



**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

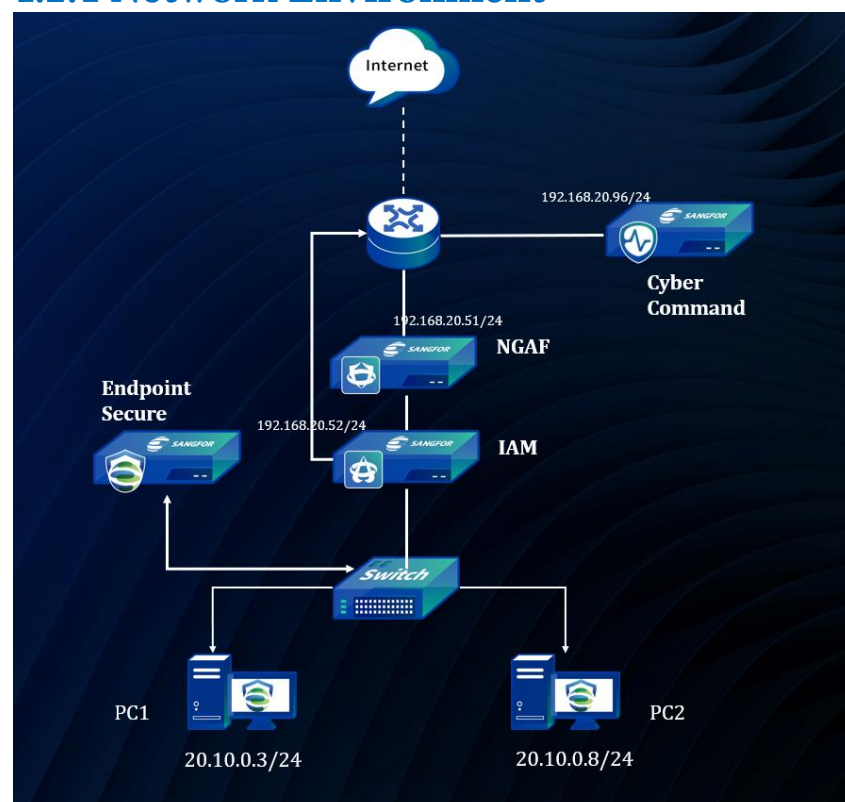
Chapter 1 Scenario .....	1
1.1 Scenario .....	1
1.2 Environment .....	1
1.2.1 Network Environment .....	1
1.3 Test Introduce.....	1
Chapter 2 Configuration.....	1
2.1 Configure NGAF .....	1
2.2 Configure Cyber Command .....	5
2.3 Run Botnet Program.....	6
2.4 Check Logs and Correlated to Block.....	7
2.4.1 Check Security Logs in NGAF .....	7
2.4.2 Check Security Log in Cyber Command .....	8
2.4.3 Correlated to Block Botnet Traffic.....	9

# 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.

## How to Correlate with NGAF to Simply the Operation

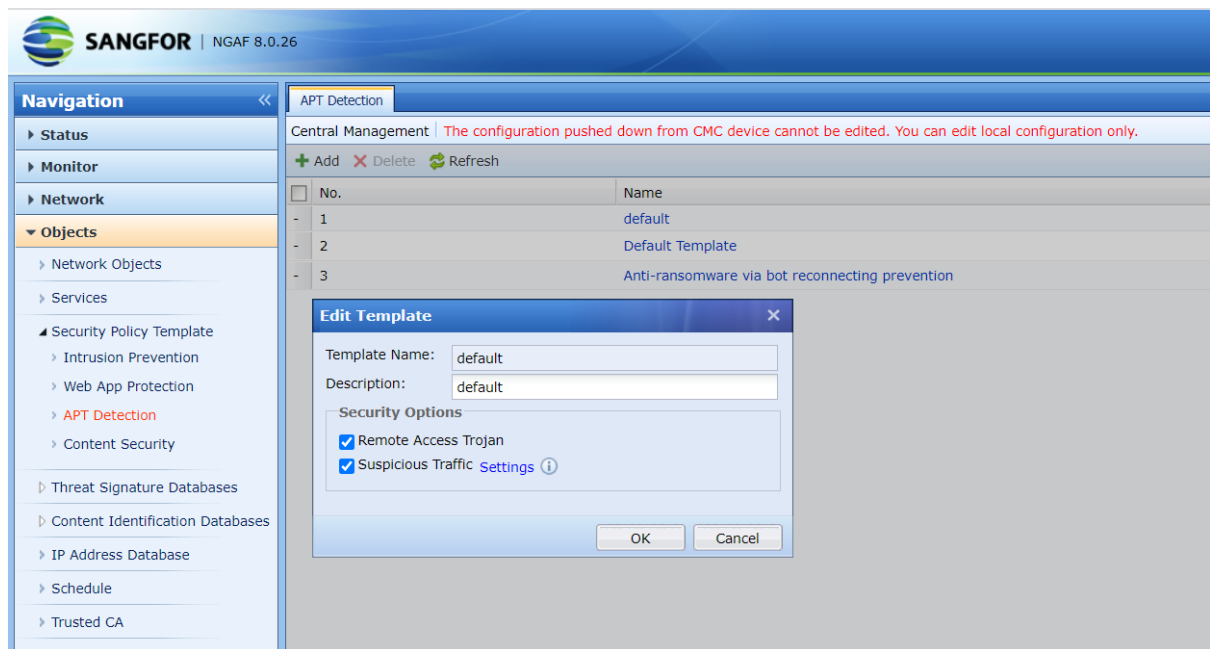
The screenshot shows the 'Logging Options' configuration page in the Sangfor NGAF 8.0.26 web interface. The left sidebar contains a 'Navigation' menu with categories like Status, Monitor, Network, Objects, Policies, System, Authentication System, and Next Gen Security System. The 'Monitor' category is expanded, showing 'Logs', 'Session', 'Statistics', 'System Status', 'Report', and 'Logging and Alarm Options'. Under 'Logging and Alarm Options', 'Logging Options' is selected. The main content area is titled 'Logging Options' and includes a message: 'Central Management: The page can be configured.' Below this, there are four sections for enabling logs: 'Security Logs', 'Application Control Logs', 'Traffic Audit Logs', and 'NAT Logs'. Each section has 'Enable' and 'Disable' buttons. Under 'Security Logs', 'Log Location' options are listed: 'Syslog' (unchecked), 'Local (Recommended)' (checked), and 'Cyber Command' (checked). Similar options are present for the other log types. Below these sections is the 'Local Logs' section, which includes 'Log Preservation/Deletion' settings (Auto-delete logs cached for 180 days), 'Merge Logs of Same Type' (checked), and 'Maximum Exported Entries' (1000). At the bottom is the 'Cyber Command and NTA Settings' section, which includes fields for 'Address' (192.168.20.96), 'Communication Port' (4430), 'Data Sync Account' (sangfor), and 'Password' (masked with dots). A 'Test' button is next to the 'Address' field, and a 'Save' button is at the bottom.

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

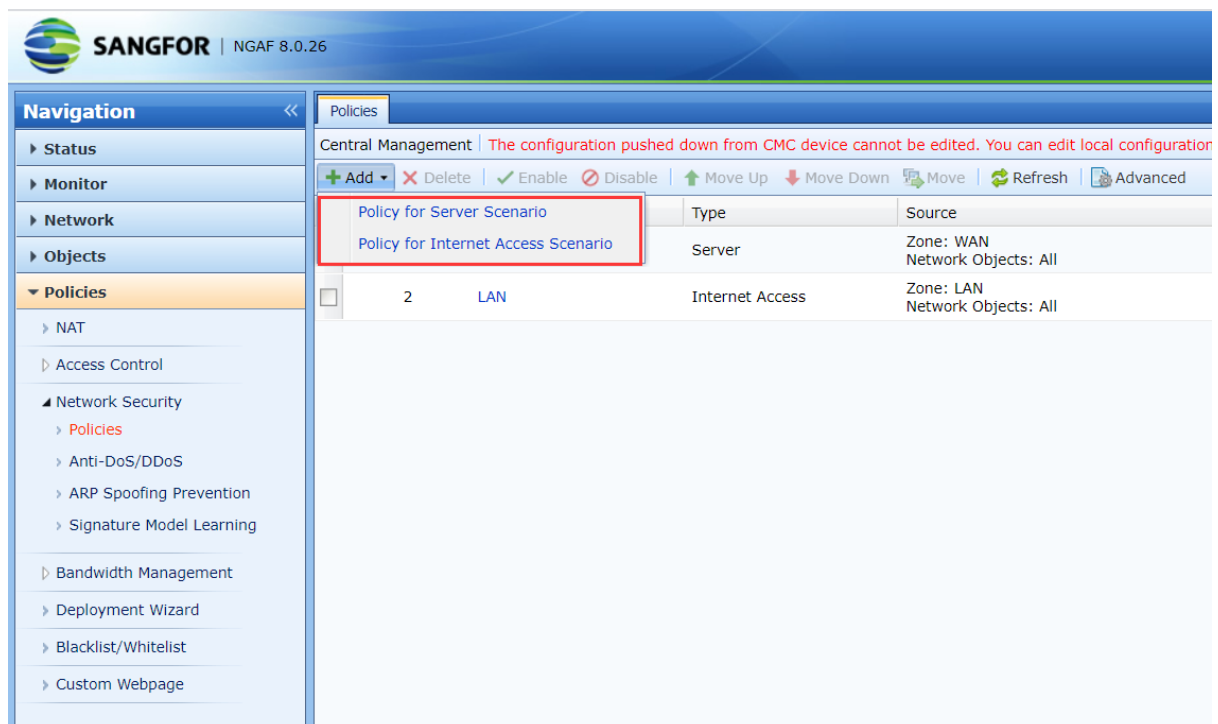
The screenshot shows the 'APT Detection' configuration page in the Sangfor NGAF 8.0.26 web interface. The left sidebar is the same as in the previous screenshot, but 'Security Policy Template' is expanded, and 'APT Detection' is selected. The main content area is titled 'APT Detection' and includes a message: 'Central Management: The configuration pushed down from CMC device cannot be edited. You can edit local configuration only.' Below this, there are 'Add', 'Delete', and 'Refresh' buttons. A table lists the APT Detection templates:

No.	Name	Protection
1	default	Remote Access Trojan, Suspicious Traffic
2	Default Template	Remote Access Trojan
3	Anti-ransomware via bot reconnecting prevention	Remote Access Trojan

## How to Correlate with NGAF to Simply the Operation



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**

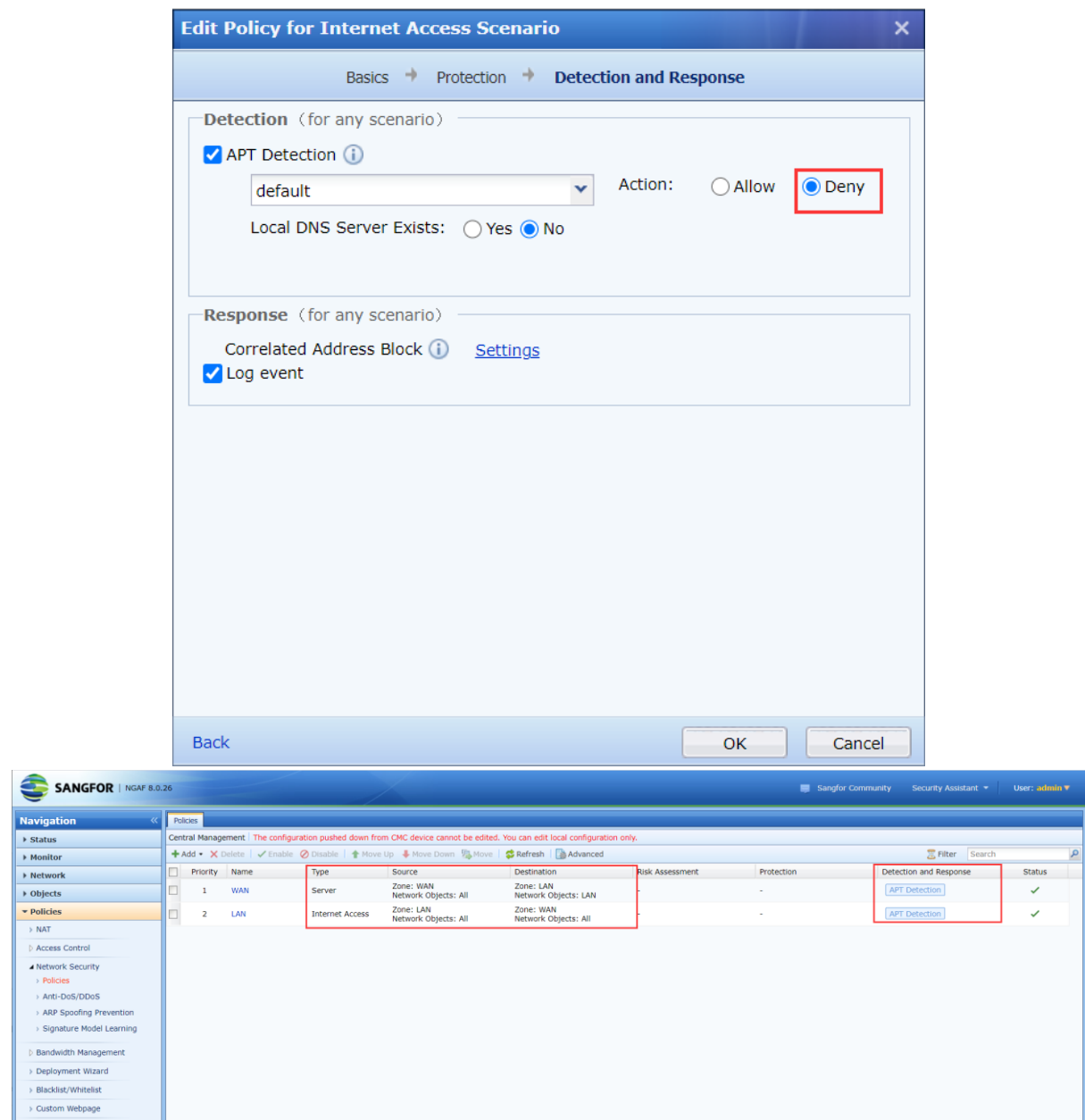
Basics → **Protection** → Detection and Response

**Basics Protection** (for any scenario)

☐ Intrusion Prevention ⓘ  
Default Template\_Internet Access Scenario Action: ☐ Allow ☒ Deny

☐ Content Security (Sangfor Engine Zero file verification) ⓘ  
Default Template Action: ☐ Allow ☒ Deny

Back Next Cancel

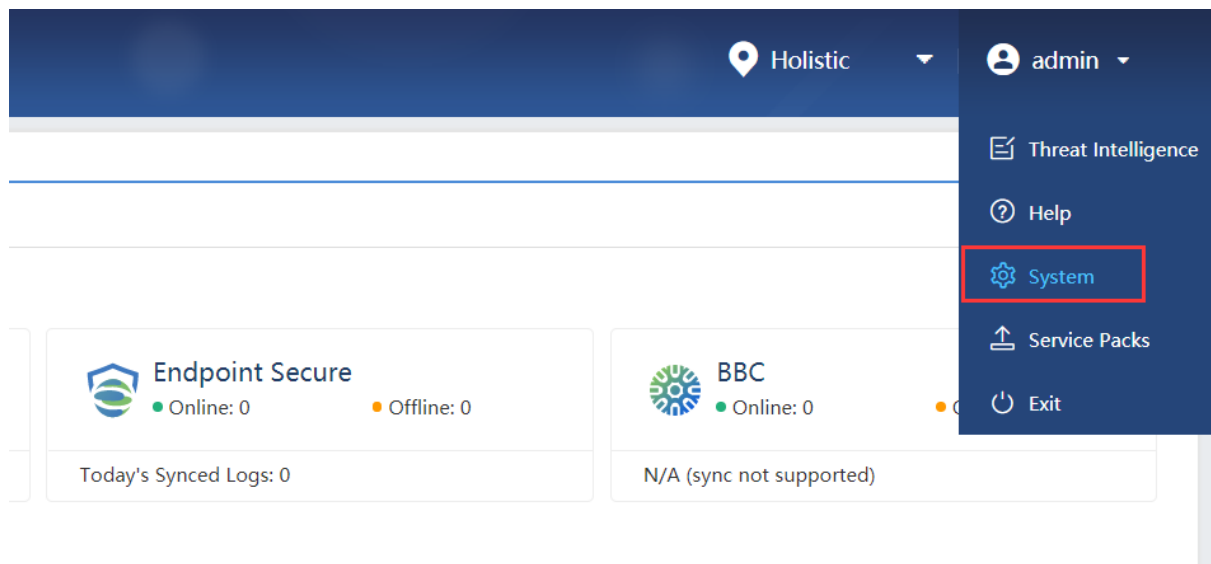


## 2.2 Configure Cyber Command

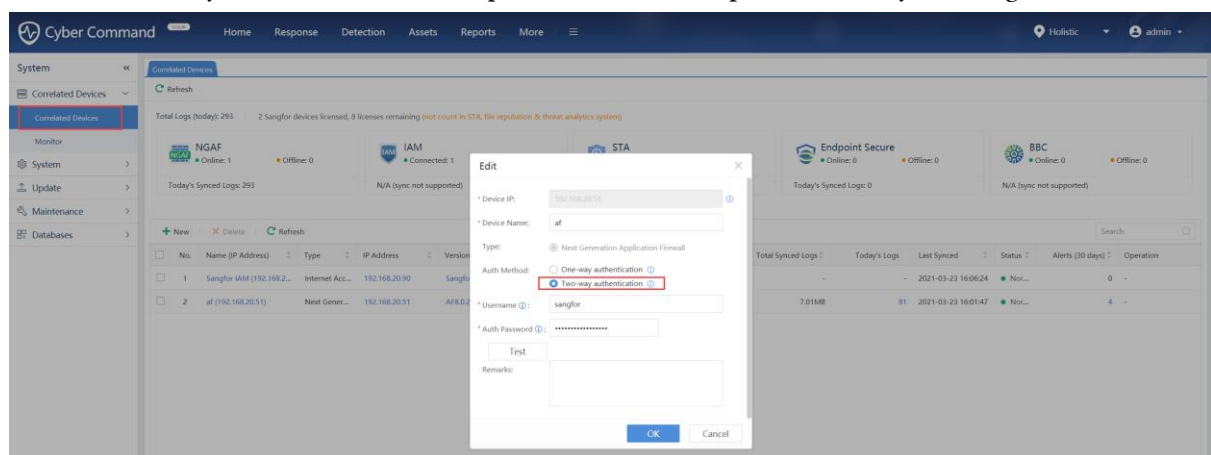
1. Go to System path.



## How to Correlate with NGAF to Simply the Operation

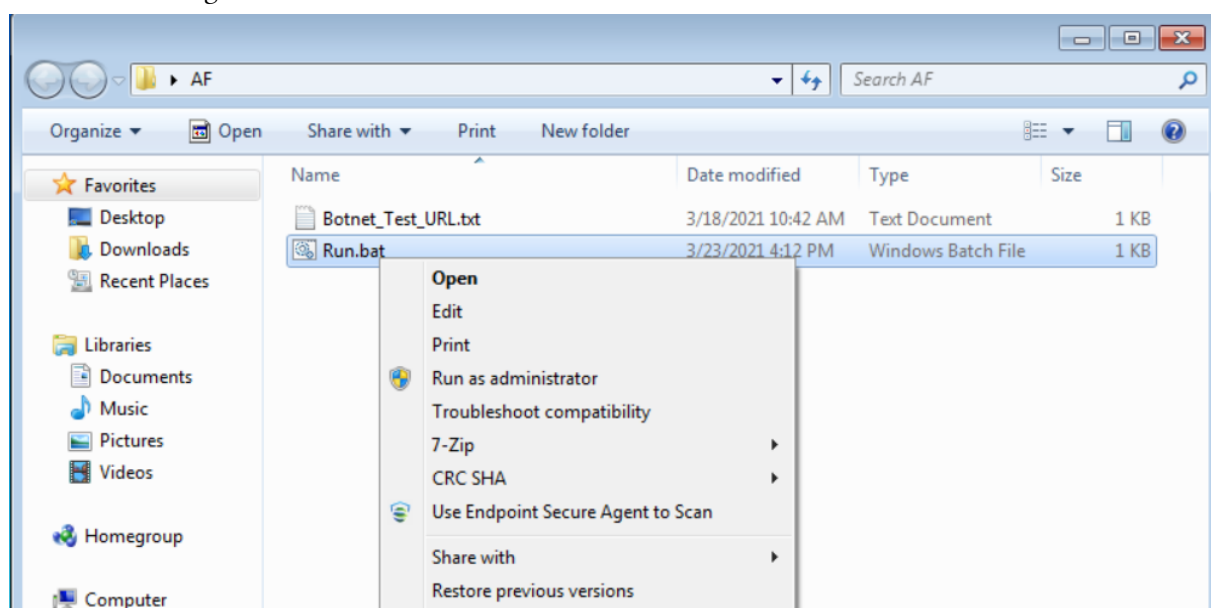


2. Enable Two-way authentication, then input the account and password that you configured in NGAF.



## 2.3 Run Botnet Program

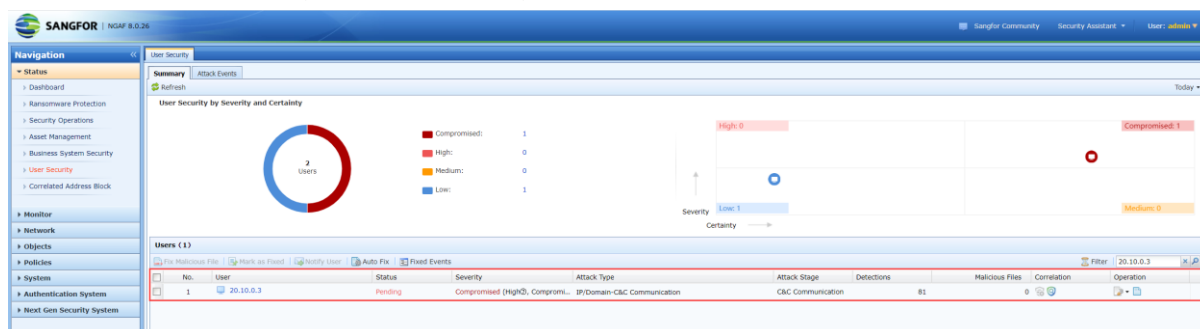
1. Run Botnet Program PC.



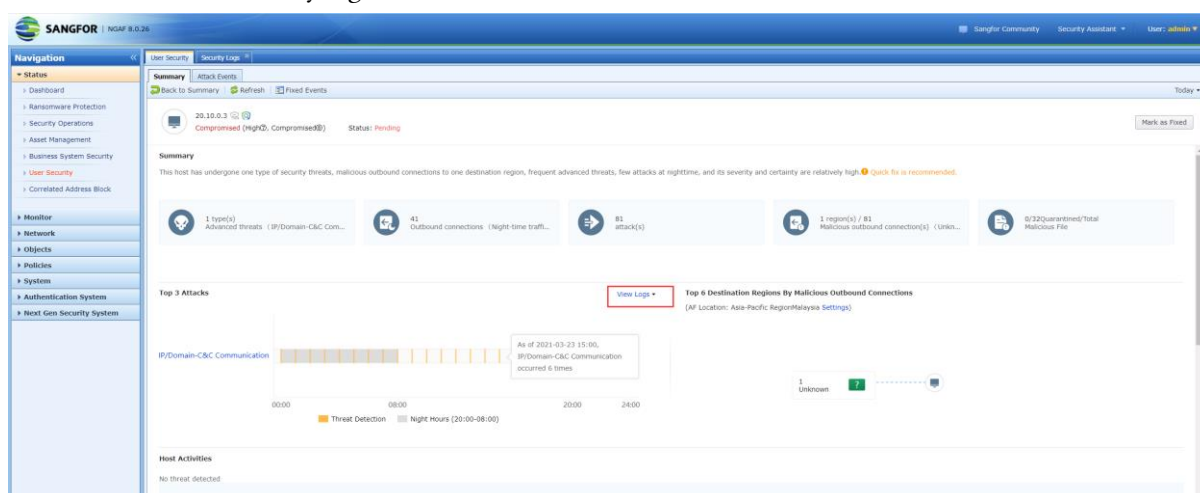
## 2.4 Check Logs and Correlated to Block

### 2.4.1 Check Security Logs in NGAF

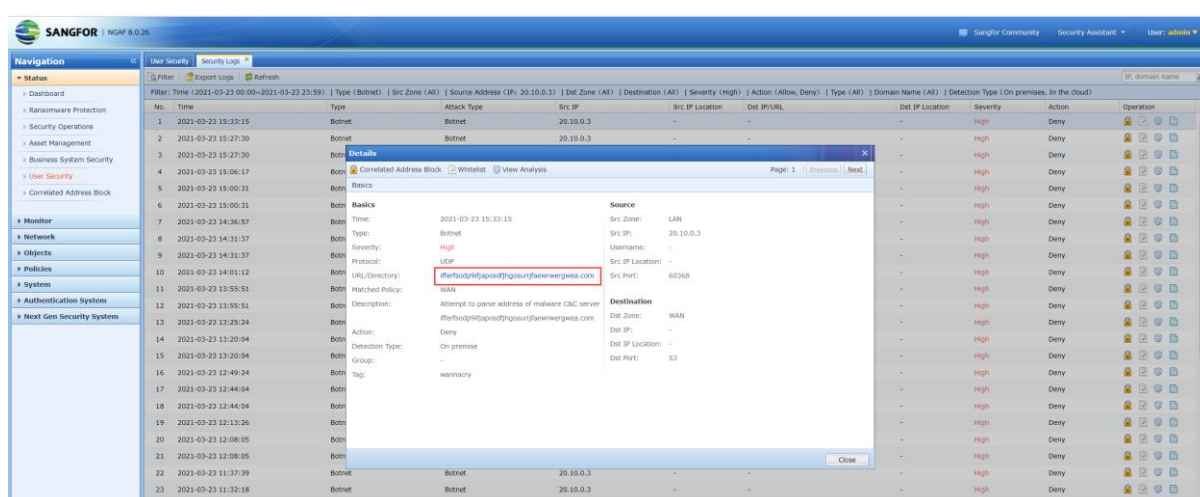
1. Check whether there's generate Secure Log.



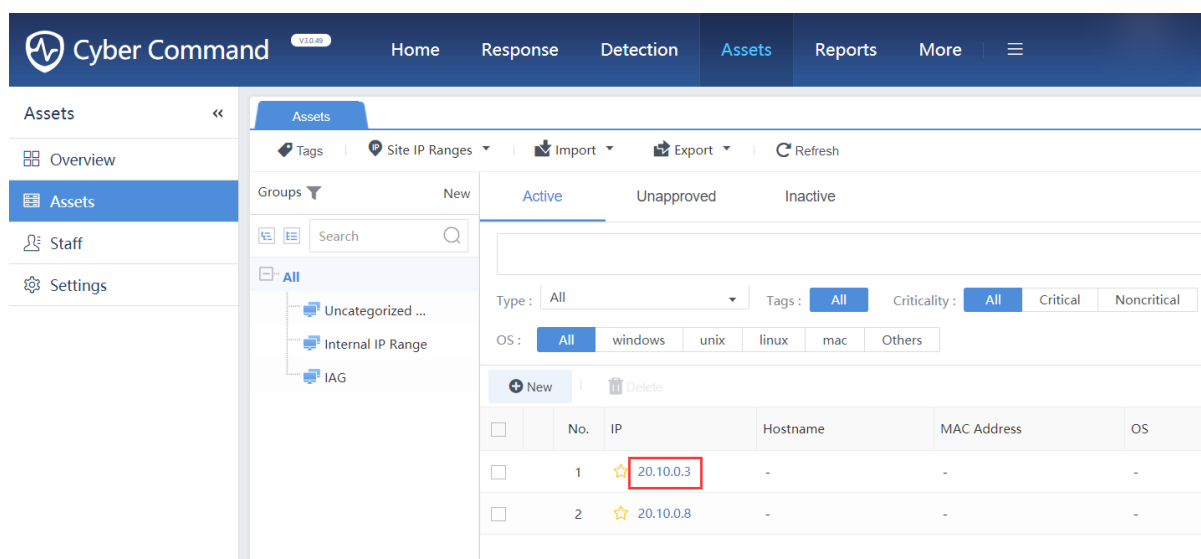
2. You can view the security log detail in NGAF



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

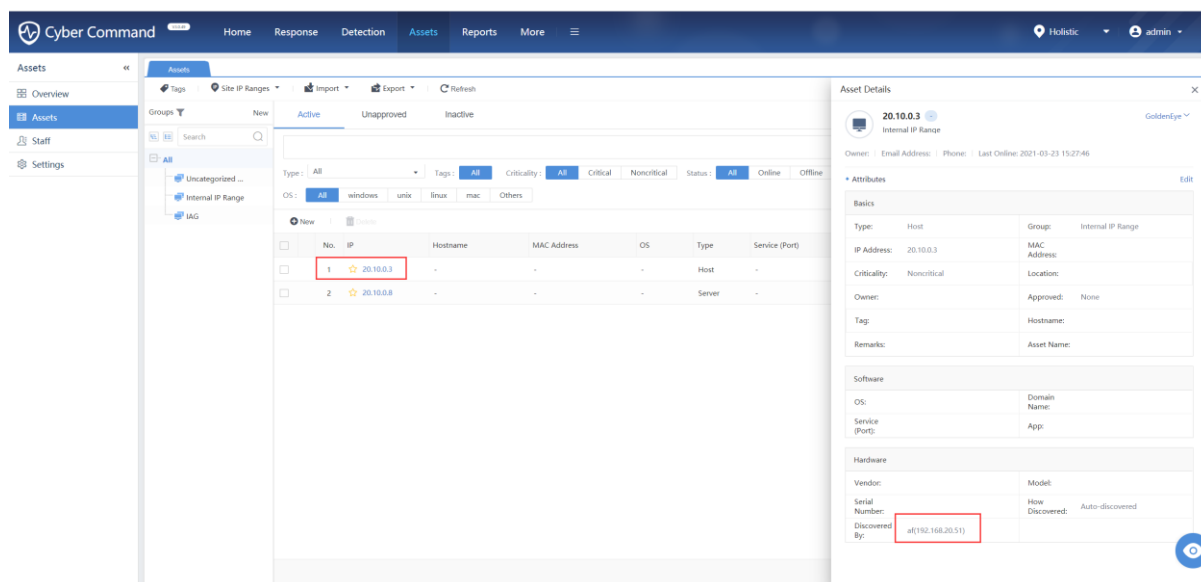


## How to Correlate with NGAF to Simply the Operation

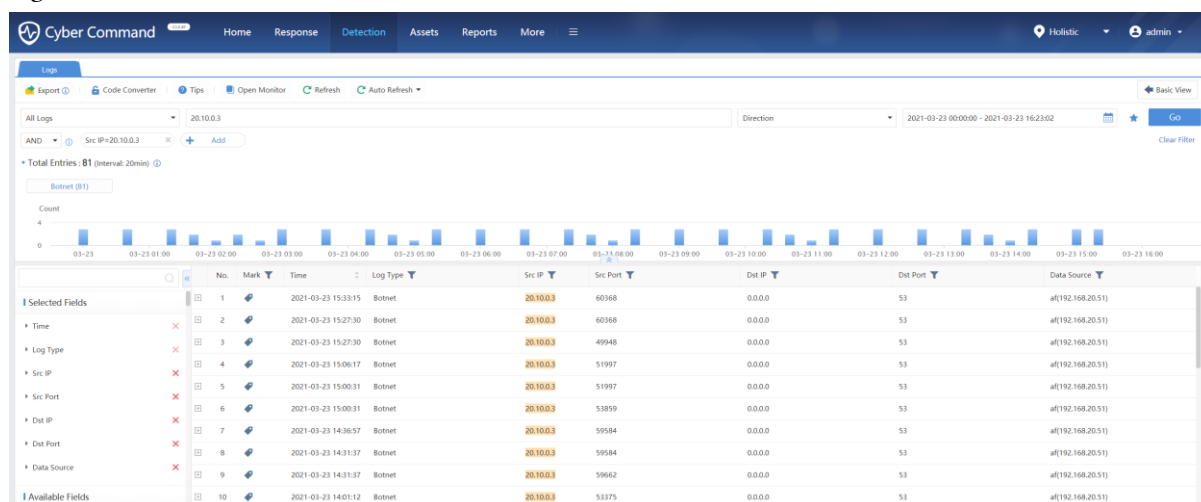


### 2.4.2 Check Security Log in Cyber Command

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

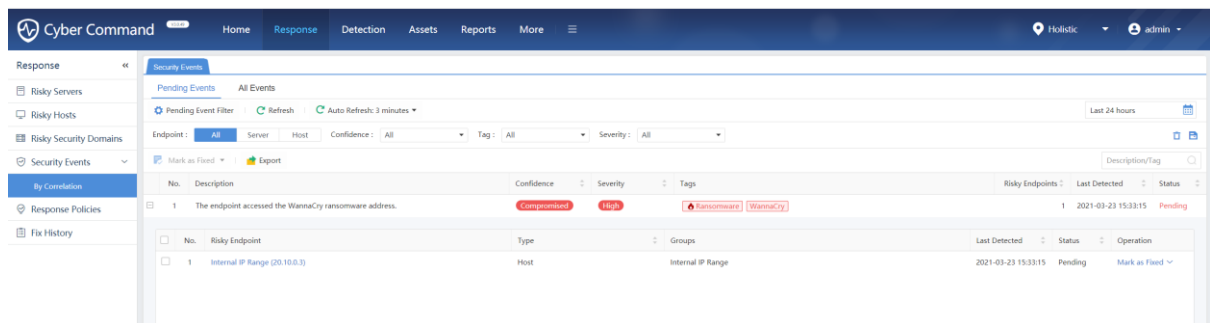


2. Go to Detection->Logs Path, filter the IP of your test PC, and check whether there exist related security logs.

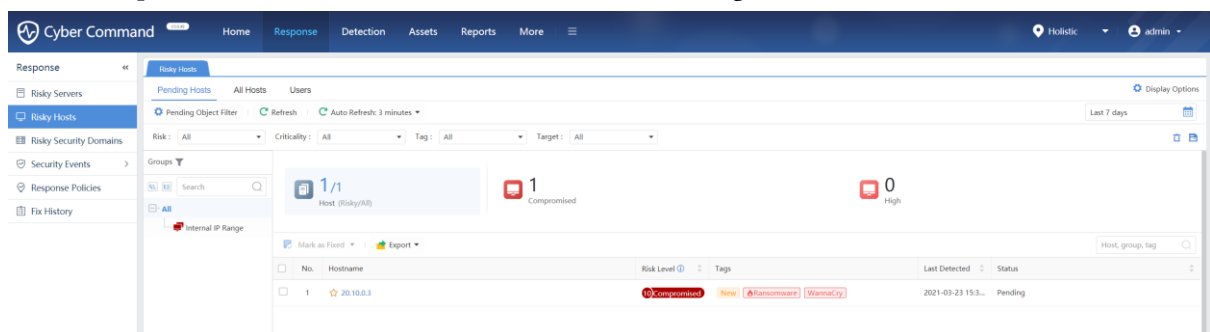


## How to Correlate with NGAF to Simply the Operation

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

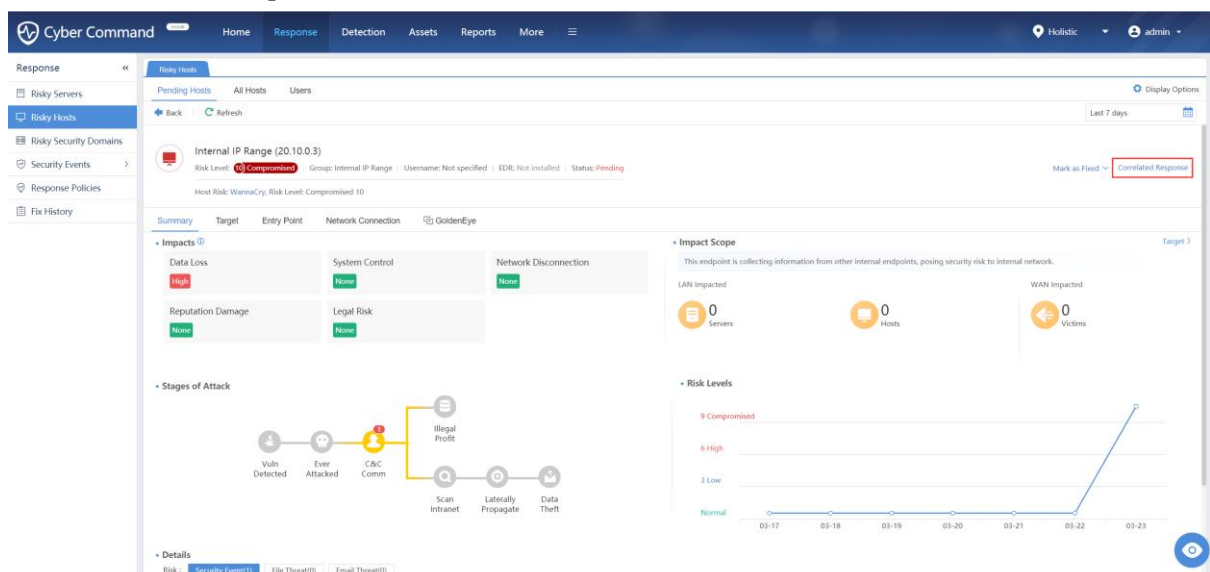


4.Go to Response->Risk Hosts, and check whether risk hosts is generated.



## 2.4.3 Correlated to Block Botnet Traffic

1. Click Correlated Response.




2. Select Correlated Response.

## How to Correlate with NGAF to Simply the Operation

Correlated Response


Botnet event occurred. Suggestion: Enable access control to block connections with controller. Enable threat scan to clean up virus-infected files. Enable forensics to clean up malicious files.

☒




**Correlated Block**  
Block all outbound accesses from a specific host or inbound accesses to that host.

☐




**Access Control** Hot  
Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.

☐




**Browsing Risk Notification**  
Notify users of risks and solutions when surfing the Internet with browser.

☐




**Account Lockout**  
Block infected hosts from accessing the Internet to reduce the risk of regulatory notification, and speed up response.

☐



**Threat Scan** ▲  
Start a full/quick scan on host and quarantine/trust detected malicious files.

☐



**Forensics** ▲  
Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.

Next

Close

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

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

**Correlated Block**

Device: ☒ NGAF Hot ☐ Endpoint Secure

IP Address: af(192.168.20.51)

**Correlated Block**

Start

Correlated Block

Direction: ☒ All ☐ Outbound ☐ Inbound

Lockout ⓘ: 1 days

Remarks:

OK

Cancel

Back

Close

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

## How to Correlate with NGAF to Simply the Operation

Correlated Response

Asset IP: 20.10.0.3

Create Response Policy ⓘ

Correlated Block

Device: ☒ NGAF Hot  
☐ Endpoint Secure

IP Address: af(192.168.20.51)

Correlated Block 🔒 Locking (1 days 0 hours 00 mins)

Edit Unlock

Direction: Outbound

Lockout: 1 days

Remarks: Manually correlate is a correlate policy that be pushed do...

Again

Close

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.

Src IP	Dst IP	Dst Port	Lockout Period	Remaining Lockout	Module	Violated Policy	Details
20.10.0.3	-	-	2023-03-23 15:50:38	23 hours 59 minutes 36 seconds	Manual Block	Command from Security Service Platform	-


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

## How to Correlate with NGAF to Simply the Operation

Correlated Response


Botnet event occurred. Suggestion: Enable access control to block connections with controller. Enable threat scan to clean up virus-infected files. Enable forensics to clean up malicious files.

☐




Correlated Block  
Block all outbound accesses from a specific host or inbound accesses to that host.

☒




Access Control Hot  
Prevent a specific host from accessing specified IP address and port to block abnormal and attack behaviors.

☐




Browsing Risk Notification  
Notify users of risks and solutions when surfing the Internet with browser.

☐




Account Lockout  
Block infected hosts from accessing the Internet to reduce the risk of regulatory notification, and speed up response.

☐



Threat Scan ▲  
Start a full/quick scan on host and quarantine/trust detected malicious files.

☐



Forensics ▲  
Perform forensic investigation against a malicious domain to locate which parent or child process accesses that domain.

Next

Close

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

Correlated Response

Asset IP: 20.10.0.3

Access Control

Device: ☒ NGAF Hot  
☐ Endpoint Secure

IP Address: af(192.168.20.51)

Access Control

Back

Start

Close

Access Control

Selected IP: ☒ As src IP ☐ As dst IP

\* Src IP/IP range: 20.10.0.3

\* Src Zone: LAN

Src Port: ☒ All ☐ Custom

\* Dst IP/IP range: 0.0.0-255.255.255.255

\* Dst Zone: WAN

Service: ☒ Predefined ☐ Custom  
Predefined Service/any  
Select

Remarks: Optional

OK

Cancel

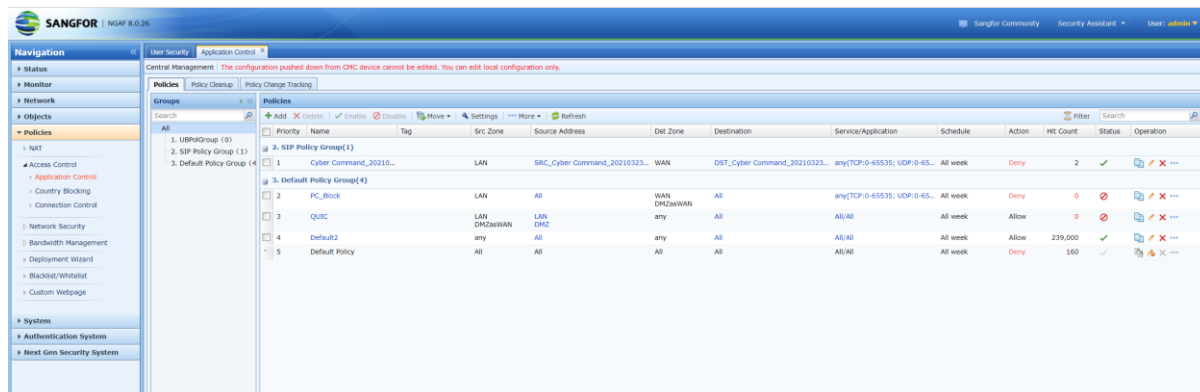
8. After a few seconds, you can log in NGAF web console, and you can find Access Control policy issued

W.: [www.sangfor.com](http://www.sangfor.com) | W.: [community.sangfor.com](http://community.sangfor.com) | E.: [tech.support@sangfor.com](mailto:tech.support@sangfor.com)

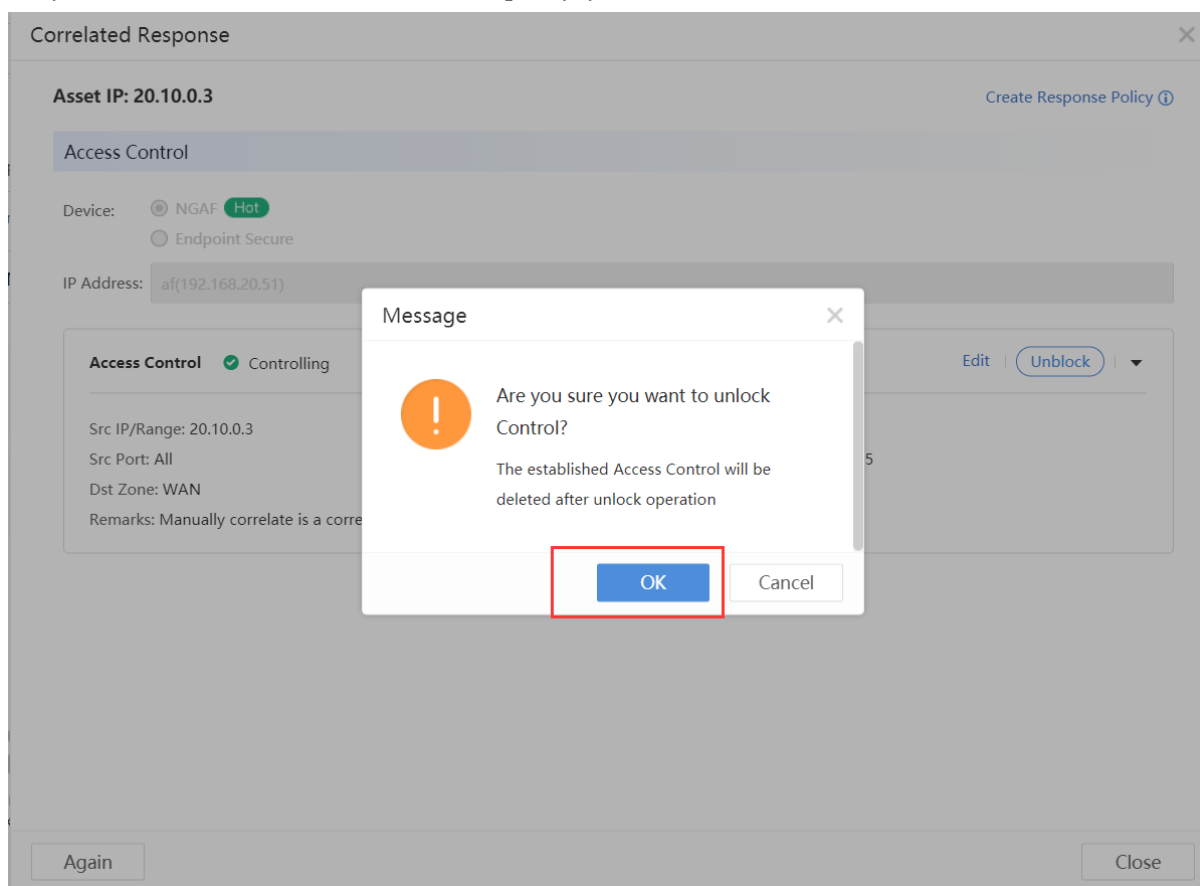
12

## How to Correlate with NGAF to Simply the Operation

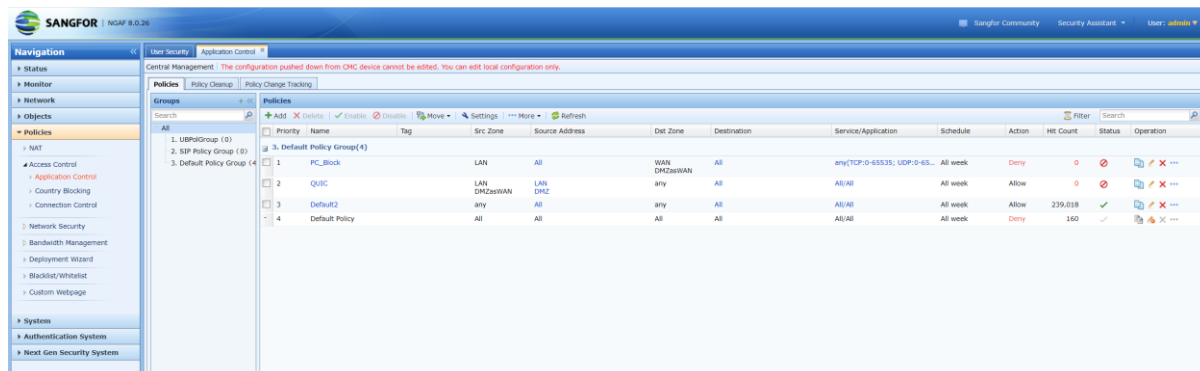
successfully.



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.







**SANGFOR**

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