



SANGFOR

SANGFOR_NGAF_v7.4_ Monitor NGAF status via SNMP

SANGFOR Technologies Inc.

6th Dec 2017

Your Future-Proof IT Enabler

Sangfor Technologies

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

T.: +86 755 2662 8888 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Declaration

Copyright © SANGFOR Technologies Inc. All rights reserved.

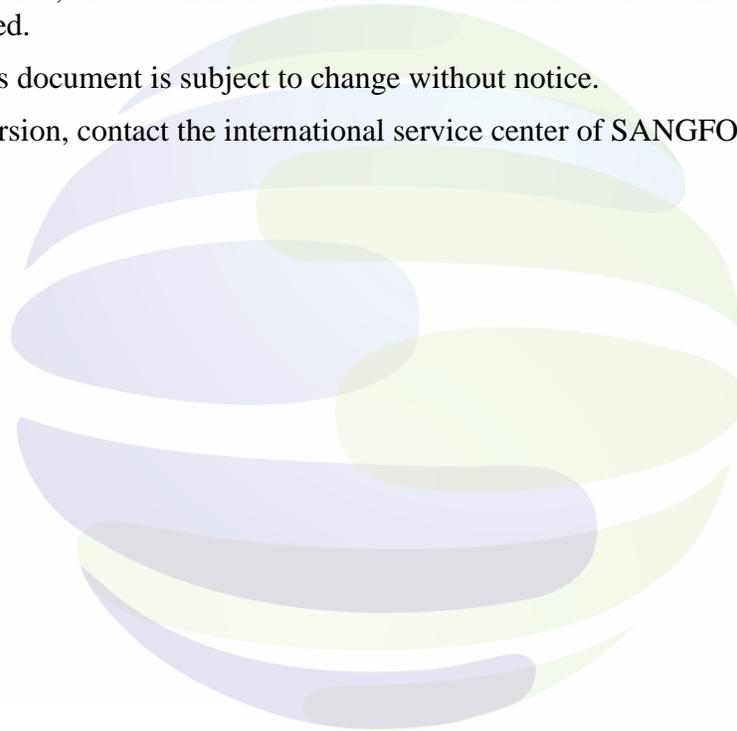
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

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 Function Briefing	4
3 Scenario	4
4 Requirements	4
5 Configuration Mind Map	4
6 Configuration steps and screenshots	5
6.1 Configure advanced network options	5
6.2 Enable Zone SNMP	7
7 Precautions	8

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 NGAF 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 Function Briefing

NGAF provides operating status information, so that customers can easily monitor the real-time status.

3 Scenario

By using SNMP protocol in third party network management software/device to manage and monitor Sangfor device's related information, such as interface status, data flow in interface, routing and etc. It provides unified platform for customer to manage, maintain and monitor network.

4 Requirements

List down the requirements for this configuration, for instance:

1. One NGAF device.
2. Third party network management software (support monitoring software of SNMP)

5 Configuration Mind Map

1. Configure advanced network options
2. Select zone where SNMP is applied

Your Future-Proof IT Enabler

Sangfor Technologies

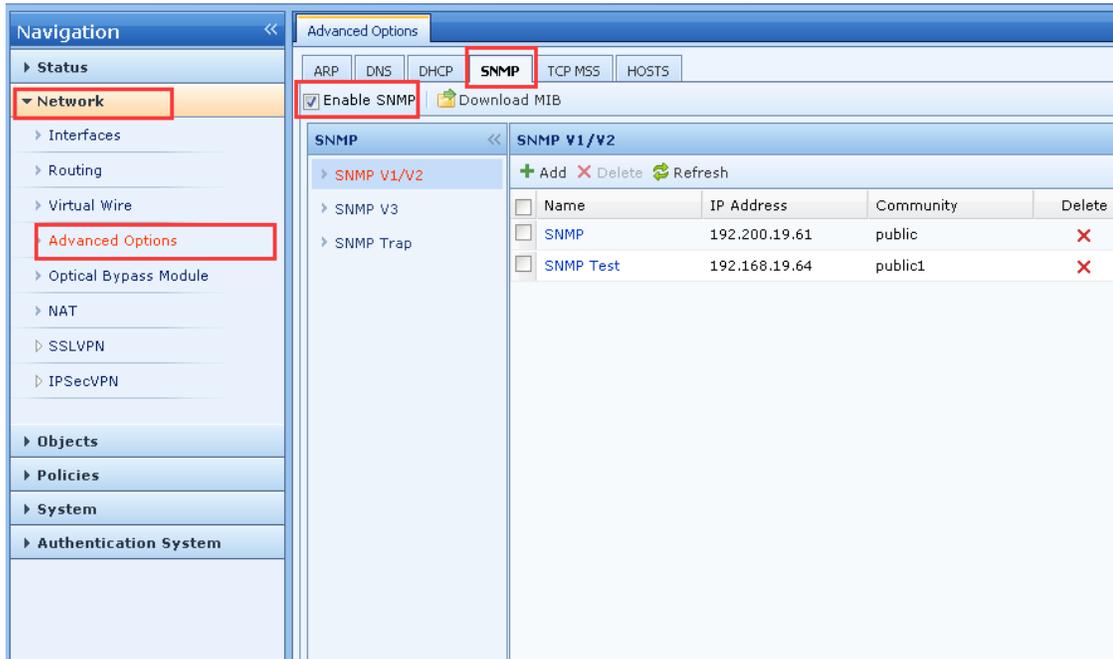
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

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

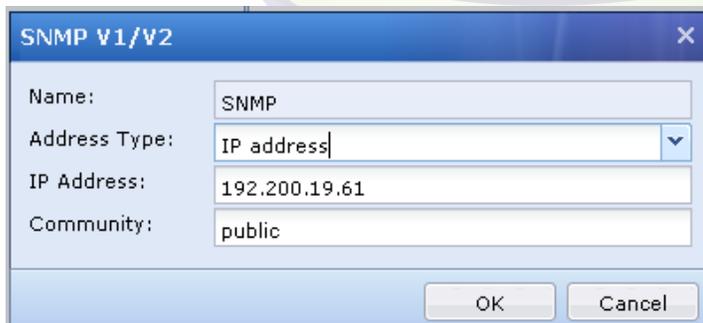
6 Configuration steps and screenshots

6.1 Configure advanced network options

- 6.1.1 Enable SNMP: under [Navigation] – [Network] – [Advanced Option], click the [SNMP] on right hand side to enter edit page. Tick [Enable SNMP] as shown in figure below:



- 6.1.2 If the third party network management software support SNMP V1/V2 protocol, click [SNMP V1/V2] – [Add], as shown in figure below:



[Name]: Given an arbitrary name for the network management host/server.

[Address Type]: The type of the management host. Could be “IP address” or “Subnet”. When “IP address” is chosen, it indicates that the management host is a device whereas when “Subnet” is chosen, it indicates that the management host is in a subnet, the hosts in the corresponding subnet can pass through SNMP device.

Your Future-Proof IT Enabler

Sangfor Technologies

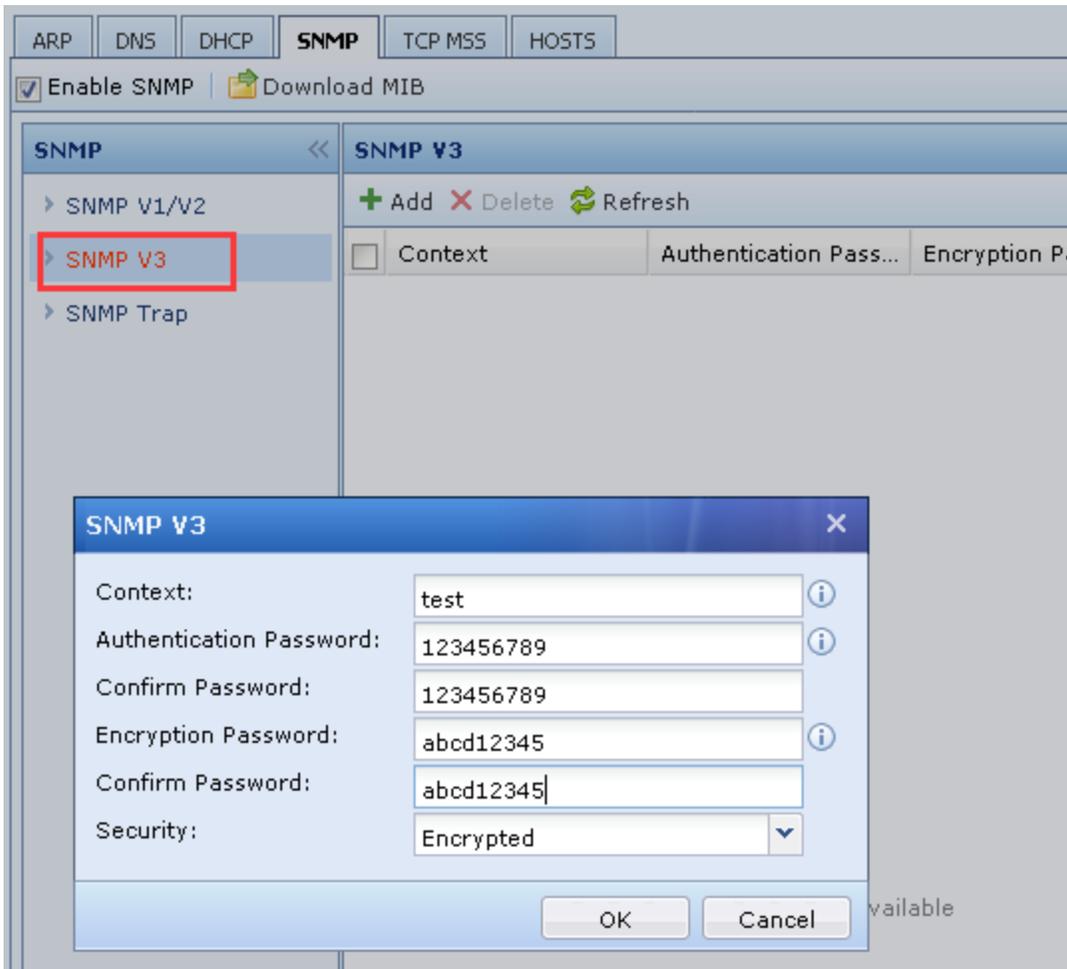
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

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

[IP Address]: Can be configured to be SNMP server's IP address or IP range. If "IP Address" is chosen in [Address Type], then specific SNMP server's IP address must be entered; if "Subnet" is chosen in [Address Type], then specify the subnet ID.

[Community]: to specify the community string when SNMP server access to the devices in the network.

- 6.1.3 If the third party network management software support SNMP V3 protocol, click [SNMP V3] – [Add], some advanced options are needed to be configured, as shown in figure below:



[Context]: Username of SNMPV3

[Authentication Password] and [Confirm Password]: password of the specific SNMPV3 user that is used for authentication purpose. Its length must be longer than eight characters without any blank space.

[Encryption Password] and [Confirm Password]: password that is used to encrypt message. The encryption password must be longer than eight characters without any blank space.

Your Future-Proof IT Enabler

Sangfor Technologies

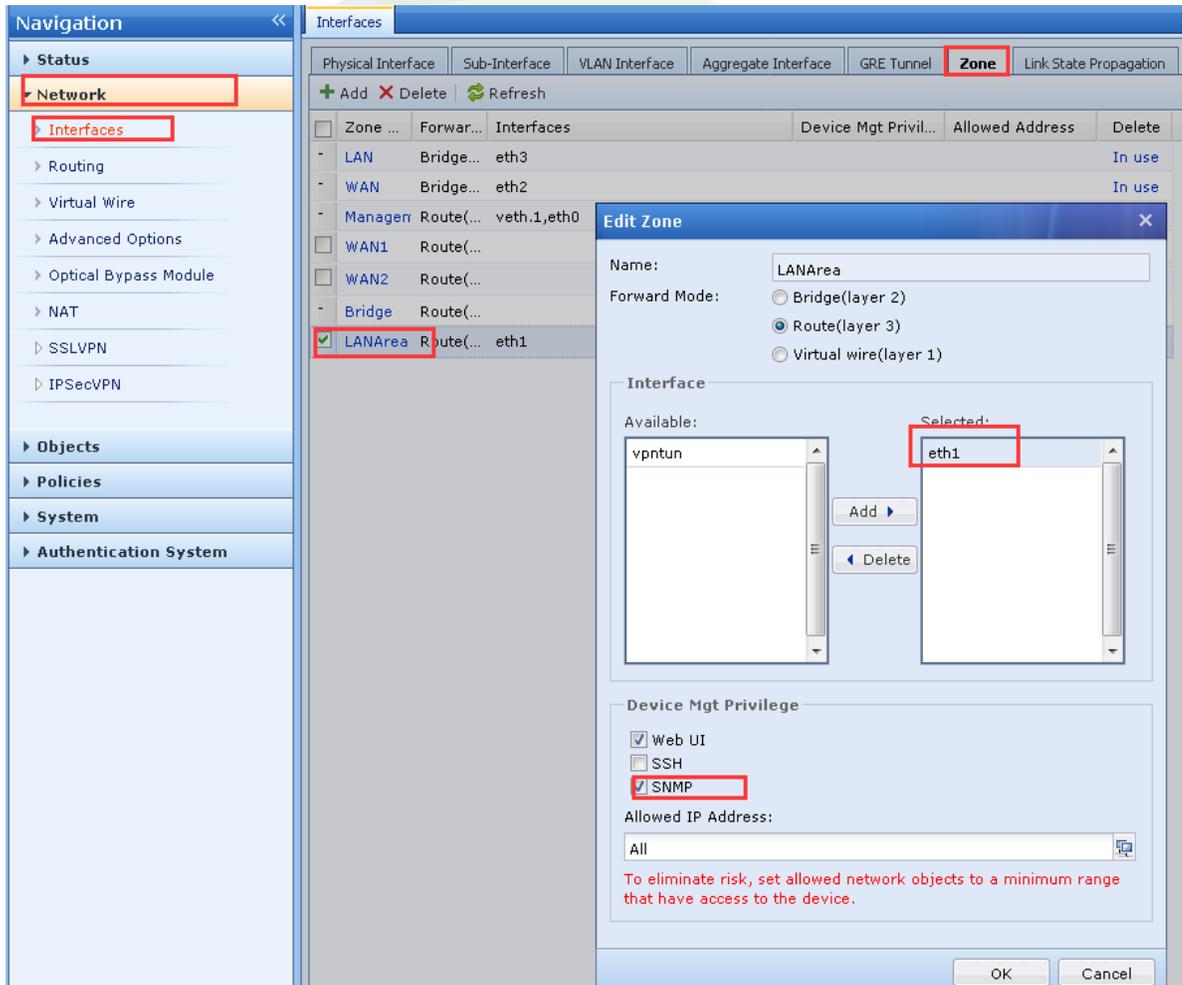
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

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

[Security]: To determine whether to execute SNMP authentication and message encryption. Options are [Encrypted] or [Not Encrypted]. When “Encrypted” is chosen, authentication and encryption are used with the first step to encrypt the data and secondly authenticate with the technique of message digest. If “Not Encrypted” is chosen, then only authentication will take effect.

6.2 Enable Zone SNMP

6.2.1 When the third part network management software is within one of the zone defined in our NGAF device, [Network] – [Interfaces] – [Zone], open the corresponding zone. Under [Device Mgt Privilege], tick [SNMP]. Ensure that the IP address of the third party network management software/device is included in the list of [Allowed IP Address], as shown in the figure below:



The screenshot displays the Sangfor NGAF web interface. On the left is a navigation tree with 'Network' and 'Interfaces' highlighted. The main area shows a table of zones. The 'LANArea' zone is selected, and its configuration is shown in a pop-up window.

Zone ...	Forwar...	Interfaces	Device Mgt Privil...	Allowed Address	Delete
- LAN	Bridge...	eth3			In use
- WAN	Bridge...	eth2			In use
- Managemer	Route(...	veth.1,eth0			
- WAN1	Route(...				
- WAN2	Route(...				
- Bridge	Route(...				
<input checked="" type="checkbox"/> LANArea	Route(...	eth1			

Edit Zone configuration details:

- Name: LANArea
- Forward Mode:
 - Bridge(layer 2)
 - Route(layer 3)
 - Virtual wire(layer 1)
- Interface Selection:
 - Available: vpntun
 - Selected: eth1
- Device Mgt Privilege:
 - Web UI
 - SSH
 - SNMP
- Allowed IP Address: All

To eliminate risk, set allowed network objects to a minimum range that have access to the 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



7 Precautions

1. When third party of network management software/device is used, all the OID value can be obtained from Sangfor technical support team.
2. The SNMP information configured in third party network management software/device must be consistent with those in NGAF device, such as “Community”
3. [SNMP] must be ticked in the correct zone which the corresponding interface of the third party of network management software/device is belongs to.



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