



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	1
Bab 2 Panduan Konfigurasi	1
2.1 Konfigurasi Security Policy.....	1
2.2 Sinkronisasi Log	2
2.3 Correlation Policy	3
2.3.1 Correlated Block.....	3
2.3.2 Membuat Aplikasi Control Policy	4

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 dipercaya 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.

CCOM Panduan Konfigurasi Versi 3.0.48
Sejalan dengan itu, perangkat juga mendukung otentikasi dua arah.

Tampilan log:

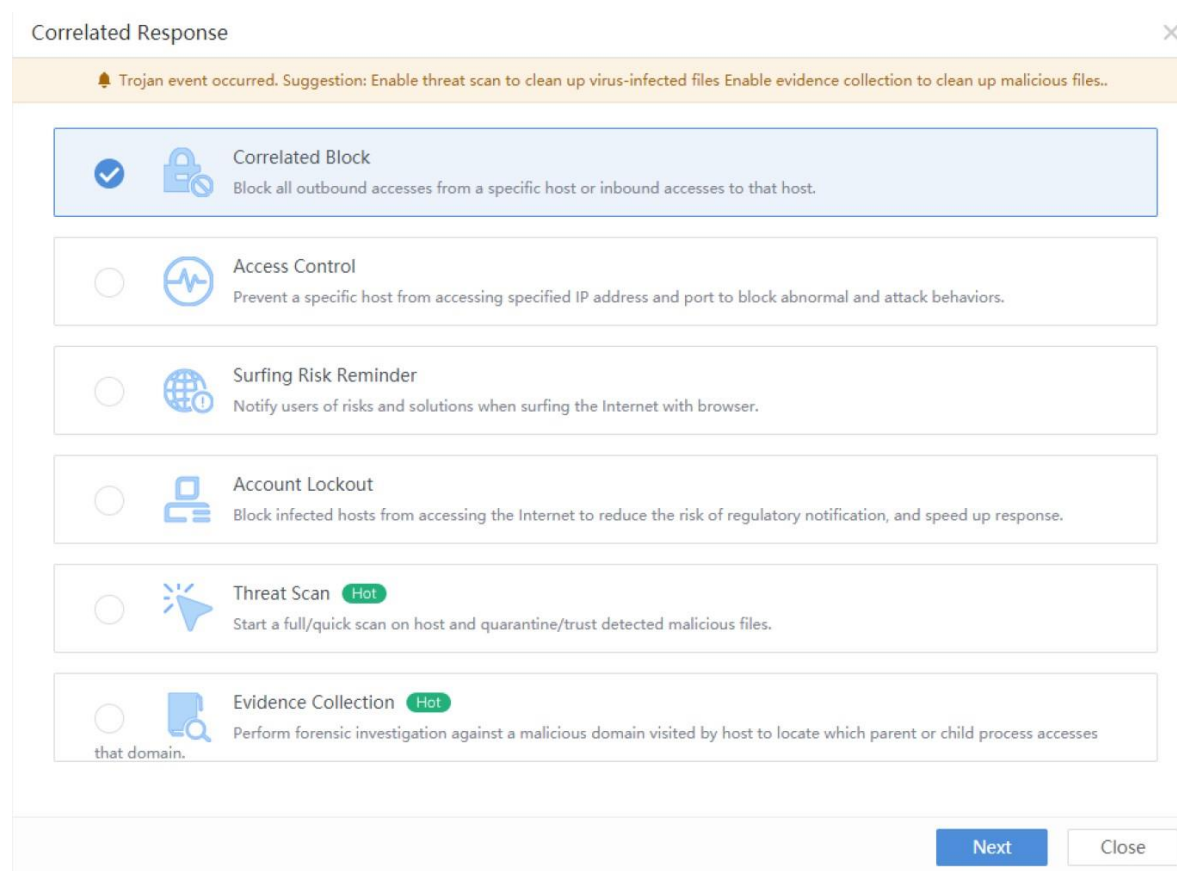
Sama seperti log yang disinkronkan ke STA.

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**.



Correlated Response ✕

Host IP: 200.200.0.2 Create Response Policy ⓘ

Correlated Block

Device: ☒ **AF Hot** (Correlate to NGAF to block target host, reducing the risk of remote control and regulatory notification)
☐ EDR (Correlate to Endpoint Secure to block outbound access from the host and lateral transmission channel)

♀ No available online NGAF device, please configure first.

IP Address:

Correlated Block Start

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

Correlated Address Block							
<div> Refresh: 5 seconds Refresh Add Whitelist Blacklist Unlock Clear All Lockout Period ⓘ Search: IP address </div>							
<input type="checkbox"/>	Src IP	Dst IP	Dst Port	Lockout Period	Remaining Lockout	Module	Violated Policy
<input type="checkbox"/>	200.200.0.2	-	-	2020-04-02 17:30:54	23 hours 59 minutes...	Add rule manually.	-

2.3.2 Membuat 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.

Trojan event occurred. Suggestion: Enable threat scan to clean up virus-infected files Enable evidence collection to clean up malicious files..



Correlated Block

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



Access Control

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

Host IP: 200.200.0.2

Create Response Policy

Access Control

Device: ☒ AF **Hot** (Block C&C communications)

☐ EDR

No available online NGAF device, please configure first.

IP Address:

Access Control

Start

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

Application Control

Central Management

The configuration pushed down from CMC device cannot be edited. You can edit local configuration only.

Policies

Policy Cleanup

Policy Change Tracking

Groups

Search

All

1. Default Policy Group (2)

Policies

Filter

Search

	Priority	Name	Tag	Src Zone	Source Address	Dst Zone	Destination	Service/Applica...	Schedule	Action	Hit C...	Status	Operation
1. Default Policy Group(25)													
<input type="checkbox"/>	1	allow whatsa...		LAN	Private Network S...	WAN	All	IM/Web-Whats... IM/Whatsapp M... File Transfer/W...	All week	Allow	0		
<input type="checkbox"/>	2	test		any	All	any	All	Remote Login/A...	All week	Allow	0		
<input type="checkbox"/>	3	TestYoutube	Default	LAN	All	WAN	All	IM/Youtube Pos... IM/Youtube_Ch... Network storag... Web Streaming ...	All week	Deny	0		
<input type="checkbox"/>	4	TestChrome	Default	LAN	All	WAN	All	QUIC(UDP:80,4...	All week	Deny	0		
<input type="checkbox"/>	5	TestAllow		LAN	All	WAN	All	any(TCP:0-655...	All week	Allow	0		
<input type="checkbox"/>	6	tempAllow		LAN	test	any	All	Remote Login/T... Remote Login/T...	All week	Allow	0		
<input type="checkbox"/>	7	Allow Remot...	Default	LAN	LAN Segment	WAN	DC DR	Remote Login/R... Remote Login/S... Remote Login/T...	All week	Allow	0		
<input type="checkbox"/>	8	Block Remot...	Default	LAN	All	WAN	All	Remote Login/2... Remote Login/... Remote Login/N... Remote Login/S...	All week	Deny	0		

NGAF untuk menampilkan policy yang dibuat.



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