# How to set up Site-to-Site VPN between Synology Router and Microsoft Azure

Site-to-Site VPN, powered by Synology VPN Plus, allows multiple networks in geographically different locations to establish secure connections to each other over the Internet.

Aside from the benefits you may experience when using a Site-to-Site VPN tunnel between two Synology Router products, you may also implement a hybrid cloud solution by setting up such tunnel between a Synology Router and

### Microsoft Azure Virtual Network service.

This tutorial will guide you through the setup of Site-to-Site VPN between Synology Router and Microsoft Azure Virtual Network.

# Contents

- 1. Before you start
- 2. <u>Site-to-Site VPN configuration on Microsoft Azure</u>
  - <u>2.1 Create a virtual network</u>
  - <u>2.2 Create Virtual Network Gateway</u>
  - <u>2.3 Create Local Network Gateway</u>
- 3. <u>Site-to-Site VPN configuration on Synology Router</u>
- 4. Establish connection between Synology Router and Microsoft Azure

#### 1. Before you start

Before you proceed with the Site-to-Site VPN setup, please make sure you have already had an adequate environment

as described below.



- Set up your Synology Router **RT2600ac** or **RT1900ac**, and make sure it is running on SRM 1.1.5 or above.
- Install VPN Plus Server 1.2.0 or above.
- In VPN Plus Server, activate the **Site-to-Site VPN** feature.

Note: For more information on our licensing plan, please refer to this webpage.

This tutorial is based on the scenario described below.

# • Synology Router (RT2600ac or RT1900ac) site

- Internal subnet: 192.168.1.0/24
- Gateway: 111.xxx.xxx.xxx
- Microsoft Azure site
  - Internal subnet: 10.0.1.0/27
  - Gateway: 13.xx.xx.xx
- Pre-shared key: 123456789
- Encryption configuration:
  - Phase 1:
    - Encryption: AES128
    - Authentication: SHA-256
    - Key life: 28800
    - DH Group: 2 (modp 1024)
    - DPD (Dead Peer Detection): disable
  - Phase 2:
    - Encryption: AES128
    - Authentication: SHA-256
    - Key life: 27000
    - DH Group: 2 (modp 1024)

# 2. Site-to-Site VPN configuration on Microsoft Azure

# 2.1 Create a virtual network

1. Log in to your <u>Microsoft Azure</u> account.

2. Go to **New > Networking**, and click **Learn more** under **Virtual network**.



# 3. Make sure the deployment model remains at **Resource Manager**, and click **Create**.

Microsoft Azure New >	Virtual network		
≡	Virtual network	* ×	ζ
+ New	Create a logically isolated section	in Microsoft Azure with this networking service. You can securely	
🔲 Dashboard	Virtual Networks make it easy for Azure while providing connectivi	you to take advantage of the scalable, on-demand infrastructure of ty to data and applications on-premises, including systems running	
All resources	on Windows Server, mainframes,	and UNIX.	
📦 Resource groups	Use Virtual Network to: • Extend your datacenter		
🔇 App Services	<ul><li> Build distributed applicati</li><li> Remotely debug your application</li></ul>	ons plications	
Iunction Apps	🗾 f in 🜿 8		
👼 SQL databases	PUBLISHER	Microsoft	
🥖 Azure Cosmos DB		Service overview	
🧕 Virtual machines	USEFUL LINKS	Documentation Pricing	
💠 Load balancers			
Storage accounts			
↔ Virtual networks			
Azure Active Directory			
😁 Monitor			
🔷 Advisor			
Security Center			
Oost Management + Billing			
Pelp + support	Select a deployment model 0		
More services >	Resource Manager	✓	

4. Complete the following setup to create a virtual network:



- a. Name: Here, we enter "Synology\_VPN".
  - b. **Address space**: Specify the address range for the virtual network. Here, we enter *10.0.1.0/27*.
  - c. Subscription: Select your subscription to Microsoft Azure service.
  - d. Resource group: Here, we select Create new and enter "Synology".
  - e. **Location**: Select the location of your virtual network.
  - f. Specify the properties of the **Subnet**:
    - a. Name: Here, we enter "GatewaySubnet".
    - Address range: Specify the address range for the subnet. This range must be within or equal to the Address space configured above. Here, we enter 10.0.1.0/27
    - g. Click **Create** when the setting is complete.

5. Do the following if you wish to connect to a specific DNS server:

Microsoft Azure Virtual n	etworks > Synology_VPN - DNS servers		$\mathcal P$ Search resources, services and docs $ imes$
	Virtual networks 🖈 🗙 部副科技股份有限公司	Synology_VPN - DNS servers	5
+ New	or Hore + Add the Columns + • • • • More		F Save X Discard
🗔 Dashboard	Filter by name	Overview	Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.
All resources	1 items 2	Activity log	DNS servers 0 2
Resource groups	↔ Synology_VPN ···	Access control (IAM)	Default (Azure-provided)     O Custom
App Services		Tags	Add DNS server
Function Apps     SOL databases		Diagnose and solve problems	
SQL Gatabases			
Virtual machines		Connected devices	
- Load balancers		Subnets 3	
Storage accounts 1		📰 DNS servers	
←> Virtual networks		Peerings	
Azure Active Directory		Service endpoints (Preview)	
Monitor		Locks	
🔷 Advisor		Automation script	
Security Center		MONITORING	
Ocst Management + Billing		👗 Diagram	
Help + support		SUPPORT + TROUBLESHOOTING	
More services >		New support request	

- In the just now created *Synology\_VPN*, go to **DNS servers** under **SETTINGS** section.
  - a. Select **Custom**, and specify the DNS server address.

.

#### 2.2 Create Virtual Network Gateway

#### 1. Go to **New > Networking**, and click **Virtual network gateway**.



2. Complete the following setup to create a virtual network gateway:

	Provisioning a virtual network gateway may take up to 45 minutes.			ОК	
More services >	Create Automation options			0	<u>o</u> a
Help + support	Pin to dashboard				
Oost Management + Billing					
📋 Security Center	East Asia				
<table-cell-rows> Advisor</table-cell-rows>	* Location 0				
🤭 Monitor	Resource group 0 Synology				
Azure Active Directory	QC4 v				
<> Virtual networks	* Subscription				
Storage accounts	Configure BGP ASN				
🚸 Load balancers	* First IP configuration (new) GatewayIP				
Virtual machines	Synology_VPN				
🧭 Azure Cosmos DB	* Virtual network 0				
a SQL databases	Enable active-active mode 0				
Function Apps	VpnGw1 v				
🔕 App Services	Route-based Policy-based	No results			
🛞 Resource groups	VPN type 0				
All resources	VPN ExpressRoute				
E Dashboard	Gateway I oSynologyVPN	No public IP addresses found in the selected subscription and location 'East Asia'.		GatewayIP	
+ New	* Name (1			* Name 5	
=	Create virtual network gateway 🗙	Choose public IP address Dynamic public IP addresses that are not in use won't have an IP address assigned to them.	×	Create public IP address X	
Microsoft Azure New >	Create virtual network gateway > Choose public IP	address > Create public IP address	ď	Search resources, services and docs	×

- a. Name: Here, we enter "GatewayToSynologyVPN".
- b. Click Virtual network, and select the just now created Synology\_VPN.
- c. Click **First IP configuration** > **Create new**, and here, we enter *Gateway IP*.
- d. Click **Create** when the setting is complete.
- 3. Go to All resources, and search for the just now created "GatewayToSynologyVPN". You will then find the

automatically assigned **Public IP address**.

Microsoft Azure All resource	es	
≡	All resources 群輝料技股份有限公司	* ×
+ New	+ Add  ≡≡ Columns  ひ Refresh  ♦ Assign Tags   □ De	lelete
🗉 Dashboard 🛛 🚺	Subscriptions: 2 - Don't see a subscription? Switch directories	
All resources	GatewayToSynologyVPN All resource groups V All typ	pes V All locations V No grouping V
Resource groups	1 items 3 Type 🗘	RESOURCE GROUP
🔇 App Services	GatewayToSynologyVPN Virtual network	k gate Synology East Asia QC4 ••••
ntion Apps		
→ Move 💼 Delete		
Resource group (change) Synology		SKU VpnGw1
Location East Asia		Gateway type VPN
Subscription (change) QC4		VPN type Route-based
Subscription ID		Virtual network Synology_VPN
		Public IP address 13. GatewayIP)
		*

2.3 Create Local Network Gateway

1. Go to **New > Networking**, and click **Local network gateway**.



#### 2. Complete the following setup to create a local network gateway:

Microsoft Azure New >	Create local network gateway
≡	Create local network gateway $ imes$
+ New	* Name
료 Dashboard	LocalNetworkGateway 🗸
All resources	* IP address 0 111
📦 Resource groups	Address space 0
🚫 App Services	192.168.1.0/24
Function Apps	Add additional address range
🗟 SQL databases	Configure BGP settings
💓 Azure Cosmos DB	• Culturalistica
Virtual machines	QC4 V
💠 Load balancers	<ul> <li>Resource group          O         Use existing</li> </ul>
🧮 Storage accounts	Synology 🗸 🗸
↔> Virtual networks	* Location
Azure Active Directory	East Asia 🗸 🗸
🕒 Monitor	
🜪 Advisor	
Security Center	
Oost Management + Billing	
Help + support	
More services >	Pin to dashboard
	Create Automation options

- a. **Name**: Here, we enter "*LocalNetworkGateway*".
- b. IP address: Enter the IP address of your Synology Router.
- c. Address space: Specify the internal subnet of your Synology Router. Here, we enter "192.168.1.0/24".
- Resource group: Select Use existing, and select the previously created Synology from the drop-down list.
- e. Click **Create** when the setting is complete.

# 3. Site-to-Site VPN configuration on Synology Router

Sign in to SRM on your Synology Router, and follow the steps below.

- 1. Go to **VPN Plus Server** > **Site-to-Site VPN**.
- 2. Click **Add** > **Manually**.

<b>@</b>		VPN Plus Server		? — E X
Overview	IPsec			
Synology VPN	Add - Edit Remove	e Clone Export Status	Remote Site	Traffic (Received/Sent)
E Standard VPN	Import Profile			
E Site-to-Site VPN				
Permission				
🖧 Object				
Sonnection				
Log				
License				

#### 3. In the **General** tab, configure the following settings:

	Add					
General Encryption						
Profile name:	Azure					
Pre-shared key:	•••••					
Confirm pre-shared key:	•••••					
Enable this connection						
Enable DNSSEC validation						
Local Site						
Outbound IP:	PPPoE (111.	•				
Local ID:	111.					
Private subnet:	Local Network (192.168.1.0/24)	• +				
Remote Site						
IP address/FQDN:	13.					
Remote ID:	13.					
Private subnet:	10.0.1.0/27	<b>T</b>				
Private subnet: Dead Peer Detection	10.0.1.0/27	Ŧ				
Private subnet: Dead Peer Detection	10.0.1.0/27	+				
Private subnet: Dead Peer Detection Enable DPD Delay:	10.0.1.0/27 30 seconds	Ŧ				

- **Profile name**: Enter a customized name for the profile. Here, we enter "*Azure*".
- **Pre-shared key**: Here, we enter "123456789".
- Under **Local Site** section, configure the following settings:
  - **Outbound IP**: Enter Synology Router's IP address. Here, we enter *111.xxx.xxx.xxx*.
  - Local ID: You can enter a public IP address or FQDN to specify the Local ID. Here, we enter *111.xxx.xxx*.
  - Private subnet: Specify the local network under the private subnet of Synology Router. Here, we select *Local Network (192.168.1.0/24)*.
- Under **Remote Site** section, configure the following settings:

- **IP address/FQDN**: Enter the public IP address of Microsoft Azure site. Here, we enter *13.xx.xx.xx*.
- **Remote ID**: You can enter a public IP address or FQDN to specify the Remote ID. Here, we enter *13.xx.xx.xx*.
- **Private subnet**: Specify the local network under the private subnet of Microsoft Azure. Here, we enter *10.0.1.0/27*.
- Under **Dead Peer Detection** section, make sure the checkbox remains unticked.
- 4. In the **Encryption** tab, make sure the following settings are identical with those on the other site:

		Edit					
General	Encryption						
Phase 1							
IKE version:		◯ IKEv1 ● IKEv2					
Mode:		Main mode(ID protection) 👻					
Encryption:		AES128	•				
Authenticatio	on:	SHA-256	-				
DH group:		2 (modp 1024) 👻					
Key lifetime:		28800	seconds				
Phase 2							
Encryption:		AES128	-				
Authenticatio	on:	SHA-256	-				
DH group:		2 (modp 1024) 👻					
Key lifetime:		27000	seconds				
Key lifetime:		Enable Perfect Forward Secrecy (PFS) 👔					
Key lifetime:	Perfect Forward S	ecrecy (PFS) 🥡					

- Under **Phase 1** section:
  - IKE version: Select IKEv2.
  - Mode: Select Main mode (ID protection).
  - Encryption: Select AES128.
  - Authentication: Select SHA-256.
  - DH group: Select 2 (modp 1024).

- **Key lifetime**: Select **28800** seconds.
- Under **Phase 2** section:
  - Encryption: Select AES128.
  - Authentication: Select SHA-256.
  - DH group: Select 2 (modp 1024).
  - Key lifetime: Select 27000 seconds.
  - Make sure the **Enable Perfect Forward Secrecy (PFS)** checkbox remains unticked.
- 4. Establish connection between Synology Router and Microsoft Azure
- 1. Go to **All resources**, and search for the previously created "*GatewayToSynologyVPN*".

Microsoft Azure All resource	es		Ъ С	1 >_	<u>نې</u>	0	@synology.co 群暉科技股份有限公	m 🧕
≡	All resources 群種科技股份有限公司							* ×
+ New	╋ Add ≣≣ Columns 🕐 Refresh 🛛 ♦ Assig	n Tags 🗴 💼 Delete						
🗉 Dashboard 🚺	Subscriptions: 2 – Don't see a subscription? Switch a							
All resources	GatewayToSynologyVPN All resource groups	✓ All types	~	All locat	tions	~	No grouping	<u> </u>
Resource groups	1 items □ NAME ↑↓ 3	туре 🗘	RESOURCE GRO	DUP 👈	LOCATION			
🔇 App Services	GatewayToSynologyVPN	Virtual network gate	Synology		East Asia		QC4	
Function Apps								

#### 2. Go to **Connections**, and click **Add**.

GatewayToSynologyVPN - C	Connections	* ×
	Add 2	
Overview	Search connections NAME STATUS CONNECTION TYPE PEER	
Activity log	No results	
Access control (IAM)		
🗬 Tags		
X Diagnose and solve problems		
SETTINGS		
🚔 Configuration 🛛 🚺		
Connections		
<ul> <li>Point-to-site configuration</li> </ul>		
Properties		
Locks		
Automation script		

3. Complete the following setup to create the Site-to-Site VPN connection:



- a. **Name**: Here, we enter *SynologyAndAzure*.
  - b. Connection type: Select Site-to-site (IPsec).
  - c. Click **Local network gateway** to select the previously created *LocalNetworkGateway*.
  - d. Shared key(PSK): Specify the same pre-shared key as on Synology Router. Here, we enter "123456789".
  - e. Click **OK** when the setting is complete.

4. When the settings are complete, you will see the status of Site-to-Site VPN tunnel on each of the two sites.

8		VPN Plus Server		2 - E X
• Overview	IPsec	Pomovo Clono Es	roort Profile	
Synology VPN	Name	Status	Remote Site	Traffic (Downloaded/Upload
Standard VPN	Azure	Connected	13.	7 КВ / 0 В
Site-to-Site VPN				
Permission				
🚯 Object				
Sonnection				
:= Log				
neport				
P License				
Second Control (NAM)         Image: Second Control (NAM)         Image: Second Control (NAM)         Image: Second Control (NAM)         Image: Second Control	NAME SynologyAndAzure	Connected	51. CONNECTION TYPE Site-to-site (IPsec)	PEER LocalNetworkGateway
	D Search connecti	ions		
Virtual network gateway  Search (Ctrl+/)	- Add			
GatewayToSynologyVPN	- Connections			*