



NGAF

Panduan terbaik untuk Skenario NGAF Access to Cyber Command Guide

Versi 8.0.17



Data Perubahan

Tanggal	Keterangan Perubahan
Nov 1, 2020	Rilis Dokumen
May 17, 2021	Pembaruan dokumen Versi 12.0.42.

DAFTAR ISI

BAB 1 Konfigurasi Dasar	1
BAB 2 Konfigurasi.....	1

BAB 1 Konfigurasi Dasar

1. Komunikasi antar port NGAF dan Cyber Command adalah sebagai berikut:

Cyber Command	NGAF accesses TCP port 4430 of CC CC accesses TCP port 7443 of NGAF	Konfigurasi Satu-arah untuk NGAF (standar) konfigurasi Dua-arah untuk NGAF+CC (Keamanan yang tinggi)	NGAF dapat mengunggah botnet dan backdoor webshell. Ketika peretas membuat tautan keamanan pada CC, yang dapat berkorelasi dengan NGAF untuk pemblokiran ancaman dan kontrol aplikasi.
---------------	--	---	--

BAB 2 Konfigurasi

Langkah konfigurasi adalah sebagai berikut (perlu dipastikan koneksi jaringan antara Cyber Command dan NGAF):

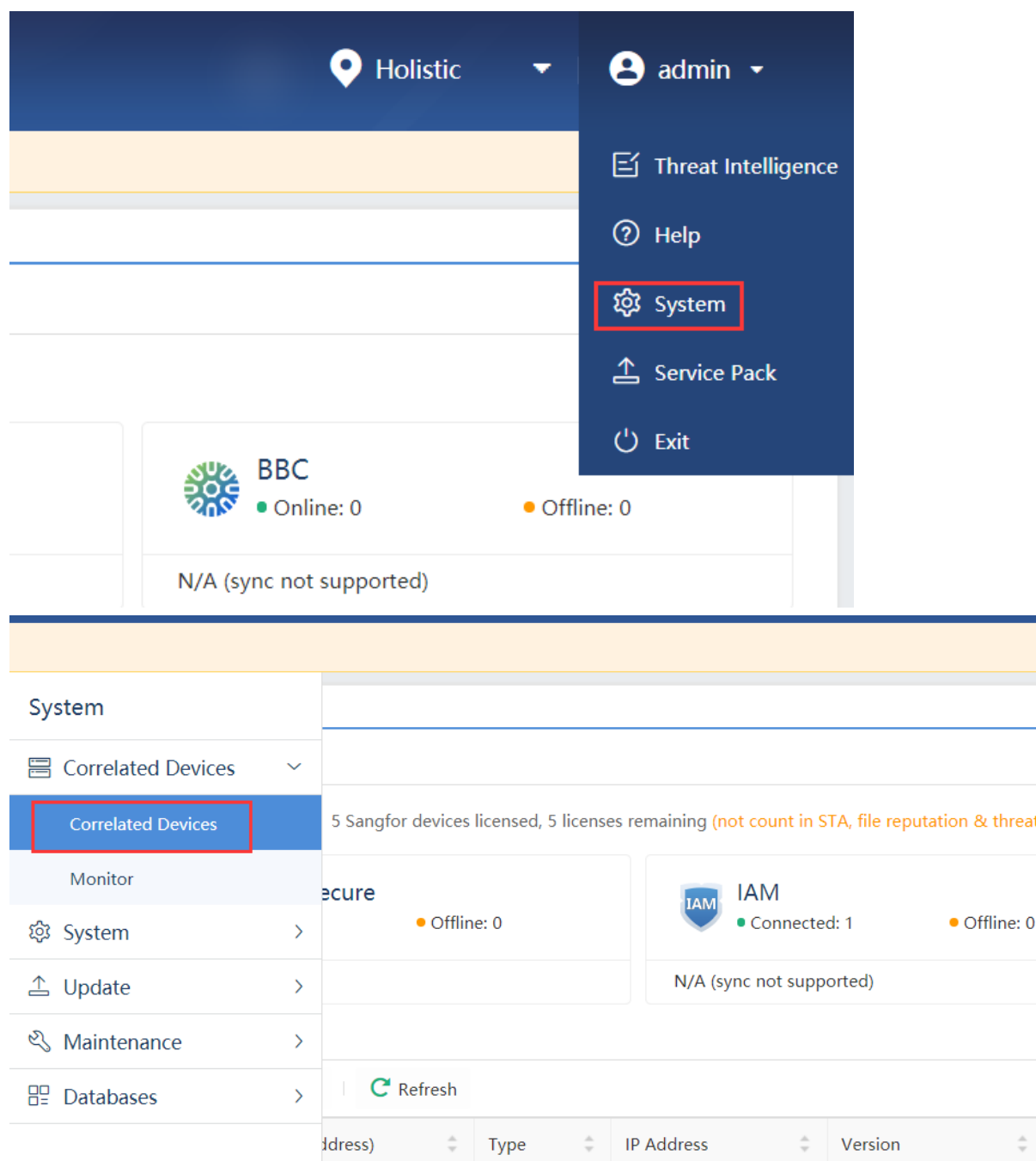
1. Konfigurasi pertama informasi perihal Cyber Command pada NGAF dan simpan.

The screenshot displays the 'Logging Options' configuration page in the Sangfor NGAF 8.0.26 web interface. The 'Cyber Command and NTA Settings' section is highlighted with a red box. It contains the following fields:

- Address: 192.168.20.188
- Communication Port: 4430
- Data Sync Account: admin
- Password: *****

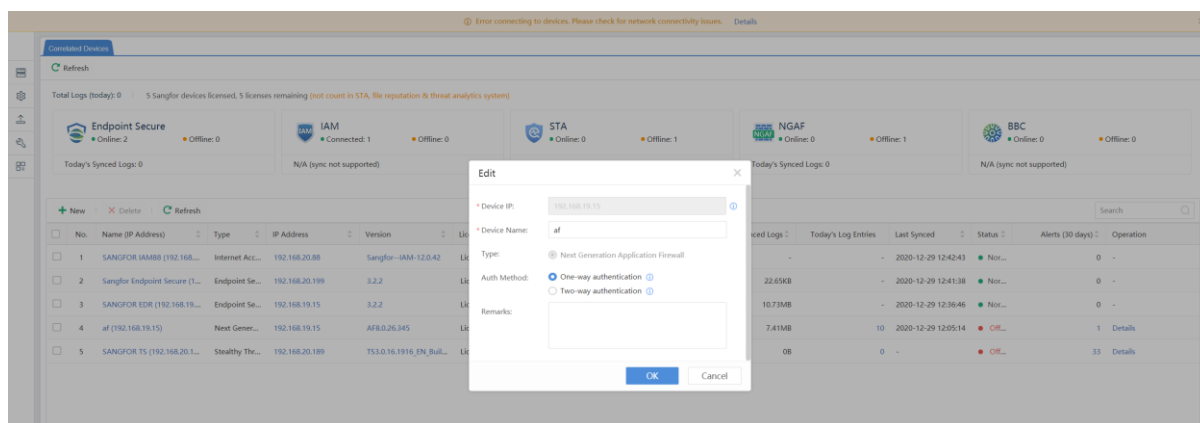
Below these fields is a 'Test' button and a 'Save' button at the bottom of the section.

2. Setelah NGAF melakukan sinkronisasi informasi dari Cyber Command, pada halaman "Correlated Devices" pada Cyber Command akan secara otomatis menambahkan Cyber Command ii. Metoda autentikasi di sisi Cyber Command adalah autentikasi satu-arah secara default.



3. Jika autentikasi akun dan kata kunci telah terkonfigurasi pada NGAF, setelah NGAF sinkronisasi informasi autentikasi ke Cyber Command, Pada dasarnya autentikasi pada Cyber Command tidak akan mempengaruhi fungsi ini.

Best Practice_NGAF Access to Cyber Command Guide



4. Jika anda ingin memperkuat tingkat keamanan, anda dapat menyunting metoda autentikasi dari perangkat NGAF pada sisi Cyber Command; autentikasi dua-arah. Dan pastikan autentikasi akun dan kata kunci pada kedua sisi yang dikonfigur supaya konsisten.

