

# NGAF

## Transparent Mode Deployment Guide

Version 8.0.5



### Change Log

Date	Change Description
October 9, 2018	Version 8.0.5 document release.

### CONTENT

Chapter 1 Applicable Environment	4
Chapter 2 Configuration Step	4
Chapter 3 Precautions	12



## **Chapter 1 Applicable Environment**

When user need to apply firewall and does not change their network environment.

## **Chapter 2 Configuration Step**

#### 2.1 Configure Zone for LAN, WAN and management

Go to [Network]  $\rightarrow$  [Interfaces]-[Physical Interfaces]

Navigation	Interfaces	
▶ Status	Physical Interface Sub-Interface VLAN Interface Aggregate Interface GRE Tunnel Zone Link	State Propagation
▼ Network	+ Add 🗙 Delete   😂 Refresh	
> Interfaces	Zone Na Forward Interfaces Device Mgt Privilege	Allowed Address E
> Routing	- LAN Bridge(I eth3,eth4	I
-	- WAN1 Route(la veth.1 WebUI,ssh	All I
> Virtual Wire	- Bridge Route(la eth0 WebUI,ssh	All I
> Advanced Options	- WAN Bridge(I eth2	I
> Optical Bypass Module	an Route(la WebUI	All
> NAT	Intranet Bridge(I	
	- mirror Bridge(I	I
> SSLVPN	manage Route(la WebUI	All
▷ IPSecVPN	Server Bridge(I	

### Configuration for LAN zone

Edit Zone				×
Name:	LAN			
Forward Mode:	Bridge(layer 2)			
	O Rout	te(layer 3)		
	🔵 Virtu	ual wire(layer	1)	
Interface				
Available:			Selected:	
		]	eth3	
			eth4	
		Add 🕨		
		Delete		
		-		

Configuration for WAN zone

Edit Zone		×			
Name:	WAN				
Forward Mode:	Forward Mode: <ul> <li>Bridge(layer 2)</li> </ul>				
	○ Route(layer 3)				
	○ Virtual wire(layer 1)				
Interface					
Available:	Selected:				
	eth2				
	Add				
	< Delete				

### Configuration for Management zone

Edit Zone		×
Name: Forward Mode:	Mgmt O Bridge(layer 2) Route(layer 3) O Virtual wire(layer 1)	
Interface Available: eth0 eth1 eth2 eth3 vpntun	Selected: Add  Add  Delete	

2.2 Interface Configuration

Go to [Network]  $\rightarrow$  [Interfaces]-[Physical Interfaces].

Edit Physical Interfa	ice	×
🗹 Enable		
Name:	eth5	
Description:		
Туре:	Bridge(layer 2)	*
Added To Zone:	WAN	~
Basic Attributes:	WAN attribute	
IPv4/IPv6		_
(	Access O Trunk	
Access:	1	
VLAN	I Interface	
Advanced		
Configure link mod	de, MTU and MAC address. Settings	
	OK Can	cel

Assign one interface for WAN attribute and WAN zone

Assign another interface for LAN zone

Enable			
Name:	eth4		
Description:			
Туре:	Bridge(layer 2)		*
Added To Zone:	LAN		~
Basic Attributes:	WAN attribute		
IPv4/IPv6			
	Access     O Trunk		
Access:	1		
VLA	N Interface		
Advanced			
Configure link me	ode, MTU and MAC address.	Settings	

### 2.3 VLAN Configuration

Create a VLAN interface and add to management zone

Edit VLAN Interfa	ce X
Name:	Veth. 1
Description:	
Added To Zone:	Mgmt 💙
Basic Attributes:	✓ Pingable IPSec VPN outgoing line: Line 1 ✓ <sup>(i)</sup>
IP Assignment:	Static ODHCP
Static IP:	192.168.19.2/255.255.0
Next-Hop IP:	192.168.19.1
Link State Dete	ction
Specify link state	detection method(s).
Advanced	
Specify Maximum	Transmission Unit (MTU). Settings
	OK Cancel

#### 2.4 Routing Configuration

Configure it from [Network] $\rightarrow$ [Routing] $\rightarrow$ [Static Route] $\rightarrow$ [Add] $\rightarrow$ [Static Route] as image shown below:

Navigation «	Overview Routing *			
→ Status	Static Route Policy-Based Routing Multicast Route			
▼ Network	IPv4			
> Interfaces	🕂 Add - 🗙 Delete 🔤 Import 📑 Export   😂 Refresh			
> Routing	Static route			
> Virtual Wire	Multiple static routes			
> Advanced Options				
> Optical Bypass Module				
> NAT				
♦ SSLVPN				
▷ IPSecVPN				

Insert destination address, subnet mask, next hop IP and choose an interface for VLAN.

Edit Static Route	×
Destination:	0.0.0.0
Subnet Mask:	0.0.0.0
Next-Hop IP:	192.168.19.1
Interface:	veth.1
Metric:	0
Link State Detection:	Disable 🔻 🛈
	OK Cancel

If you need other static route in your network then you can proceed it in the same section here as well.

2.5 Application Control Policy

Navigation «	C	overview Appl	ication Control ×	
→ Status	+	• Add 🗙 Delete	e   🗸 Enable ⊘ D	Disable   🕇 Move Up
▶ Network		Priority	Name	Group
▶ Objects		1	block p2p	Default group
▼ Policies		-		2 g. oop
Access Control     Application Control     Country, Blocking		2	Allow	Default group
Connection Control	-	3	Default Policy	-
▲ Network Security → Policies				
> Anti-DoS/DDoS				
> ARP Spoofing Prevention				
> Decryption				
Bandwidth Management				
> Configuration Wizard				
> Blacklist/Whitelist				

Edit Application	Control	Policy	×
🗹 Enable			
Name:	Allow A		
Group:	Default	group	~
Source			
Network Objects/Users:	(	Network Objects	
		All	<u> </u>
	(	User/Group	
Zoper	ſ	Select	<u>.</u>
Port:			
- orti	(	Specified Port (i)	
Destination			
Network Objects:		All	<u></u>
Zone:		WAN	<b></b>
Comico (Appli			
Service/Application			
Service/Application:		Service     Bradefined Service (any	6
			별
		IM/skype	<b></b>
Schedule:		All week	~
Action:		Allow     Openy	
Advanced Settir	ngs:	Settings	
Remark:		Optional, up to 256 characters	
		ок	Cancel

Default Access Control policy will deny all the service and user need to configure manually to allow the service. User can configure other policy based on their needs as well.

## **Chapter 3 Precautions**

Transparent deployment mode is standing between 2nd and 3rd layer. But adding policy will only allows 3rd layer to 3rd layer zone to work. It will not working if user set policy for 2nd layer to 3rd later. Besides, configuration for routing is allow device to have internet access and update their database automatically.



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 is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective