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

Declaration

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

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.

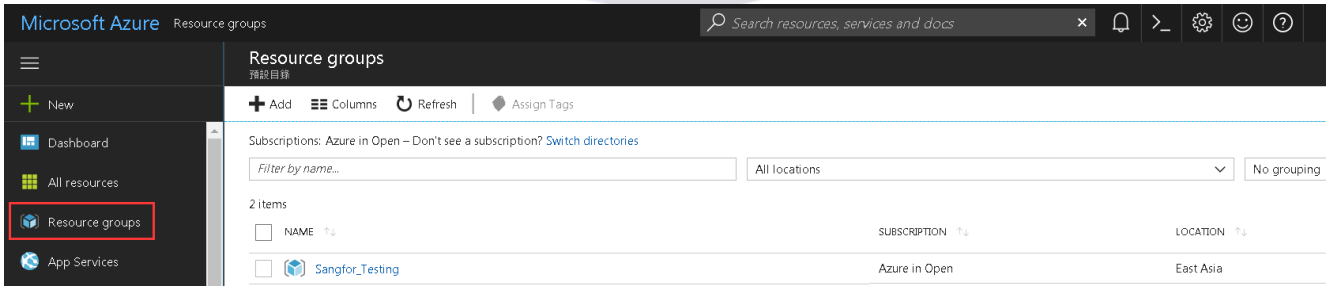
2 Background

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

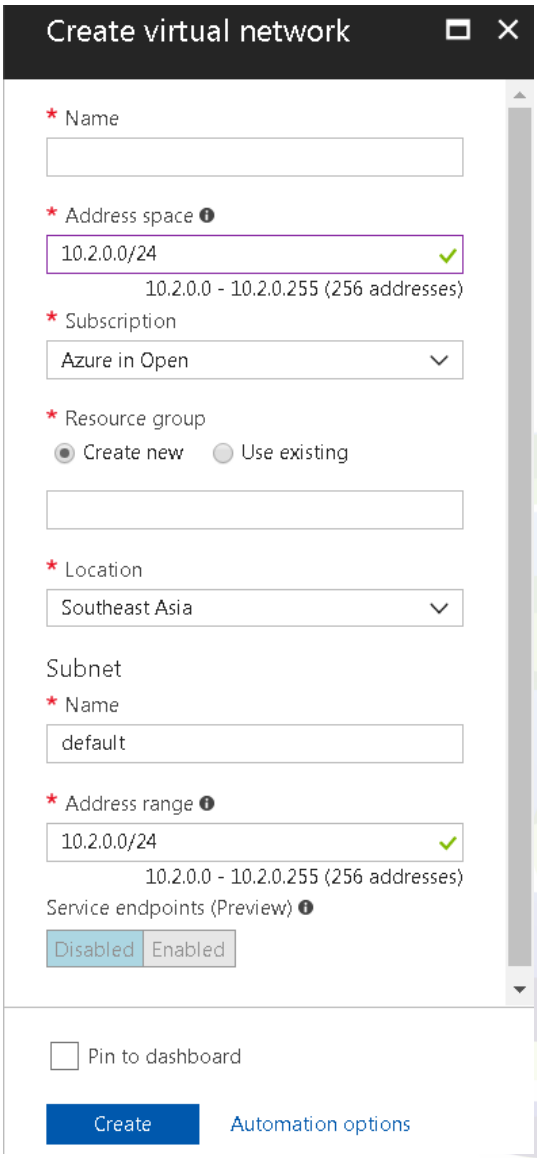
3.1 Resource Group

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

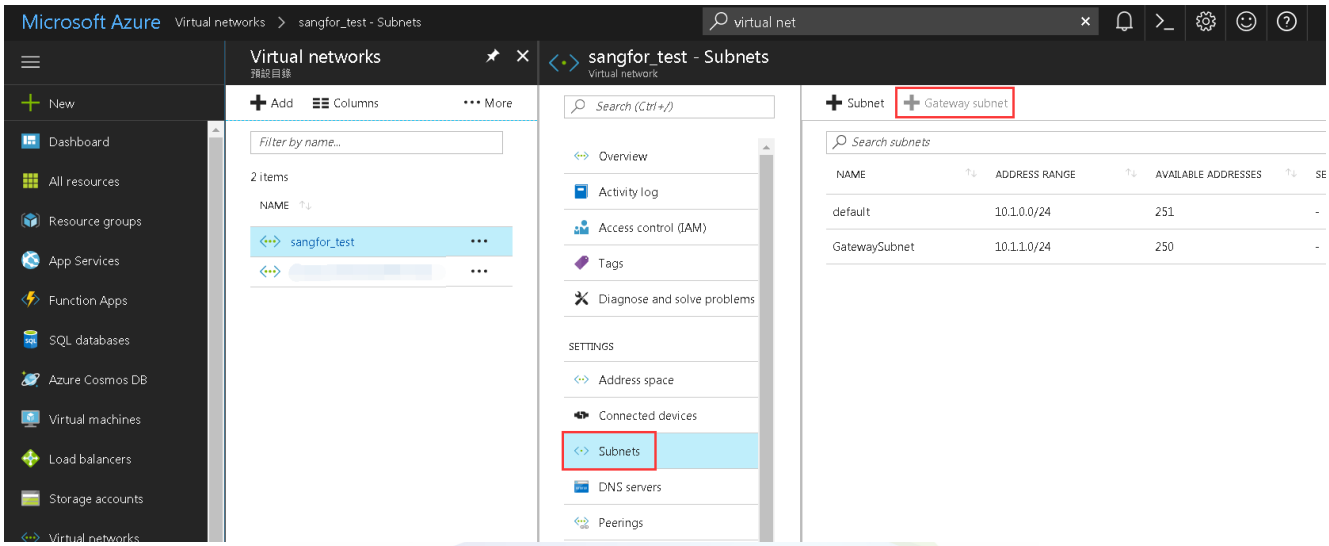
Virtual Network is like assigning virtual IP to the resources or VMs. The IP range that declared in Virtual Network will be used during configuration of Phase 2 on peer device.



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).

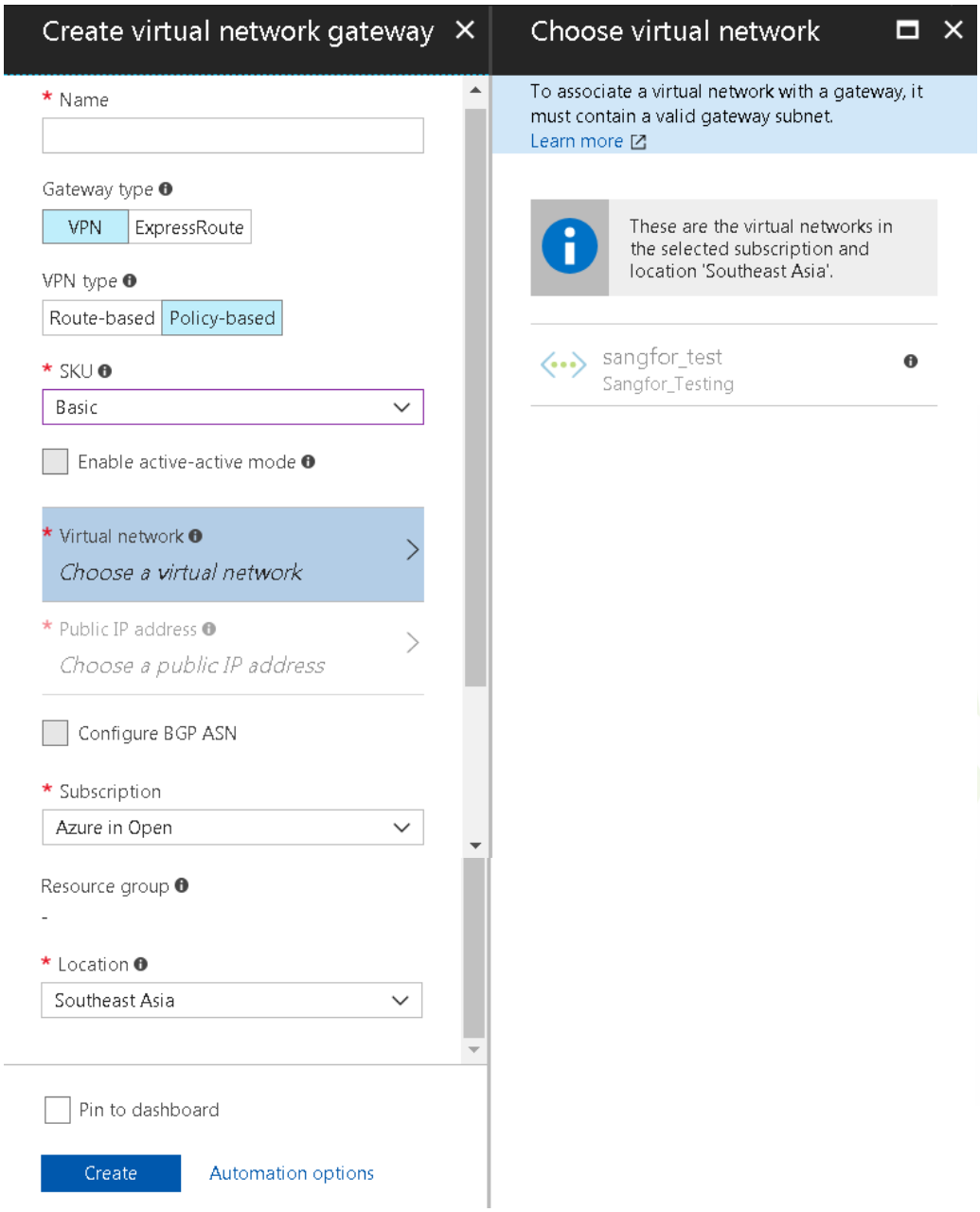
After created Virtual Network, Gateway Subnet must be created. For Gateway Subnet, the subnet mask 24 is sufficient but smaller subnet mask can be used too.

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.



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.

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

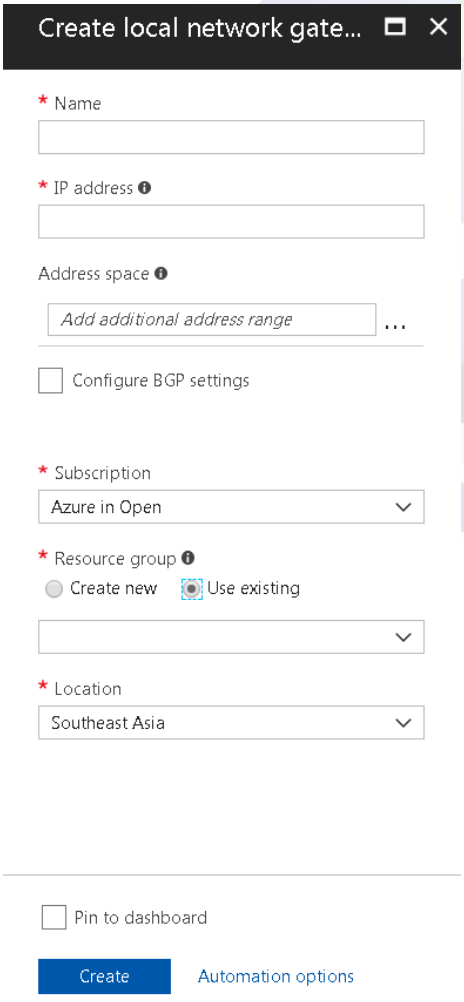
VPN type
Policy-based

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.

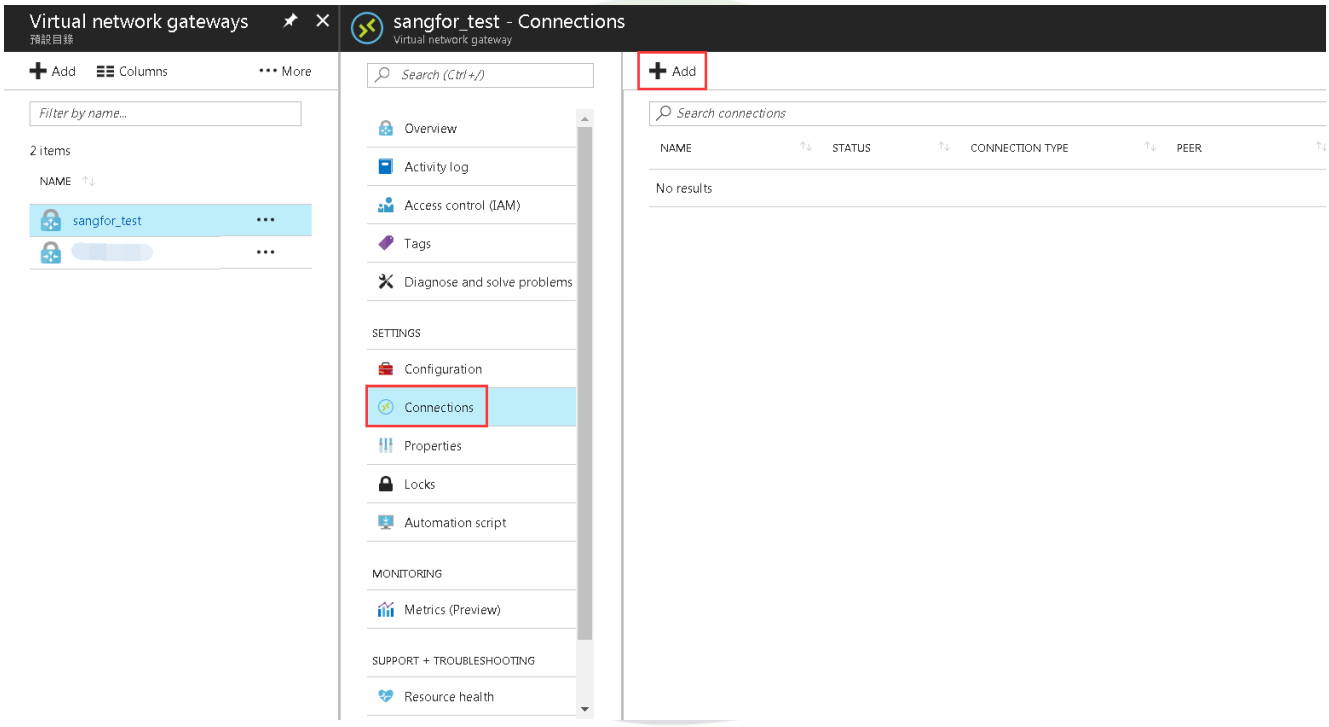


Sangfor Technologies
Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China
T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

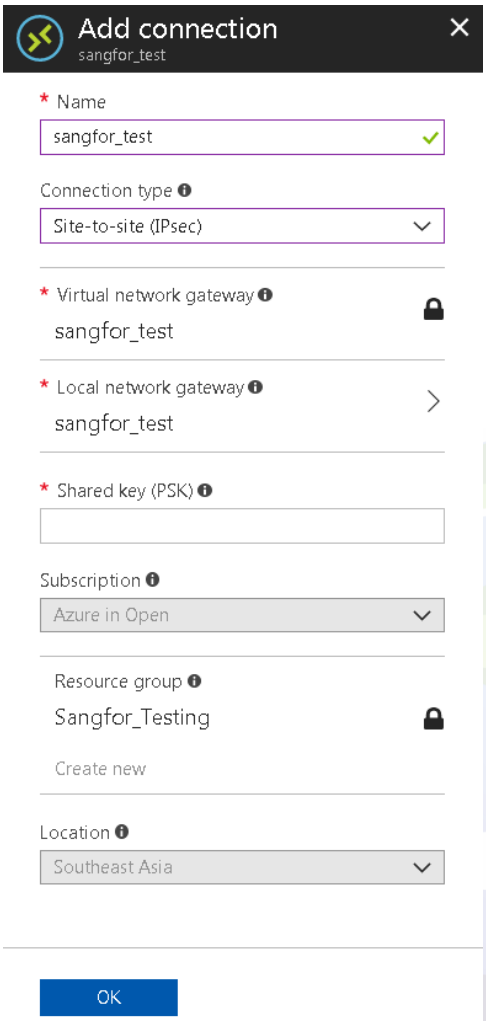
Name: Name for the Local Network Gateway.
IP Address: Public IP configured on peer device.
Address Space: Local IP segment of peer device. It should match with peer device Phase 2 outbound IP segment.
Resources Group: Can create new Resource Group or select existing Resource Group.
Location: Location 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.



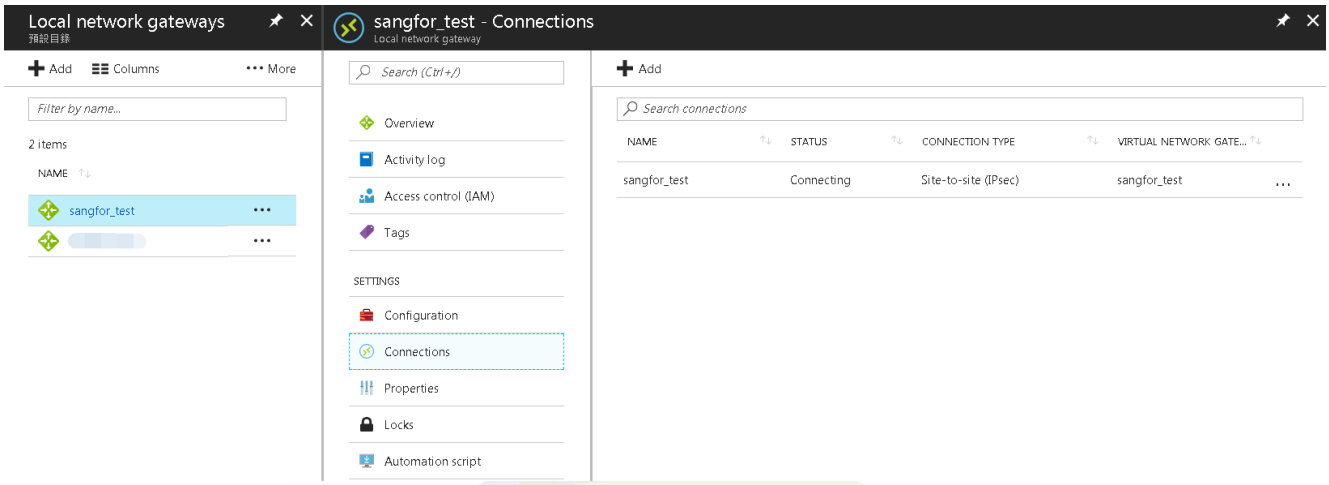
Sangfor Technologies
Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China
T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Name: Name 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

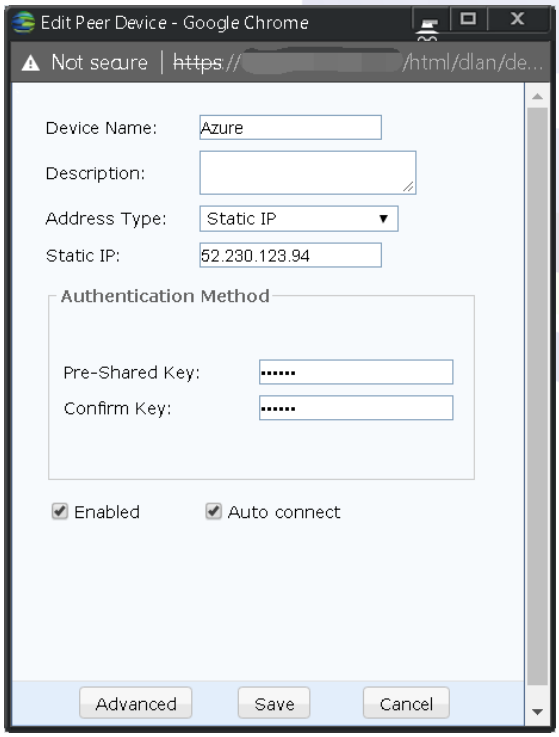
Status can be checked in either Virtual Network Gateway or Local Network Gateway page.

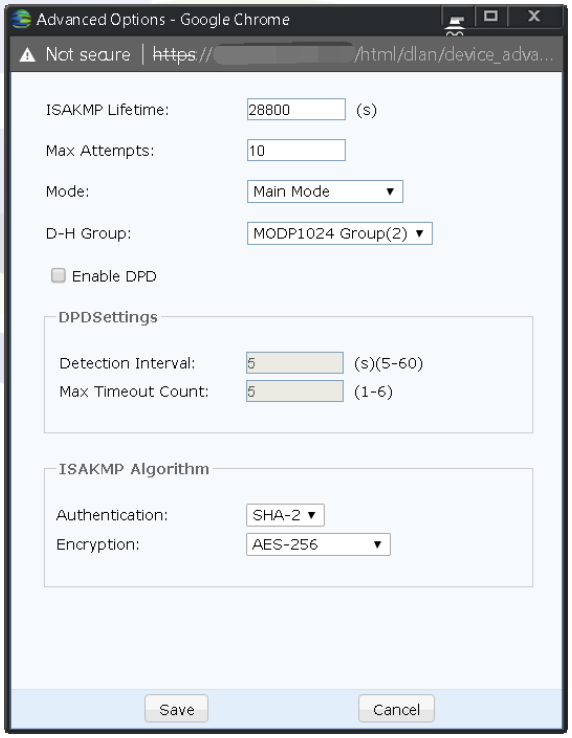


4 Configuration on Sangfor NGAF

4.1 Phase 1

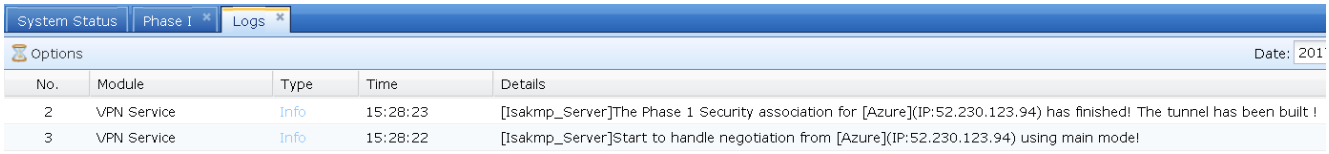
Microsoft Azure is not using DPD, therefore DPD should be disabled.





4.1.1 Check status (Phase 1)

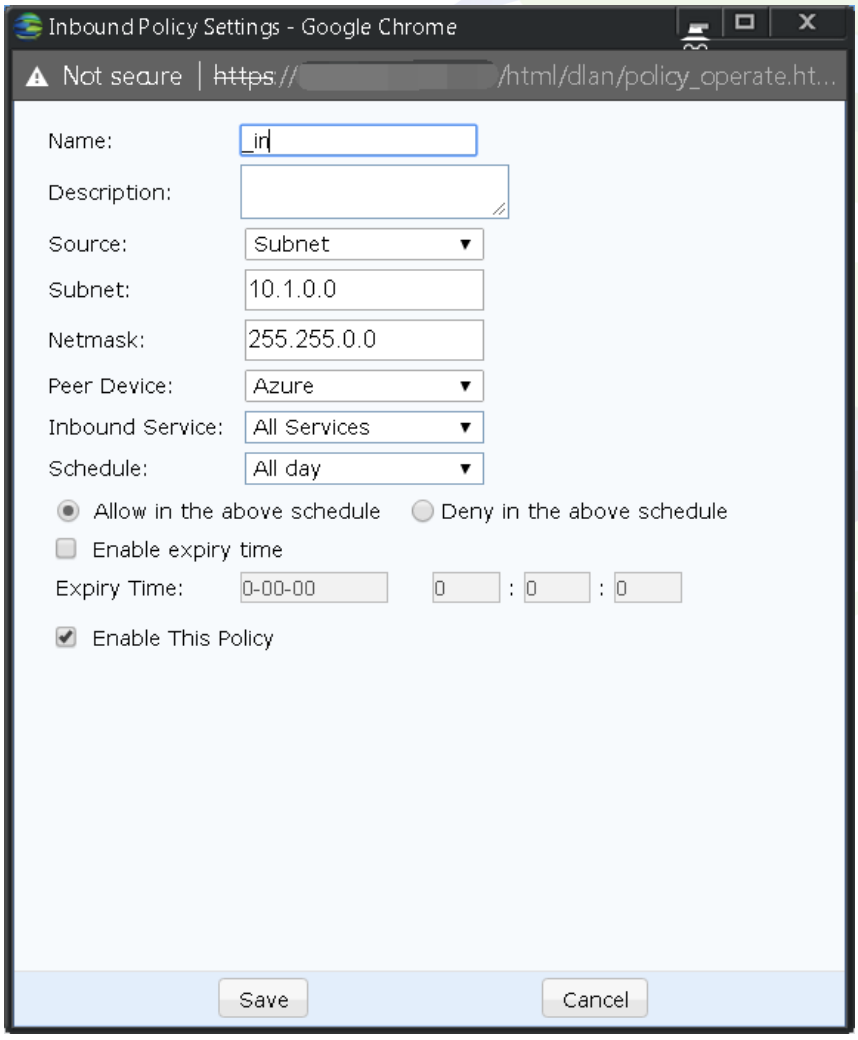
Ensure the Phase 1 is finished before proceed to Phase 2.



4.2 Phase 2

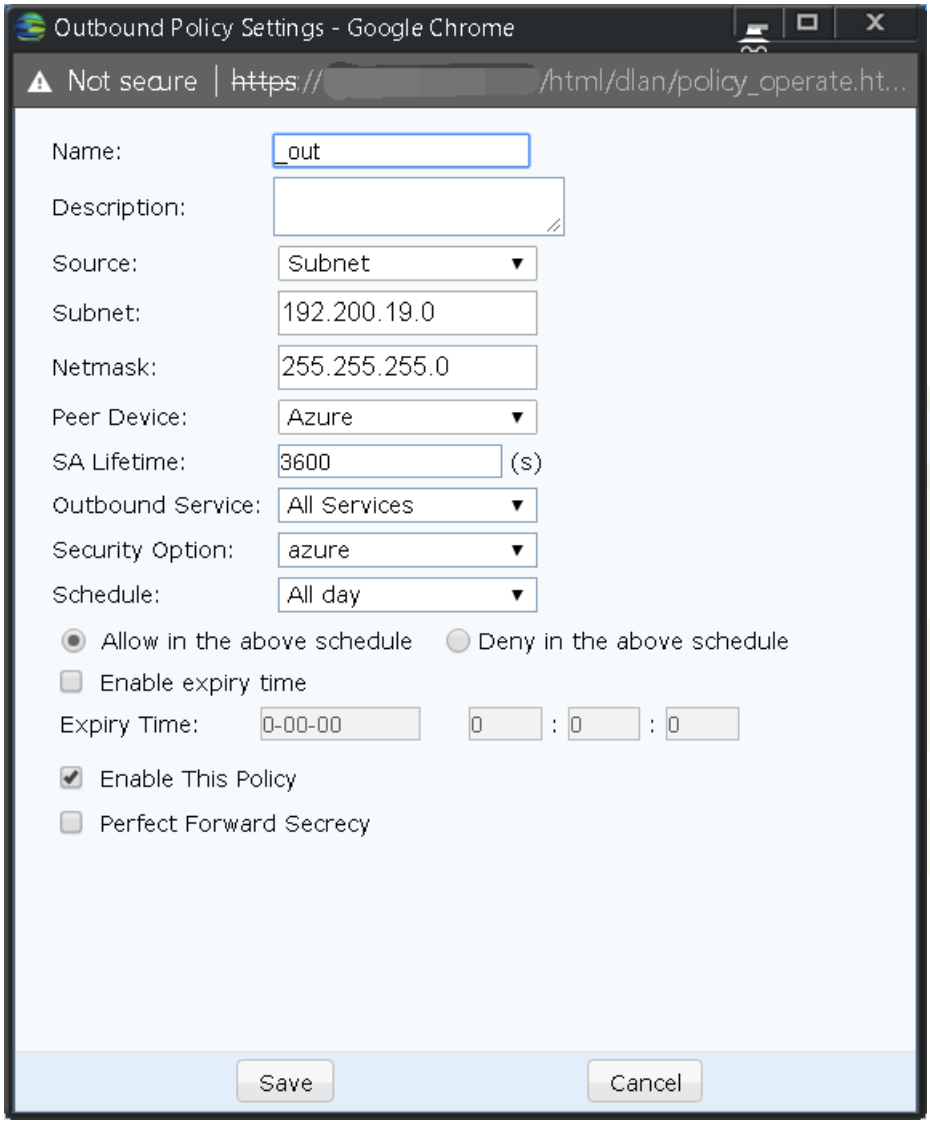
4.2.1 Inbound Policy

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

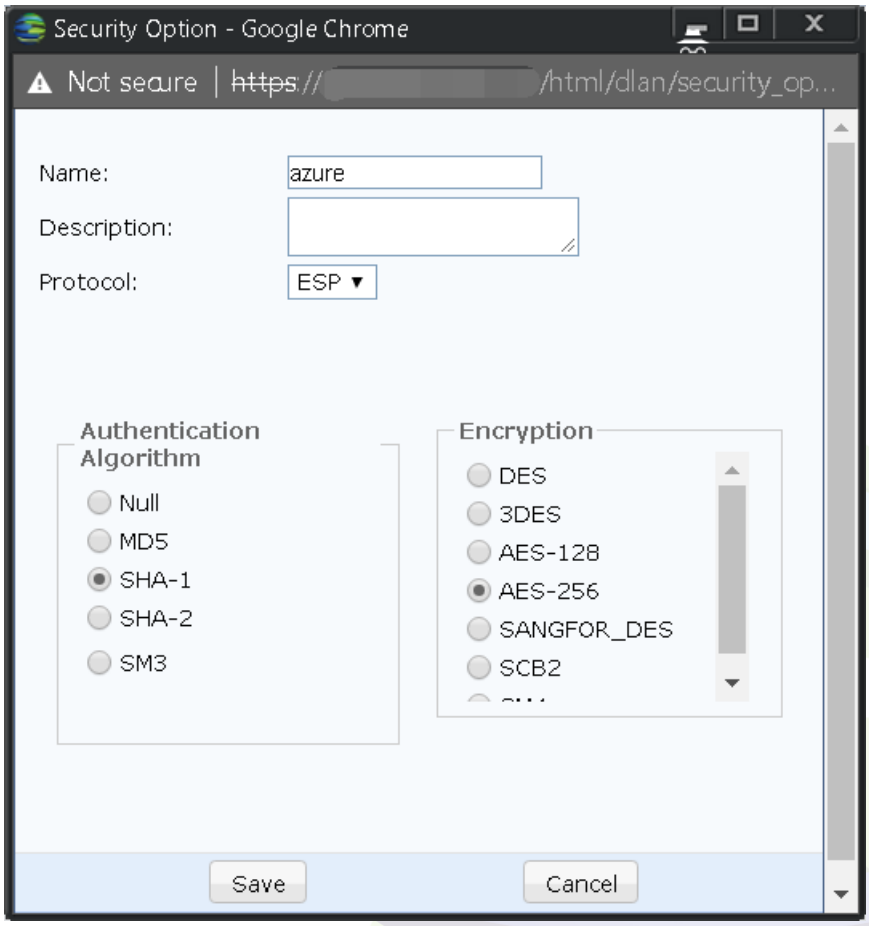


4.2.2 Outbound Policy

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

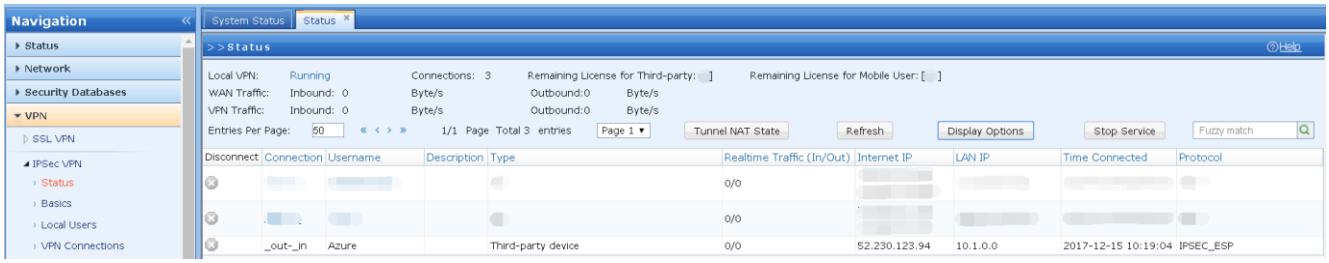


Phase 2 Security Associations as shown below.



4.2.3 Check status (Phase 2)

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



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 Descirption : 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

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