



SANGFOR

NGAF

Bypass Mode Deployment Guide

Version 8.0.5

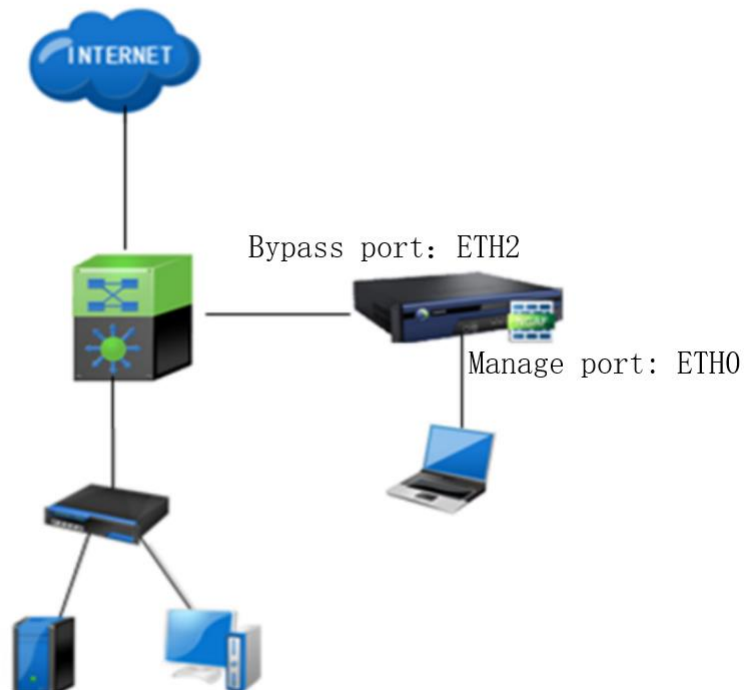
Change Log

Date	Change Description

CONTENT

Chapter 1 Applicable Scenario	4
Chapter 2 Configuration Steps	5
2.1 Configure Interfaces and Logging Option	5
2.2 Configure Logging Option	6
2.3 Configure IPS and WAF policies	7
Chapter 3 Precautions.....	11

Chapter 1 Applicable Scenario

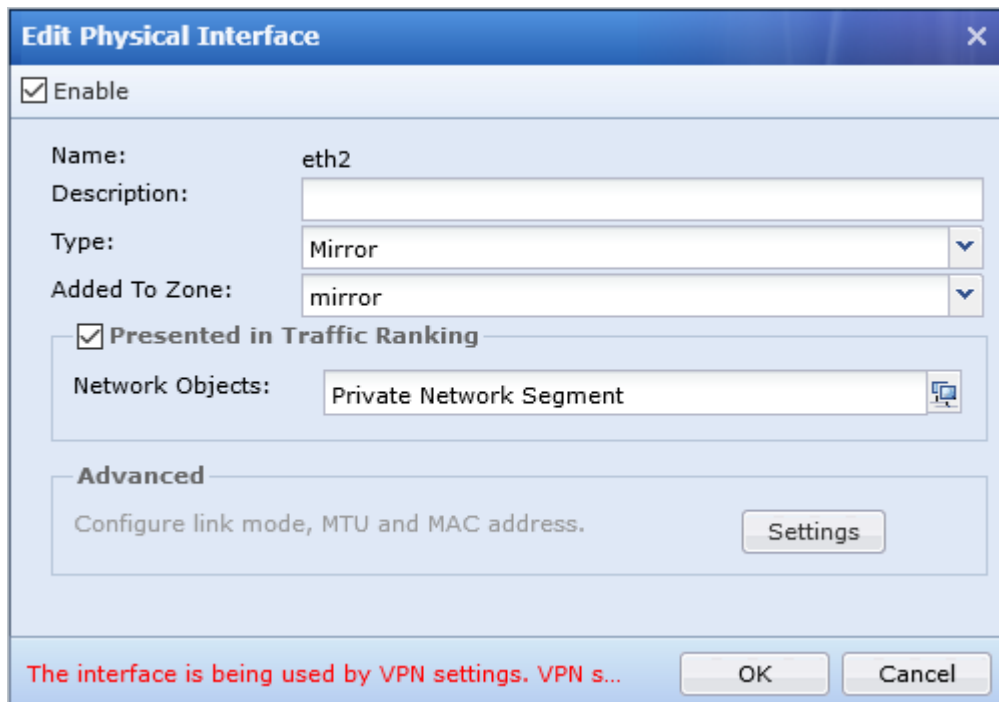


Bypass Mode: It can provide protection in the meanwhile does not affect the user network environment and able to avoid downtime risk caused by NGAF device. It will connect on mirror port of switch to ensure that traffic will go through switch when user accessing the server.

Chapter 2 Configuration Steps

2.1 Configure Interfaces and Logging Option

Modify "Network"—>"Interface" to add or modify the zone and the type of Physical Interface. Set the "Network Objects" into your desired group of users.



Edit Physical Interface

☒ Enable

Name: eth2

Description:

Type: Mirror

Added To Zone: mirror

☒ Presented in Traffic Ranking

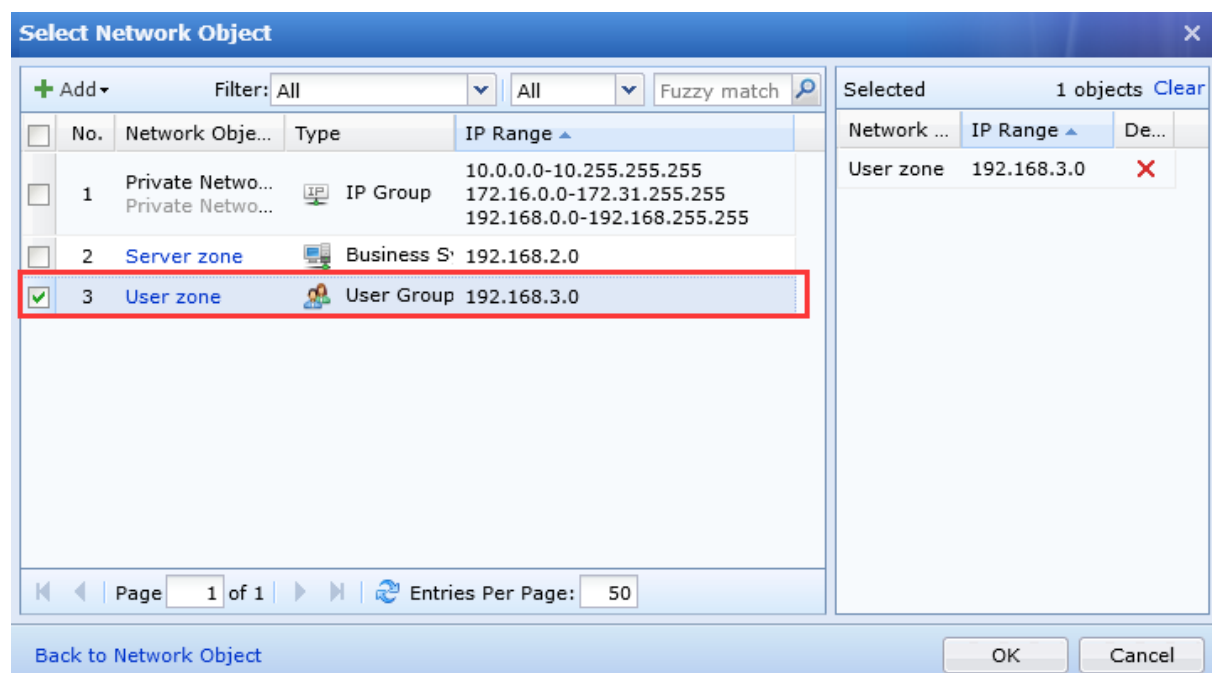
Network Objects: Private Network Segment

Advanced

Configure link mode, MTU and MAC address. [Settings](#)

The interface is being used by VPN settings. VPN s...

OK Cancel



Select Network Object

+ Add Filter: All All Fuzzy match

No.	Network Object	Type	IP Range
1	Private Network...	IP Group	10.0.0.0-10.255.255.255 172.16.0.0-172.31.255.255 192.168.0.0-192.168.255.255
2	Server zone	Business S...	192.168.2.0
3	User zone	User Group	192.168.3.0

Selected: 1 objects Clear

Network ...	IP Range	De...
User zone	192.168.3.0	X

Page 1 of 1 Entries Per Page: 50

Back to Network Object OK Cancel

2.2 Configure Logging Option

Access “System”→“Logging Option” activate the “Internal Report Center” from “Traffic audit logs” section as image shown below. Kindly make sure to click “Apply” button to save the configuration in order to allow NGAF to audit the user’s traffic in their network activities.

The screenshot displays the Sangfor NGAF 8.0.5 web interface. The left navigation pane shows the 'System' menu expanded, with 'Logging Options' highlighted. The main content area is titled 'Logging and Archiving' and contains four sections: 'Security logs', 'Application control logs', 'Traffic audit logs', and 'NAT logs'. Each section has 'Enable' and 'Disable' buttons. The 'Traffic audit logs' section is highlighted, and the 'Internal Report Center' is selected as the log location. Below this, the 'Syslog Server' section shows the IP Address as 192.200.19.57 and Port as 514. The 'Internal Report Center Logging Options' section shows the 'Log Preservation/Deletion' settings, with 'Preserve logs for certain days' selected, 'Number of Days' set to 60, and 'Delete logs of the earliest day if disk usage reaches threshold' selected. The 'Disk Usage Threshold(%)' is set to 80. The 'Log repetitive events only once' checkbox is checked. An 'Apply' button is at the bottom.

Section	Enable	Disable	Log Location
Security logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Syslog <input checked="" type="checkbox"/> Internal Report Center(recommended) <input checked="" type="checkbox"/>
Application control logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Syslog(recommended) <input checked="" type="checkbox"/> Internal Report Center <input checked="" type="checkbox"/>
Traffic audit logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Syslog(recommended) <input checked="" type="checkbox"/> Internal Report Center <input checked="" type="checkbox"/>
NAT logs	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Syslog <input checked="" type="checkbox"/>

Syslog Server

IP Address: 192.200.19.57
Port: 514

Internal Report Center Logging Options

Log Preservation/Deletion:
☒ Preserve logs for certain days
Number of Days: 60
☐ Delete logs of the earliest day if disk usage reaches threshold [Settings](#)
Disk Usage Threshold(%): 80
☒ Log repetitive events only once

Apply

2.3 Configure IPS and WAF policies

Access to “Policies” and configure IPS and WAF features.

Add Policy for Server Scenario [X]

Basics → Risk Assessment → Protection → Detection and Response

Name: test

Description: Optional, 0 to 95 characters

Status: ☒ Enable

Source

Zone: mirror

Network Objects/Users: ☒ Network Objects
All

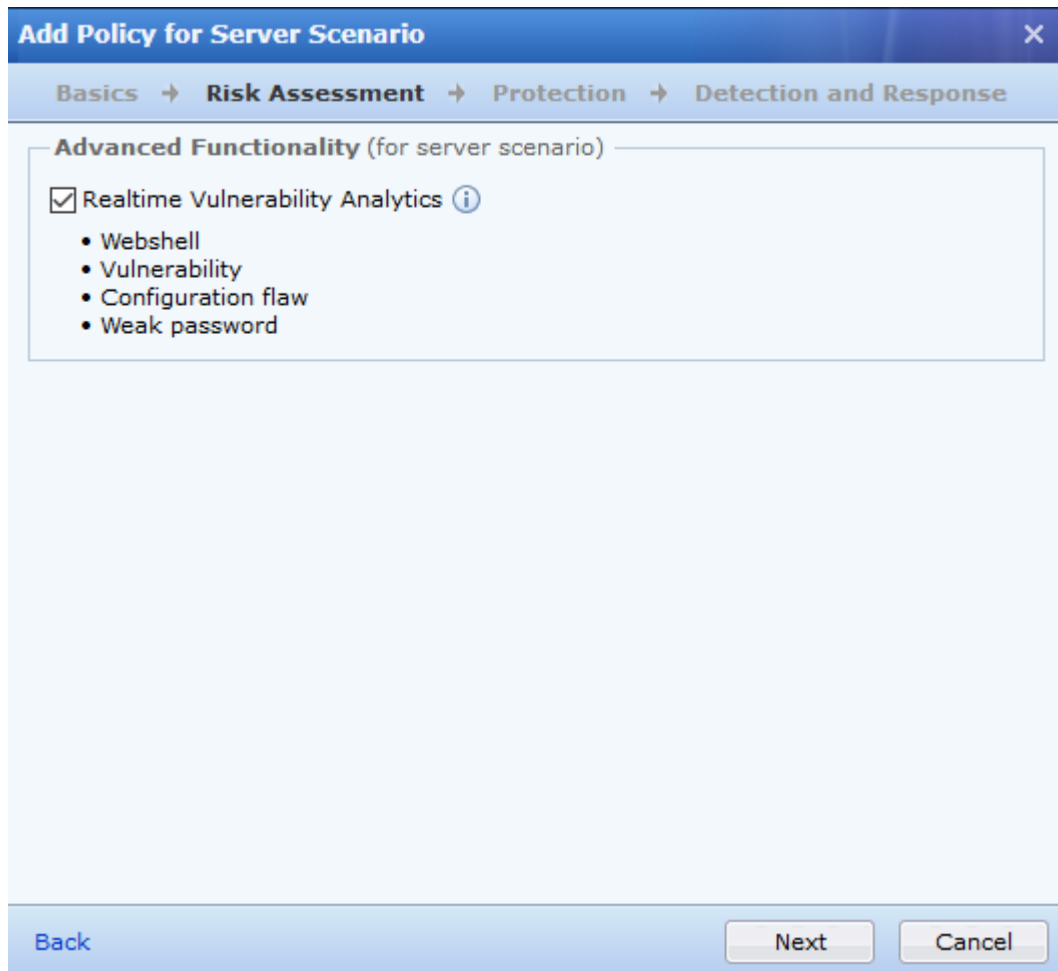
Destination

Zone: Bridge

Network Objects: Server zone

Next Cancel

You can tick for “Realtime Vulnerability Analytics” if you need it for your server.



The screenshot shows a Windows-style dialog box titled "Add Policy for Server Scenario". It has a blue header bar with a close button (X) in the top right corner. Below the header is a breadcrumb navigation bar with four steps: "Basics", "Risk Assessment", "Protection", and "Detection and Response", separated by right-pointing arrows. The "Detection and Response" step is currently selected. The main content area is titled "Advanced Functionality (for server scenario)". Inside this area, there is a checkbox labeled "Realtime Vulnerability Analytics" which is checked. To the right of this checkbox is a small circular icon containing an 'i'. Below the checkbox is a bulleted list of four items: "Webshell", "Vulnerability", "Configuration flaw", and "Weak password". At the bottom of the dialog box, there are three buttons: "Back" on the left, and "Next" and "Cancel" on the right.

Add Policy for Server Scenario [X]

Basics → Risk Assessment → Protection → Detection and Response

Advanced Functionality (for server scenario)

☒ Realtime Vulnerability Analytics ⓘ

- Webshell
- Vulnerability
- Configuration flaw
- Weak password

Back Next Cancel

In “Protection” can activate IPS and WAF functionalities.

Add Policy for Server Scenario [X]

Basics → Risk Assessment → **Protection** → Detection and Response

Basics Protection (for any scenario)

☒ Intrusion Prevention ⓘ

Default Template_Server Scenario Action: ☐ Allow ☒ Deny

☐ Content Security ⓘ

Default Template Action: ☒ Allow ☐ Deny

Advanced Functionality (for server scenario)

☒ Web App Protection ⓘ

Default Template Action: ☐ Allow ☒ Deny

Back Next Cancel

In “System”→“General”→“System”→“Network” and activate the option of “Send TCP Reset message in mirror mode to reject” to prevent the packets from entering the network from WAF/IPS.

The screenshot shows the configuration interface for a security device. The left sidebar contains a navigation menu with the following items: Status, Network, Objects, Policies, System (expanded), General, System (selected), Logging Options, Alarm Options, Administrator, Maintenance, Troubleshooting, High Availability, Central Management, Authentication System, and Security Solution. The main content area is titled 'Network' and contains various configuration options. A red box highlights the option 'Send TCP Reset message in mirror mode to reject request', which is currently checked. A tooltip is visible next to this option, stating: 'Decide whether TCP Reset message can be sent to reject request when this device is in mirror mode'. Other visible options include 'Send TCP Reset message to reject request' (checked), 'Packet detection' (checked), 'Base64 decoding' (checked), 'In-depth hex packets decoding' (unchecked), 'High performance for Internet access' (unchecked), 'Connection to HA pair' (unchecked), 'Visible to Linux with traceroute command' (unchecked), 'Always detect data packets that traverse repeatedly' (unchecked), 'Enable network load balancing on network adapter' (unchecked), and 'Enable protection against outside DoS attacks' (unchecked). The 'ARP Broadcast Interval' is set to 30 seconds. The 'SIP Port' is set to UDP:5060, TCP:5060. The 'H.323 Port' is checked. The 'RAS' is set to UDP:1719 and 'Q931' is set to TCP:1720. The 'TCP Conn Timeout(s)' is 1800, 'UDP Conn Timeout(s)' is 180, and 'ICMP Timeout(s)' is 30. The 'SSH Port' is 22345, 'FTP Port' is TCP:21, 'RTSP Port' is TCP:554, 'SQLNET Port' is TCP:1521, 'TFTP Port' is UDP:69, and 'PPTP Port' is TCP:1723. An 'OK' button is located at the bottom right of the configuration area.

Option	Status
Send TCP Reset message in mirror mode to reject request	Checked
Send TCP Reset message to reject request	Checked
Packet detection	Checked
Base64 decoding	Checked
In-depth hex packets decoding	Unchecked
High performance for Internet access	Unchecked
Connection to HA pair	Unchecked
Visible to Linux with traceroute command	Unchecked
Always detect data packets that traverse repeatedly	Unchecked
Enable network load balancing on network adapter	Unchecked
Enable protection against outside DoS attacks	Unchecked

Chapter 3 Precautions

1. AF traffic ranking will show the traffic of local IP group and non-local IP group.
2. If there is any other protection functionalities, bypass mode need to tick "System"→"Network"→" Send TCP Reset message in mirror mode to reject". Else, WAF, IPS or any other functionalities will not be effective.



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 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