **Advanced > Advanced Settings**, select:

- Enable Keep Alive.
- Deselect **Enable Windows Networking (NetBIOS) Broadcast**.
- Under **IKEv2 Settings**, select **Do not send trigger packet during IKE SA negotiation**.

General Proposals **Advanced**

Advanced Settings

Enable Keep Alive

Disable IPsec Anti-Replay

Allow Advanced Routing

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

Permit Acceleration

Display Suite B Compliant Algorithms Only

Apply NAT Policies

Allow SonicPointN Layer 3 Management

Management via this SA: HTTPS

User login via this SA: HTTP

VPN Policy bound to: Interface

IKEv2 Settings

Do not send trigger packet during IKE SA negotiation

7 Navigate to **Manage | System Setup | Network > Routing**.

8 Select **Route Policies** and click **Add**.

#	Name	Source	Destination	Service	App	TOS/Mask	Route	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1		MGMT IP	Any	Any	N/A	Any	Standard	MGMT Default Gateway	MGMT	1	1			
2		Any	MGMT IP	Any	N/A	Any	Standard	0.0.0.0	MGMT	1	2			
3		Any		Any	N/A	Any	Standard	0.0.0.0	X0	20	6			
4		Any		Any	N/A	Any	Standard	0.0.0.0	X1	20	7			
5		Any	X0 Subnet	Any	N/A	Any	Standard	0.0.0.0	X0	20	9			
6		Any	X1 Subnet	Any	N/A	Any	Standard	0.0.0.0	X1	20	10			
7		X1 IP	Any	Any	N/A	Any	Standard	X1 Default Gateway	X1	20	11			
8		Any	0.0.0.0/0	Any	N/A	Any	Standard	10.203.20.1	X1	20	12			

- 9 Under **Route Policy Settings**, create a new policy.
- 10 Set the destination for the **Azure Network** and select the Azure interface.

General
Advanced

Route Policy Settings

Source:

Destination:

Service:

Standard Route Multi-Path Route

Interface:

Gateway:

Metric:

Comment:

Disable route when the interface is disconnected

Permit Acceleration

Auto-add Access Rules

Probe:

Disable route when probe succeeds

Probe default state is UP

It takes 5-7 minutes for the VPN policy to come up. Once the VPN policy is up you see a green indicator and a new entry under **Currently Active VPN Tunnels**.

- 11 Click **OK**.

References

[Tutorial: Create and manage a VPN gateway using PowerShell](#)

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.


The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.


For more information, visit <https://www.sonicwall.com/legal>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>.

Legend

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 4/23/19