



SANGFOR

Sangfor_NGAF_V7.3_ Build IPsec VPN with Microsoft Azure

SANGFOR Technologies Inc.

30th December 2017

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +86 755 2669 8888 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Declaration

Copyright © SANGFOR Technologies Inc. All rights reserved.

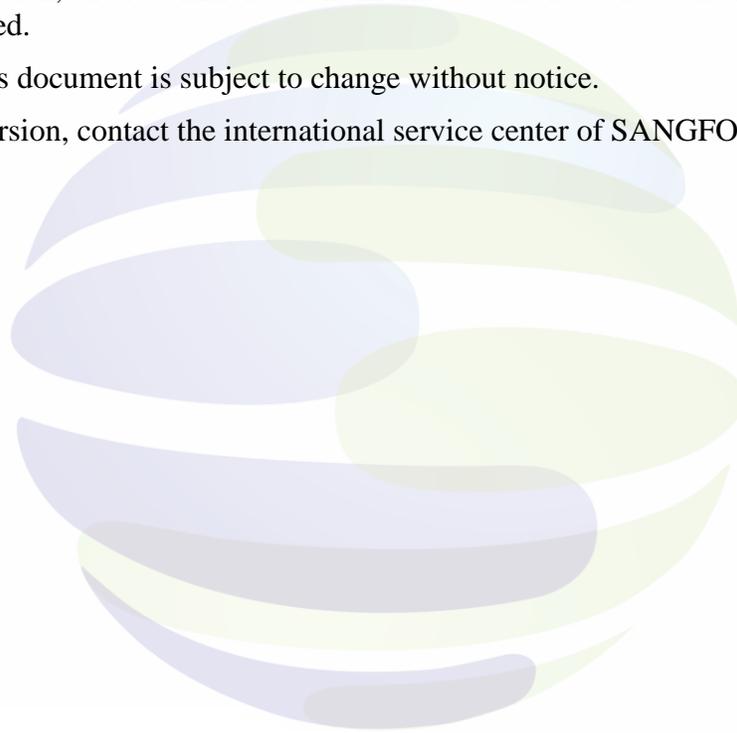
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR, SINFOR and  logo are the trademarks of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc.



Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

Table of contents

Declaration	2
Table of contents	3
1 Introduction	4
1.1 Abbreviations and conventions	4
1.2 Feedback	4
2 Background	4
3 Configuration on Microsoft Azure	4
3.1 Resource Group	4
3.2 Virtual Network	4
3.3 Virtual Network Gateway	6
3.4 Local Network Gateway	8
3.5 Site-to-Site VPN configuration	9
3.6 Check status	10
4 Configuration on Sangfor NGAF	11
4.1 Phase 1	11
4.1.1 Check status (Phase 1)	12
4.2 Phase 2	12
4.2.1 Inbound Policy	12
4.2.2 Outbound Policy	13
4.2.3 Check status (Phase 2)	14
5 Additional Information	15
5.1 Security Associations (Phase 1 and Phase 2)	15

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

1 Introduction

1.1 Abbreviations and conventions

NGAF in this article refers to the SANGFOR Next-Generation Application Firewall device.

1.2 Feedback

If you find any questions of this documents, please feel free to give us feedback, email: tech.support@sangfor.com.

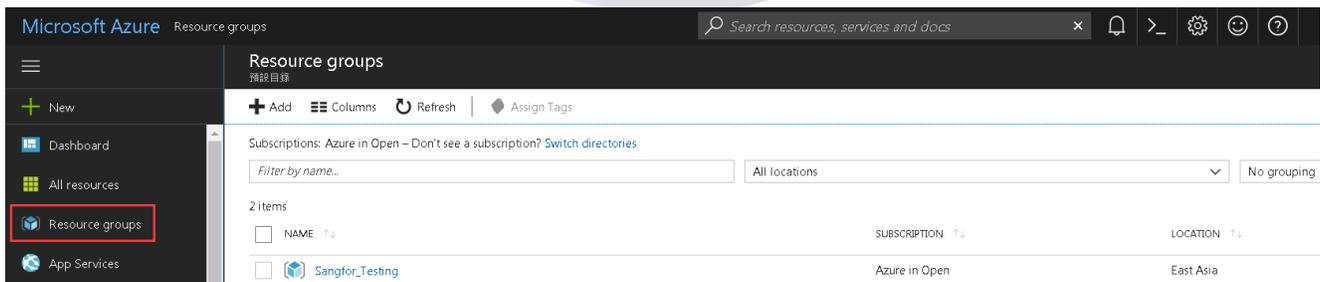
2 Background

Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Microsoft Azure support both IKEv1 and IKEv2. In Microsoft Azure term, Policy-Based VPN represent IKEv1, while Route-Based VPN represent IKEv2.

3 Configuration on Microsoft Azure

3.1 Resource Group

Resource Group is where all the resources or VM deploy and it is the first step before proceed to configure other part. Resource Group may also create while deploying **Virtual Network** as well. Upon create complete, it is an empty group that needs to manually deploy resource or VM in it.



3.2 Virtual Network

Virtual Network is like assigning virtual IP to the resources or VMs. The IP range that declared in Virtual Network will be used during configuration of Phase 2 on peer device.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Create virtual network

* Name

* Address space ⓘ
10.2.0.0/24 ✓
10.2.0.0 - 10.2.0.255 (256 addresses)

* Subscription
Azure in Open ▼

* Resource group
 Create new Use existing

* Location
Southeast Asia ▼

Subnet

* Name
default

* Address range ⓘ
10.2.0.0/24 ✓
10.2.0.0 - 10.2.0.255 (256 addresses)

Service endpoints (Preview) ⓘ

Pin to dashboard

[Automation options](#)

Name: Name for the Virtual Network.

Address Space: IP range for the Virtual Network. Recommend to use subnet mask /16.

Resource Group: Can create new Resource Group or select existing Resource Group.

Location: Location of the Virtual Network.

Subnet Name: Name for the subnet.

Subnet Address range: Subnet IP range (it must be within the Address Space listed before).

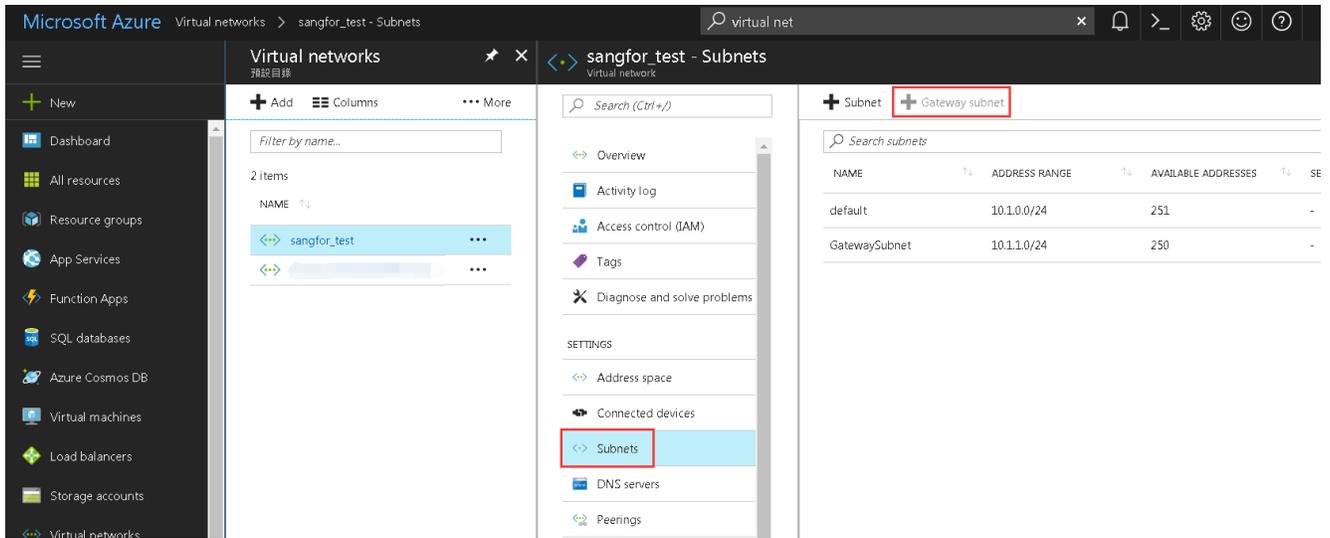
After created Virtual Network, Gateway Subnet must be created. For Gateway Subnet, the subnet mask 24 is sufficient but smaller subnet mask can be used too.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



3.3 Virtual Network Gateway

Virtual Network Gateway will be assigned with a Public IP after all the required field is filled in. The Public IP will be used in Phase 1 of peer device.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Create virtual network gateway

* Name

Gateway type ⓘ
 VPN ExpressRoute

VPN type ⓘ
 Route-based Policy-based

* SKU ⓘ

Enable active-active mode ⓘ

* Virtual network ⓘ
[Choose a virtual network](#)

* Public IP address ⓘ
[Choose a public IP address](#)

Configure BGP ASN

* Subscription

Resource group ⓘ
-

* Location ⓘ

Pin to dashboard

[Automation options](#)

Choose virtual network

To associate a virtual network with a gateway, it must contain a valid gateway subnet.
[Learn more](#)

These are the virtual networks in the selected subscription and location 'Southeast Asia'.

	sangfor_test Sangfor_Testing	ⓘ
--	---------------------------------	---

Name: Name for the Virtual Network Gateway.

Gateway Type: ExpressRoute for IKEv2 or Route-based VPN type only while VPN is for site-to-site.

VPN Type: Route-based is for IKEv2 and Policy-based is for IKEv1.

SKU: By default is Basic, no other available option to be selected.

Virtual Network: Select Virtual Network that created on 3.2

Public IP Address: Select or create a new record for this connection.

Location: Location of the Virtual Network.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

After complete create Virtual Network Gateway, it will takes around 30 minutes to obtain the Public IP.

Resource group ([change](#))
[Sangfor_Testing](#)

Location
Southeast Asia

Subscription ([change](#))
[Azure in Open](#)

Subscription ID
bc48045a-c34b-4ad6-8367-6b1fc0d5e955

SKU
Basic

Gateway type
VPN

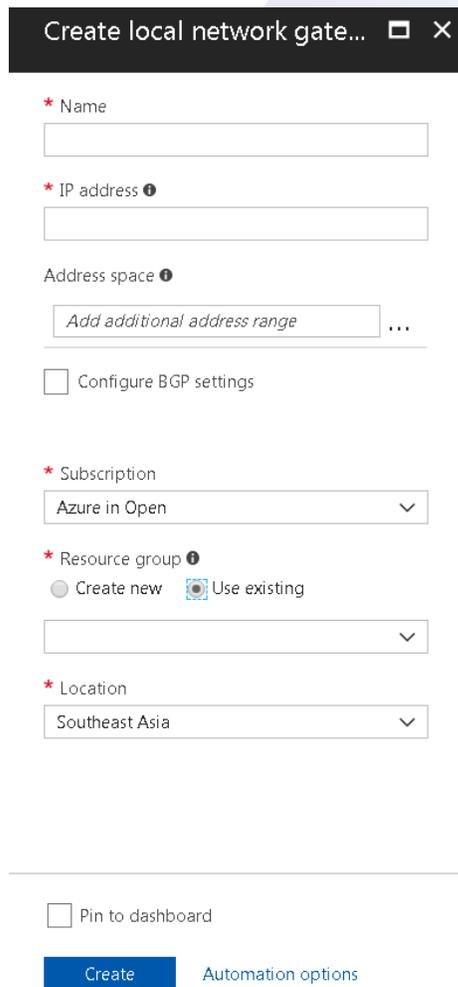
VPN type
Policy-based

Virtual network
[sangfor_test](#)

Public IP address
[52.230.123.94 \(sangfor_test\)](#)

3.4 Local Network Gateway

Local Network Gateway will define the peer site Public IP and also local IP segments.



Create local network gate... [] [X]

* Name

* IP address ⓘ

Address space ⓘ
 ...

Configure BGP settings

* Subscription
 ▼

* Resource group ⓘ
 Create new Use existing

* Location
 ▼

Pin to dashboard

[Automation options](#)

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

Name: Name for the Local Network Gateway.

IP Address: Public IP configured on peer device.

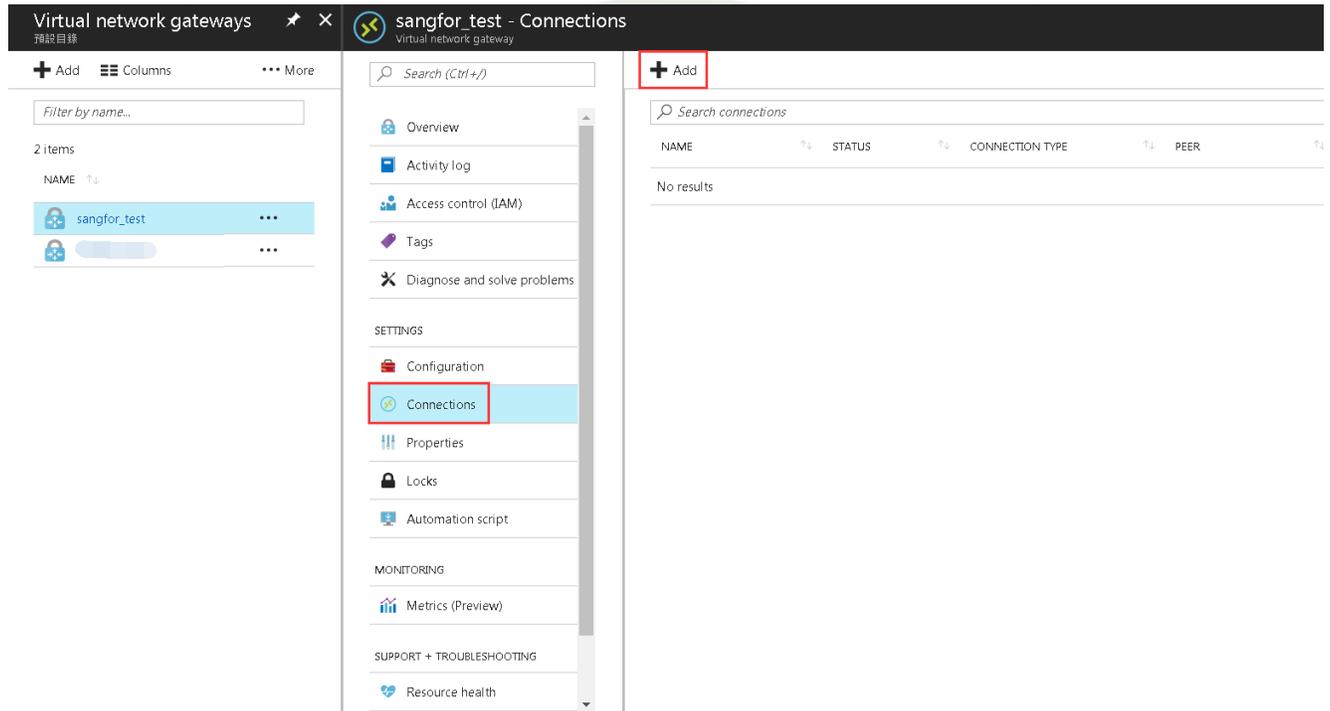
Address Space: Local IP segment of peer device. It should match with peer device Phase 2 outbound IP segment.

Resources Group: Can create new Resource Group or select existing Resource Group.

Location: Location of the Local Network Gateway.

3.5 Site-to-Site VPN configuration

After created Virtual Network Gateway and Local Network Gateway, connection towards the peer device are required to add in to establish it.



The screenshot displays the Sangfor Cloud Management Console interface. The main window is titled 'Virtual network gateways' and shows a list of two items, with 'sangfor_test' selected. The left sidebar contains a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Connections (highlighted), Properties, Locks, Automation script, Metrics (Preview), and Resource health. The right pane shows the 'Connections' page for 'sangfor_test', featuring a search bar and a table with columns for NAME, STATUS, CONNECTION TYPE, and PEER. The table currently displays 'No results'. A red box highlights the '+ Add' button in the top right corner of the Connections pane.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Add connection ✕
sangfor_test

* Name
 ✓

Connection type ⓘ
 ▼

* Virtual network gateway ⓘ

* Local network gateway ⓘ >

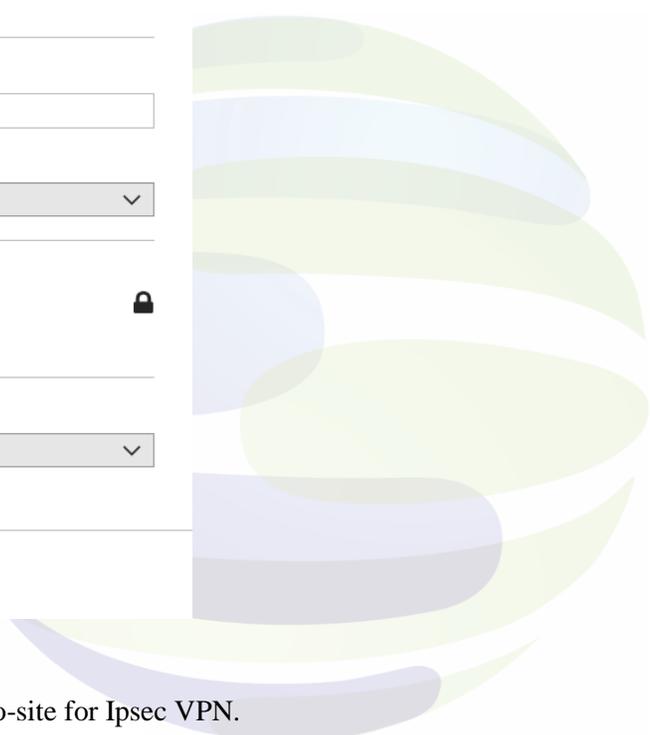
* Shared key (PSK) ⓘ

Subscription ⓘ
 ▼

Resource group ⓘ

[Create new](#)

Location ⓘ
 ▼



Name: Name of the connection

Connection Type: Select Site-to-site for IPsec VPN.

Virtual Network Gateway: Select the Virtual Network Gateway that created previously.

Local Network Gateway: Select the Local Network Gateway that created previously.

Shared key: Shared key for to verify both parties during establish of VPN connection.

Resources Group: Select the Resources Group that created previously.

3.6 Check status

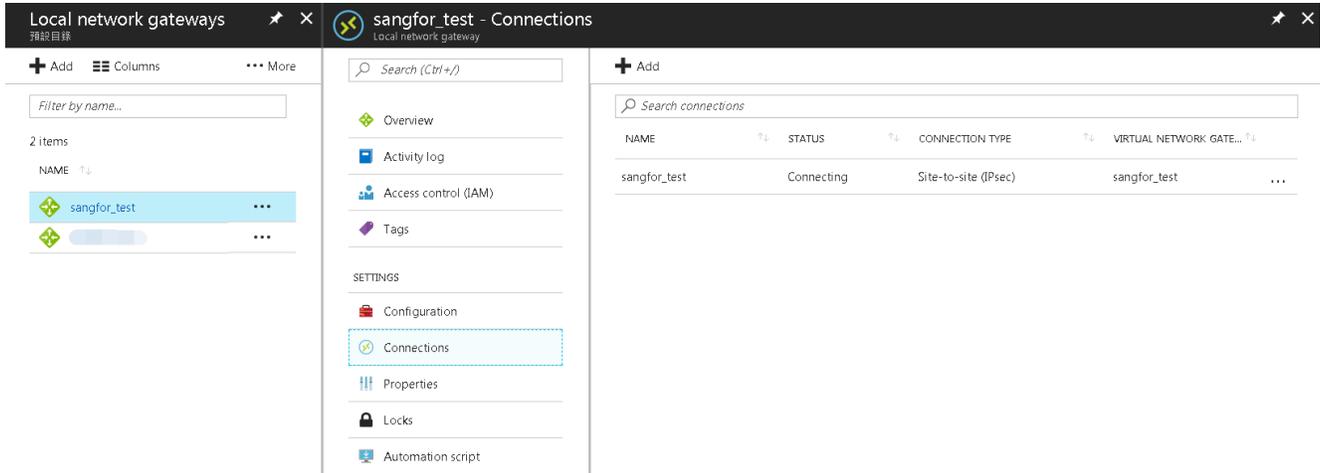
Status can be checked in either Virtual Network Gateway or Local Network Gateway page.

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

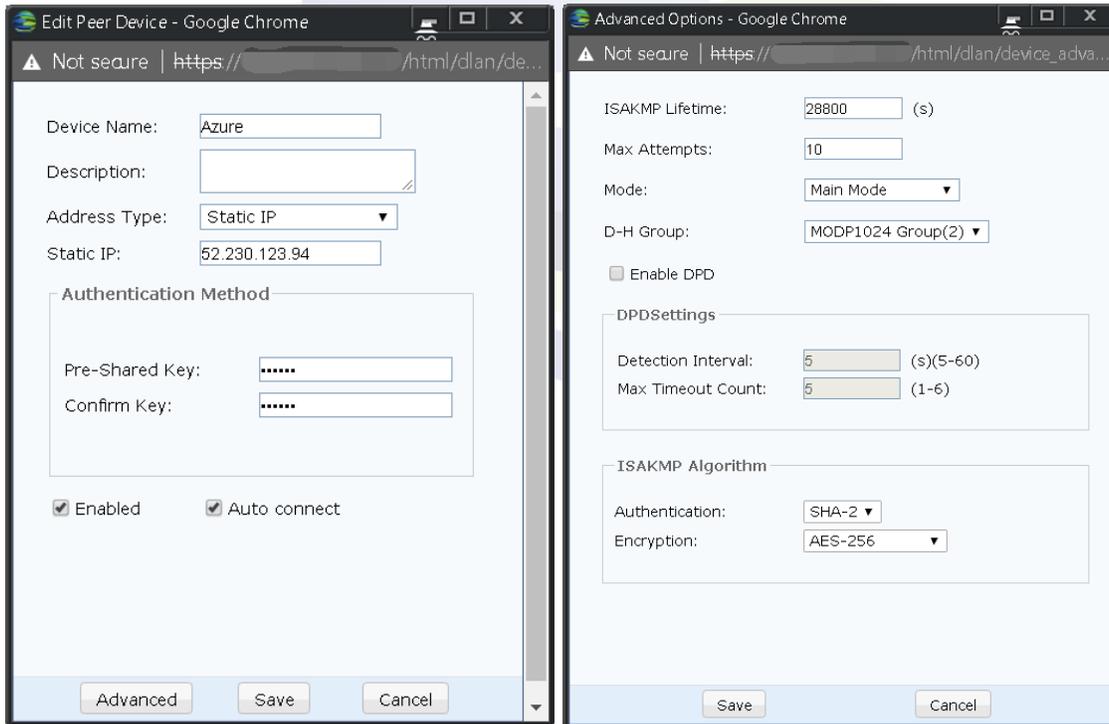
T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



4 Configuration on Sangfor NGAF

4.1 Phase 1

Microsoft Azure is not using DPD, therefore DPD should be disabled.



Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

4.1.1 Check status (Phase 1)

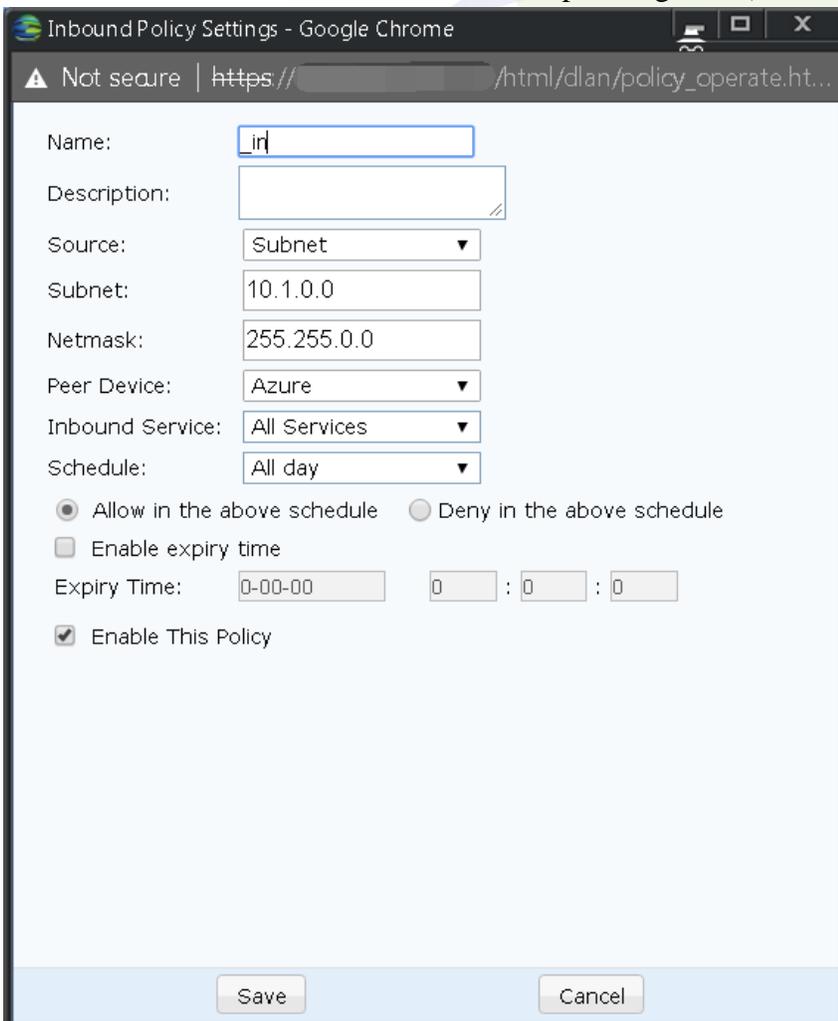
Ensure the Phase 1 is finished before proceed to Phase 2.

No.	Module	Type	Time	Details
2	VPN Service	Info	15:28:23	[Isakmp_Server]The Phase 1 Security association for [Azure](IP:52.230.123.94) has finished! The tunnel has been built !
3	VPN Service	Info	15:28:22	[Isakmp_Server]Start to handle negotiation from [Azure](IP:52.230.123.94) using main mode!

4.2 Phase 2

4.2.1 Inbound Policy

Subnet is Azure Virtual Network Address Space segment (refer to 3.2).



Inbound Policy Settings - Google Chrome

Not secure | https://.../html/dlan/policy_operate.ht...

Name:

Description:

Source:

Subnet:

Netmask:

Peer Device:

Inbound Service:

Schedule:

Allow in the above schedule
 Deny in the above schedule

Enable expiry time
 Expiry Time: : :

Enable This Policy

Save Cancel

Your Future-Proof IT Enabler

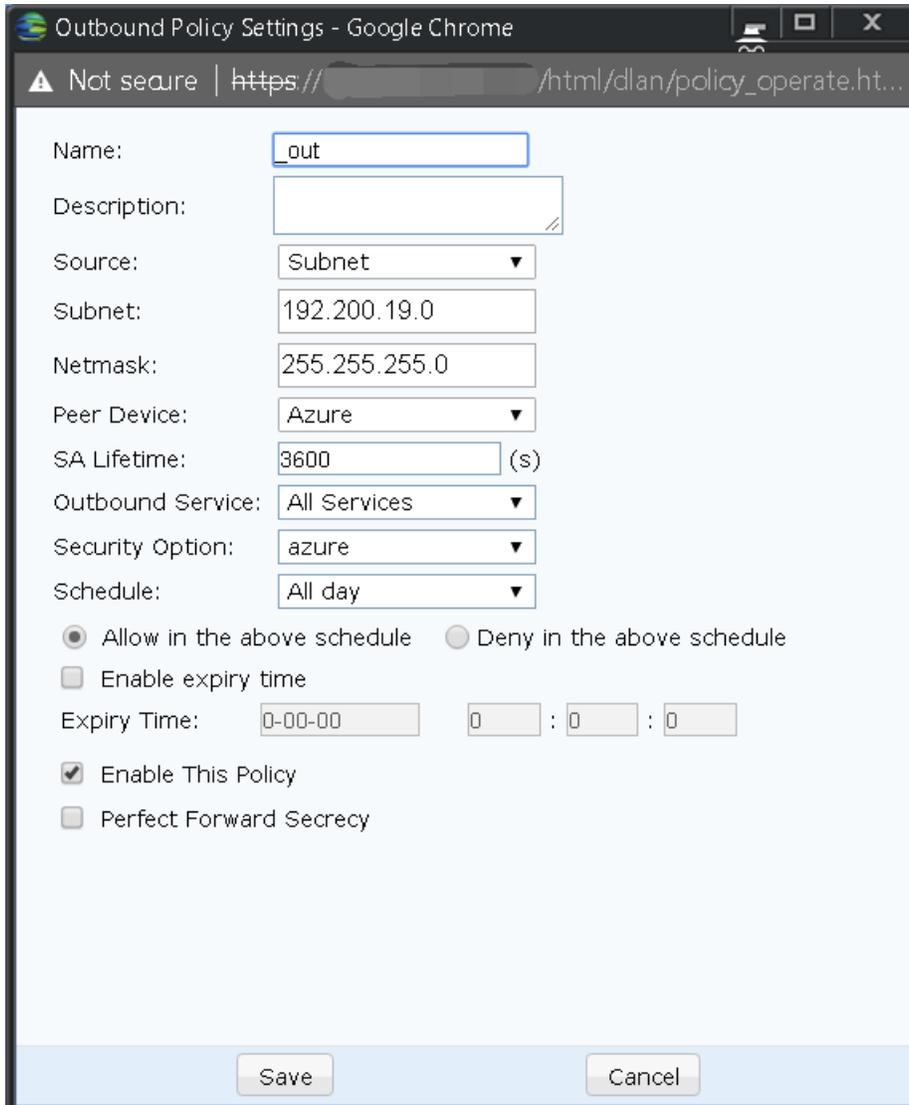
Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

4.2.2 Outbound Policy

SA Lifetime for Azure by default is 3600 seconds. Azure **do not** support Perfect Forward Secrecy, therefore it must be **disabled**.



The screenshot shows a web browser window titled "Outbound Policy Settings - Google Chrome". The address bar shows a URL starting with "https://". The page content is a form for configuring an outbound policy. The fields are as follows:

- Name:
- Description:
- Source:
- Subnet:
- Netmask:
- Peer Device:
- SA Lifetime: (s)
- Outbound Service:
- Security Option:
- Schedule:

Below the form, there are two radio buttons: "Allow in the above schedule" (selected) and "Deny in the above schedule". There is also a checkbox for "Enable expiry time" which is unchecked. Below that, there are four input fields for "Expiry Time" with values "0-00-00", "0", "0", and "0". There are two more checkboxes: "Enable This Policy" (checked) and "Perfect Forward Secrecy" (unchecked). At the bottom of the form, there are two buttons: "Save" and "Cancel".

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

Phase 2 Security Associations as shown below.



4.2.3 Check status (Phase 2)

Ensure the Phase 2 is finished and the connection has been established successfully.



No.	Module	Type	Time	Details
24	VPN Service	Info	17:45:11	[Isakmp_Server]The Phase 2 Security association for policy[_out] and policy[_in] has finished! The connection has been built!
25	VPN Service	Info	17:45:11	[Isakmp_Server]The Phase 1 Security association for [Azure](IP:52.230.123.94) has finished! The tunnel has been built!
26	VPN Service	Info	17:45:11	[Isakmp_Server]Start to initiate negotiation with [Azure](IP:52.230.123.94) using main model!



Disconnect	Connection	Username	Description	Type	Realtime Traffic (In/Out)	Internet IP	LAN IP	Time Connected	Protocol
					0/0				
		Azure	Third-party device		0/0	52.230.123.94	10.1.0.0	2017-12-15 10:19:04	IPSEC_ESP

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



5 Additional Information

5.1 Security Associations (Phase 1 and Phase 2)

Below is the details of Security Associations that Microsoft Azure used. It includes Group Description, ISAKMP Lifetime Encryption Algorithm and Hash Algorithm.

Group Description : MODP 1024 (Group 2)
ISAKMP Lifetime : 28800 seconds

Set 1:

Encryption Algorithm : AES-256
Hash Algorithm : SHA2

Set 2:

Encryption Algorithm : AES-256
Hash Algorithm : SHA1

Set 3:

Encryption Algorithm : AES-128
Hash Algorithm : SHA1

Set 4:

Encryption Algorithm : 3DES
Hash Algorithm : SHA1

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com