SANGFOR

Cyber Command

Best Practices for Scenarios_How to Correlate with NGAF to Simply the Operation

Version 3.0.49

Change Log

Date	Change Description
Mar 19, 2021	Document release.
May 17, 2021	Document update.

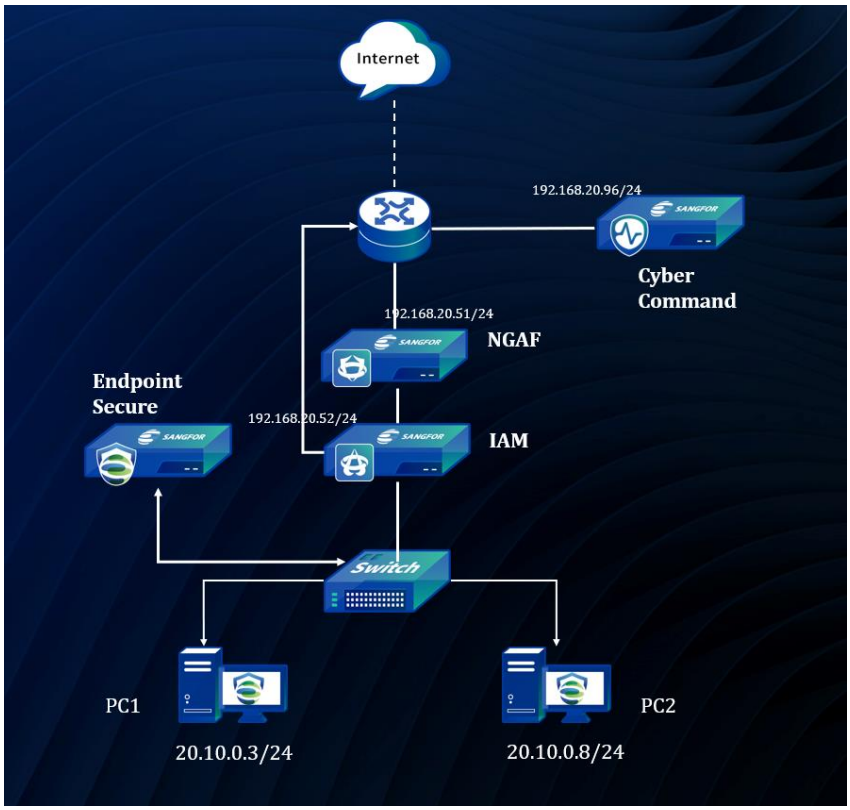
CONTENT

Chapter 1 Scenario

1.1 Scenario

1.2 Environment

1.2.1 Network Environment



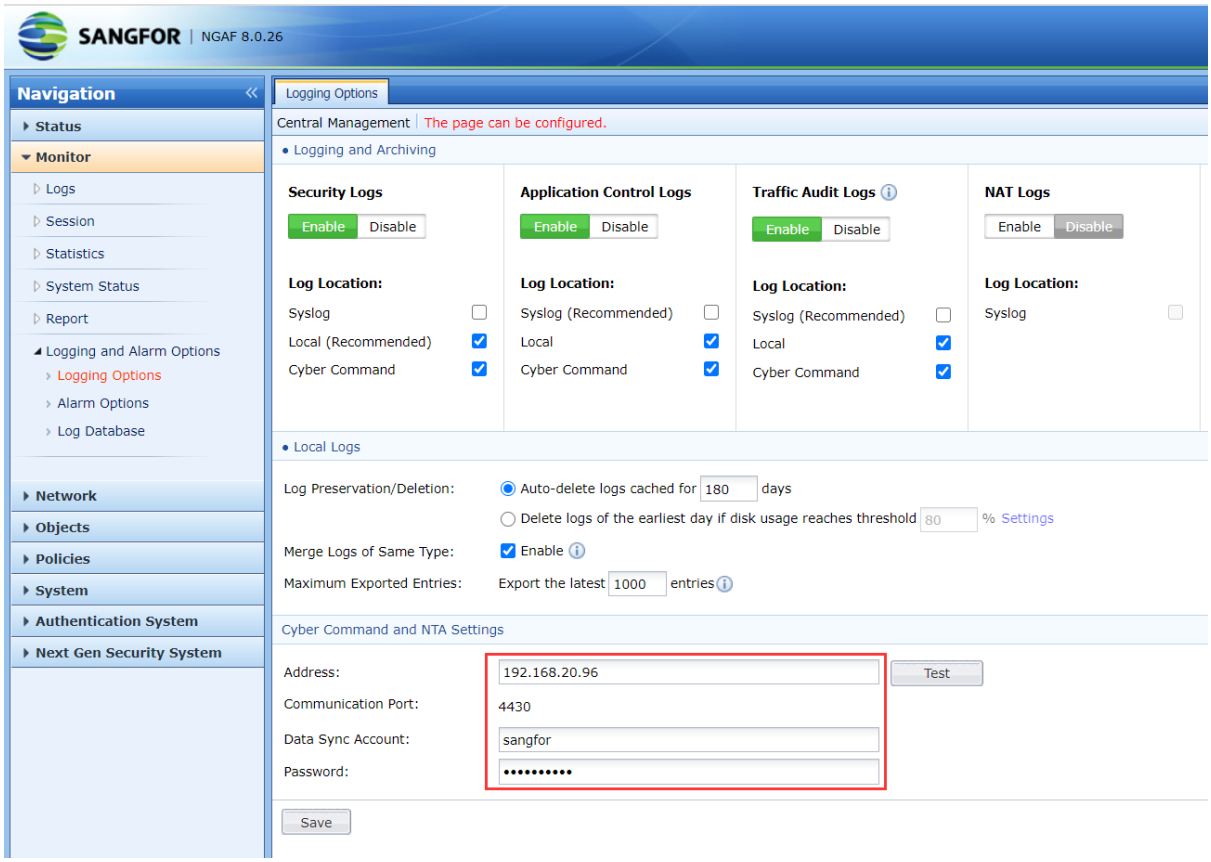
1.3 Test Introduce

1. It only needs to analyze the traffic of the Botnet URL domain name to pass through NGAF, and it does not need to visit these URLs.

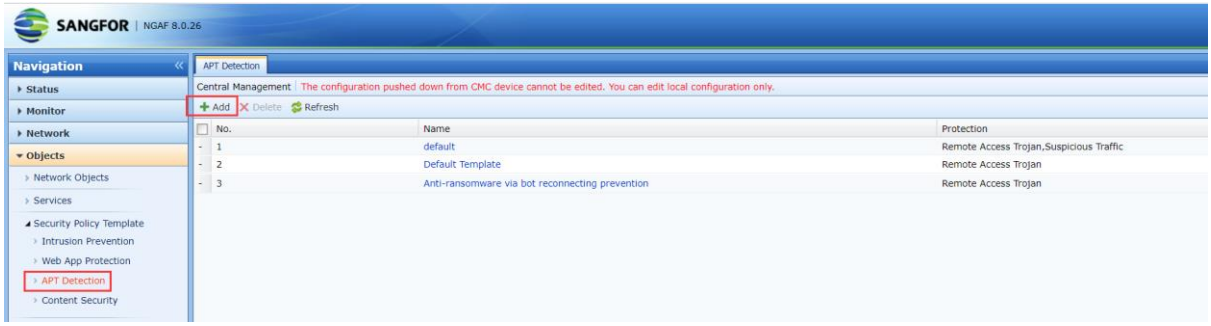
Chapter 2 Configuration

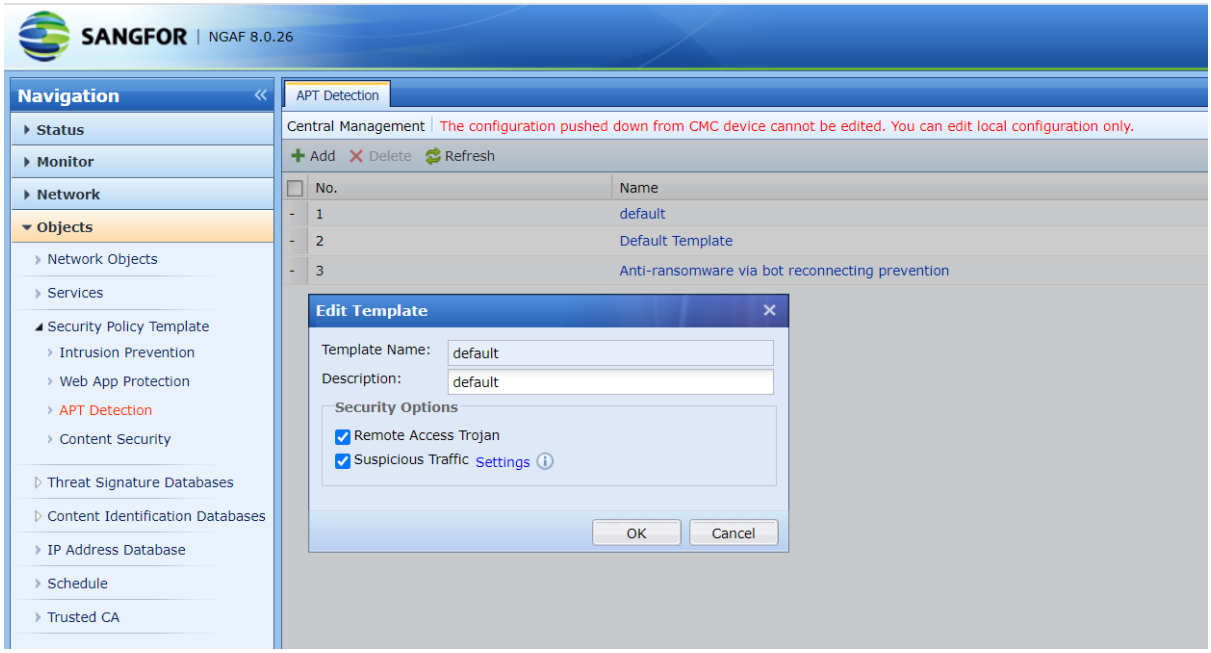
2.1 Configure NGAF

1. Go to Monitor->Logging and Alarm Options-> Logging Options Path, configure the correlation options, such as IP of Cyber Command, you can set up an account and password, it will be used in Cyber Command.

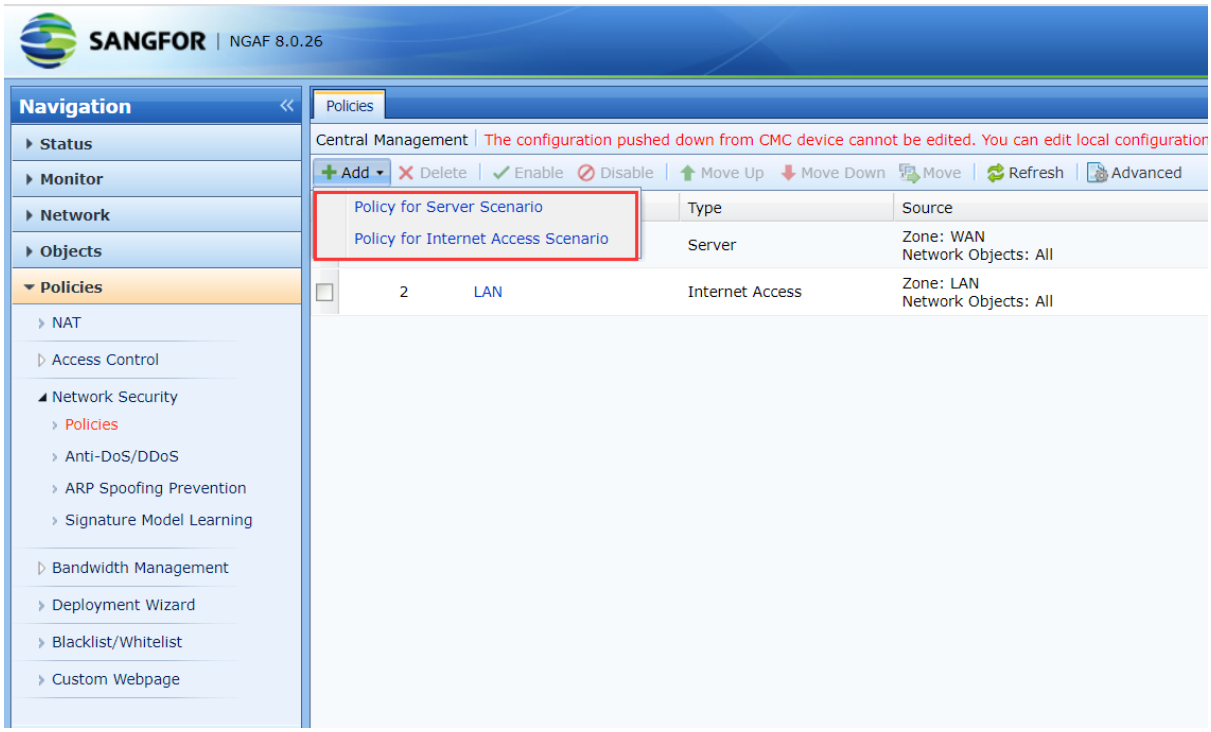


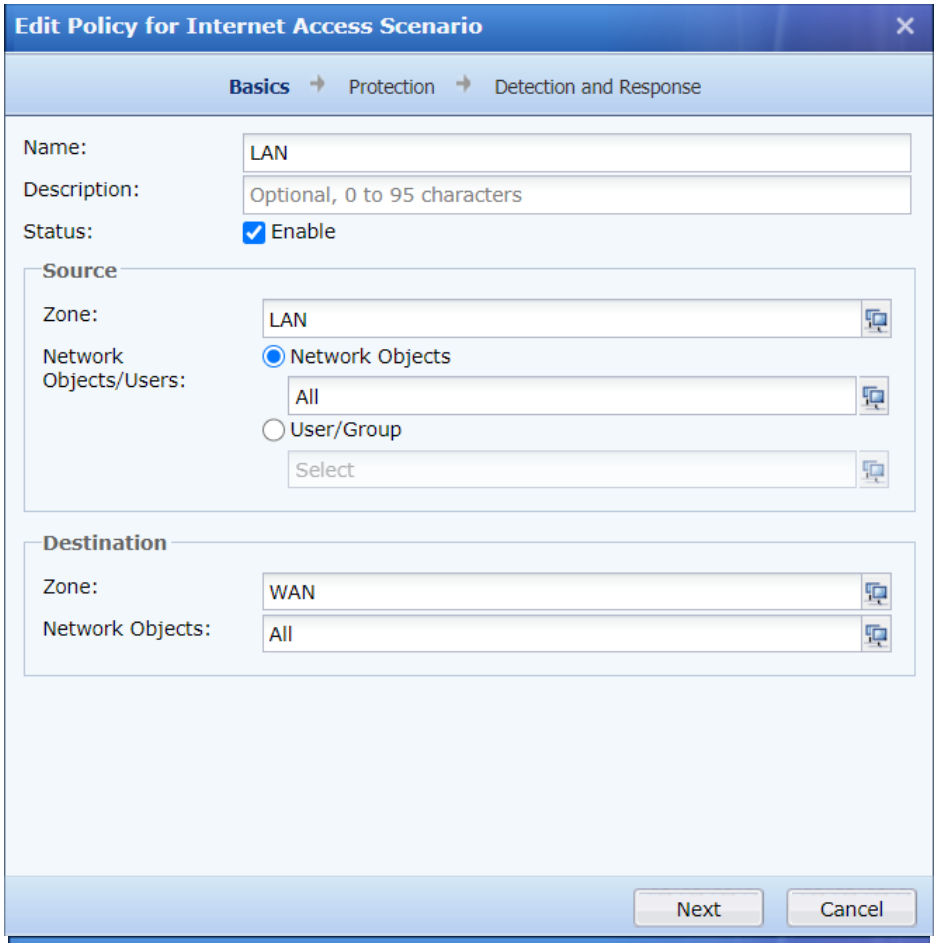
2.Go to Objects-> Security Policy Template->APT Detection, add an APT template.

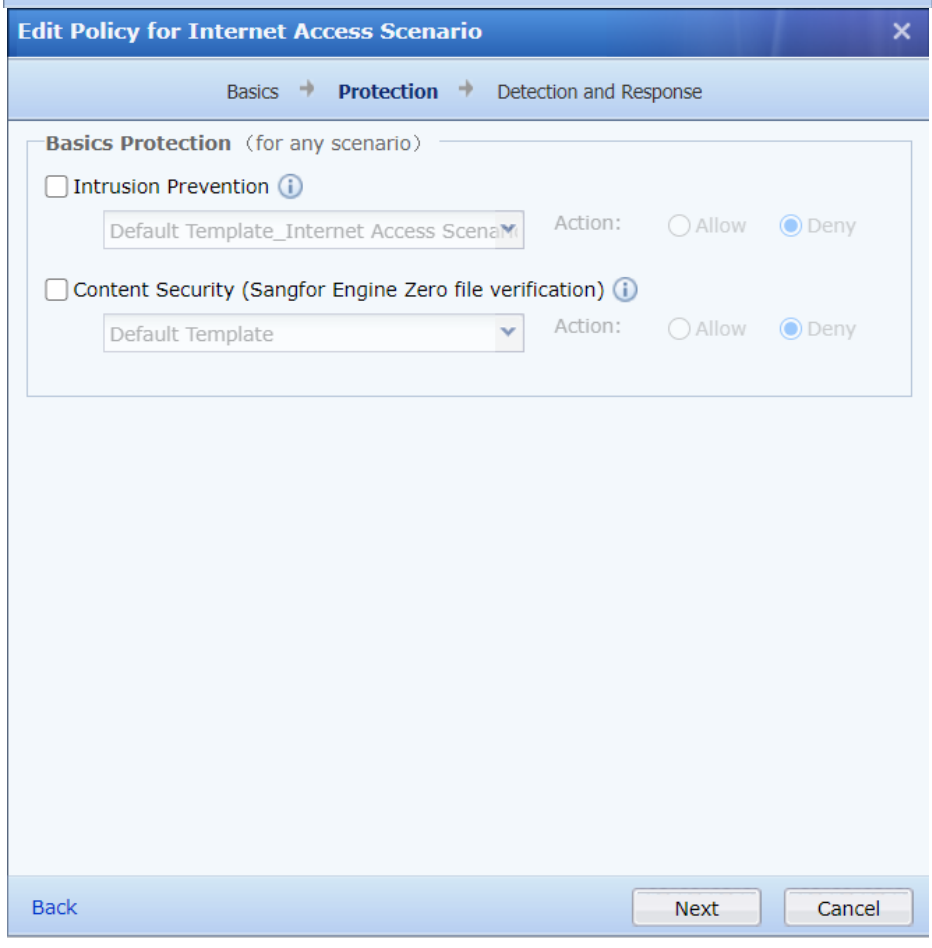


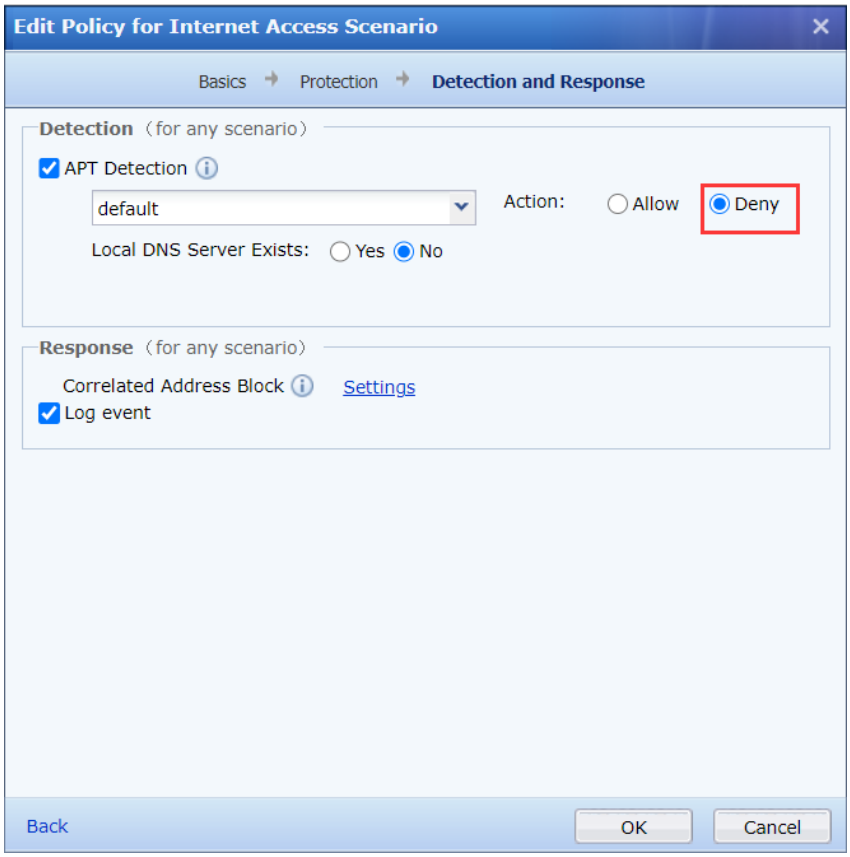


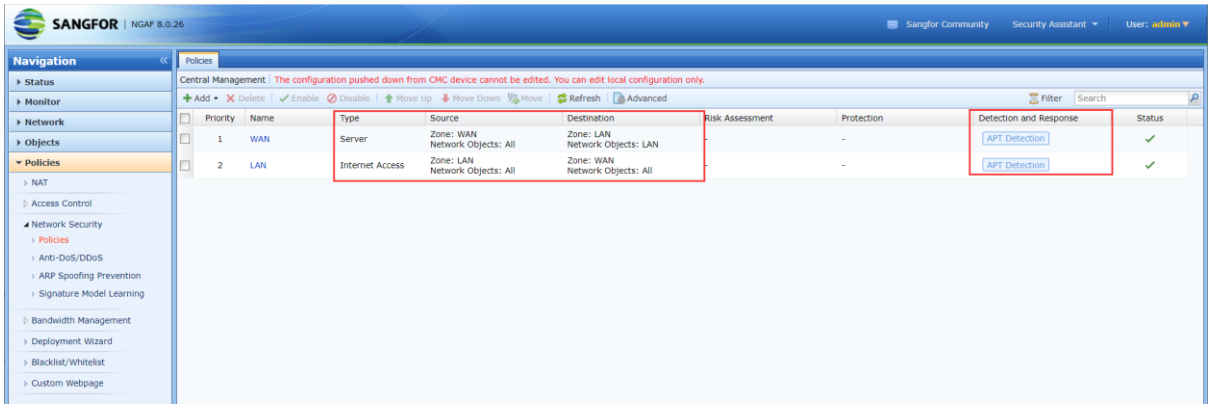
3.Go to Policies->Network Security->Policies path, add two policies to block the botnet traffic.




Edit Policy for Internet Access Scenario
Basics
Protection
Detection and Response
Name:
LAN
Description:
Optional, 0 to 95 characters
Status:
Enable
Source
Zone:
LAN
Network Objects/Users:
Network Objects
All
User/Group
Select
Destination
Zone:
WAN
Network Objects:
All
Next
Cancel

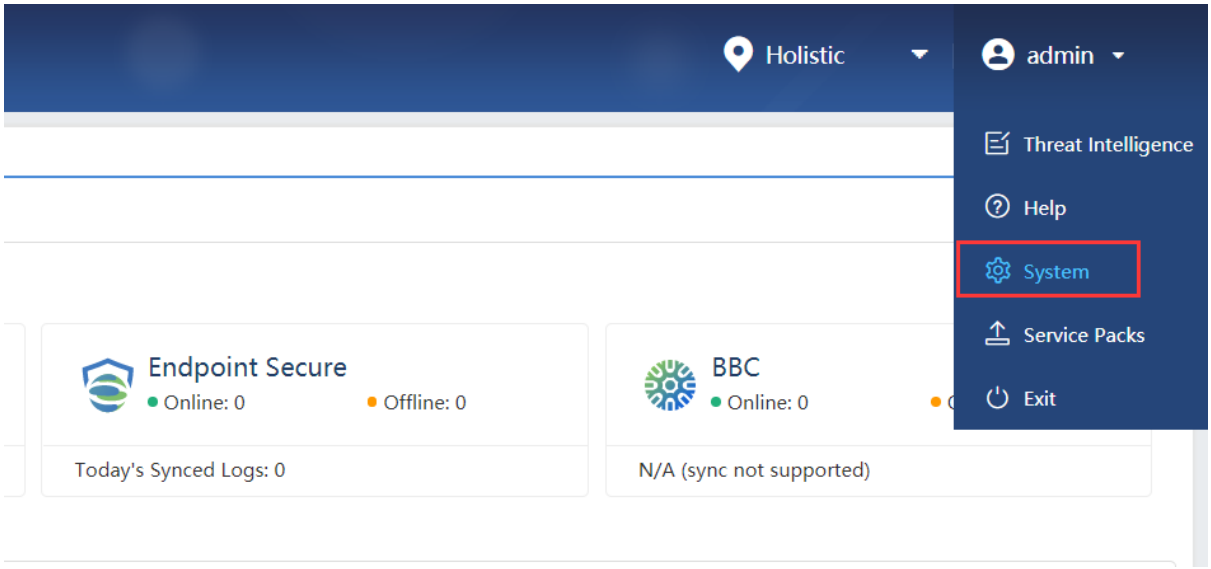

Edit Policy for Internet Access Scenario
Basics
Protection
Detection and Response
Basics Protection (for any scenario)
Intrusion Prevention
Default Template_Internet Access Scena
Action:
Allow
Deny
Content Security (Sangfor Engine Zero file verification)
Default Template
Action:
Allow
Deny
Back
Next
Cancel



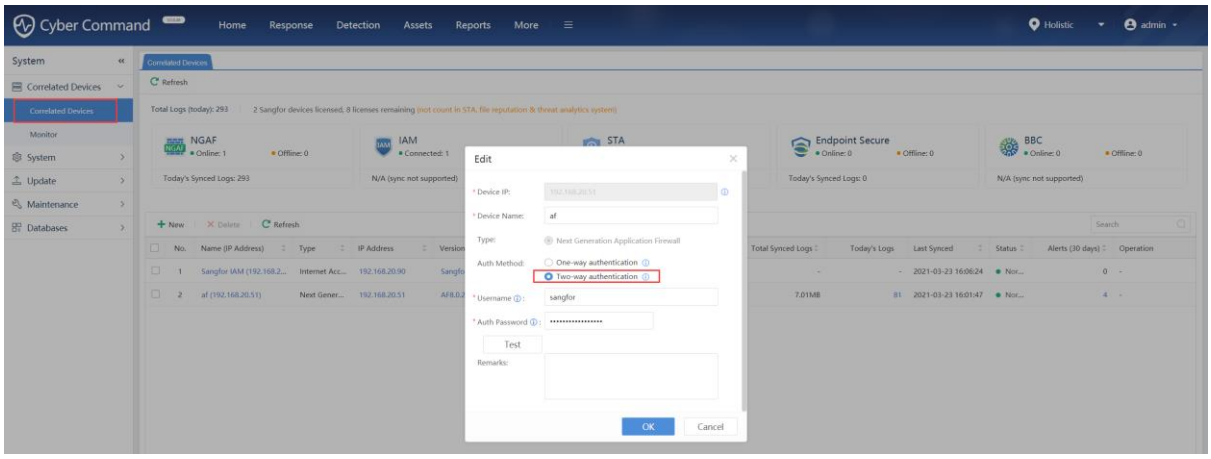


2.2 Configure Cyber Command

1. Go to System path.

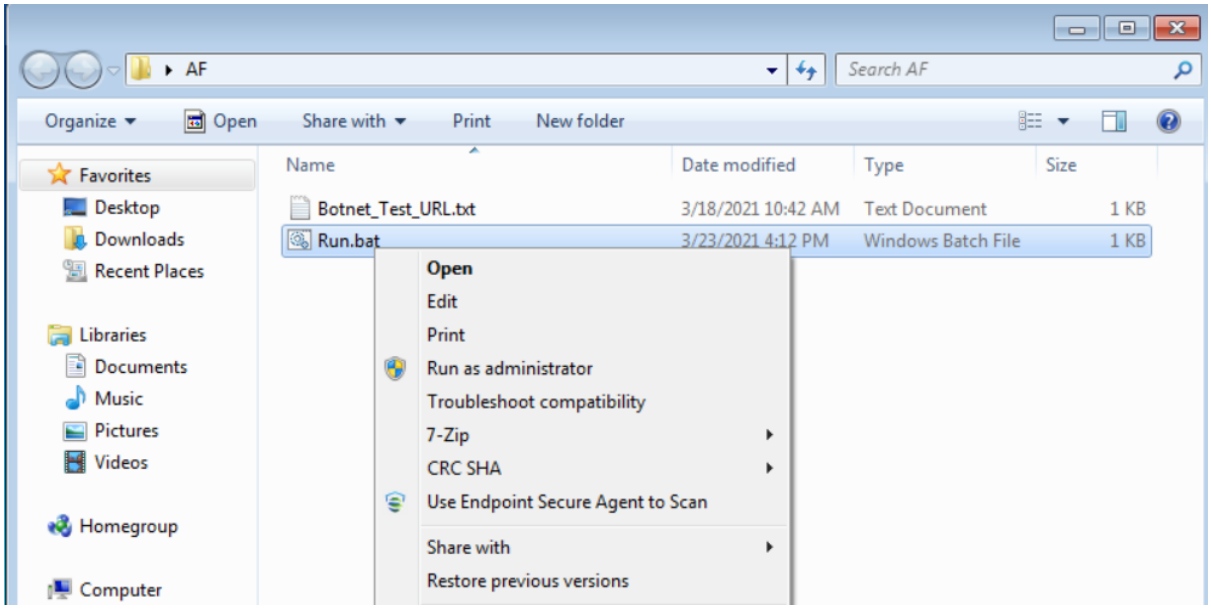


2.Enable Two-way authentication, then input the account and password that you configured in NGAF.



2.3 Run Botnet Program

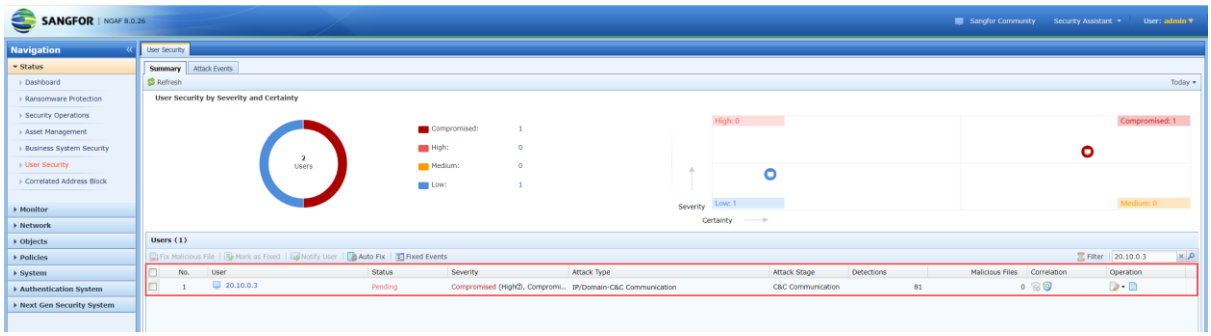
1.Run Botnet Program PC.



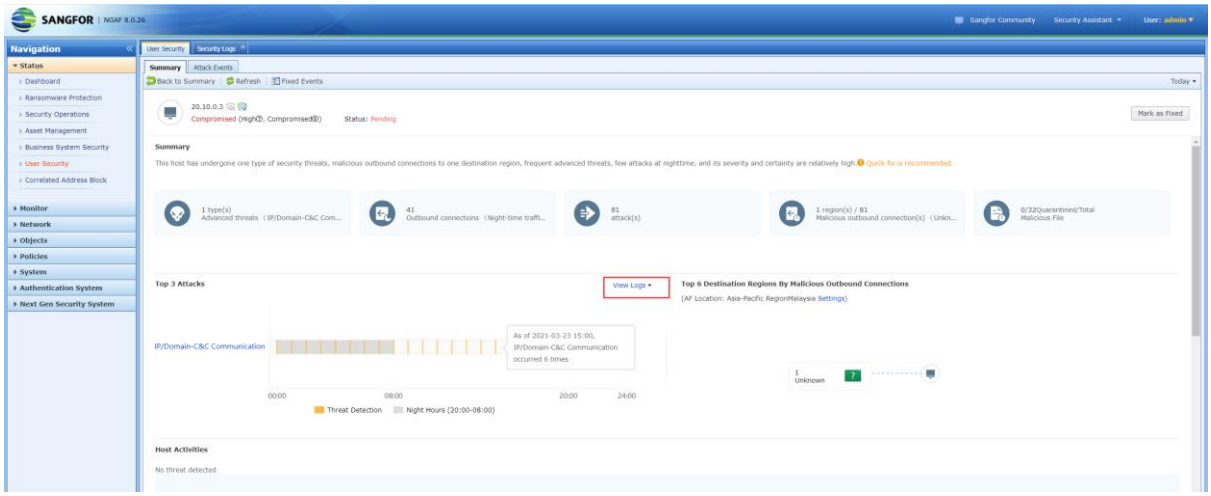
2.4 Check Logs and Correlated to Block

2.4.1 Check Security Logs in NGAF

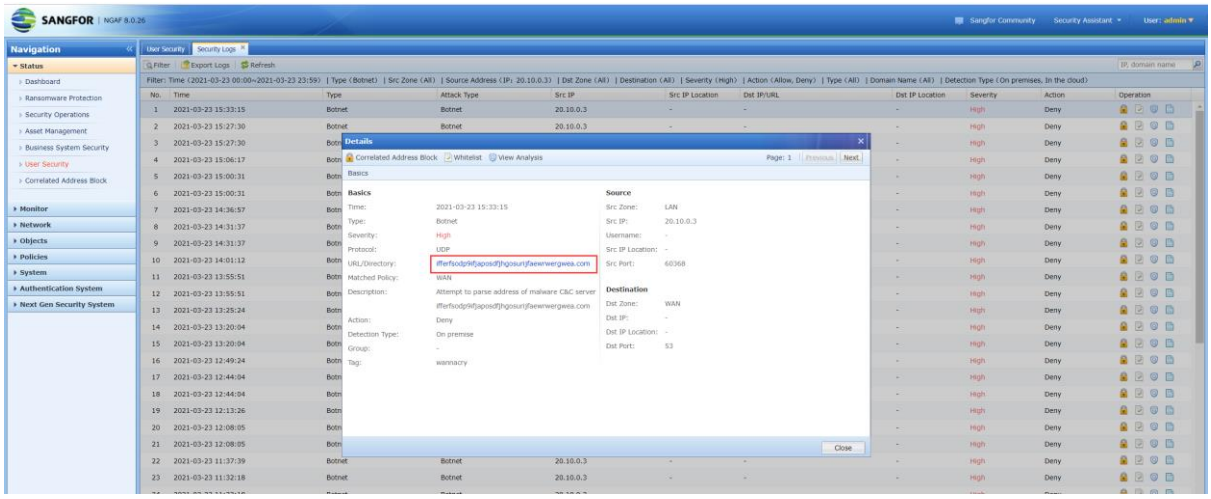
1. Check whether there's generate Secure Log.

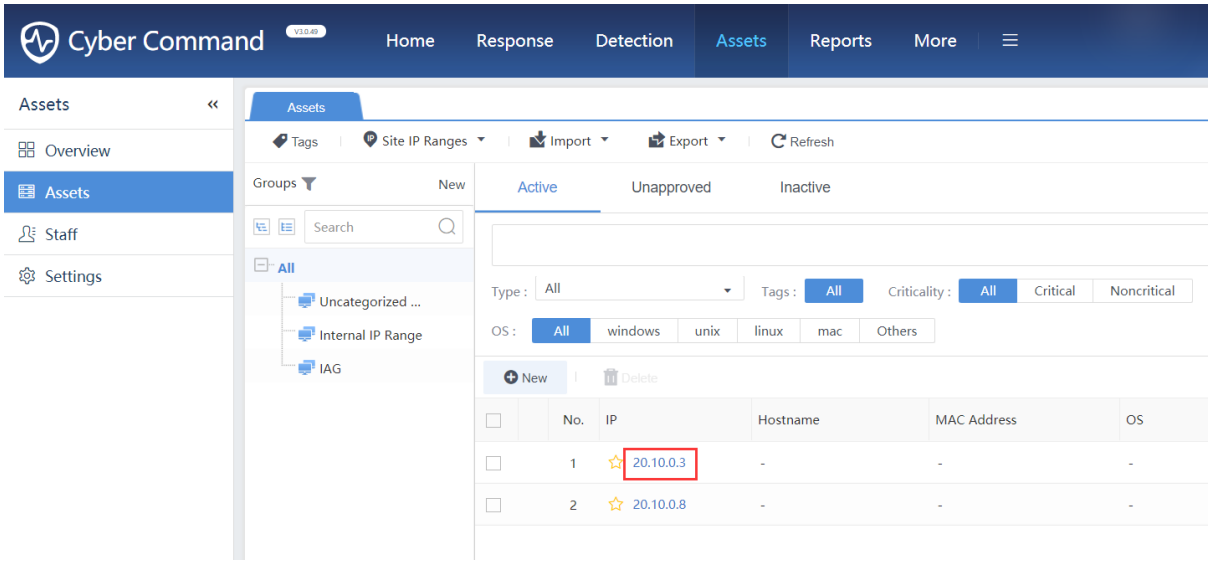


2.You can view the security log detail in NGAF



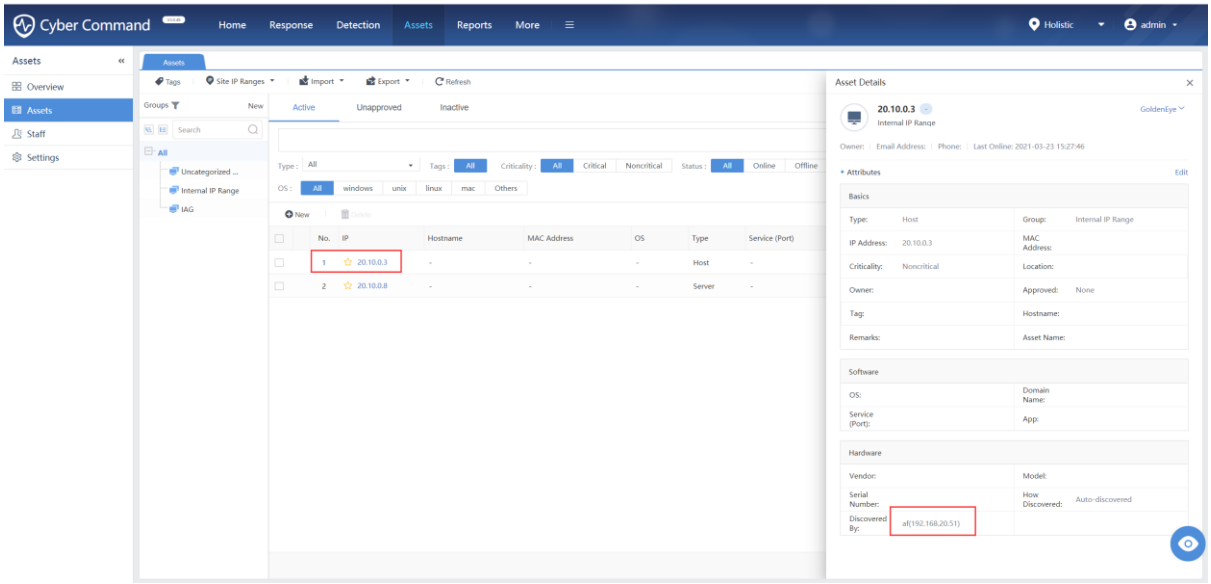
3. Confirm whether the URL is included in Botnet Tools.



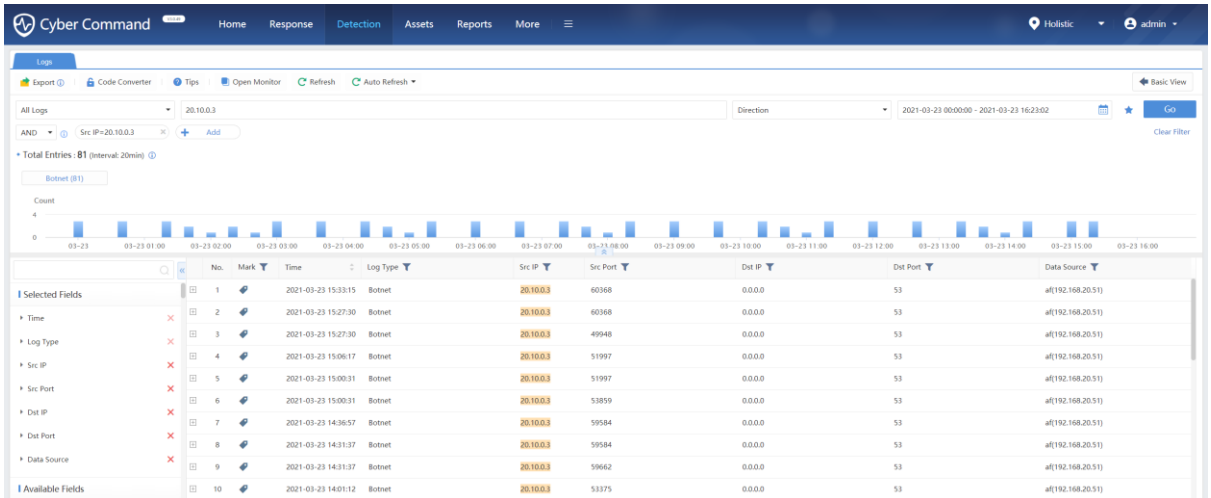


2.4.2 Check Security Log in Cyber Command

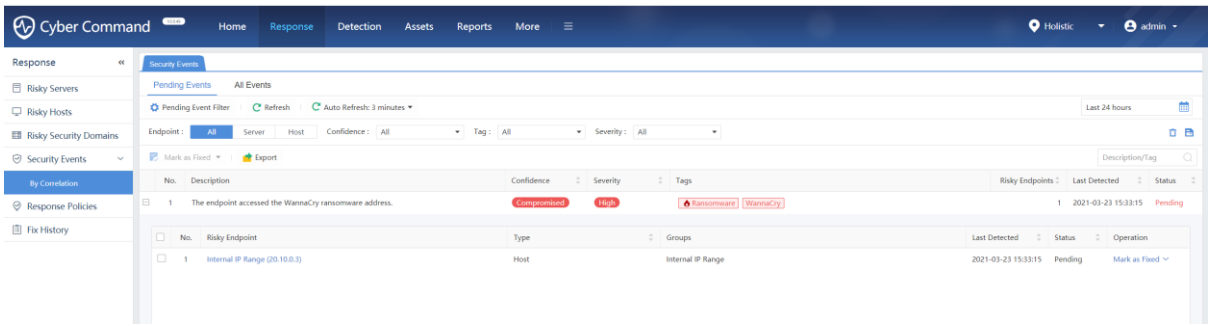
1. Ensure Cyber Command generates assets according to logs and traffic that NGAF synchronized. Otherwise, you need create asset manually in Cyber Command.



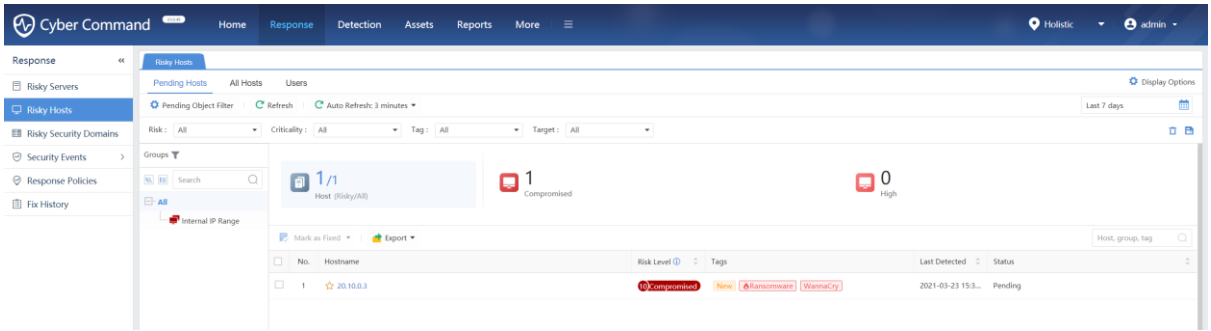
2.Go to Detection->Logs Path, filter the IP of your test PC, and check whether there exist related security logs.



3.Go to Response->Security Events->By Correlation path, then check whether Cyber Command generates Security Events.

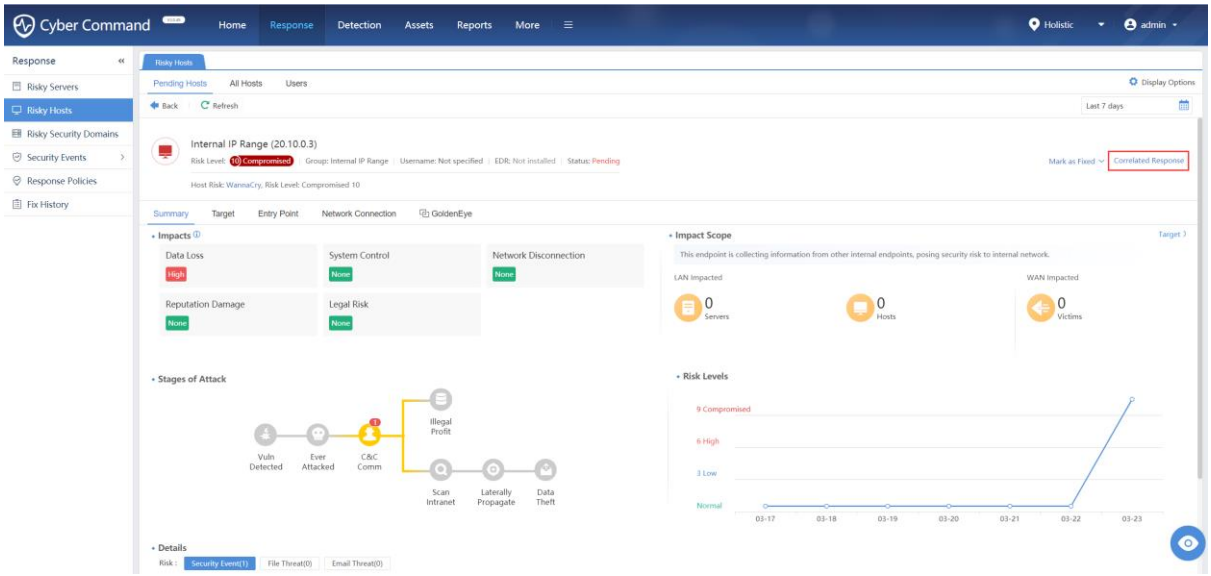


4.Go to Response->Risk Hosts, and check whether risk hosts is generated.

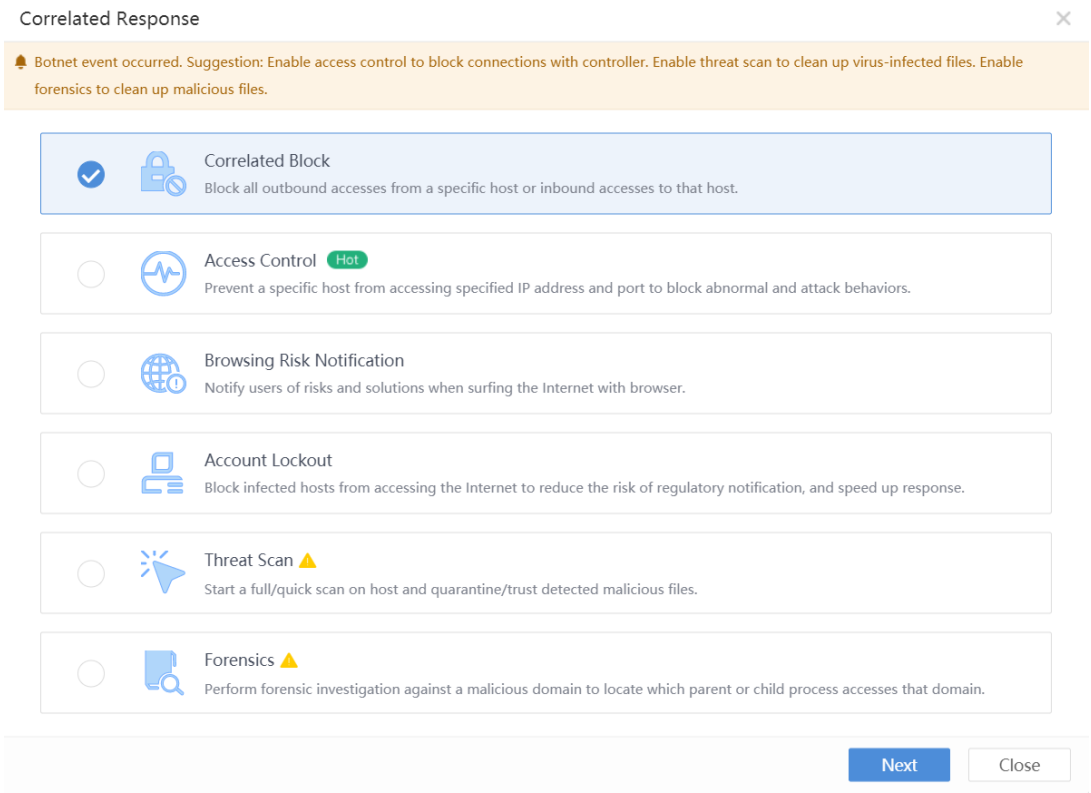


2.4.3 Correlated to Block Botnet Traffic

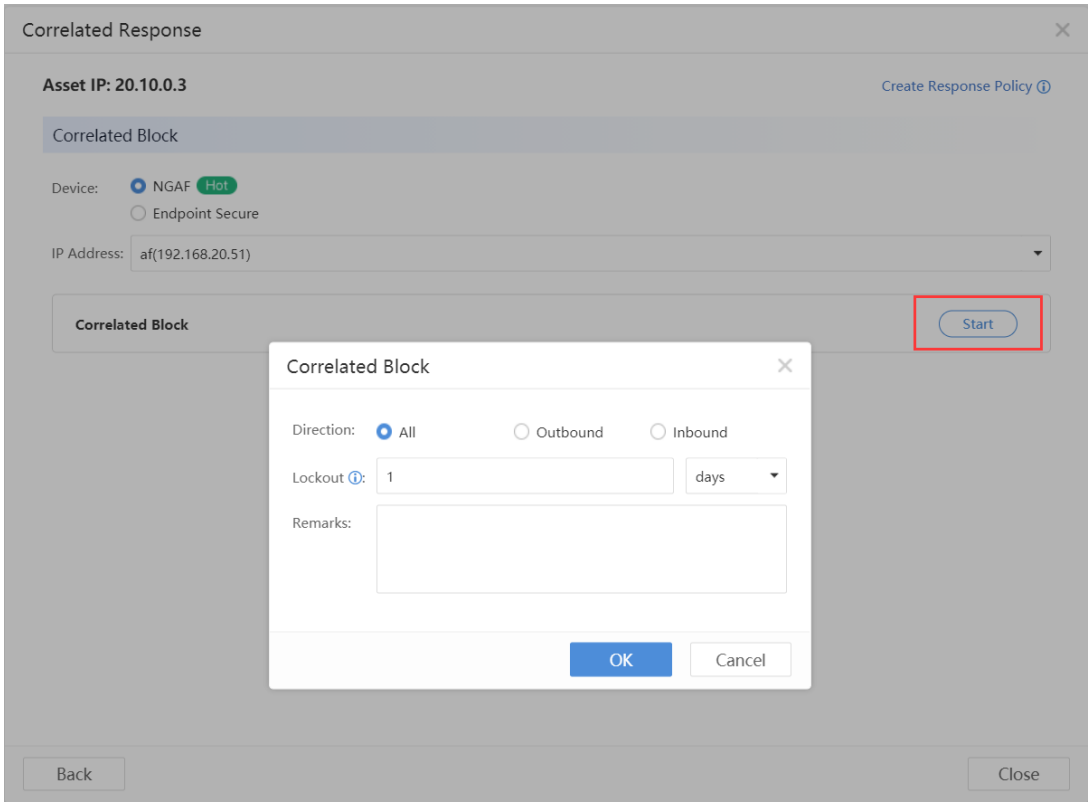
1. Click Correlated Response.



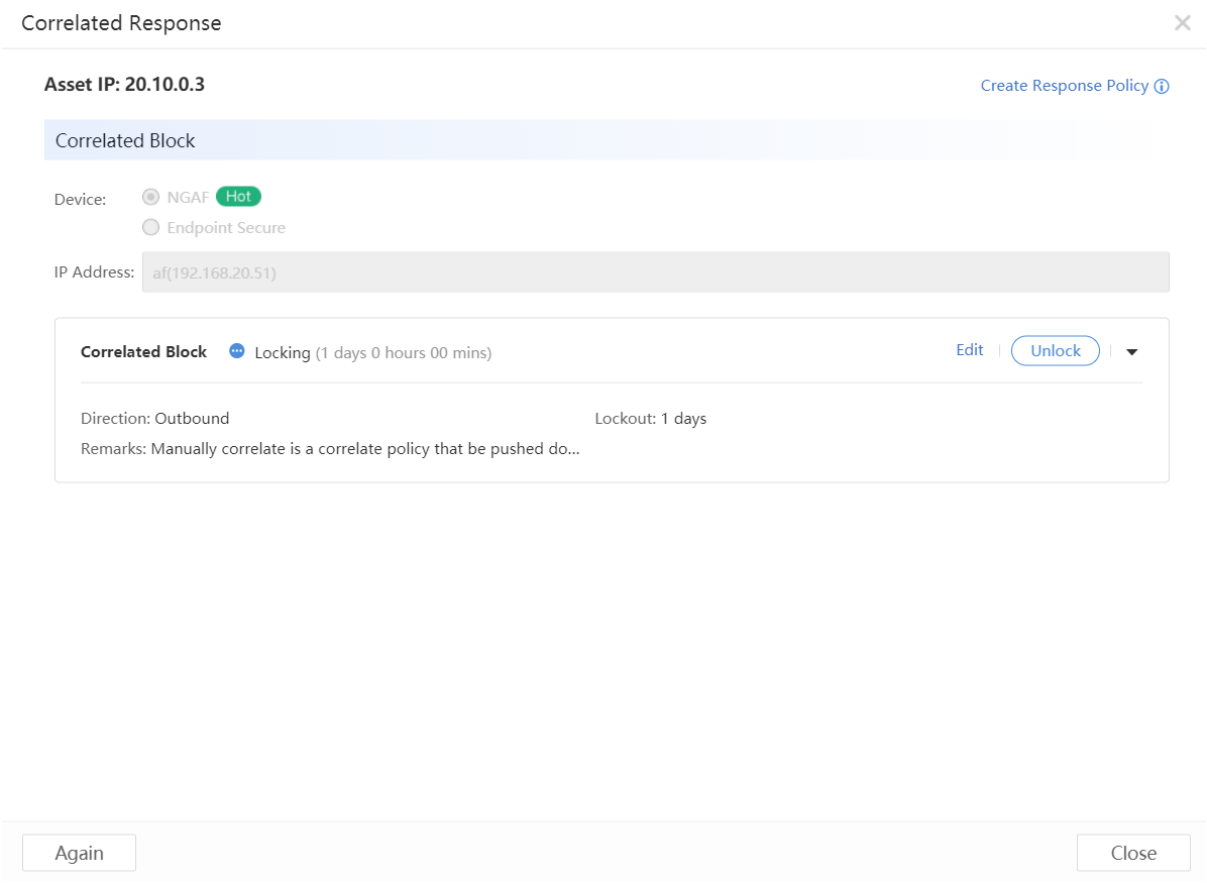
2. Select Correlated Response.



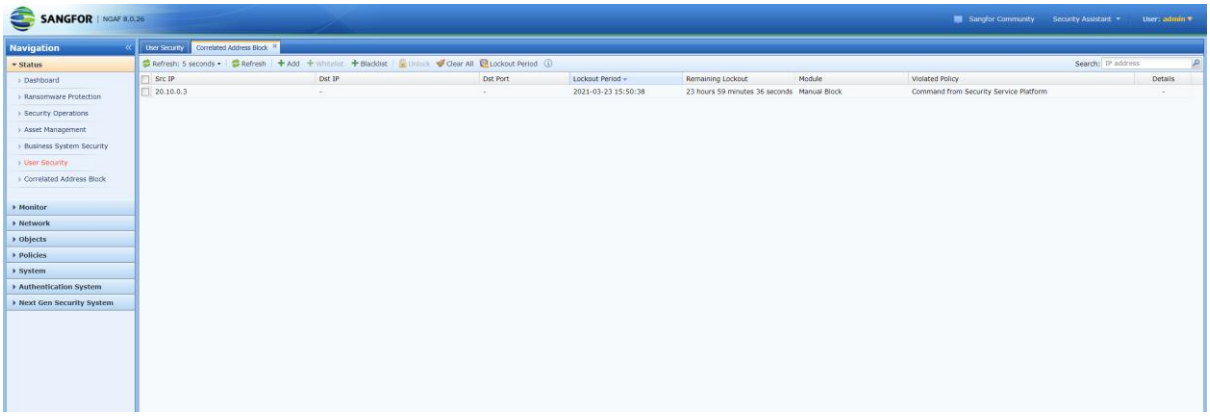
3. Click Start and set up lockout time, then click OK.



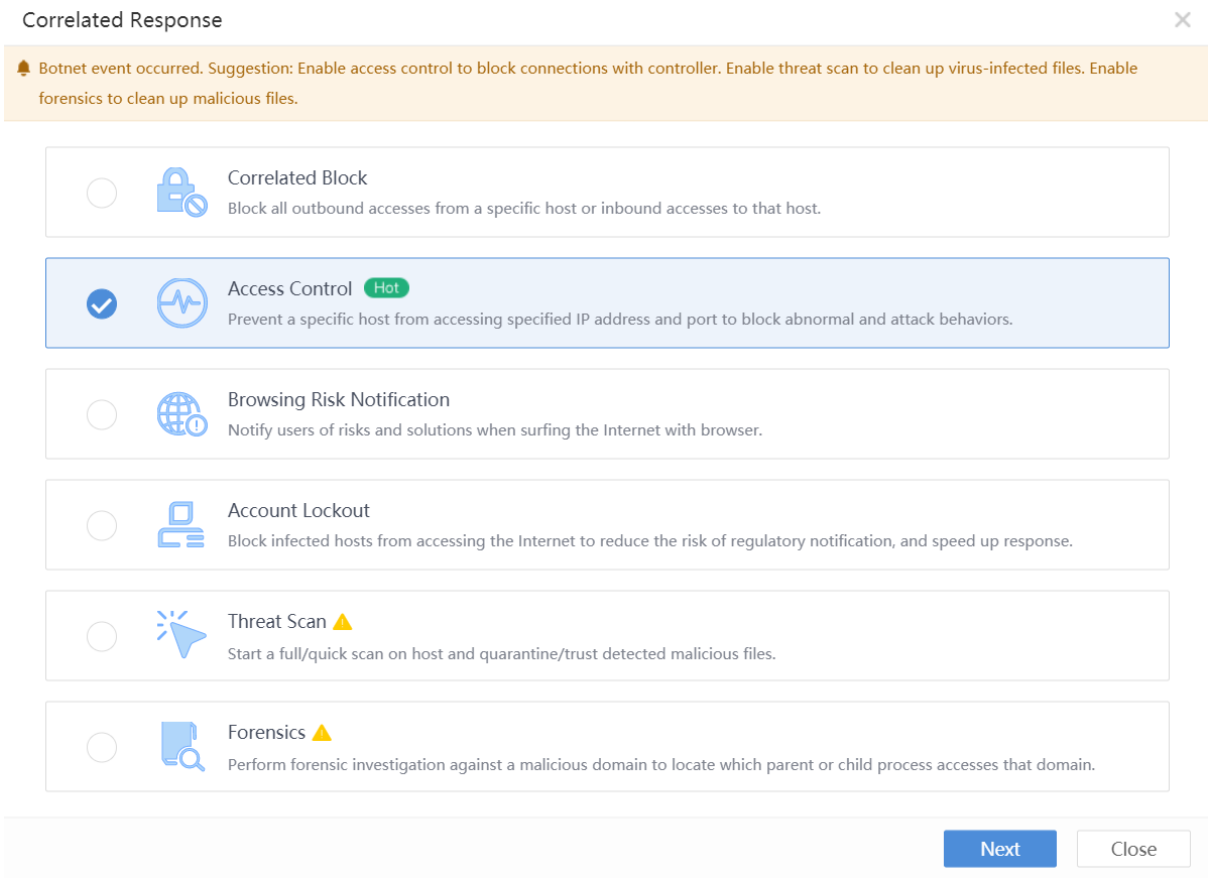
4. After a few seconds, you can see the policy issued successfully.



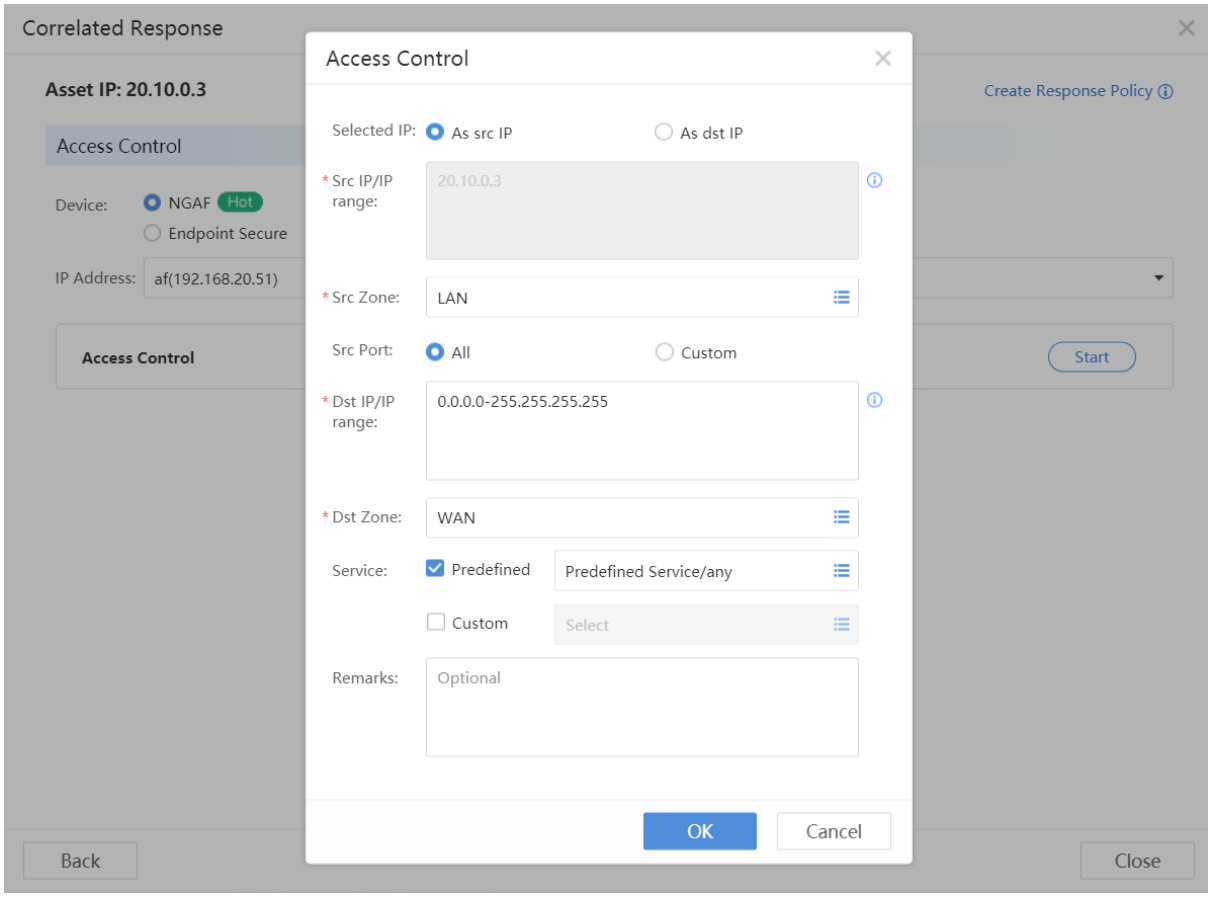
5.You can log in NGAF we console, and go to Status-> Correlated Address Block path, then you can check the IP that blocked by Cyber Command.



6. If you want to use access control policy to block botnet traffic, you can select Access Control.

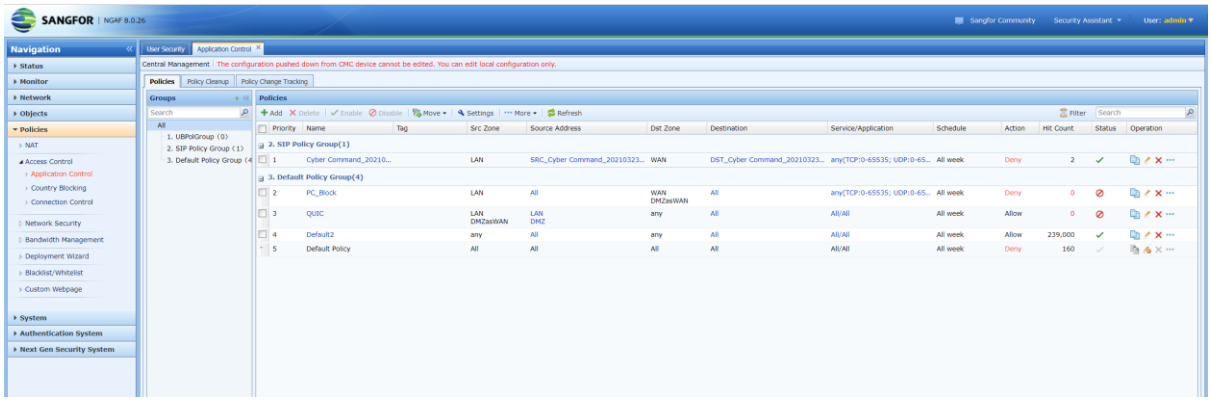


7.Click Start and configure the Zones and IP that you want to block.

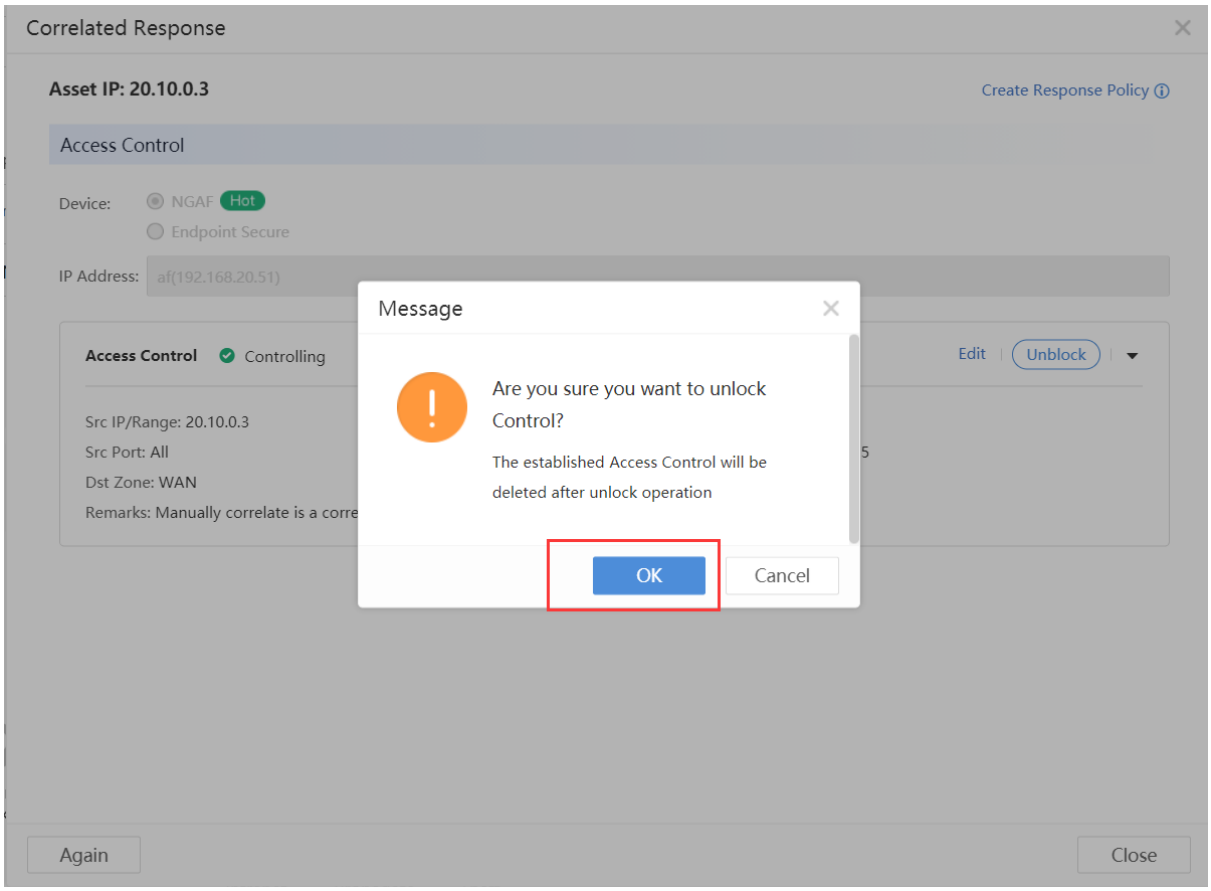


8. After a few seconds, you can log in NGAF web console, and you can find Access Control policy issued

successfully.



9.If you want to unblock the access control policy, you can click Unblock.



10. You can log in NGAF web console and check whether access control policy deleted by Cyber Command.