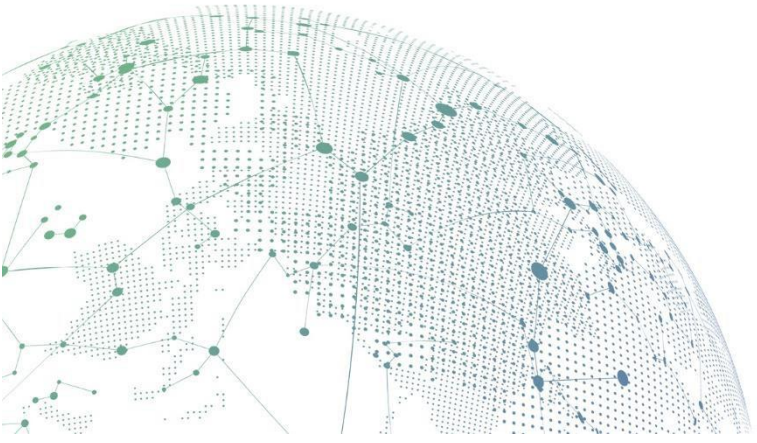
SANGFOR

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

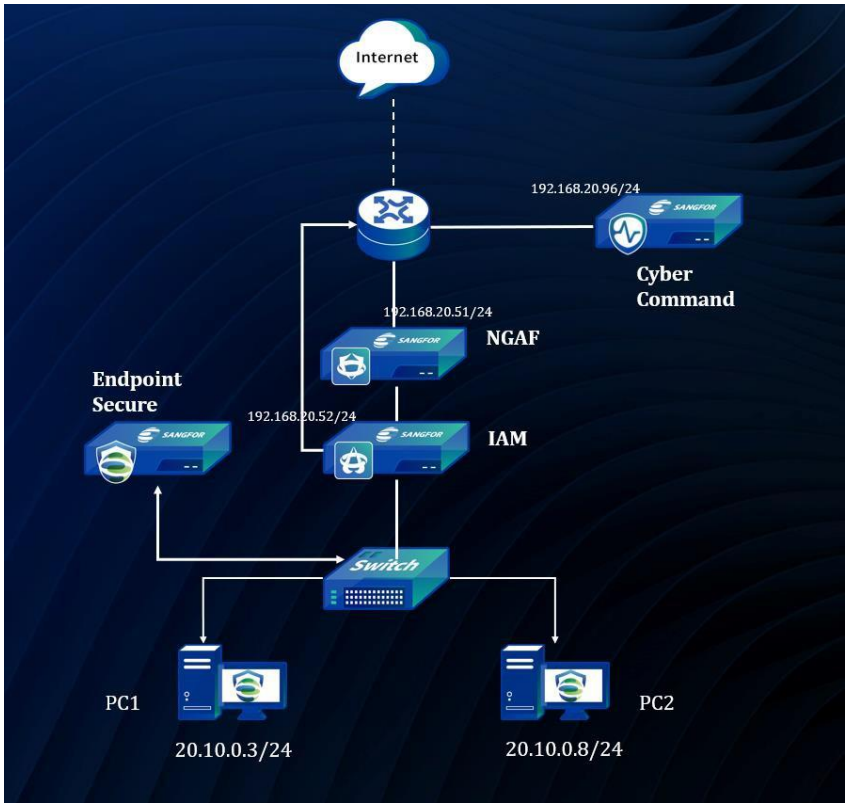
Bab 1 Skenario 1
1.1 Skenario 1
1.2 Lingkungan 1
1.2.1 Lingkungan Network 1
1.3 Tes Perkenalan 1
Bab 2 Konfigurasi 1
2.1 Konfigurasi NGAF 1
2.2 Konfigurasi Cyber Command 5
2.3 Run Botnet Program 6
2.4 Periksa log dan Korelasi ke Block 7
2.4.1 Periksa Security Logs di NGAF 7
2.4.2 Periksa Security Log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

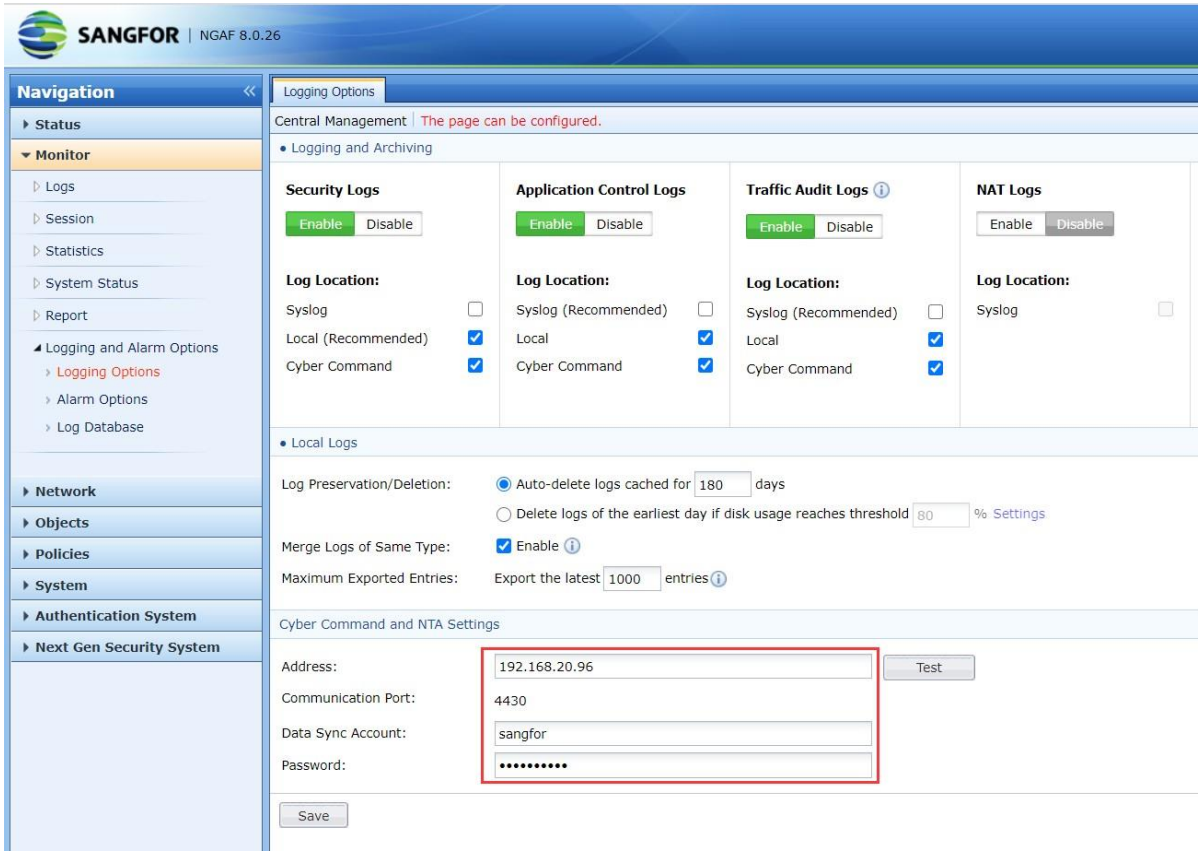
1. Hanya perlu menganalisa traffic Botnet URL domain name untuk melewati NGAF, dan itu tidak perlu mengunjungi URL ini.

Bab 2 Konfigurasi

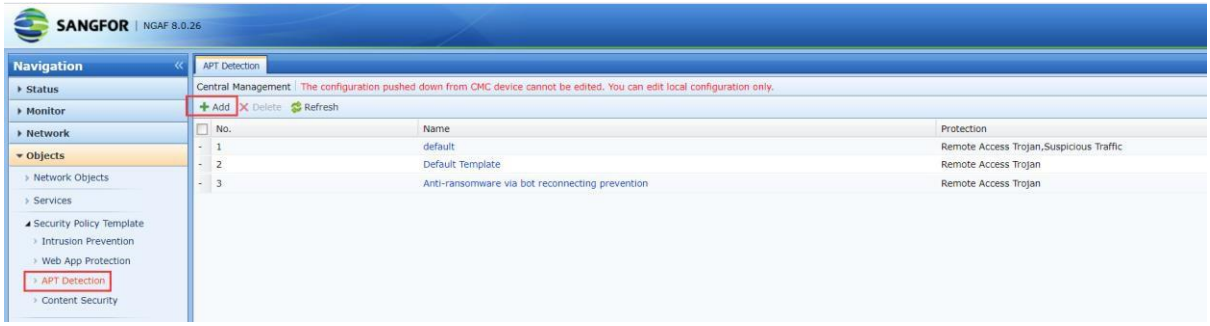
2.1 Konfigurasi NGAF

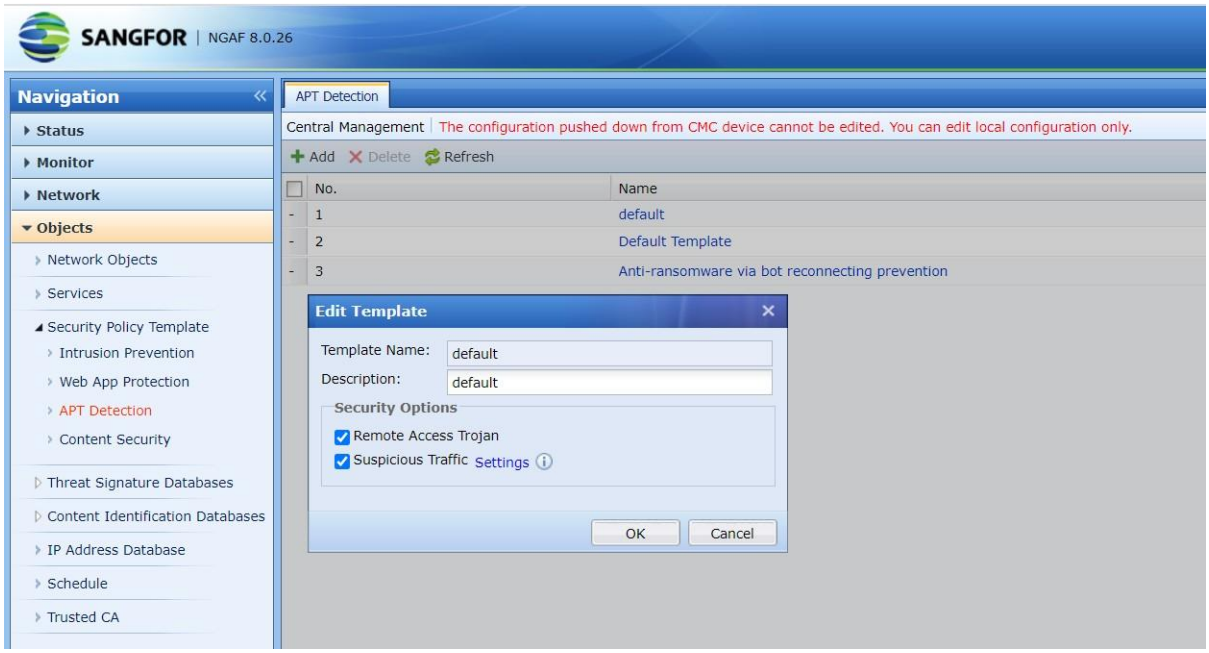
1. Pergi ke Monitor->Logging dan Alarm Options-> Logging Options Path, konfigurasi correlation options, seperti IP dari Cyber Command, Anda dapat mengatur akun dan password, itu akan digunakan di Cyber Command.

Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

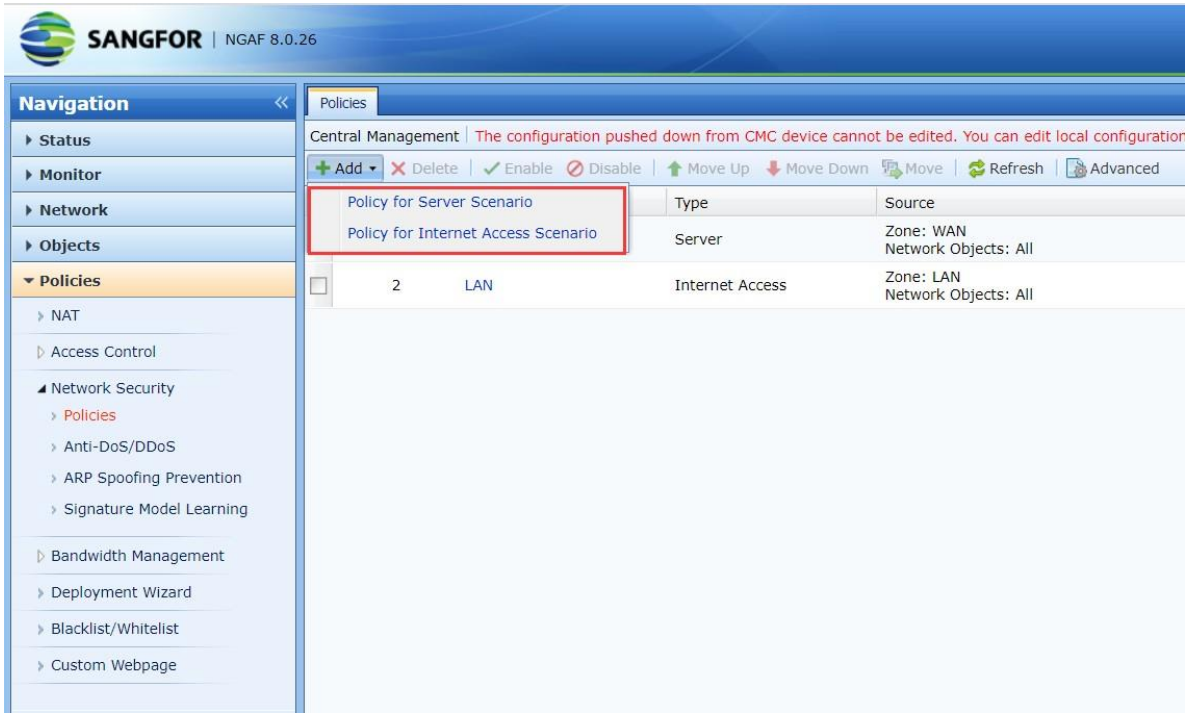


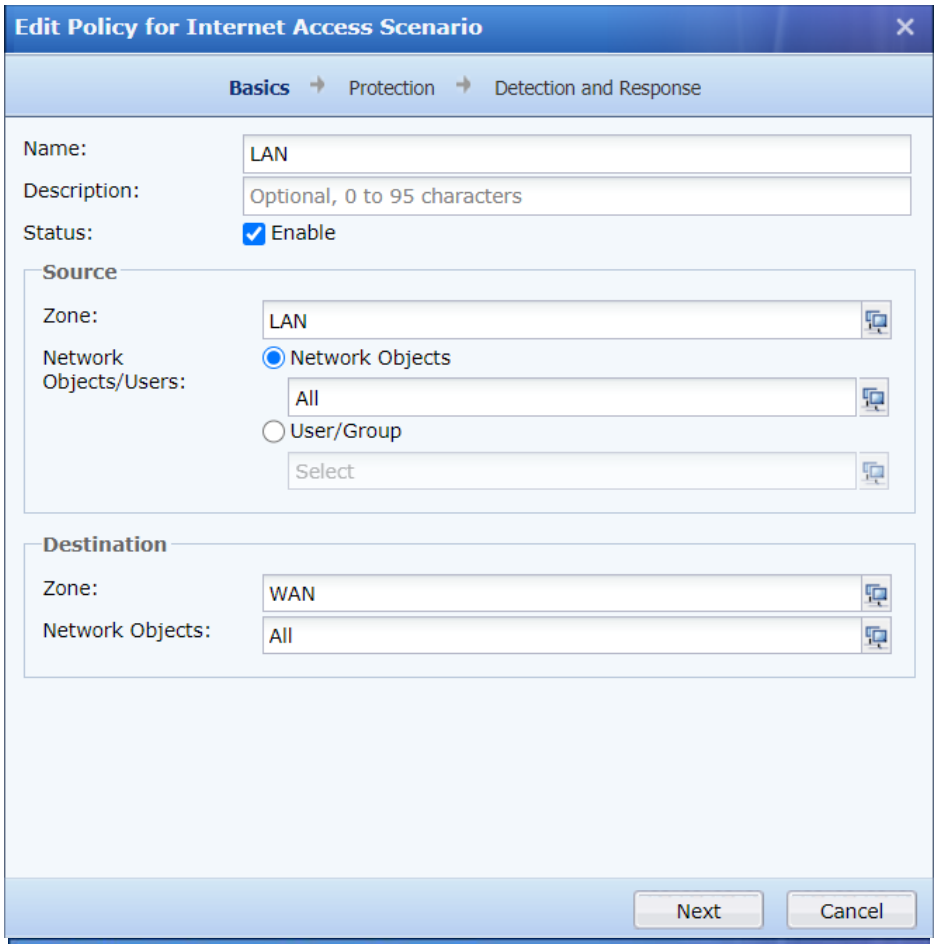
2. Pergi ke Objects-> Security Policy Template->APT Detection, add APT template.

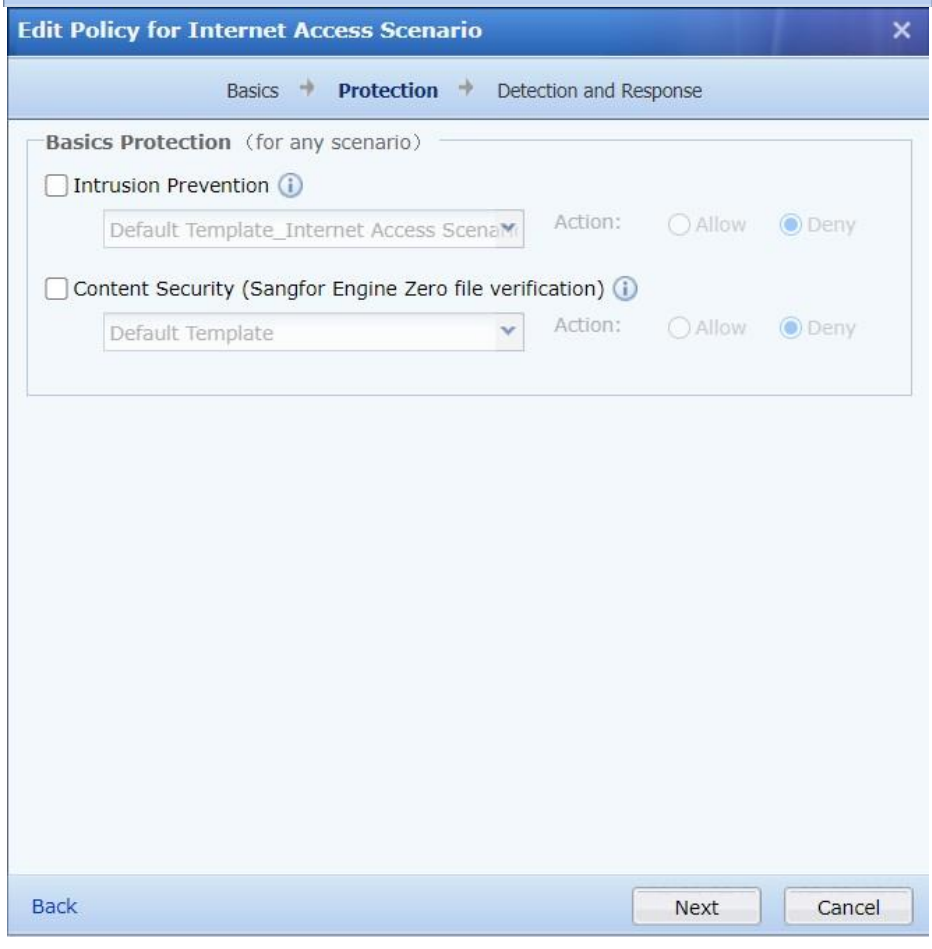


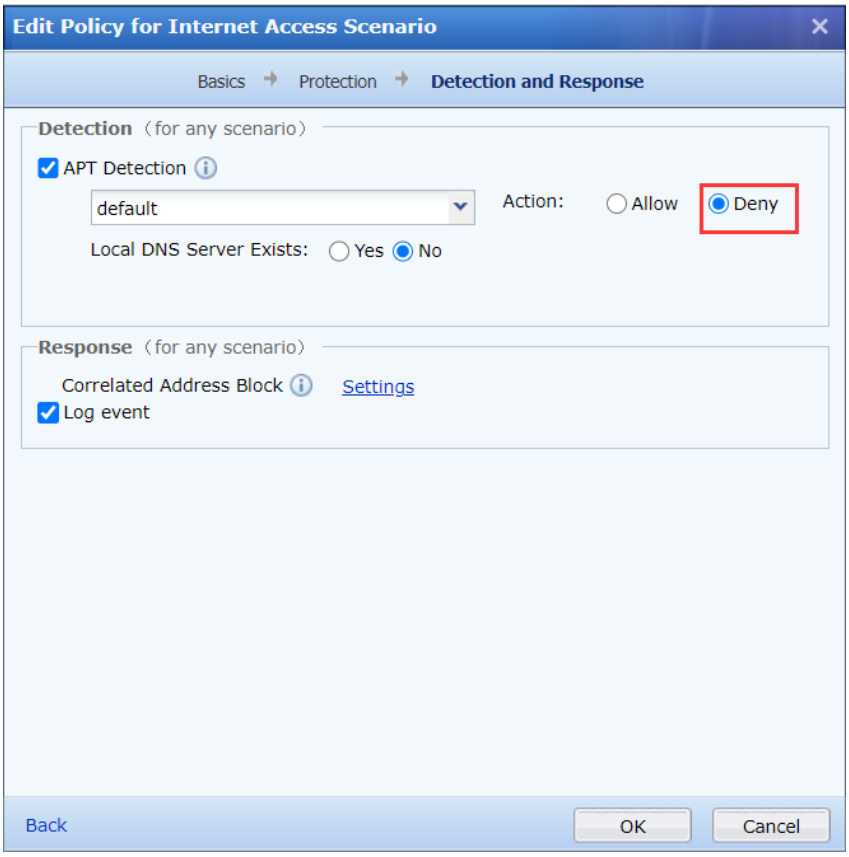


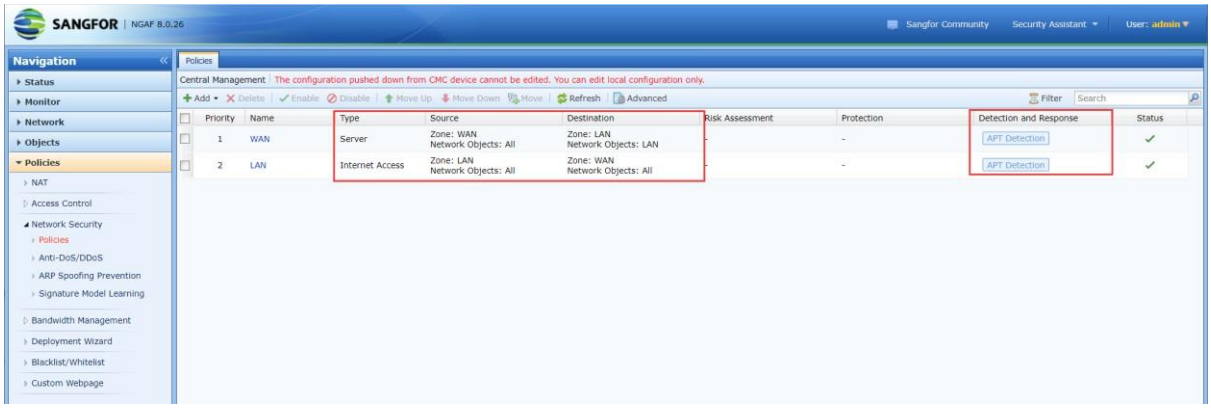
3. Pergi ke Policies->Network Security->Policies path, add dua policies untuk block botnet traffic.




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

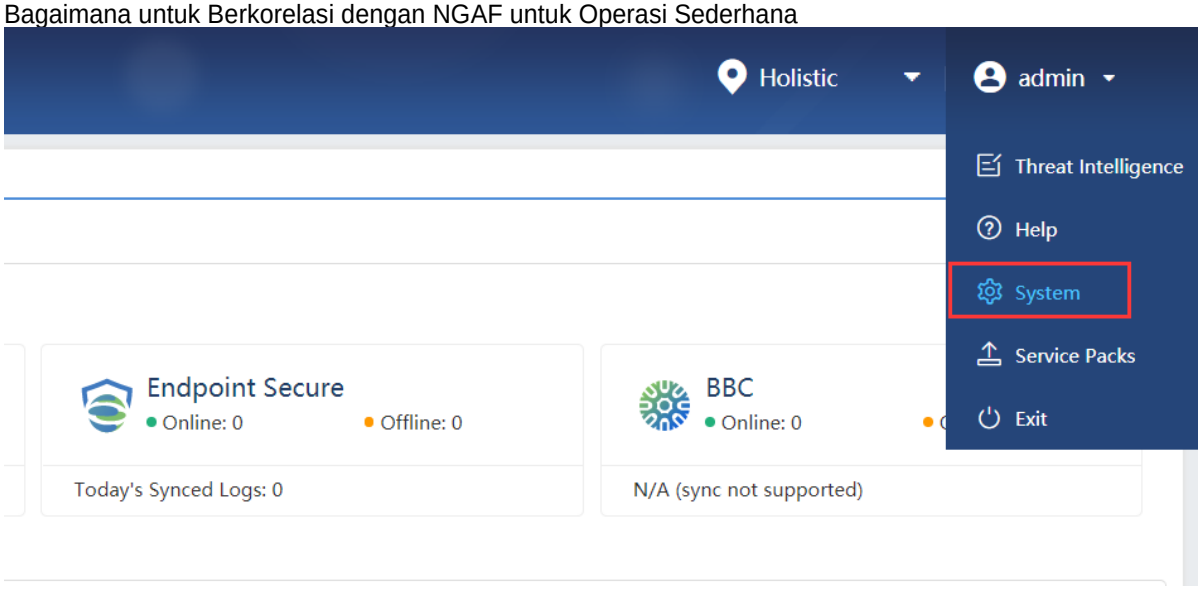

Edit Policy for Internet Access Scenario
Basics
Protection
Detection and Response
Basics Protection (for any scenario)
Intrusion Prevention
Default Template_Internet Access Scena
Action:
Allow
Deny
Content Security (Sangfor Engine Zero file verification)
Default Template
Action:
Allow
Deny
Back
Next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



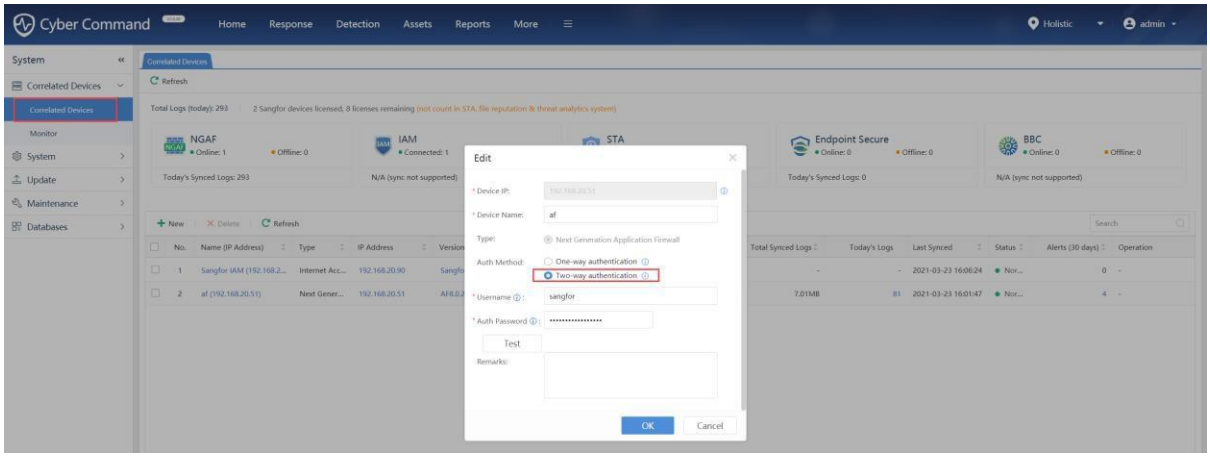


2.2 Konfigurasi Cyber Command

1. Pergi ke System path.

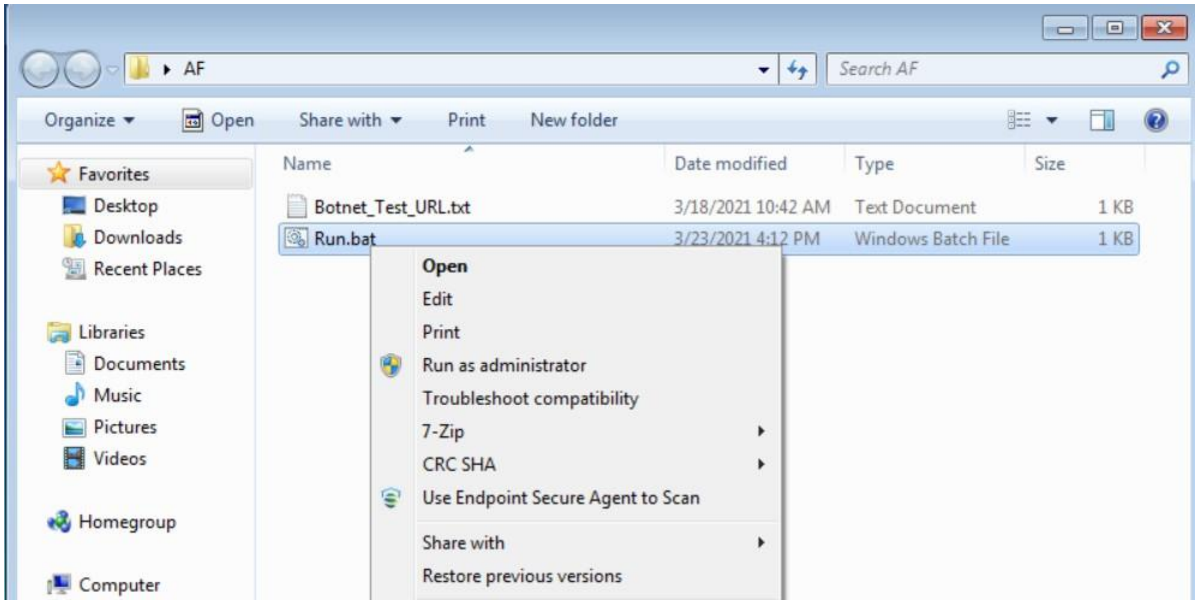


2. Enable Two-way authentication, lalu masukkan akun dan password yang Anda konfigurasi di NGAF.



2.3 Run Botnet Program

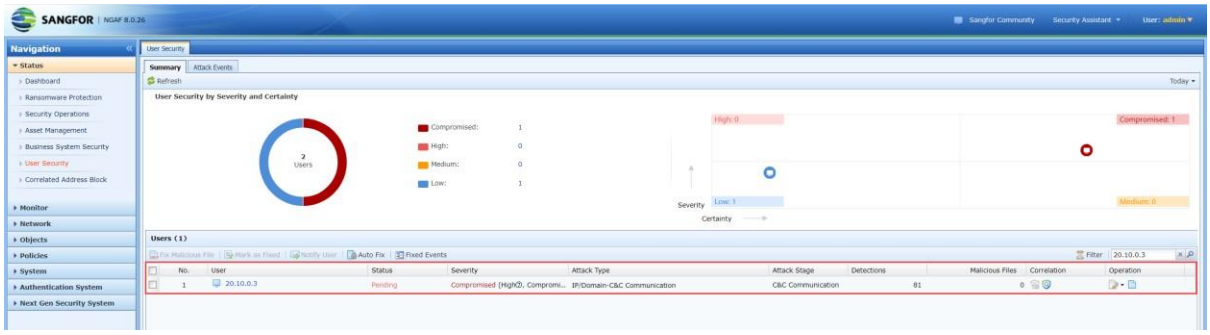
1. Run Botnet Program PC.



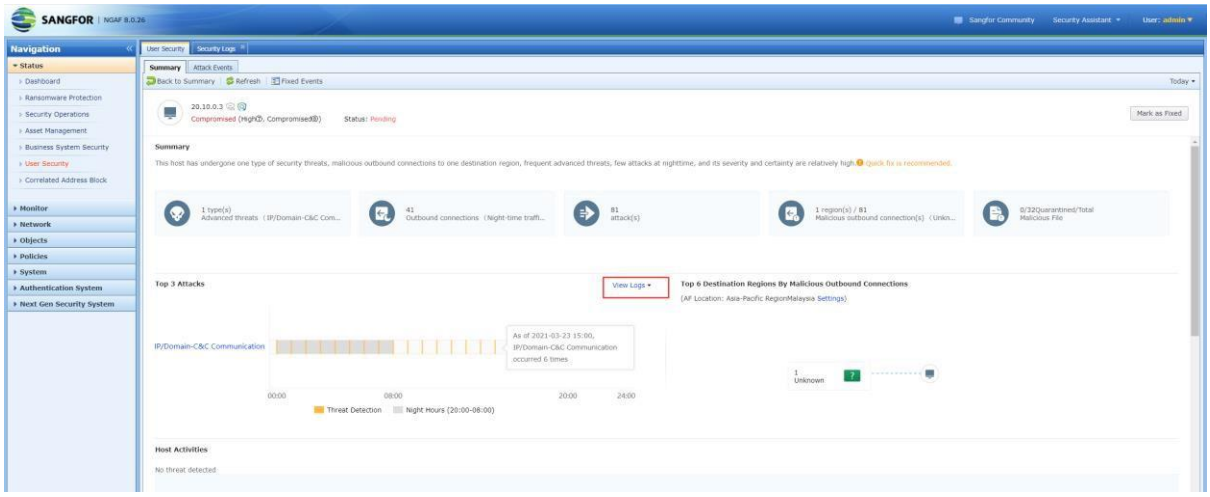
2.4 Periksa Logs dan Korelasi ke Block

2.4.1 Periksa Security Logs di NGAF

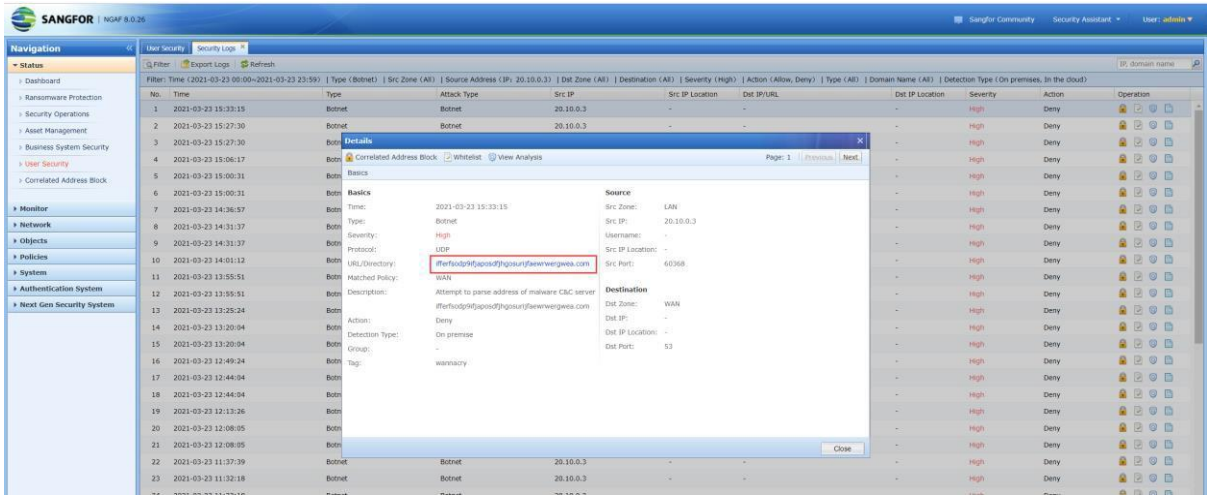
1. Periksa apakah ada hasil Secure Log.



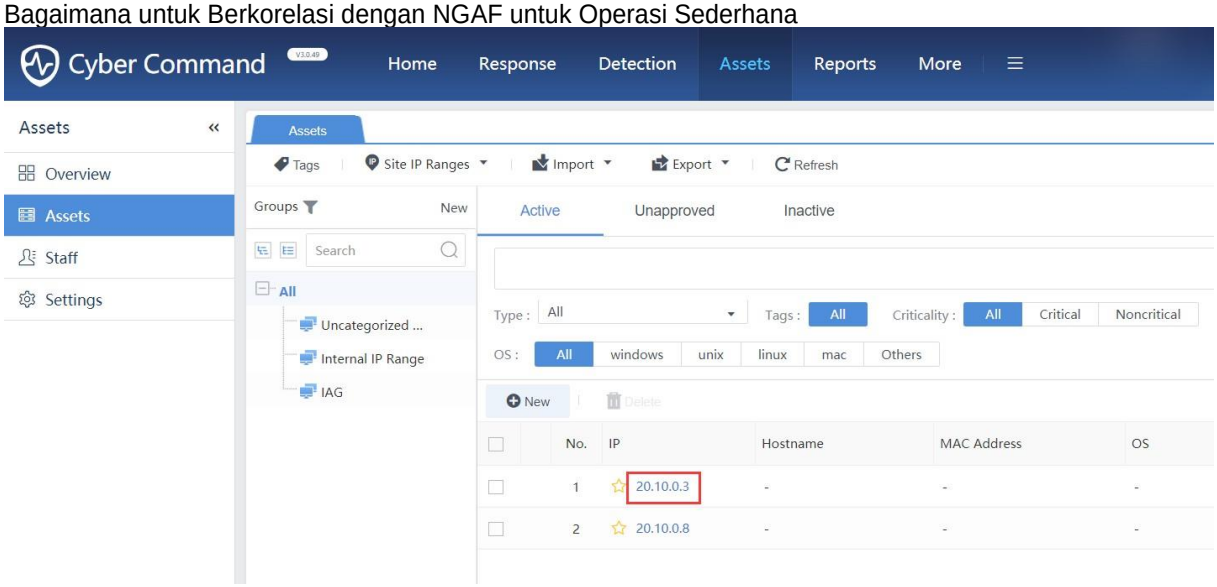
2. Anda dapat melihat detail security log di NGAF.



3. Konfirmasi apakah URL termasuk di Botnet Tools.

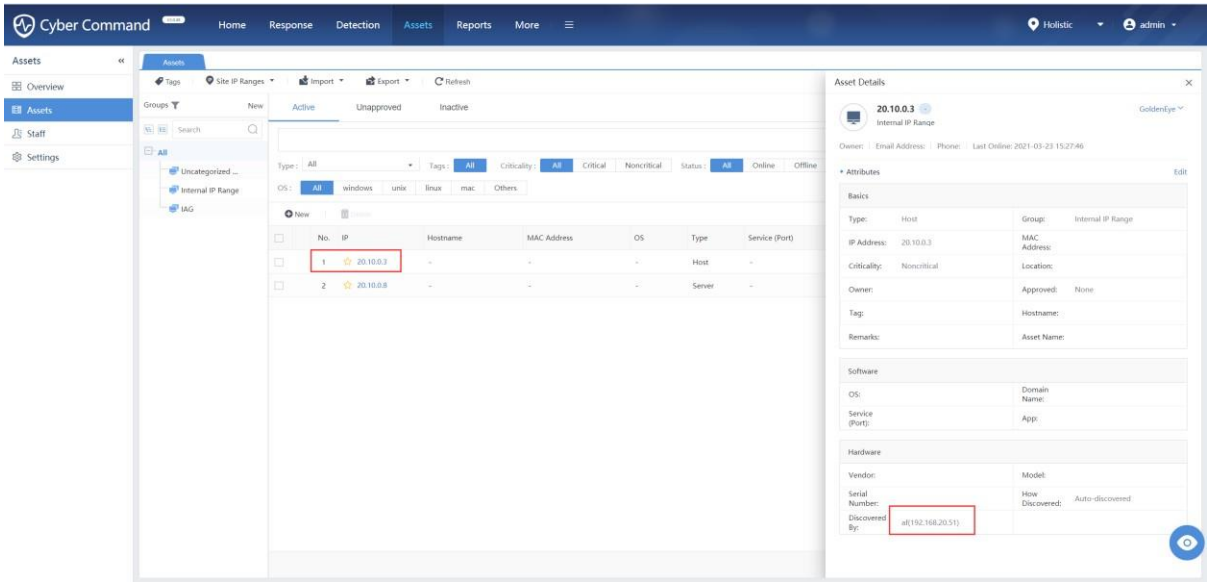


Bagaimana untuk Berkorelasi dengan NGAF untuk Operasi Sederhana

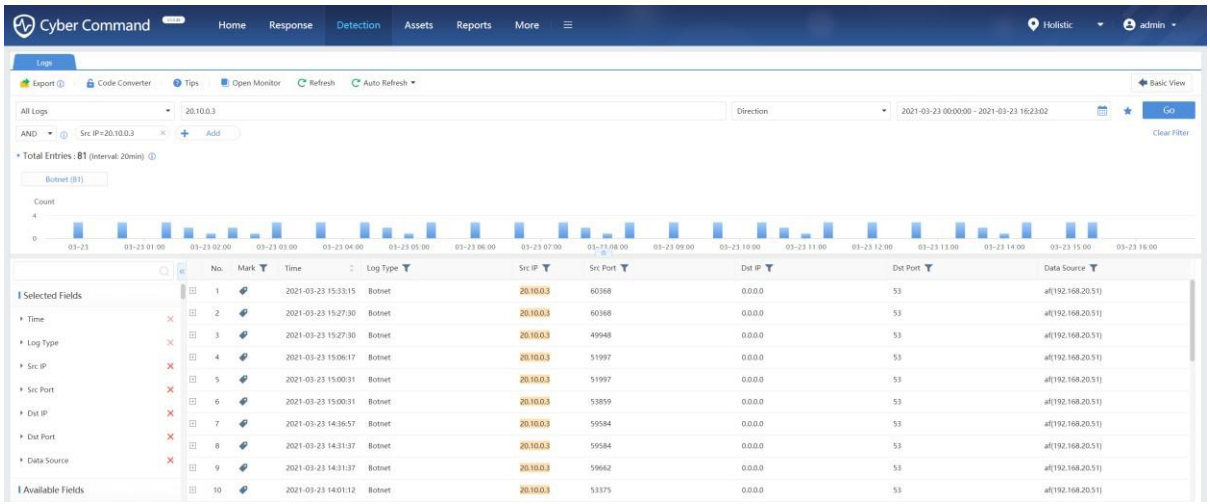


2.4.2 Periksa Security Log di Cyber Command

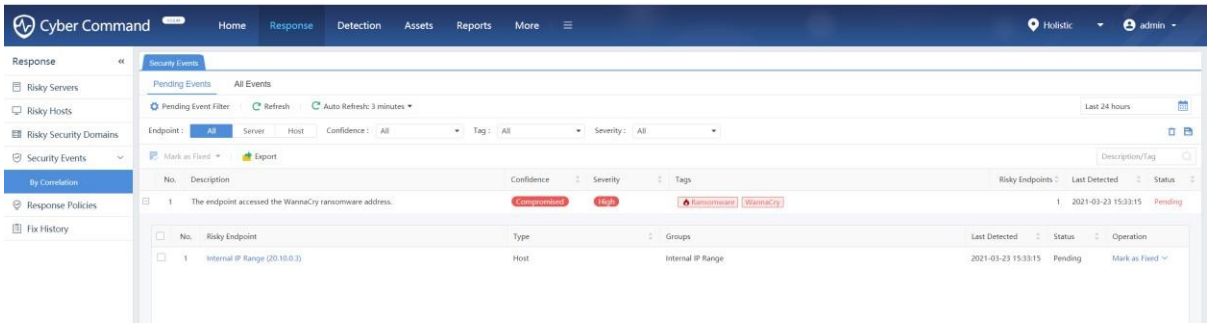
1. Pastikan Cyber Command menghasilkan asset menurut logs dan traffic yang disinkronisasi NGAF. Jika tidak, Anda perlu membuat asset secara manual di Cyber Command.



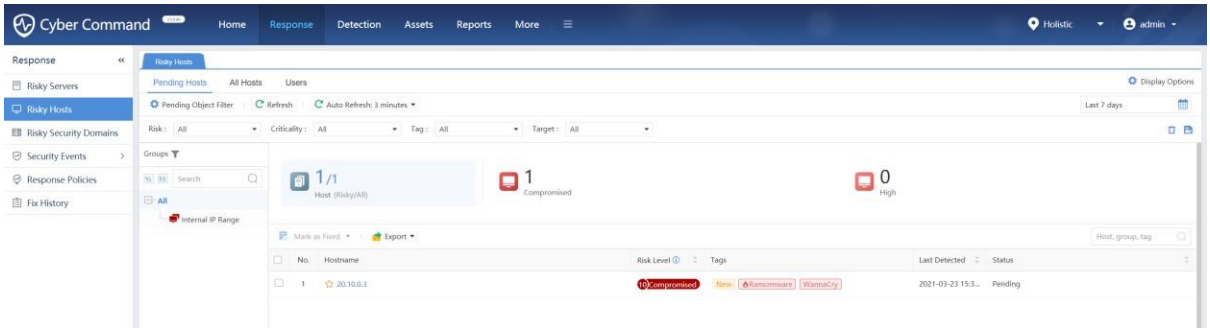
2. Pergi ke Detection->Logs Path, filter IP dari Anda tes PC, dan periksa apakah ada security log terkait.



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

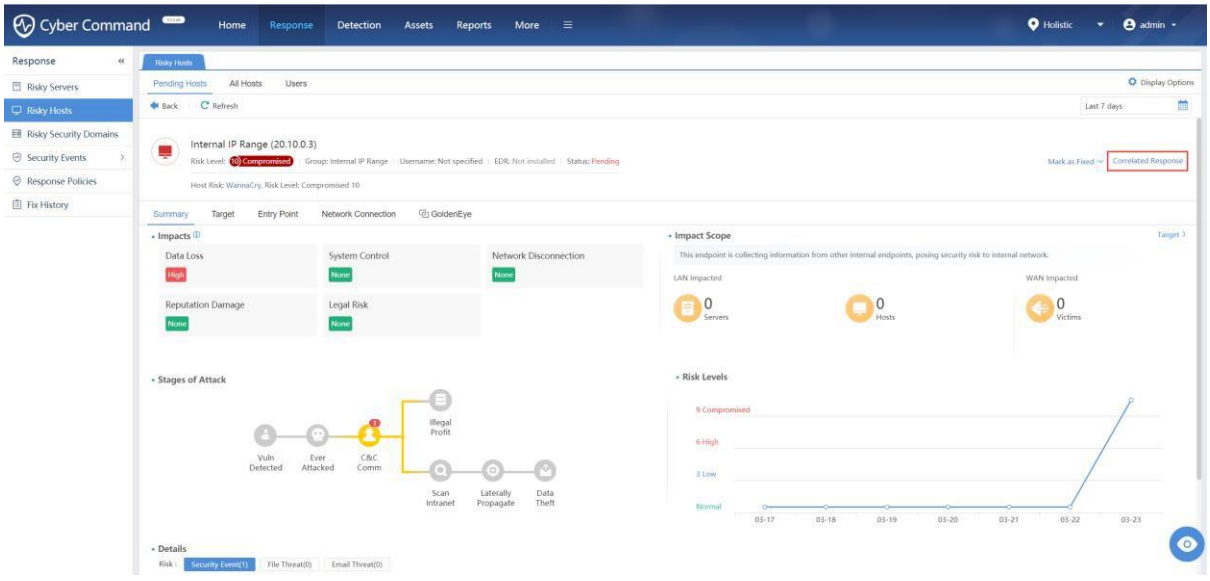


4. Pergi ke Response->Risk Hosts, dan periksa apakah ada risk hosts.

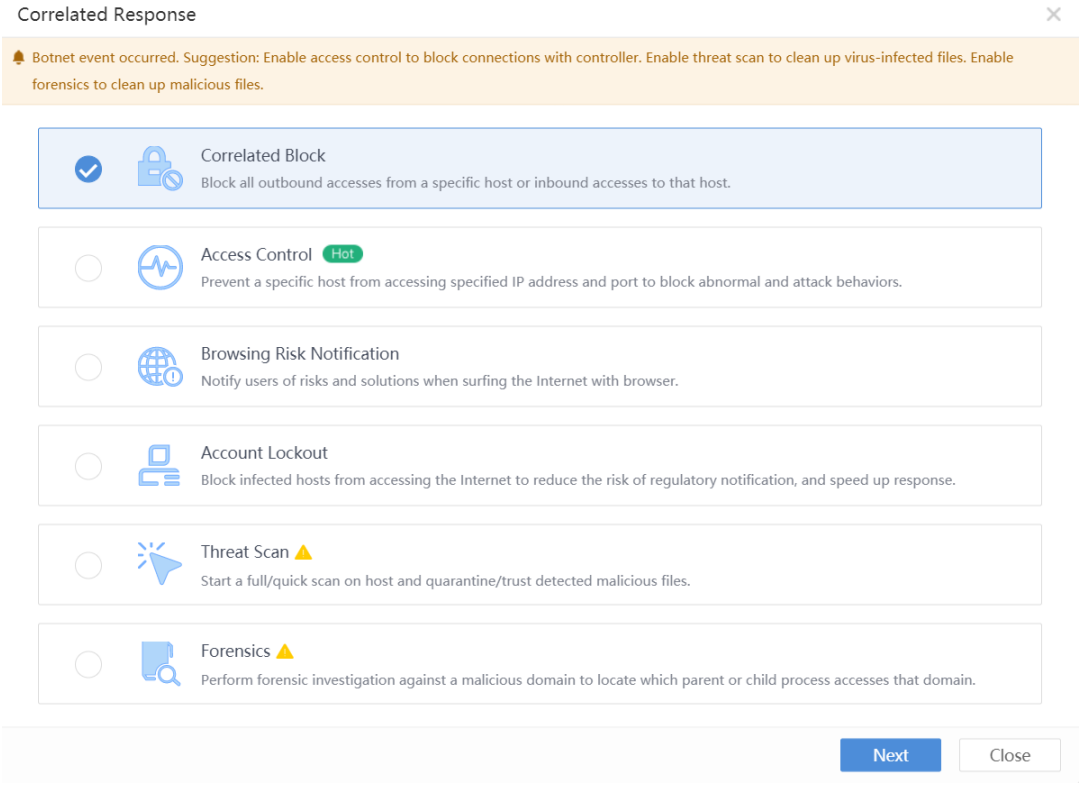


2.4.3 Berkorelasi ke Block Botnet Traffic

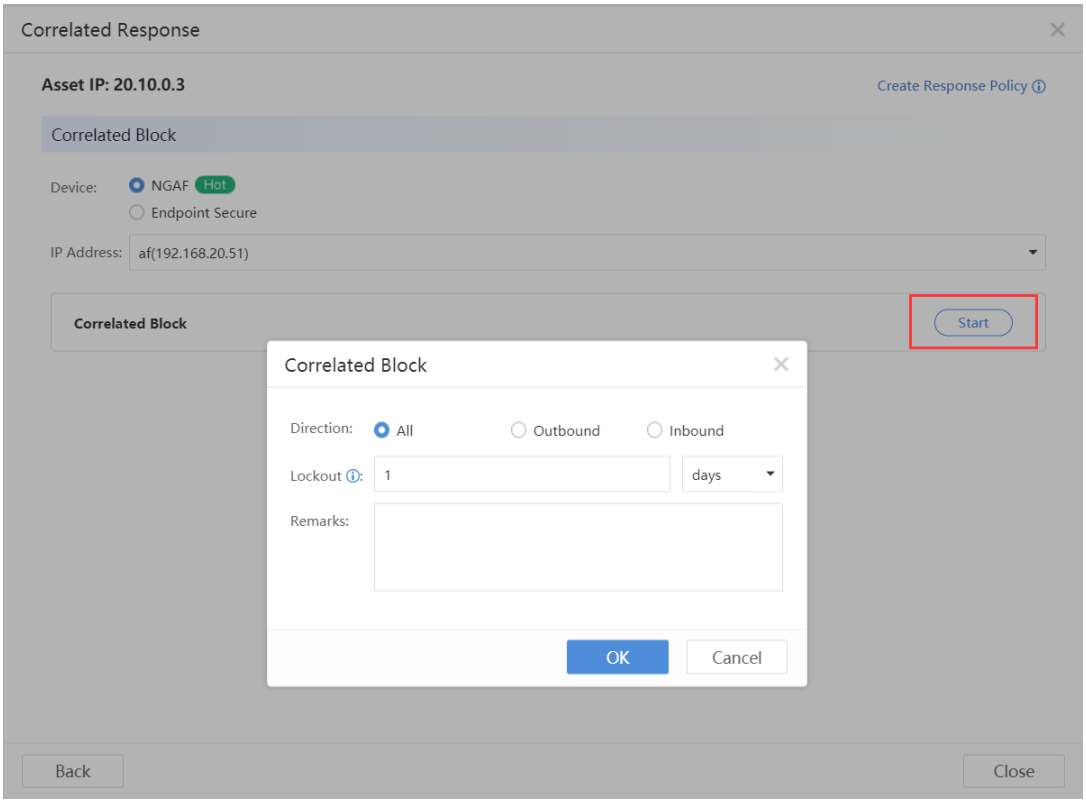
1. Klik Correlated Response.



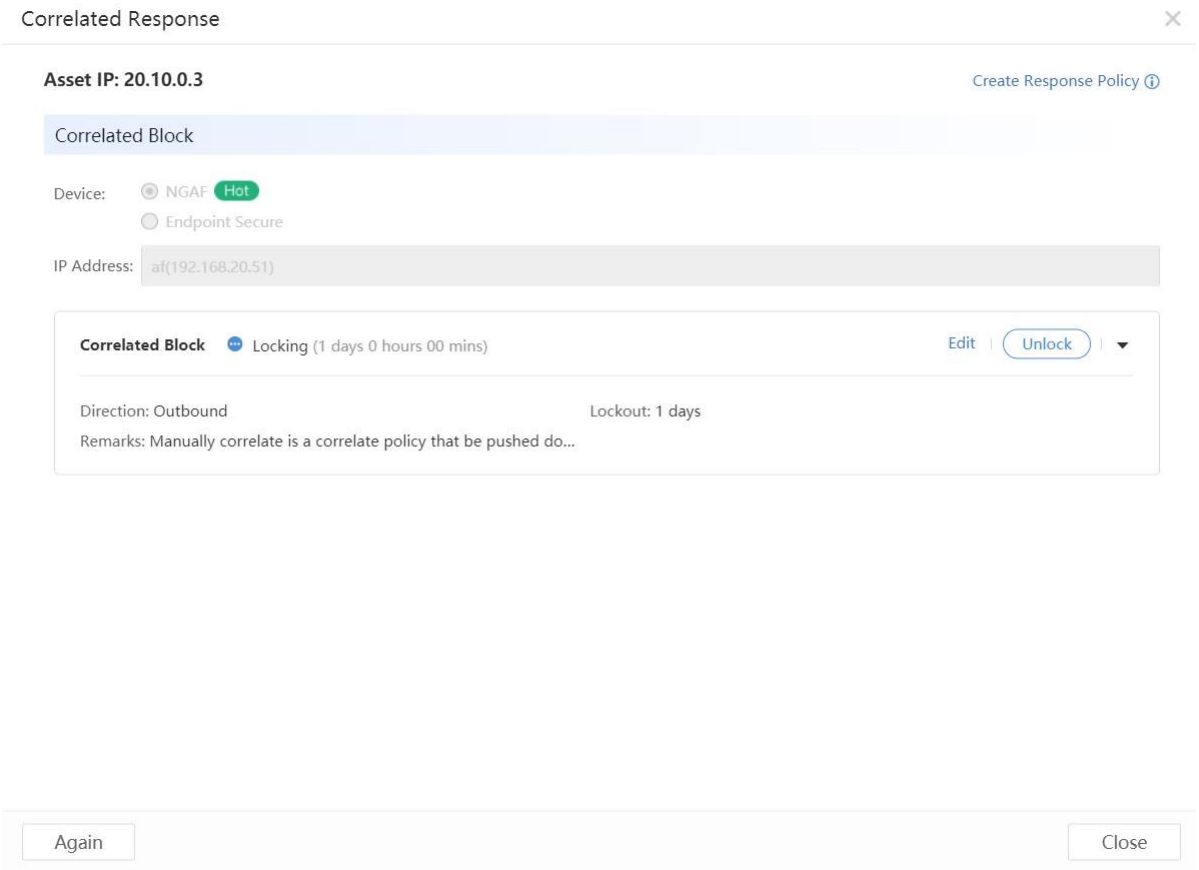
2. Pilih Correlated Response.



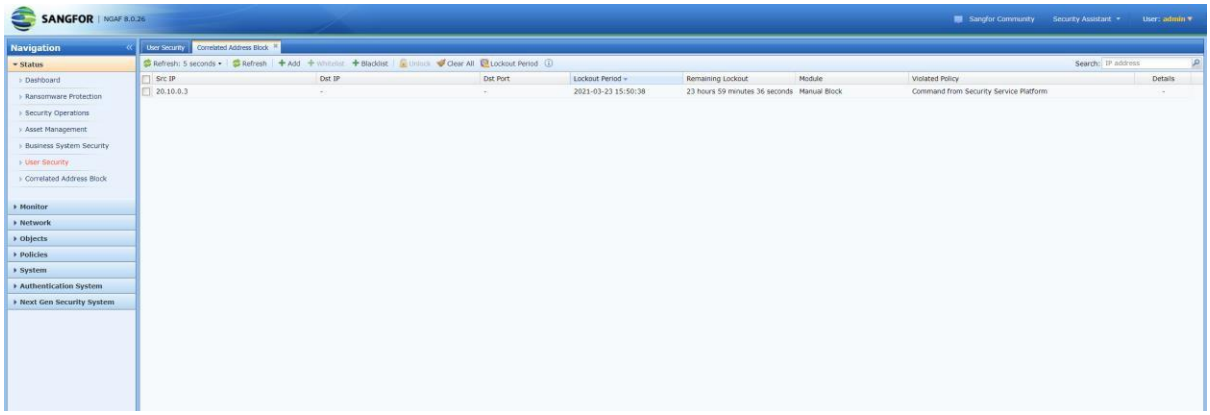
3. Klik Start dan atur waktu lockout, lalu klik OK.



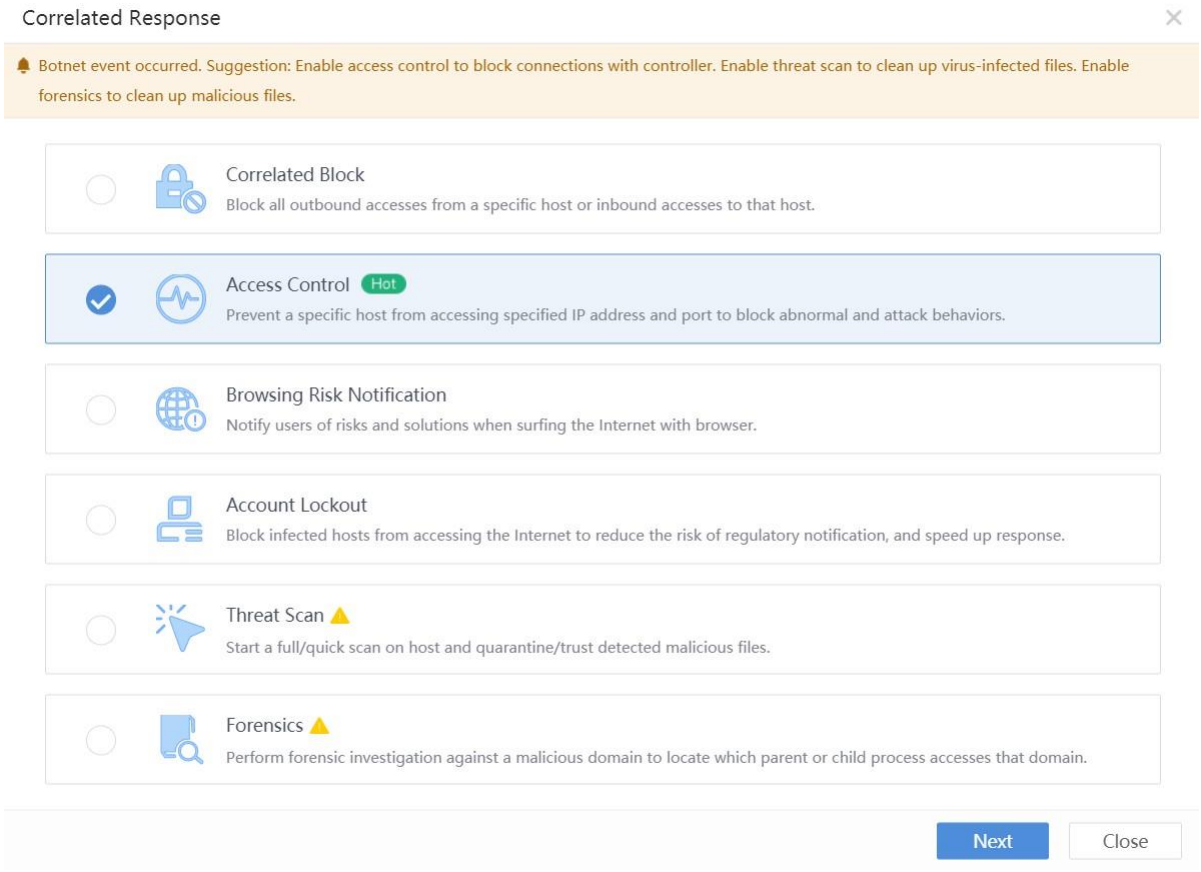
4. Setelah beberapa detik, Anda dapat melihat policy yang dikeluarkan berhasil.



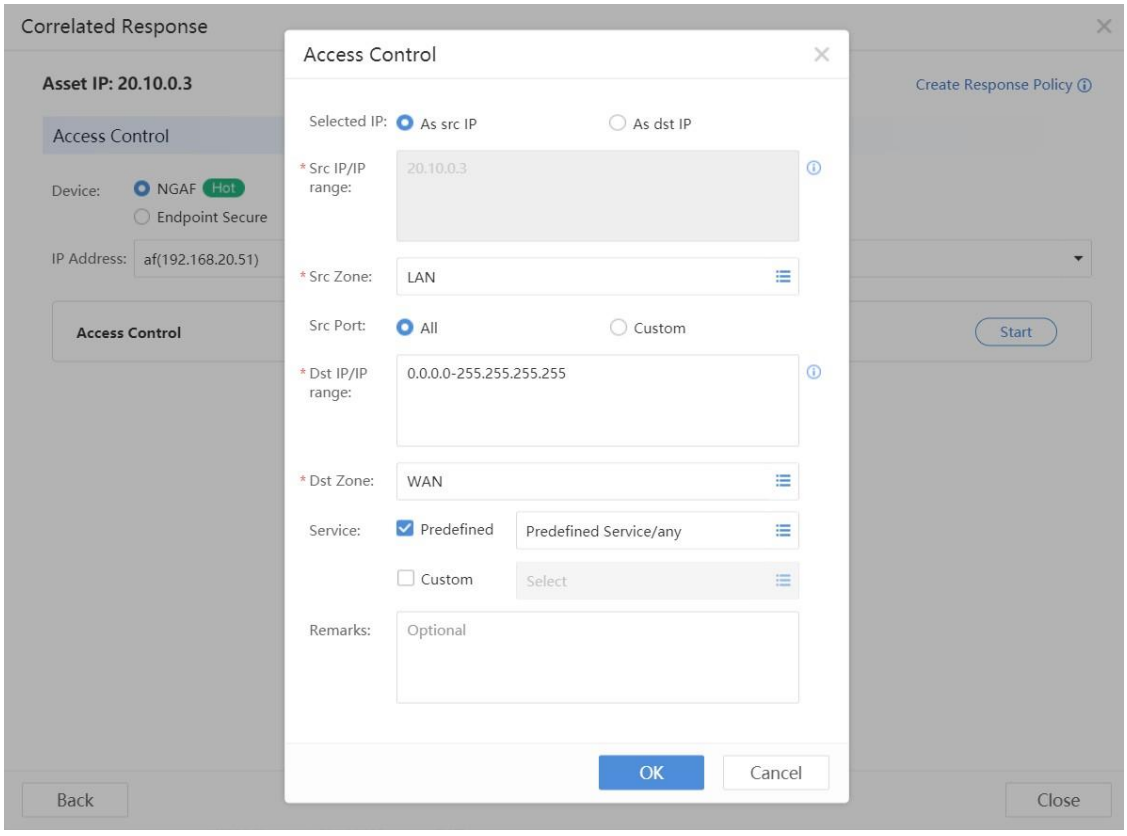
5. Anda dapat log in ke NGAF web console, dan pergi ke Status-> Correlated Address Block path, kemudian Anda dapat periksa IP yang diblokir oleh Cyber Command.



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



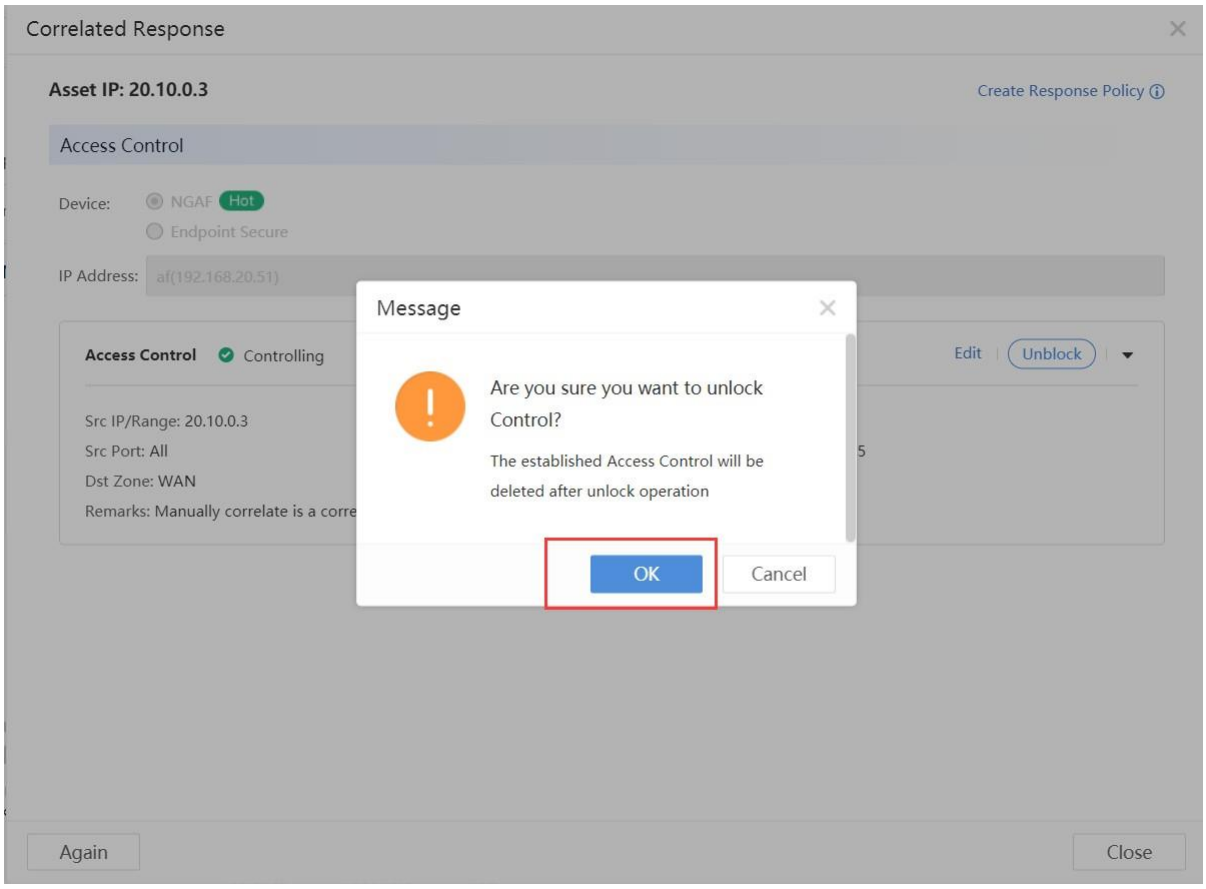
7. Klik Start dan konfigurasi Zone dan IP yang Anda ingin blokir.



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

berhasil.

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.