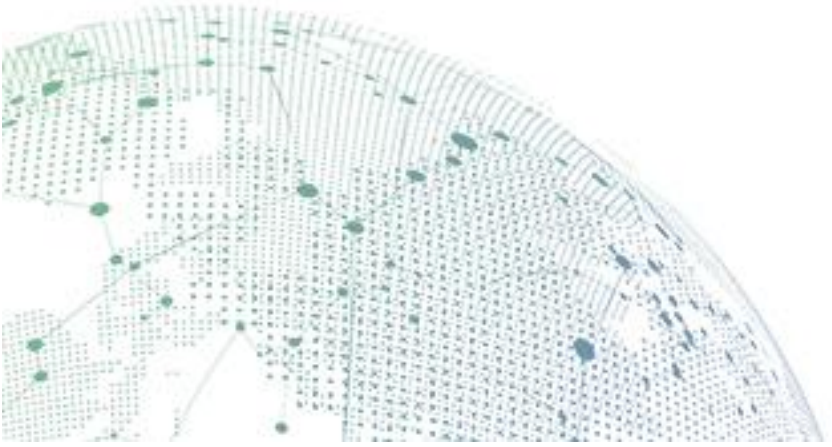
SANGFOR

# NGAF

## Bypass Mode Deployment Guide

Version 8.0.5

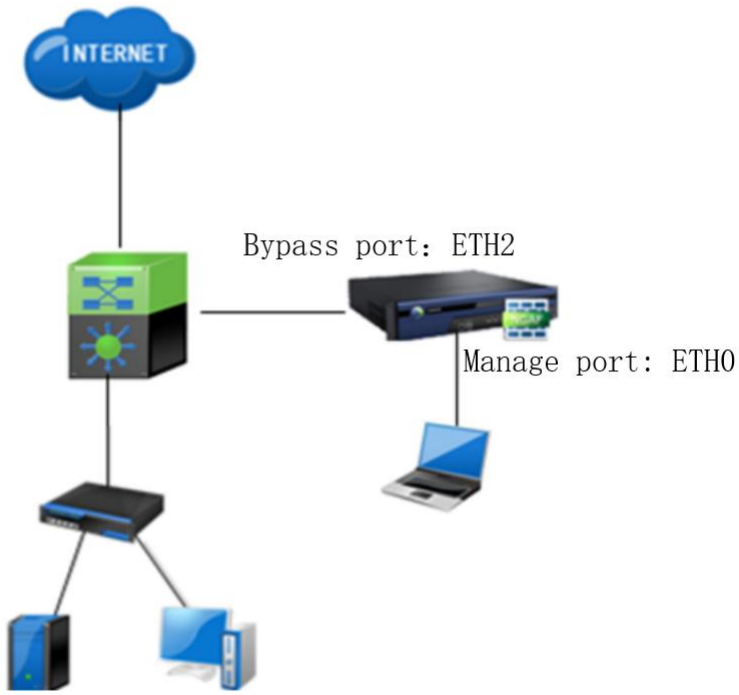


## Change Log

| Date | Change Description |
| --- | --- |
| | |
| | |

# CONTENT

# Chapter 1 Applicable Scenario

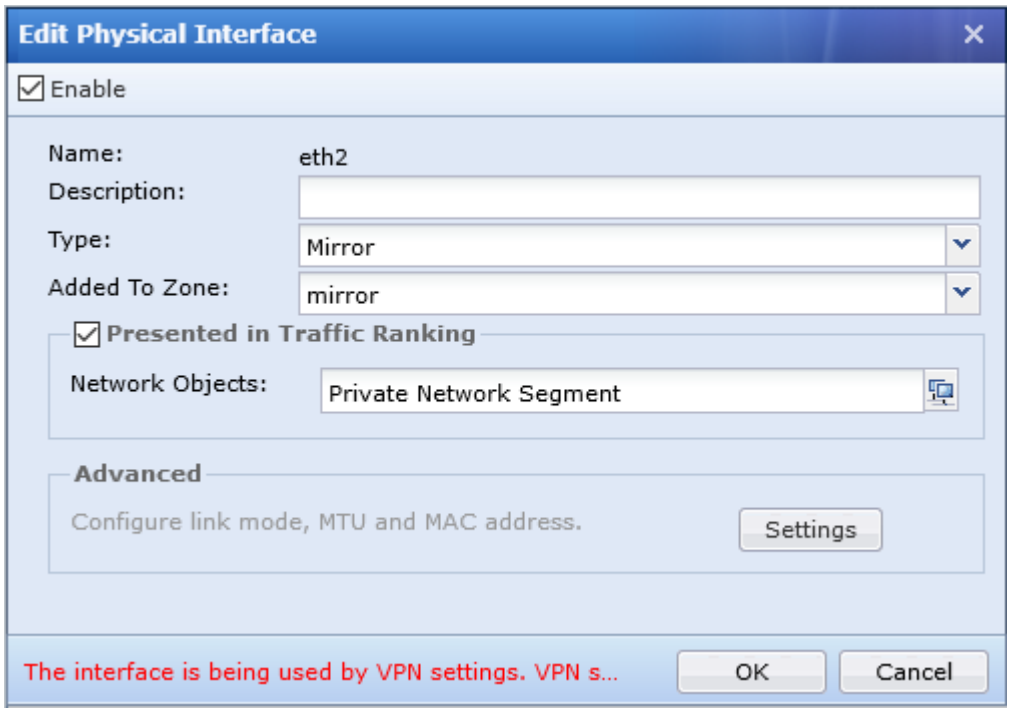


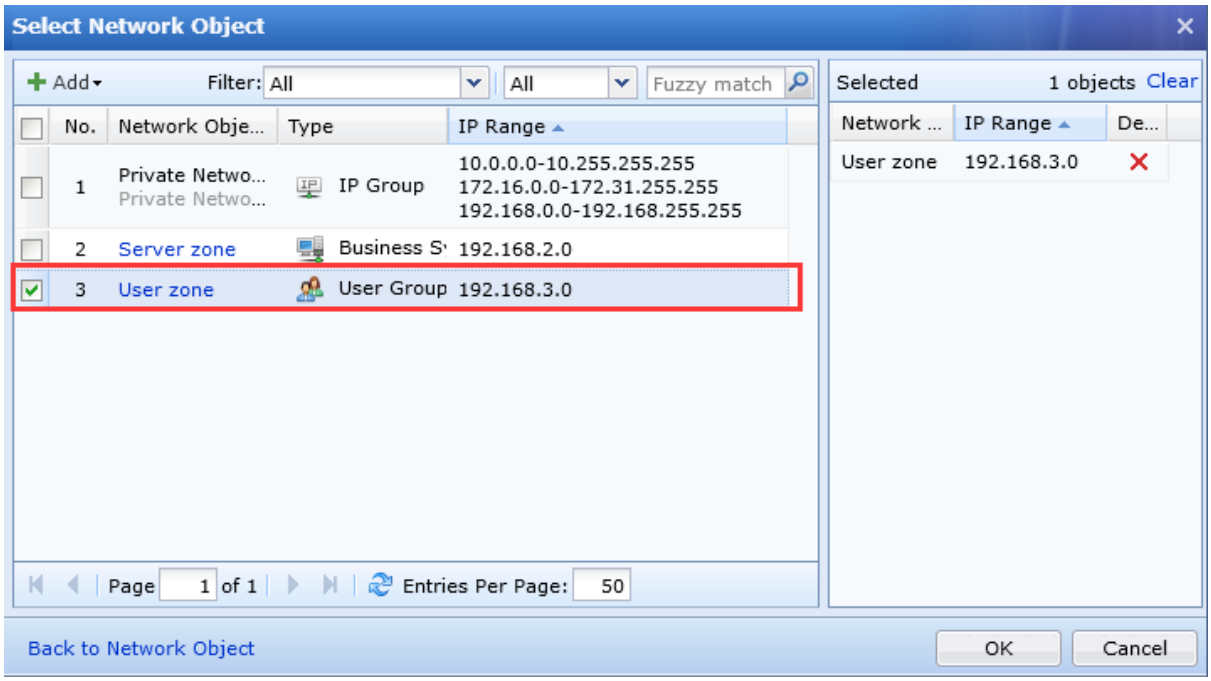

Bypass Mode: It can provide protection in the meanwhile does not affect the suer network environment and able to avoid downtime risk caused by NGAF device. It will connect on mirror port of switch to ensure that traffic will go through switch when user accessing the server.

# Chapter 2 Configuration Steps

## 2.1 Configure Interfaces and Logging Option

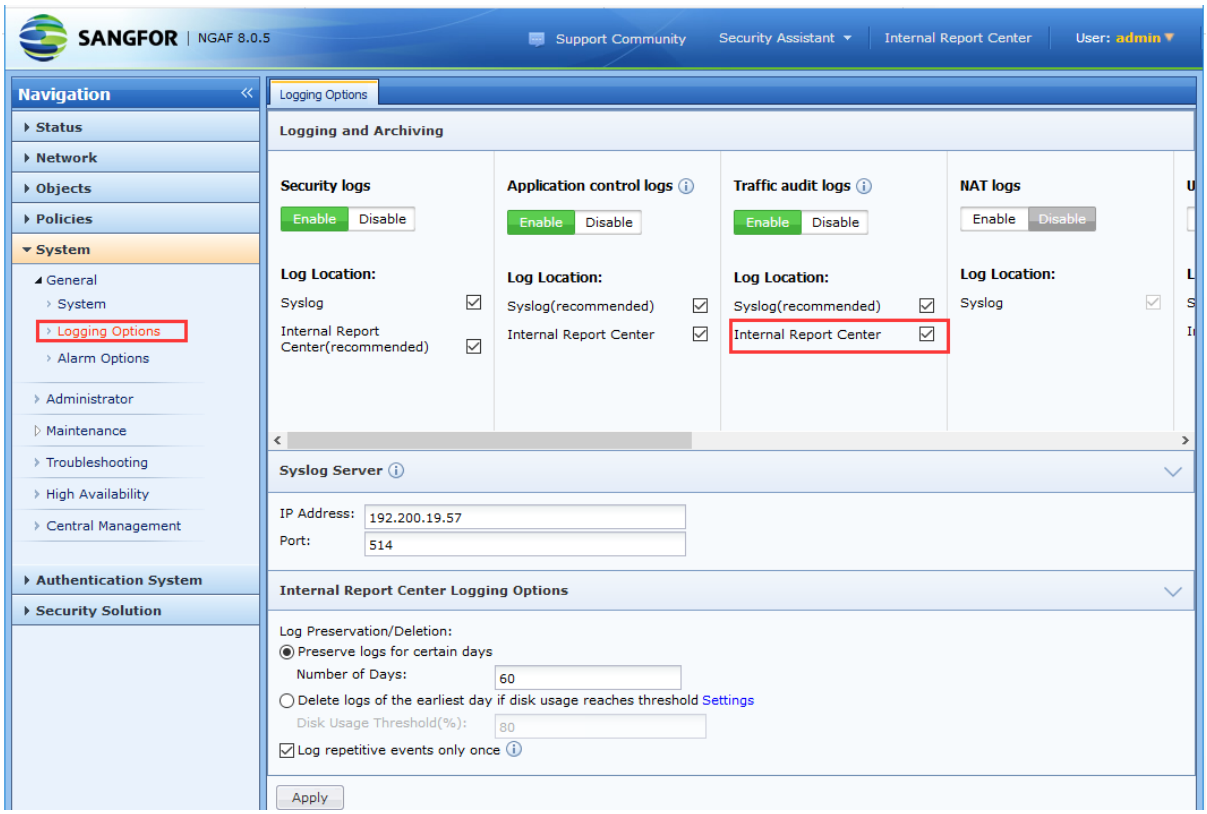
Modify"**Network**"—>"**Interface**" to add or modify the zone and the type of Physical Interface. Set the "Network Objects" into your desired group of users.



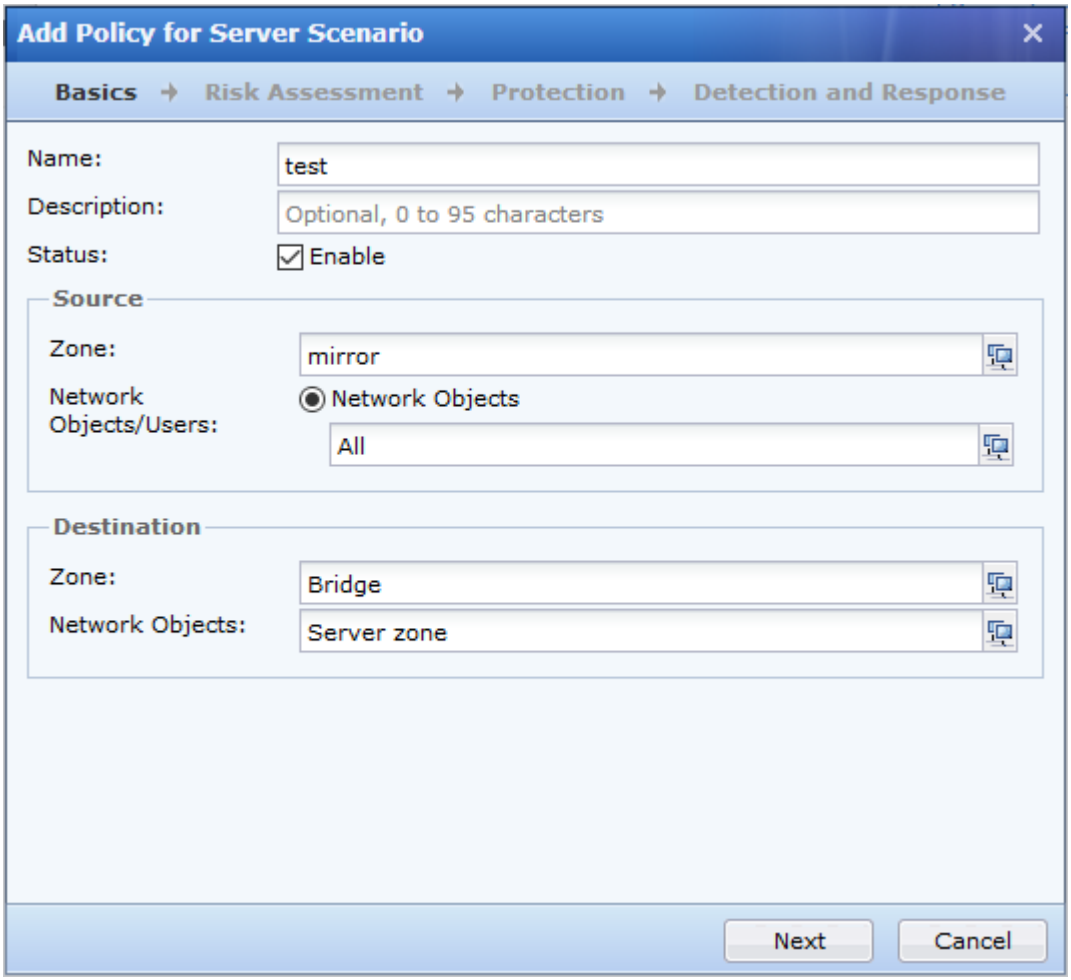
## 2.2 Configure Logging Option

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.

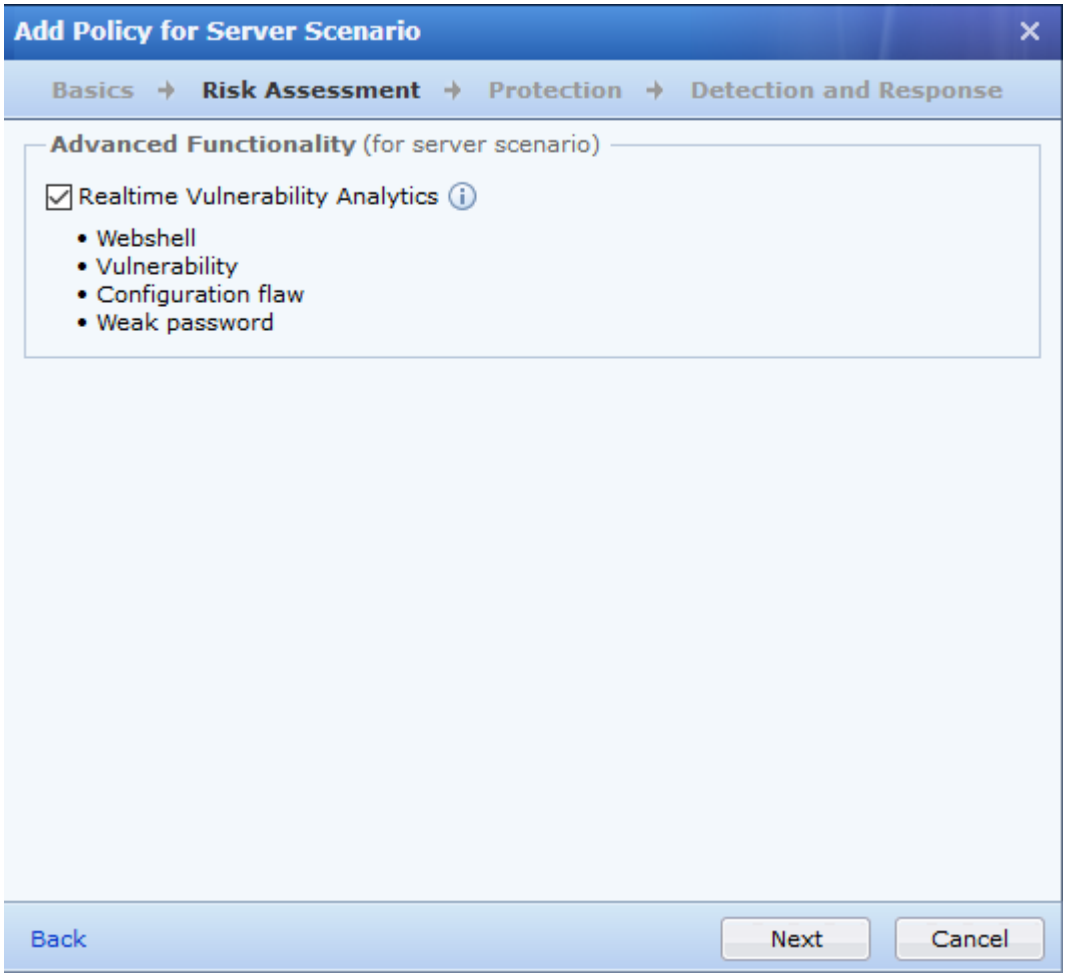


## 2.3 Configure IPS and WAF policies

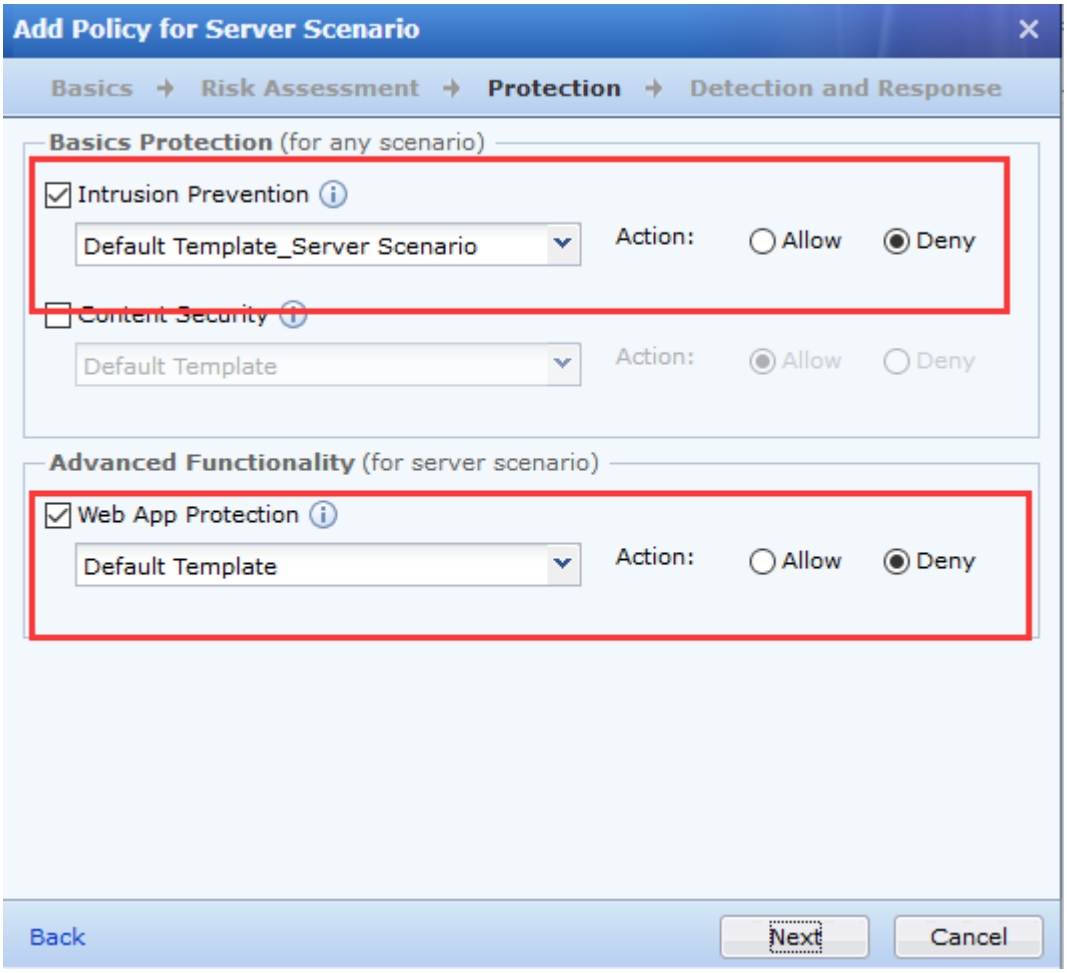
Access to “Policies” and configure IPS and WAF features.



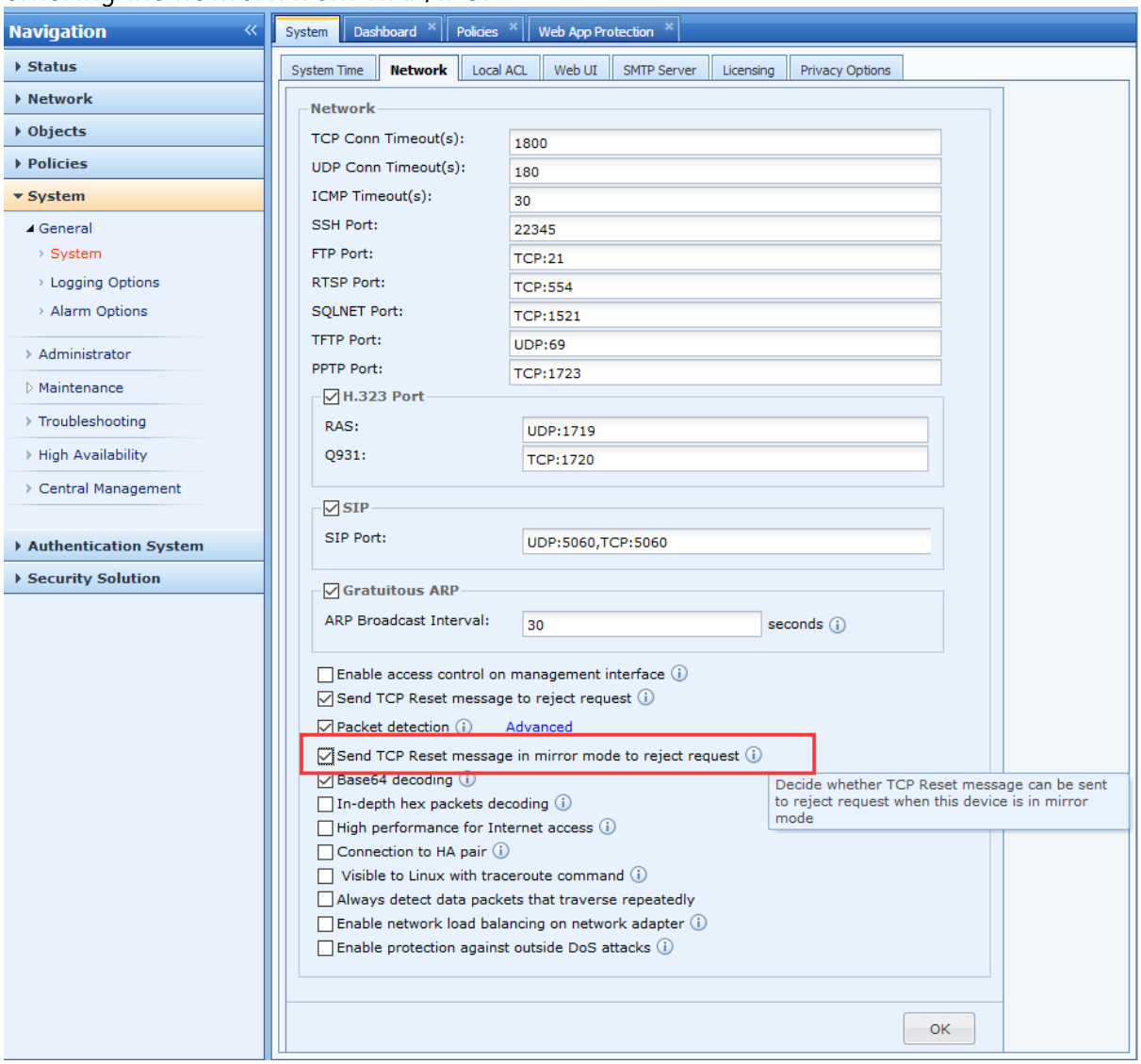
You can tick for “Realtime Vulnerability Analytics” if you need it for your server.



In “Protection” can activate IPS and WAF functionalities.



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.



# 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.

SANGFOR