SANGFOR

CCOM Panduan Konfigurasi

Cyber Command dan Korelasi NGAF

Versi 3.0.48

Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Desember 2020	Panduan Konfigurasi Cyber Command dan NGAF Correlation.

DAFTAR ISI

Bab 1 Skenario Aplikasi

Hal ini juga diperlukan untuk menggunakan NGAF versi 8.0.23 atau versi yang lebih baru dan untuk memungkinkan TCP (4430) port untuk lalu lintas dari NGAF ke CCOM (Cyber Command) dan TCP (7443) port untuk lalu lintas dari CCOM ke NGAF. NGAF dapat mengunggah security logs (IPS, WAF dan botnet) dan control logs aplikasi dan akan mengaktifkan record logs pada NGAF untuk tujuan ini.

Bab 2 Panduan Konfigurasi

2.1 Konfigurasi Security Policy

Periksa konfigurasi untuk security protection policy untuk mendeteksi host yang disusupi.

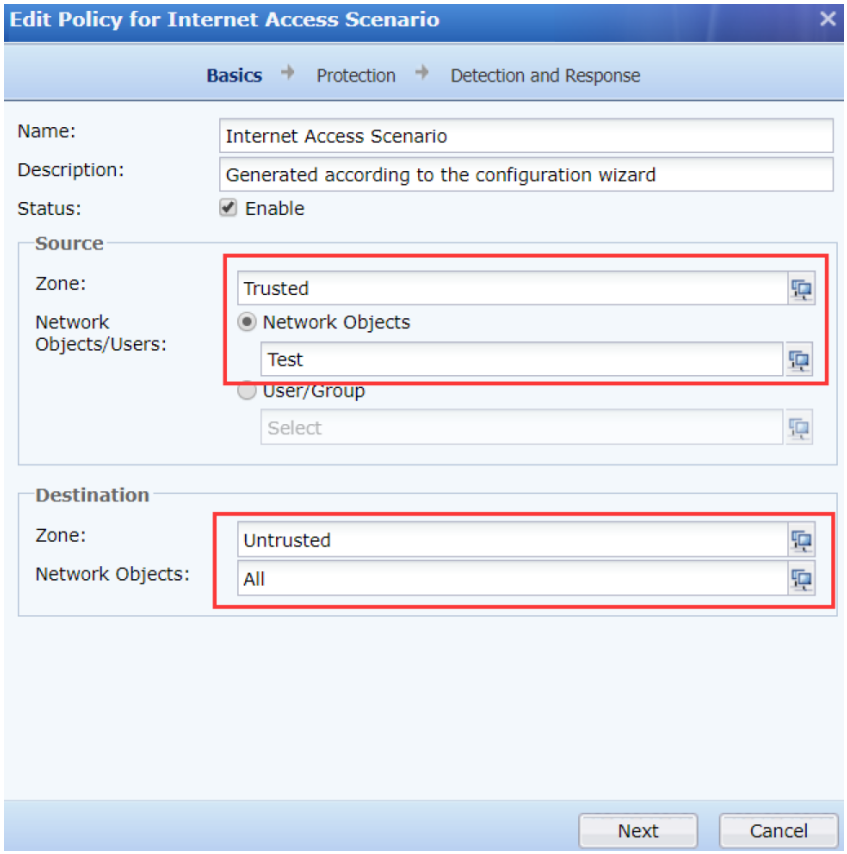
Alasan: Ketika host di LAN terinfeksi atau dalam kondisi abnormal, itu menyerang host lain di Internet atau LAN atau terlibat dalam perilaku tidak normal. Dalam hal ini, diperlukan untuk menambahkan reverse konfigurasi dari security policy pada NGAF untuk mendeteksi ketidaknormalan host di LAN dan kemudian mengunggah log ke CCOM untuk analisis host berisiko. Tindakan NGAF dapat dianulir, tetapi log harus dicatat.

Konfigurasi Akses Internet security policy memerlukan:

1. Klien memiliki STA di LAN, tetapi lalu lintas keluar host tidak dicitrakan ke STA. Oleh karena itu, lalu lintas dari area terpercaya ke area yang tidak dipercaya membutuhkan konfigurasi reverse security policy pada NGAF.
2. Klien tidak memiliki STA di LAN, sehingga lalu lintas keluar dari area terpercaya ke area yang tidak tepercaya memerlukan konfigurasi Akses Internet security policy pada NGAF.

Konfigurasi Akses Internet security policy tidak memerlukan:

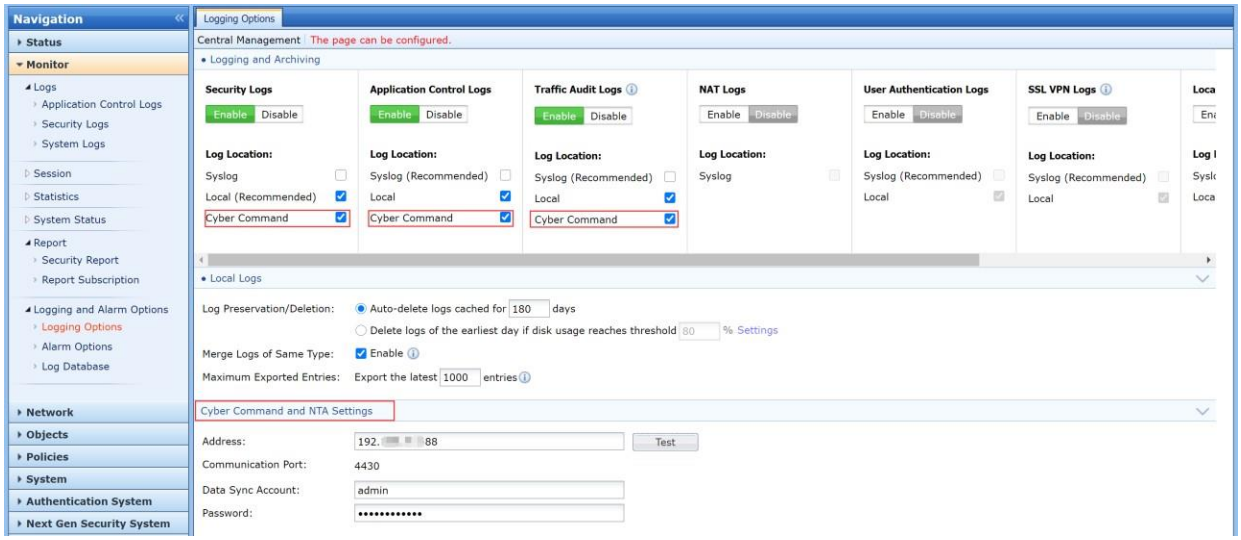
1. Karena STA telah mengumpulkan lalu lintas keluar dari host, itu tidak memerlukan



reverse konfigurasi policy pada NGAF bahkan jika lalu lintas juga melewati NGAF.

2.2 Sinkronisasi Log

Konfigurasi: Konfigurasikan alamat IP CCOM di halaman pengaturan log pada NGAF, seperti yang ditunjukkan di bawah ini:



Setelah konfigurasi pada NGAF, CCOM menambahkan NGAF ke dalam daftar device management nya secara otomatis, setiap kali ada log yang disinkronkan ke CCOM.

Sejalan dengan itu, perangkat juga mendukung otentikasi dua arah.

Tampilan log:

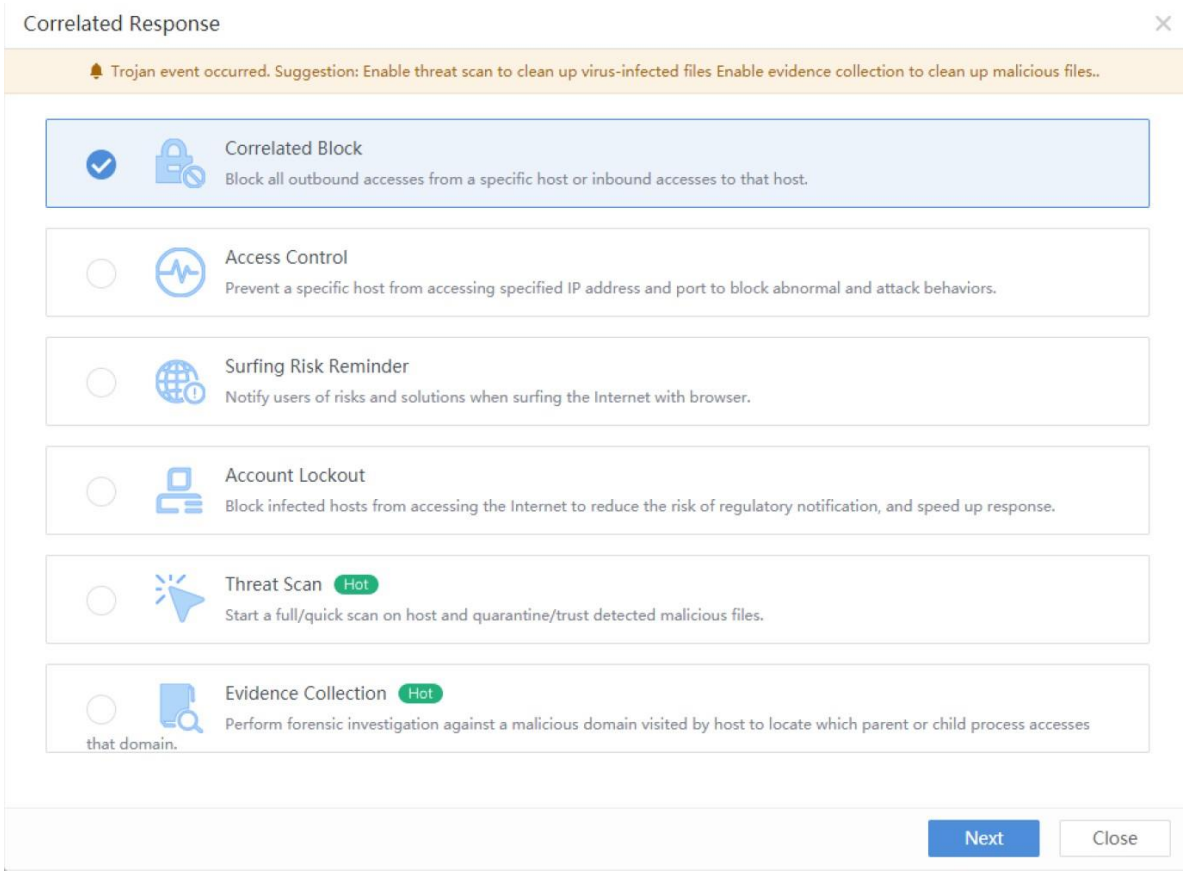
Sama seperti log yang disinkronkan ke STA.

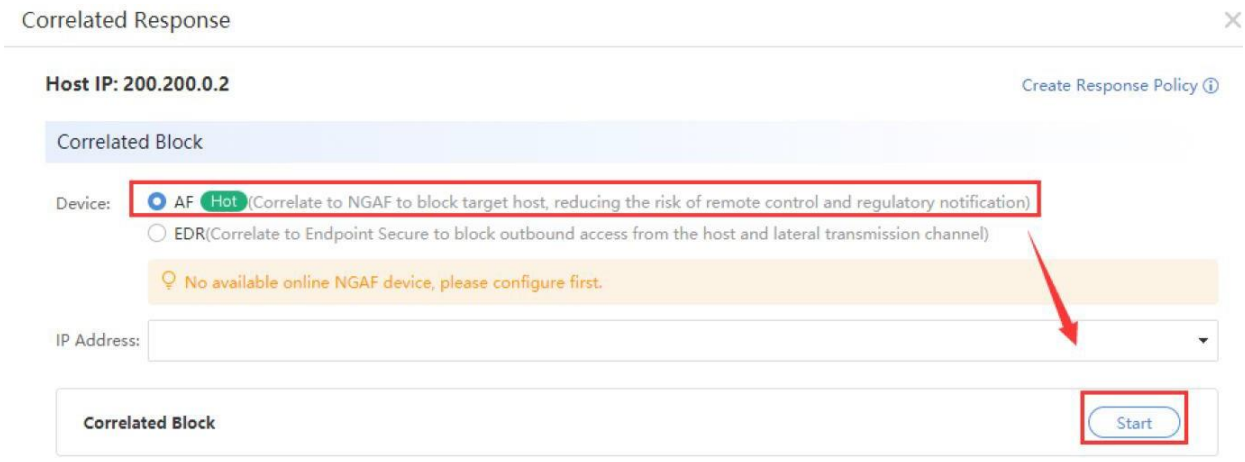
2.3 Correlation Policy

2.3.1 Correlated Block

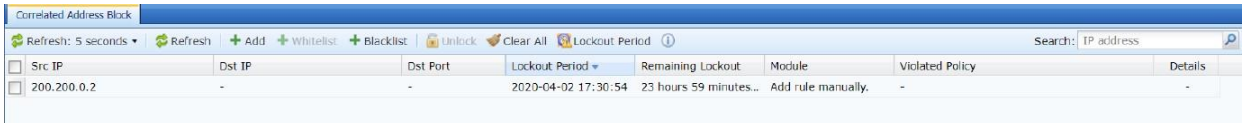
Temukan fungsi ini di platform :

1. Klik **Response -> Correlated Response** pada halaman Server beresiko atau Host beresiko.
2. Korelasi antara NGAF dan CCOM memiliki 2 tipe, termasuk **Correlated Block** dan **Access Control**.





Setelah korelasi berhasil, pilih Status -> Correlated Address Block pada NGAF untuk menampilkan IP yang diblokir.

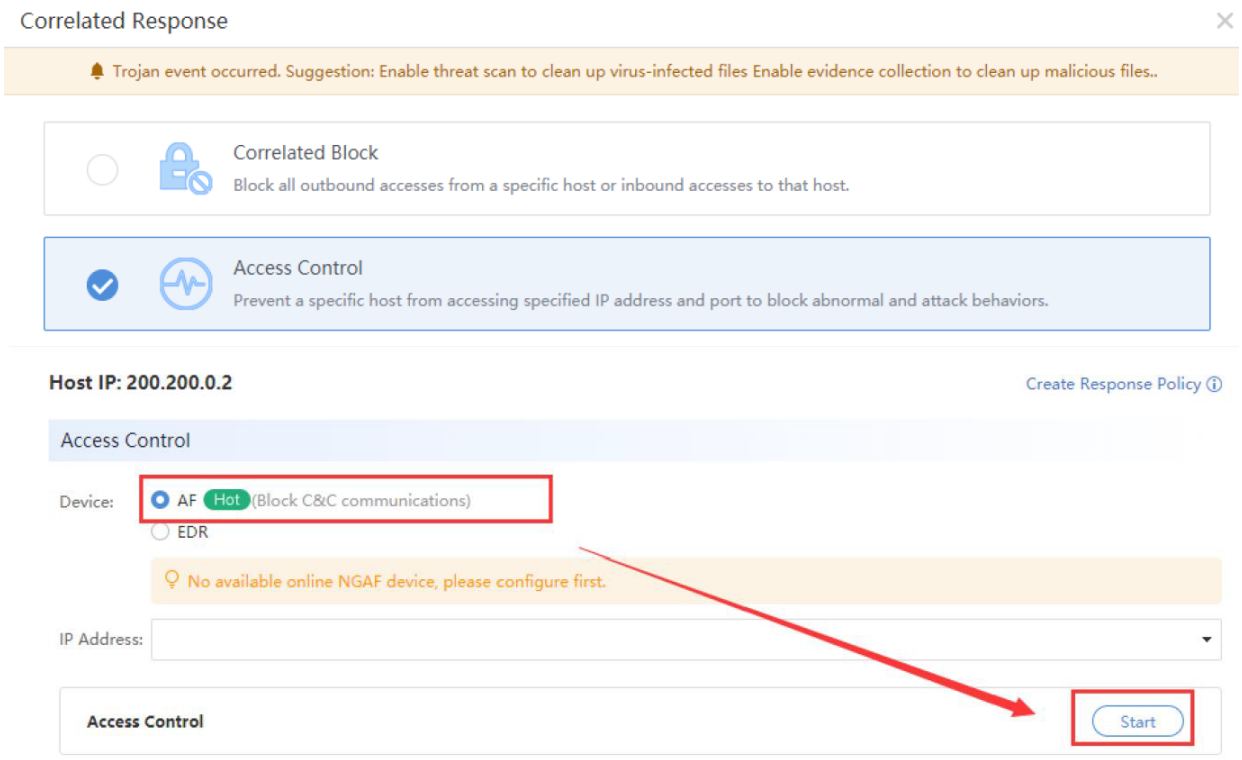


2.3.2Membuat Aplikasi Control Policy

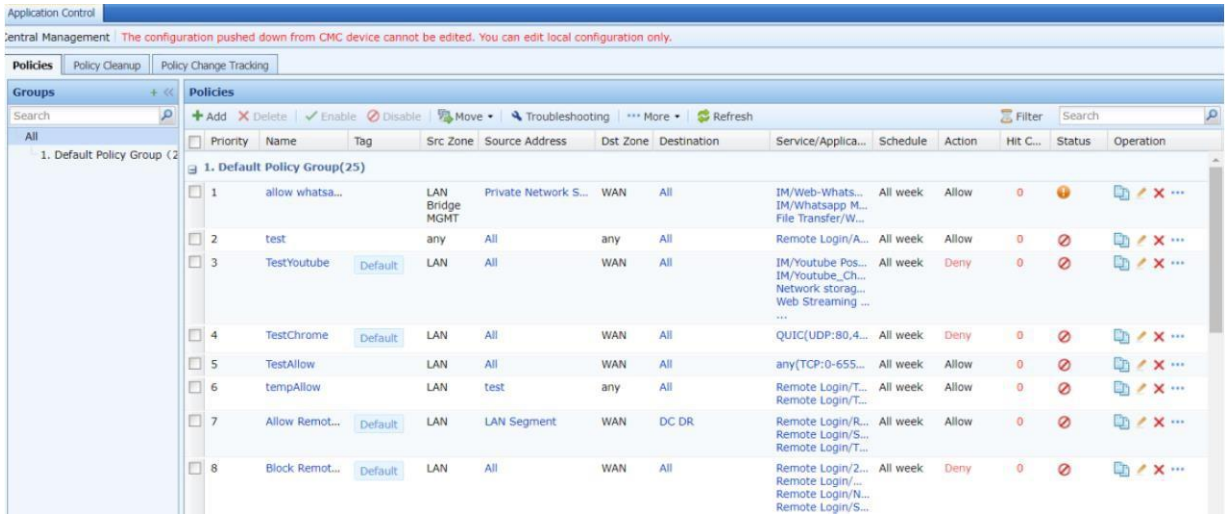
Temukan fungsi ini di platform :

1. Klik Response -> Correlated Response pada halaman Server beresiko atau Host beresiko.
2. Pilih Access Control

Operasi ini membutuhkan NGAF versi resmi 8.0.23.



Setelah berhasil dibuat, pilih **Policy** -> **Access Control** -> **Application Control Policy** pada



NGAF untuk menampilkan policy yang dibuat.