



**SANGFOR**



# Cyber Command

**Praktik Terbaik untuk Skenario\_Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana**

**Versi 3.0.49**



## Catatan Perubahan

Tanggal	Deskripsi Perubahan
Maret 19, 2021	Rilis Dokumen.
Mei 17, 2021	Dokumen update.

# Daftar Isi

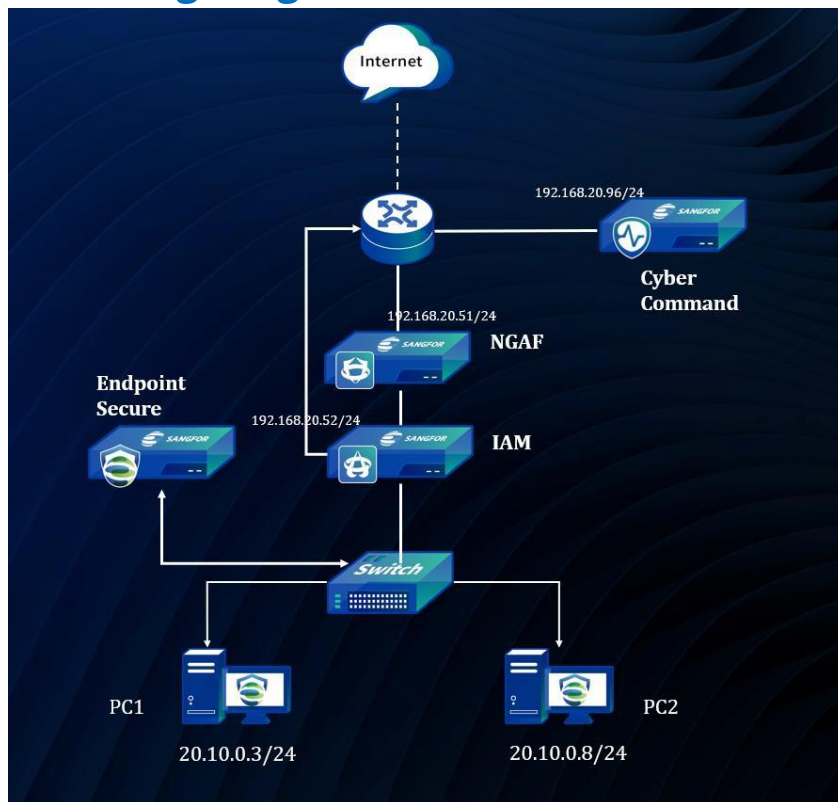
Bab 1 Skenario .....	1
1.1 Skenario.....	1
1.2 Lingkungan .....	1
1.2.1 Lingkungan Network.....	1
1.3 Tes Perkenalan.....	1
Bab 2 Konfigurasi .....	1
2.1 Konfigurasi NGAF.....	1
2.2 Konfigurasi Cyber Command .....	5
2.3 Run Botnet Program .....	6
2.4 Periksa log dan Korelasi ke Block .....	7
2.4.1 Periksa Security Logs di NGAF .....	7
2.4.2 Periksa Security Log di Cyber Command.....	8
2.4.3 Berkorelasi ke Block Botnet Traffic .....	9

## Bab 1 Skenario

### 1.1 Skenario

### 1.2 Lingkungan

#### 1.2.1 Lingkungan Network



### 1.3 Tes Perkenalan

1. Hanya perlu menganalisa traffic Botnet URL domain name untuk melewati NGAF, dan itu tidak perlu mengunjungi URL ini.

## Bab 2 Konfigurasi

### 2.1 Konfigurasi NGAF

1. Pergi ke Monitor->Logging dan Alarm Options-> Logging Options Path, konfigurasi correlation options, seperti IP dari Cyber Command, Anda dapat mengatur akun dan password, itu akan digunakan di Cyber Command.

## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

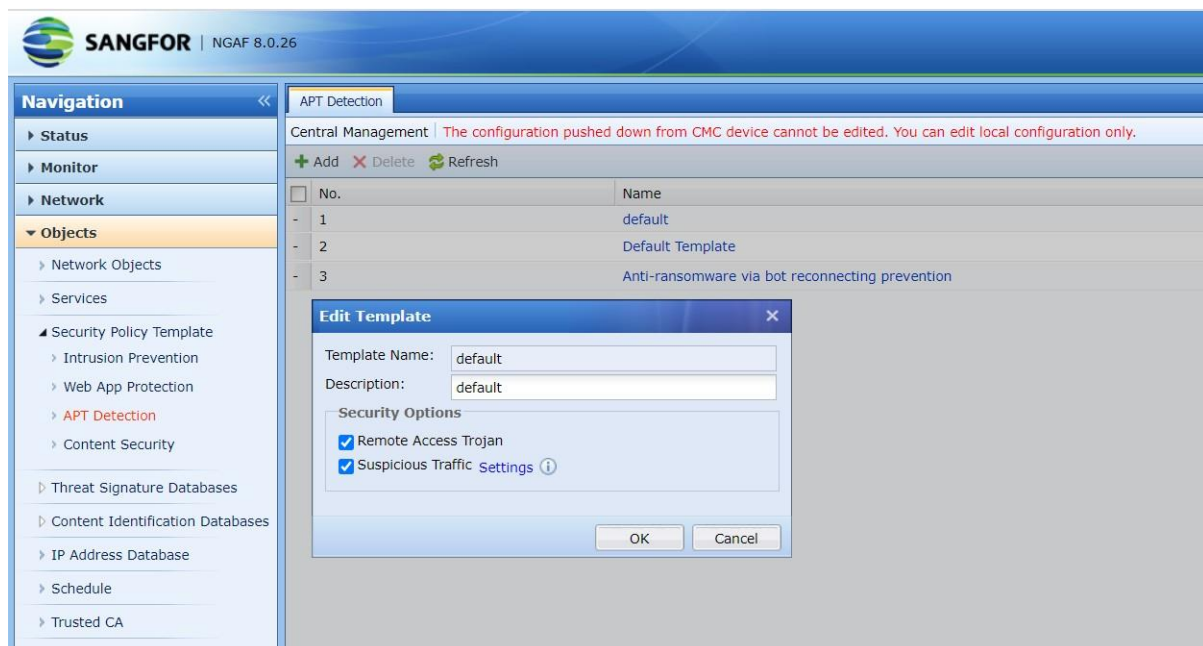
The screenshot shows the 'Logging Options' configuration page in the Sangfor NGAF 8.0.26 web interface. The left sidebar contains a 'Navigation' menu with categories like Status, Monitor, Network, Objects, Policies, System, Authentication System, and Next Gen Security System. The 'Monitor' category is 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 warning: 'Central Management | The page can be configured.' Below this is a section for 'Logging and Archiving' with four log types: Security Logs, Application Control Logs, Traffic Audit Logs, and NAT Logs. Each log type has 'Enable' and 'Disable' buttons. Under 'Security Logs', 'Log Location' is set to 'Local (Recommended)' with checkboxes for 'Syslog', 'Local (Recommended)', and 'Cyber Command'. Similar settings are shown for the other log types. Below these is a 'Local Logs' section with 'Log Preservation/Deletion' options (Auto-delete logs cached for 180 days or Delete logs of the earliest day if disk usage reaches threshold 80%), 'Merge Logs of Same Type' (Enable), and 'Maximum Exported Entries' (Export the latest 1000 entries). At the bottom is a 'Cyber Command and NTA Settings' section with 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. Pergi ke Objects-> Security Policy Template->APT Detection, add APT template.

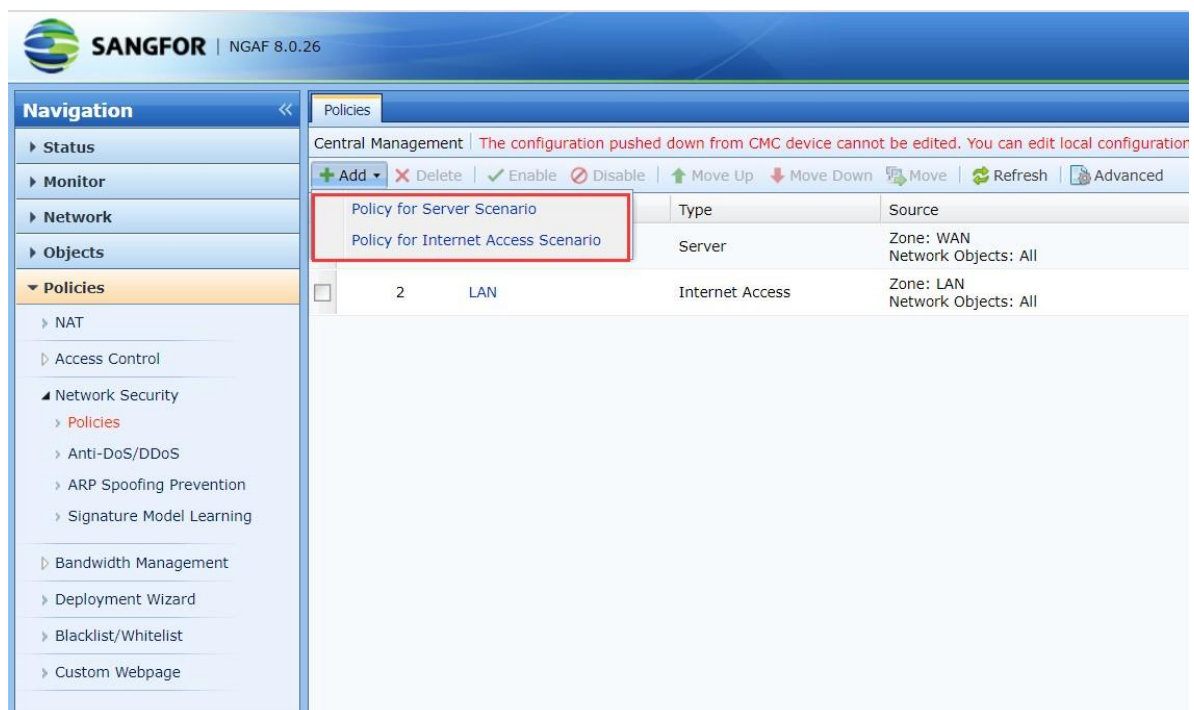
The screenshot shows the 'APT Detection' configuration page in the Sangfor NGAF 8.0.26 web interface. The left sidebar is the same as the previous screenshot, but 'APT Detection' is selected under 'Security Policy Template'. The main content area is titled 'APT Detection' and includes a warning: 'Central Management | The configuration pushed down from CMC device cannot be edited. You can edit local configuration only.' Below this are '+ Add', 'X 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

## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana



3. Pergi ke Policies->Network Security->Policies path, add dua policies untuk block botnet traffic.



Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

**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

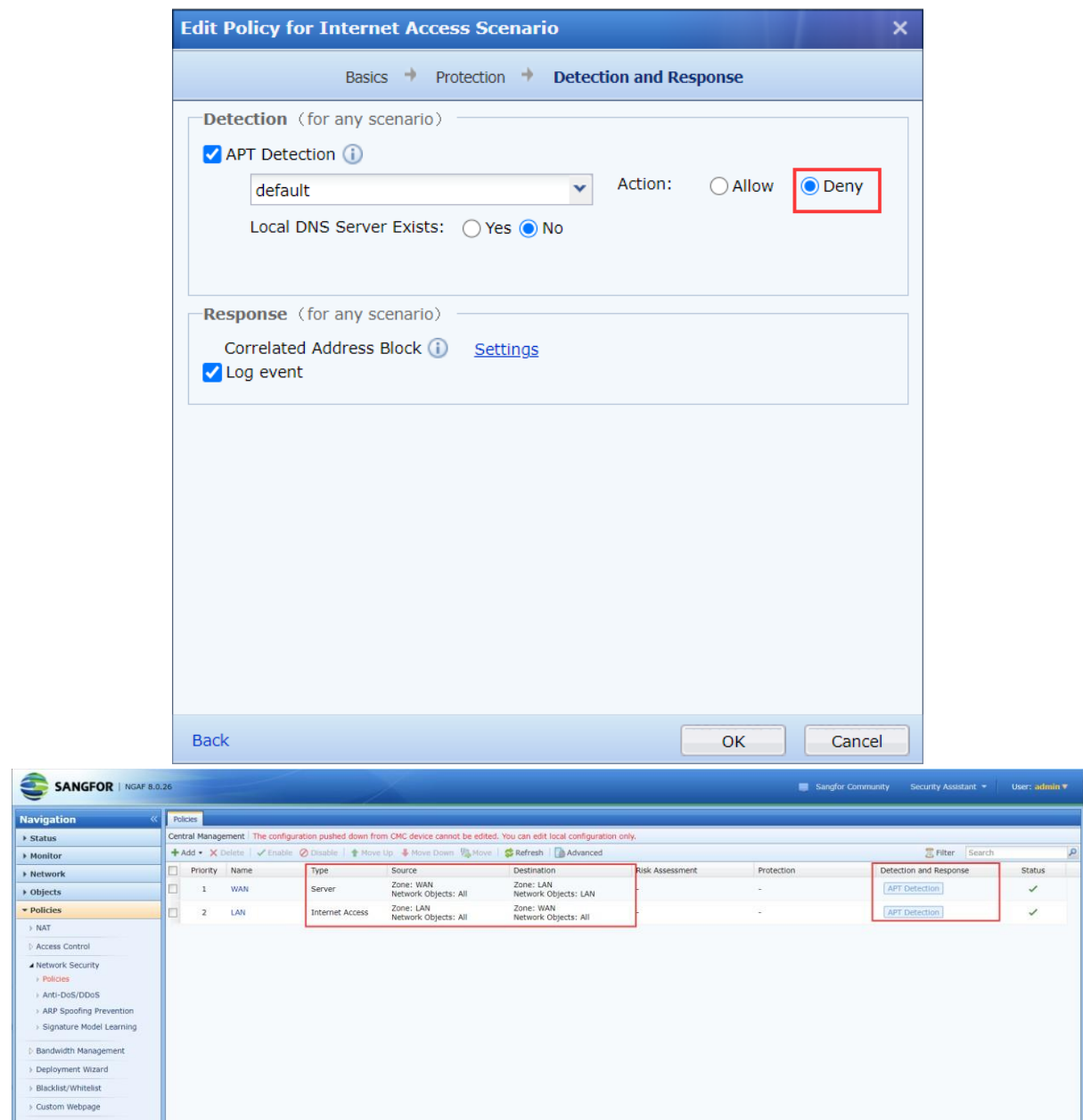
**Basics Protection** (for any scenario)

☐ 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

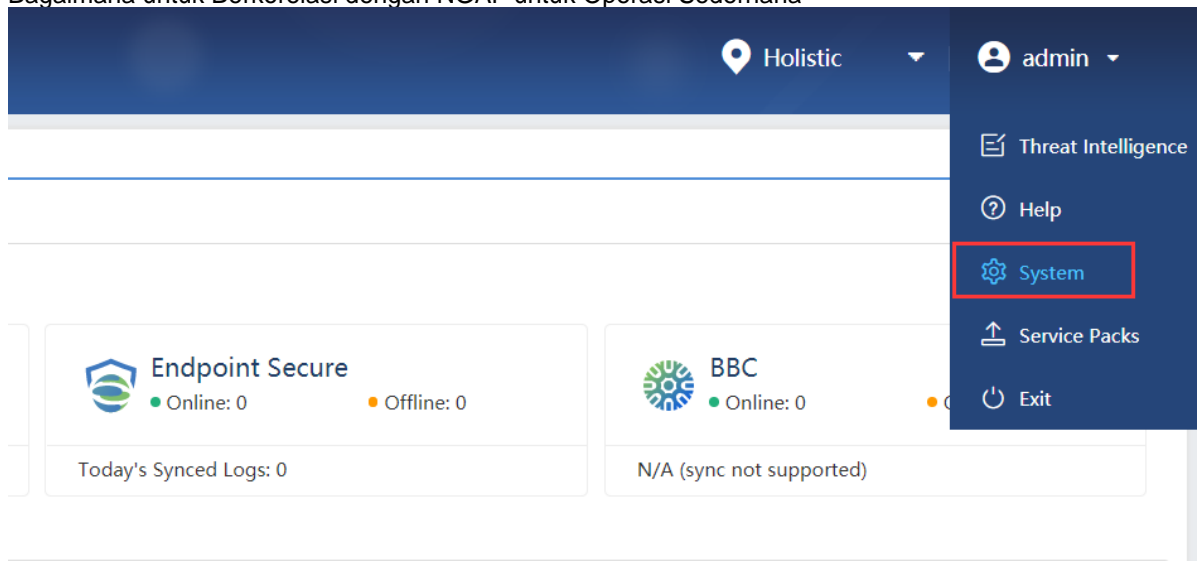
Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana



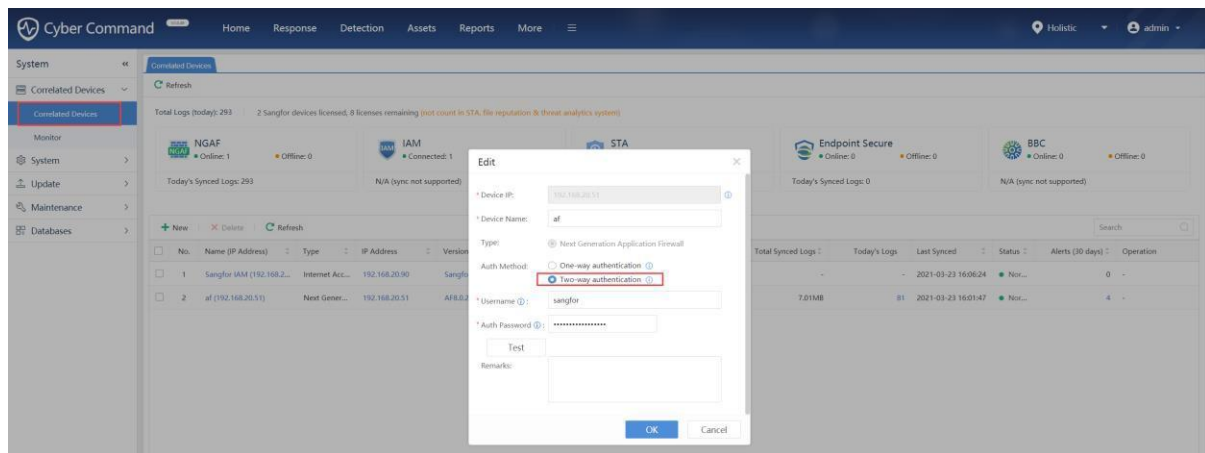
## 2.2 Konfigurasi Cyber Command

1. Pergi ke System path.

Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

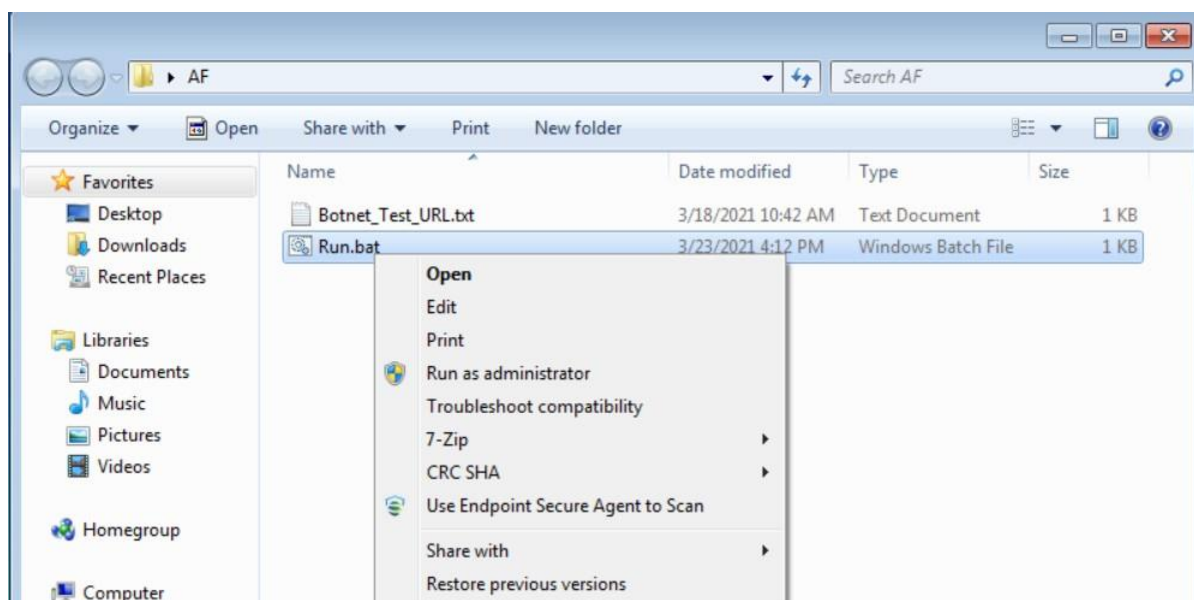


2. Enable Two-way authentication, lalu masukkan akun dan password yang Anda konfigurasi di NGAF.



## 2.3 Run Botnet Program

1. Run Botnet Program PC.

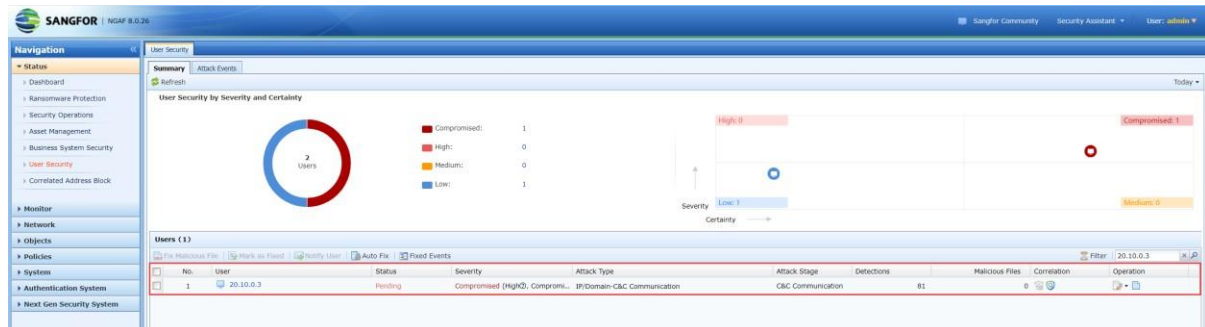


Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

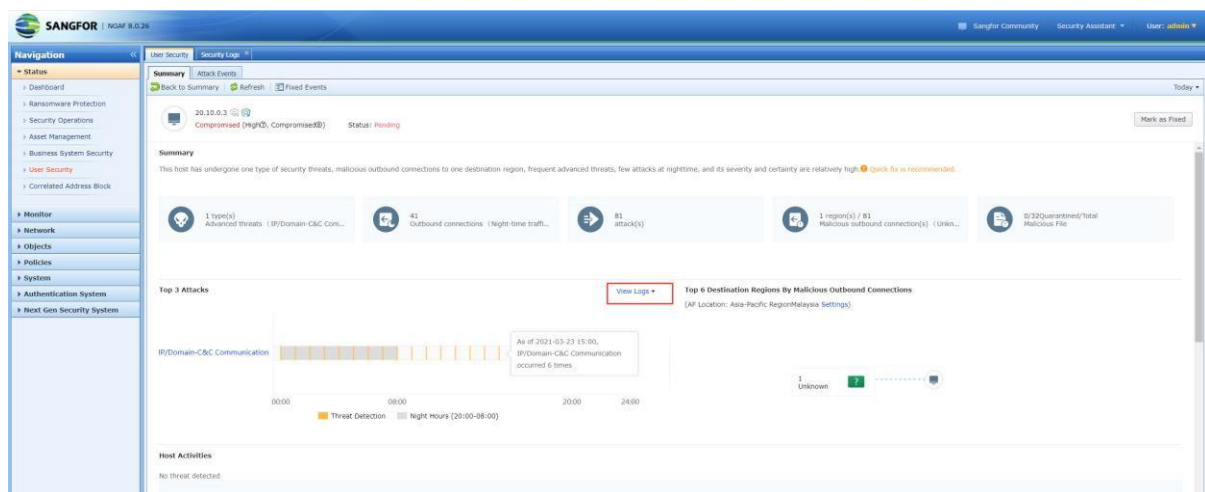
## 2.4 Periksa Logs dan Korelasi ke Block

### 2.4.1 Periksa Security Logs di NGAF

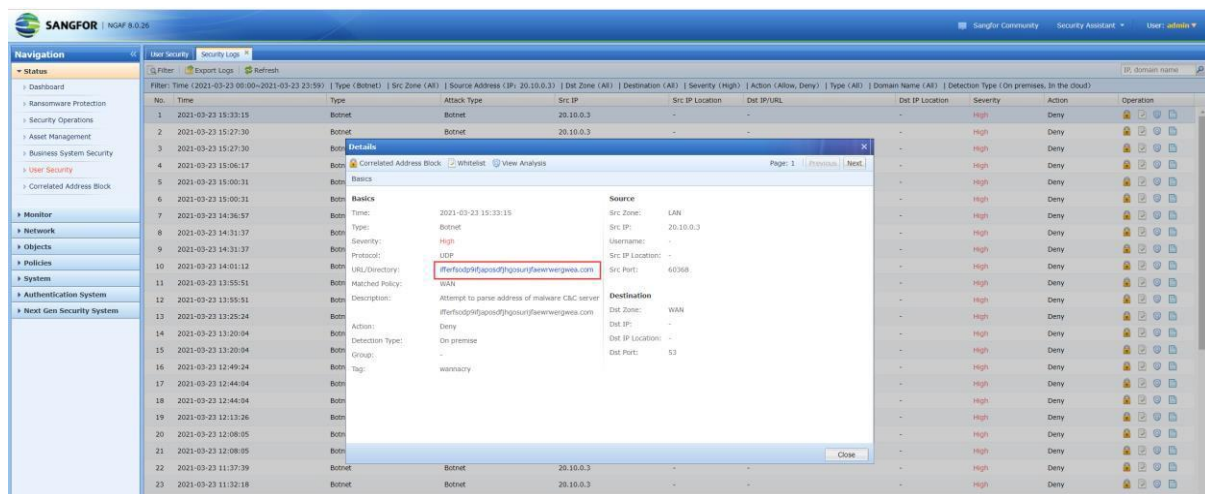
1. Periksa apakah ada hasil Secure Log.



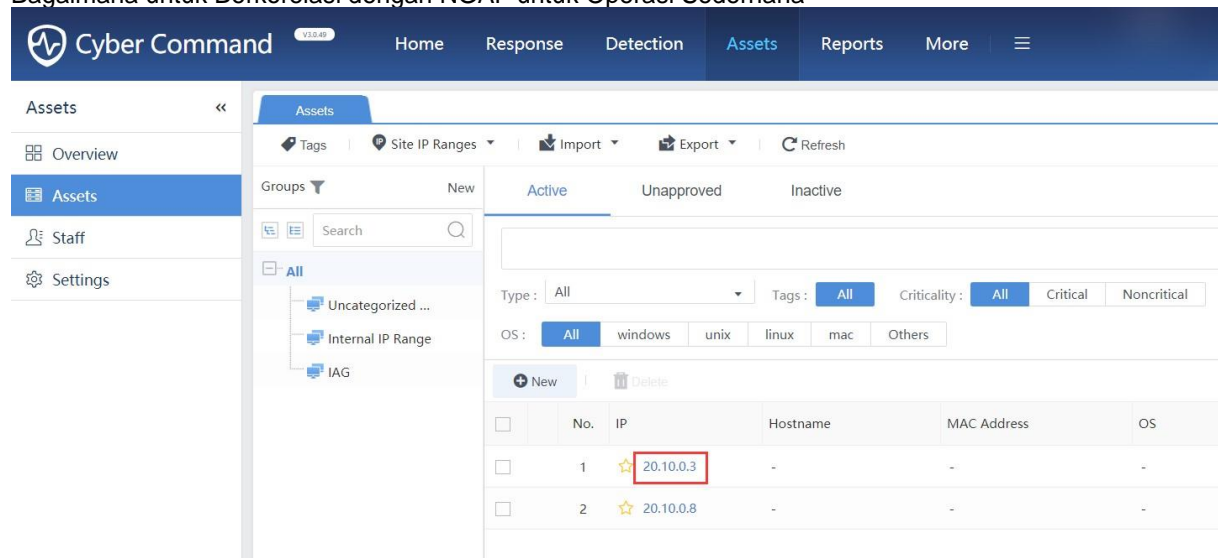
2. Anda dapat melihat detail security log di NGAF.



3. Konfirmasi apakah URL termasuk di Botnet Tools.

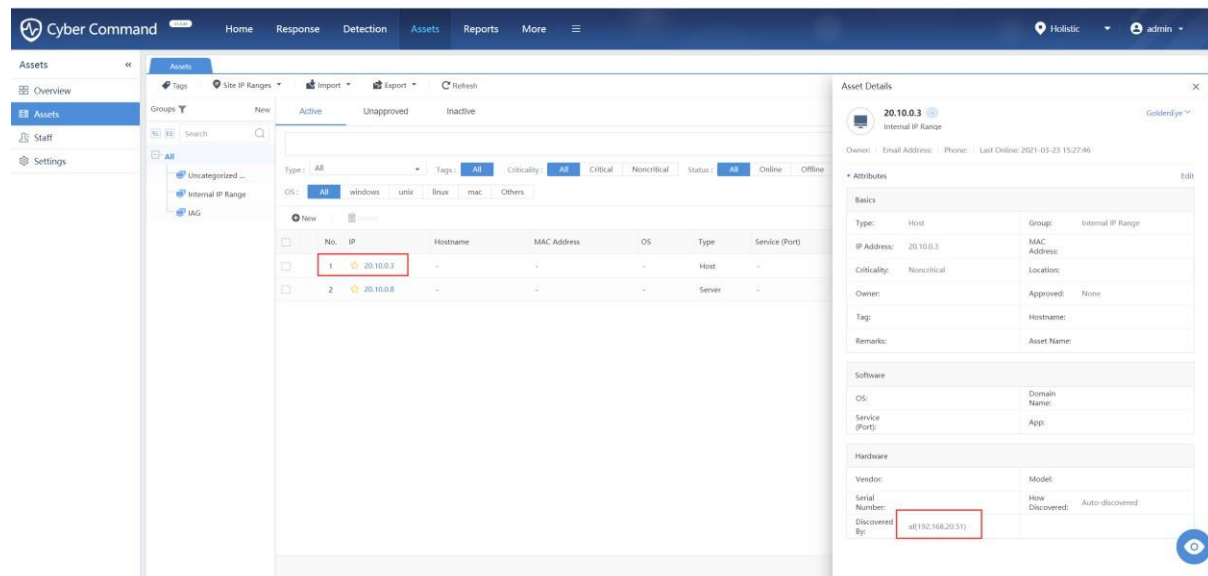


## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

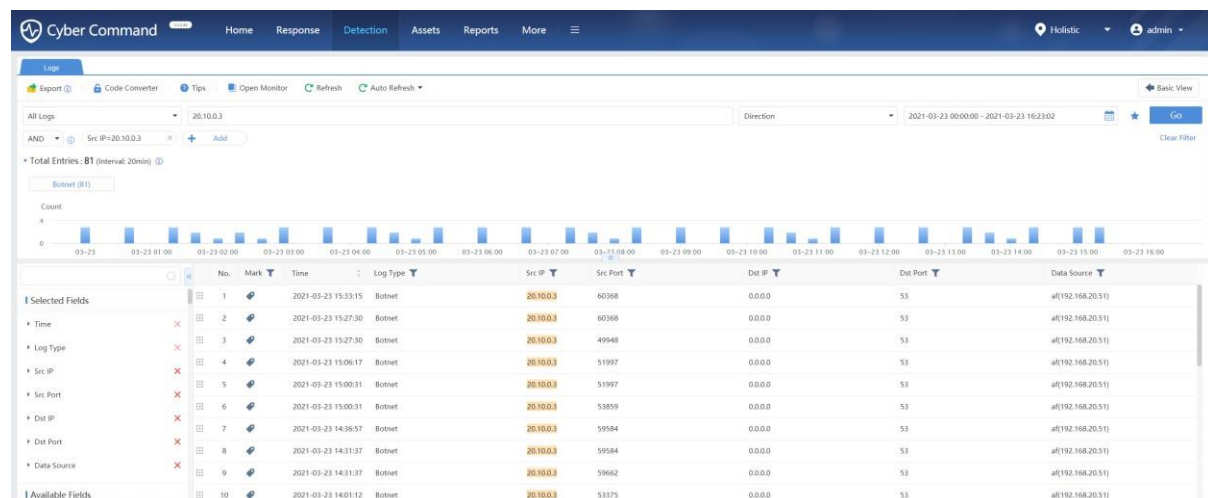


### 2.4.2 Periksa Security Log di Cyber Command

1. Pastikan Cyber Command menghasilkan asset menurut logs dan traffic yang disinkronisasi NGAF. Jika tidak, Anda perlu membuat asset secara manual di Cyber Command.

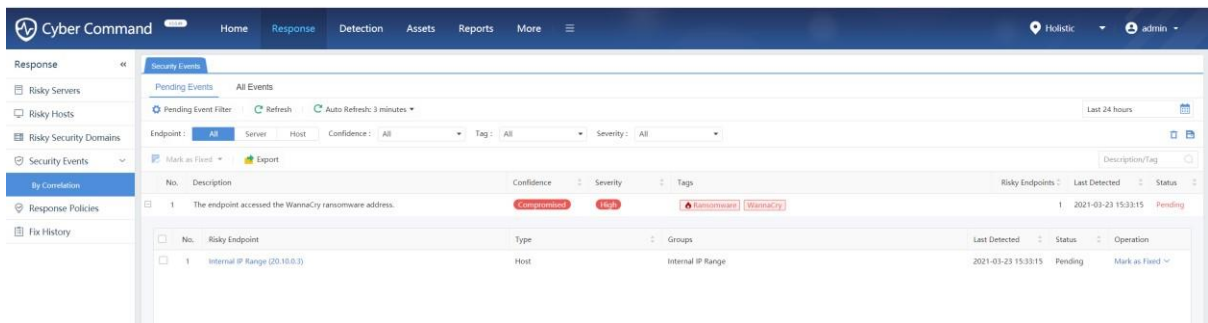


2. Pergi ke Detection->Logs Path, filter IP dari Anda tes PC, dan periksa apakah ada security log terkait.

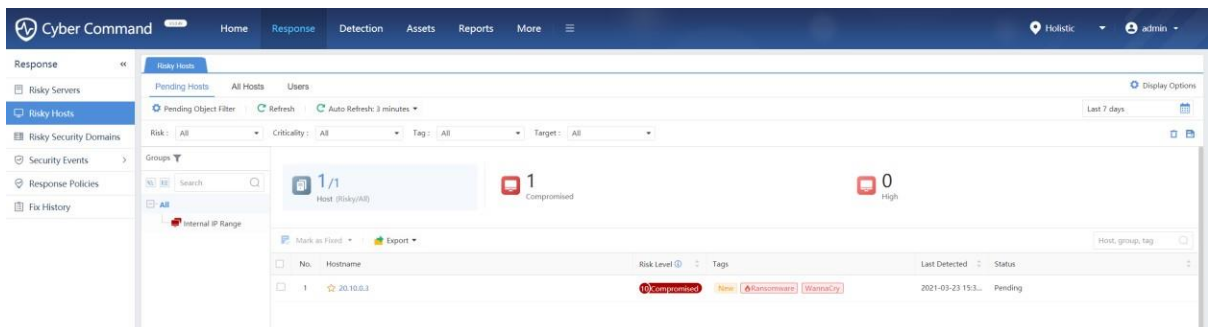


Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

3. Pergi ke Response->Security Events->By Correlation path, lalu periksa apakah Cyber Command menghasilkan Security Events.

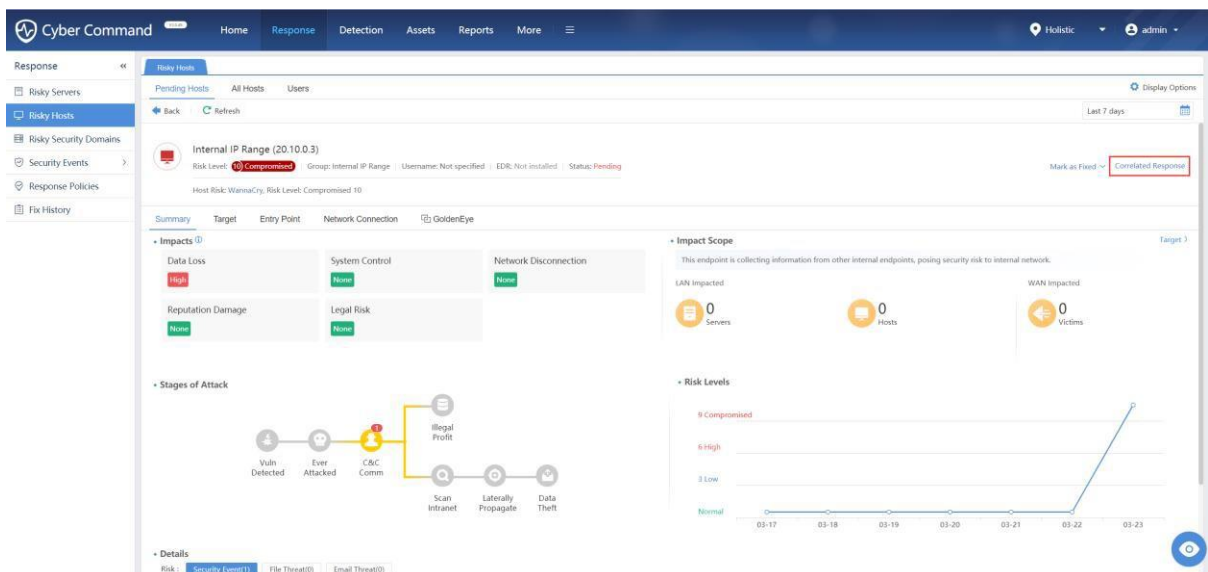


4. Pergi ke Response->Risk Hosts, dan periksa apakah ada risk hosts.



## 2.4.3 Berkorelasi ke Block Botnet Traffic

1. Klik Correlated Response.





2. Pilih Correlated Response.


## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana


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. Klik Start dan atur waktu lockout, lalu klik 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. Setelah beberapa detik, Anda dapat melihat policy yang dikeluarkan berhasil.

## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

### 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

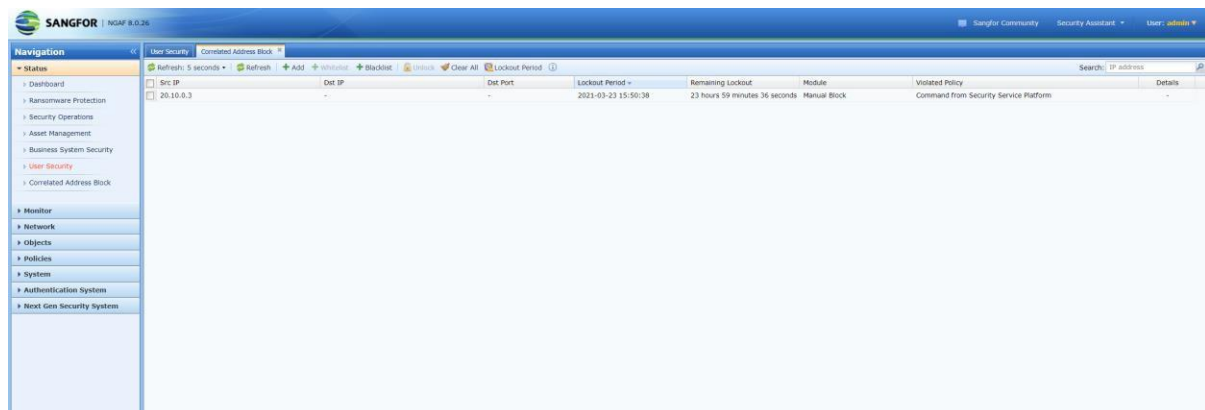
Lockout: 1 days

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

Again

Close

5. Anda dapat log in ke NGAF web console, dan pergi ke Status-> Correlated Address Block path, kemudian Anda dapat memeriksa IP yang diblokir oleh Cyber Command.





6. Jika Anda ingin menggunakan access control policy untuk memblokir botnet traffic, Anda dapat pilih Access Control.


## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana


### 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. Klik Start dan konfigurasi Zone dan IP yang Anda ingin blokir.

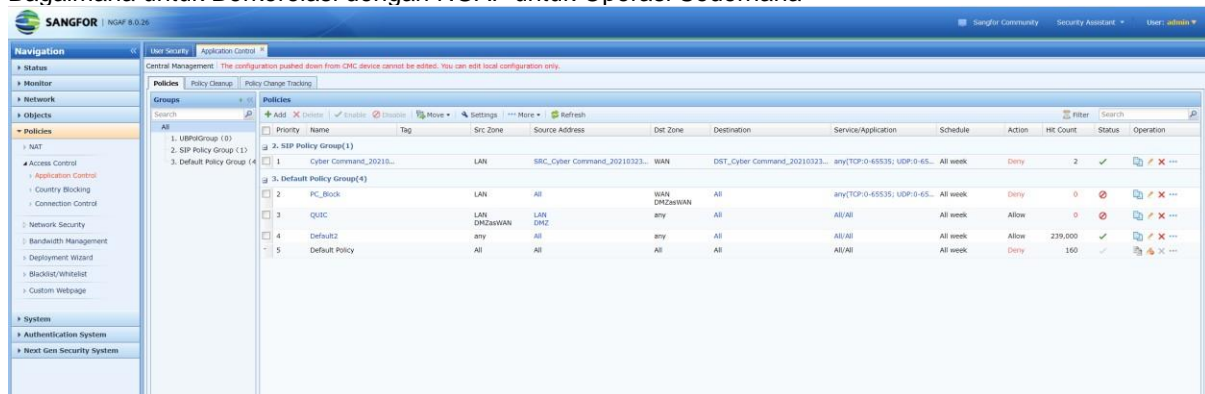
**Correlated Response**  
**Asset IP: 20.10.0.3**  
**Access Control**  
Device: ☒ NGAF Hot ☐ Endpoint Secure  
IP Address: af(192.168.20.51)  
**Access Control**

**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: 0.0.0.0-255.255.255.255  
\* Dst Zone: WAN  
Service: ☒ Predefined ☐ Custom  
Predefined Service/any  
Select  
Remarks: Optional  
**OK** **Cancel**

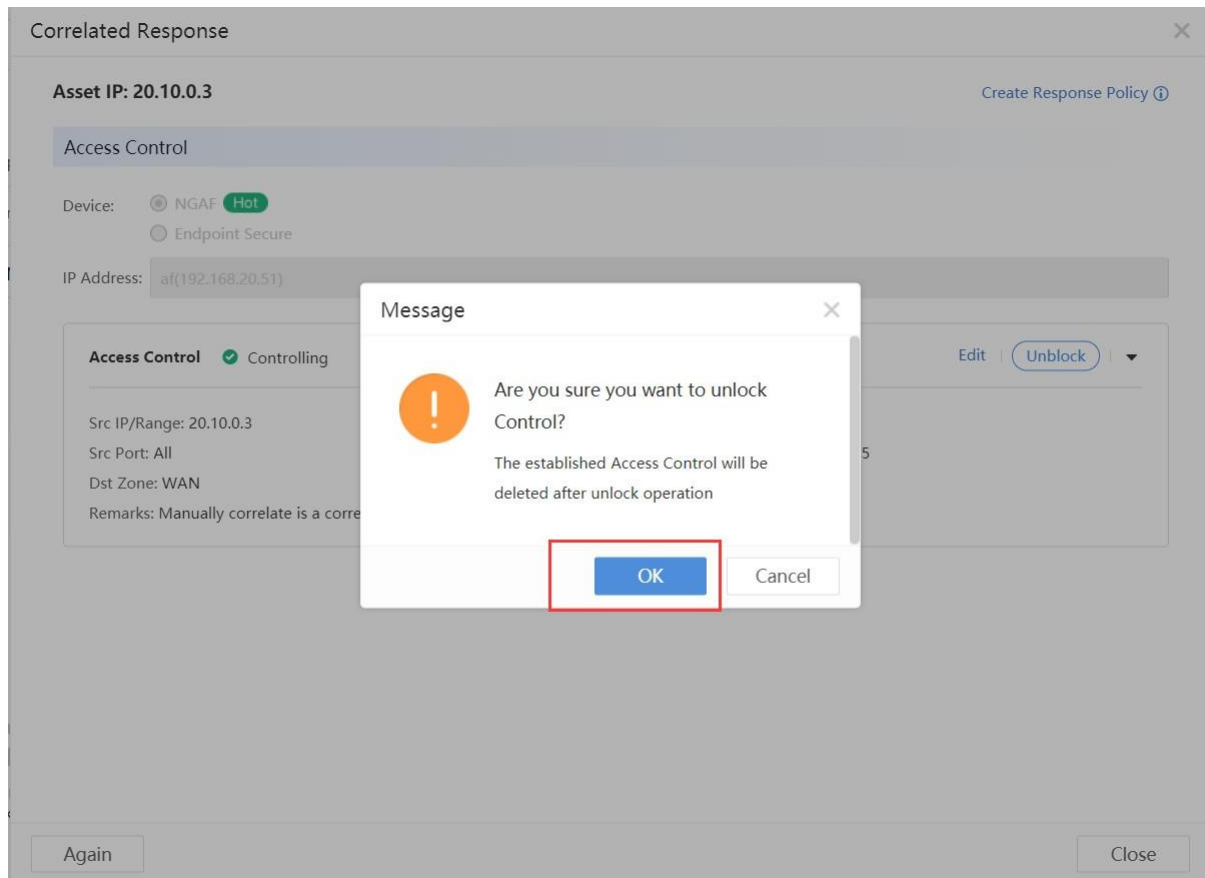
[Create Response Policy](#)  
**Start**  
**Close**

8. Setelah beberapa detik, Anda dapat log in NGAF web console, dan Anda dapat menemukan Access Control policy dikeluarkan berhasil.

## Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana



9. Jika Anda ingin unblock access control policy, Anda dapat klik Unblock.



10. Anda dapat log in ke NGAF web console dan periksa apakah access control policy dihapus oleh 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