SANGFOR

Sangfor NGAF

Pedoman terbaik untuk Scenarios_NGAF Correlate with Endpoint Scure to Anti Proxy Tools

Produk Versi	9.0.38
Dokumen Versi	1.0
Rilis pada	Jun. 19, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

Data Perubahan

Tanggal	Keterangan Perubahan
Jun. 19, 2021	Dokumen ini adalah rilis paling pertama.

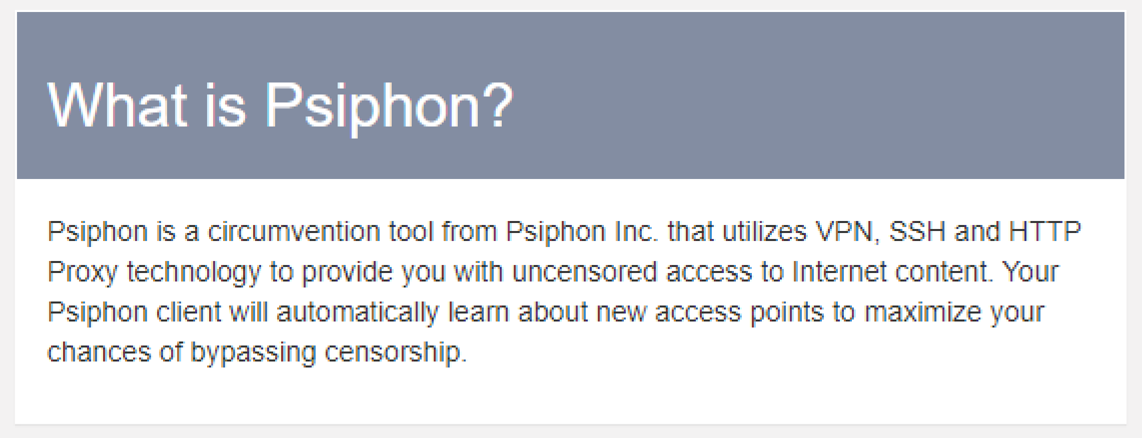
DAFTAR ISI

1 Skenario

1.1 Pengenalan Skenario

Kebanyakan para pengguna menggunakan alat VPN untuk mengakses aplikasi yang tidak diperbolehkan oleh admin jaringan, seperti situs pornografi dan darkweb. Selain itu, penggunaan alat VPN dapat menyebabkan kebocoran informasi dan prilaku jahat yang tidak dapat di audit. Untuk admin jaringan, alat VPN ini perlu diblokir.

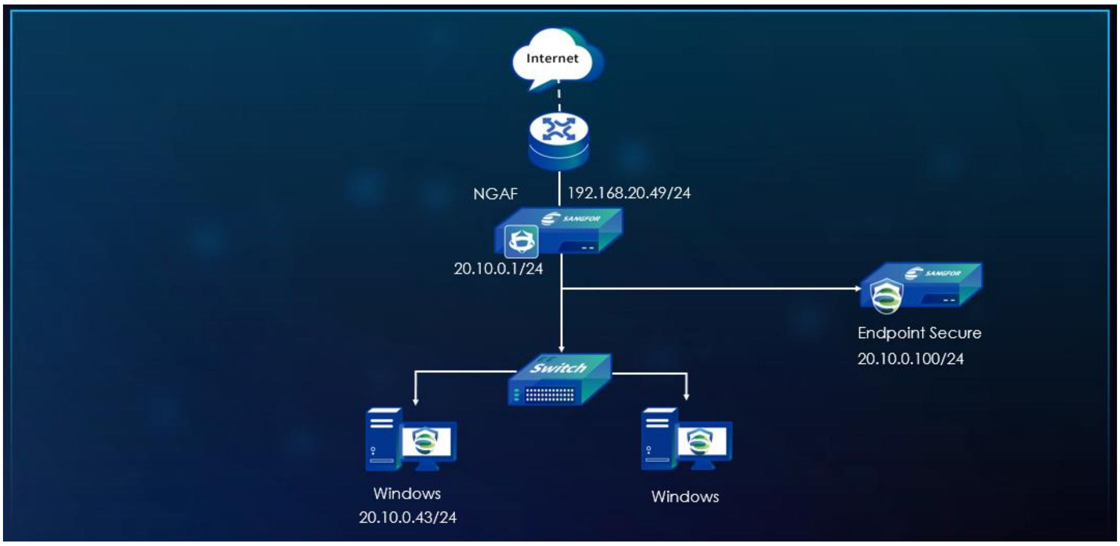
Secara tradisional, metoda anti-proxy akan melakukan blokir nama domain dan IP yang berhubungan dengan proxy-tool tersebut didalam dimensi dari lalulintas jaringan, akan tetapi pada umumnya tidaklah maksimal. Seperti yang diklaim oleh beberapa piranti proxy, lalu lintas disamarkan sebagai SSH standar, protokol HTTP dan protokol DNS untuk terlewat dari diteksi keamanan piranti lunak, dan beberapa piranti lunak proxy menempatkan server pada publik cloud, memblokir IP akan menyebabkan situs web normal menjadi terblokir. Oleh karena itu, diperlukan cara yang lebih baik untuk mencegah alat proxy, yaitu, melalui NGAF dan ES, secara langsung memblokir pengoperasian alat proxy terkait proses.



What is Psiphon?

Psiphon is a circumvention tool from Psiphon Inc. that utilizes VPN, SSH and HTTP Proxy technology to provide you with uncensored access to Internet content. Your Psiphon client will automatically learn about new access points to maximize your chances of bypassing censorship.

1.2 Topologi



1.3 Kondisi Pengujian

1. Versi dari NGAF harus versi 8.0.39 dan lebih barunya

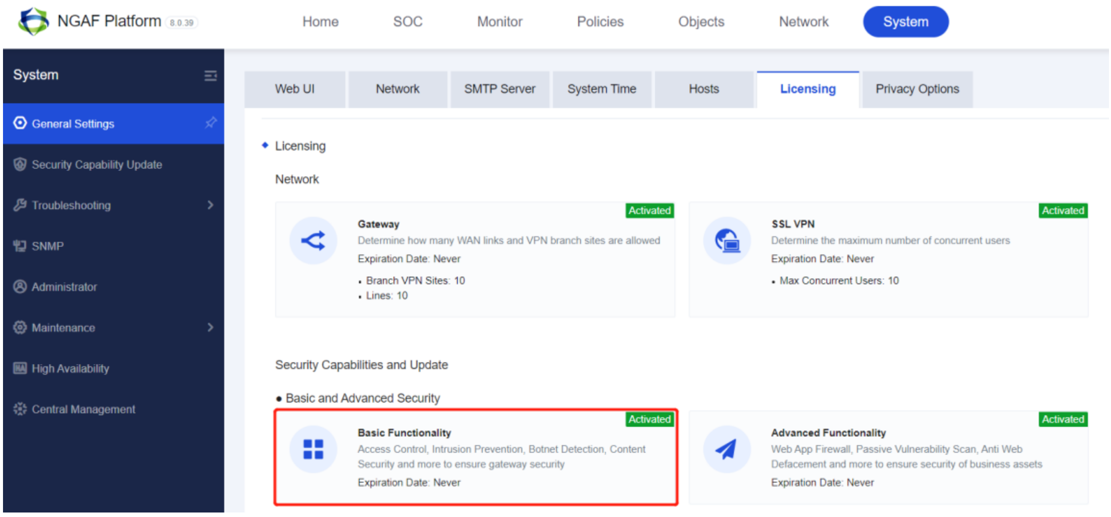
2. Endpoint Secure perlu mengunakan versi 3.5.5 dan lebih barunya

2 Rekomendasi Pedoman Terbaik

2.1 Konfigurasi Policy pada NGAF

2.1.1 Periksa Lisensi dan Database

1. Periksa apakah lisensi application control telah diaktifkan. Fungsi Anti-Proxy memerlukan penggunaan application control, dimana memerlukan otorisasi yang relevan untuk diaktifkan



Licensing

Network

Gateway — Activated
Determine how many WAN links and VPN branch sites are allowed
Expiration Date: Never
- Branch VPN Sites: 10
- Lines: 10

SSL VPN — Activated
Determine the maximum number of concurrent users
Expiration Date: Never
- Max Concurrent Users: 10

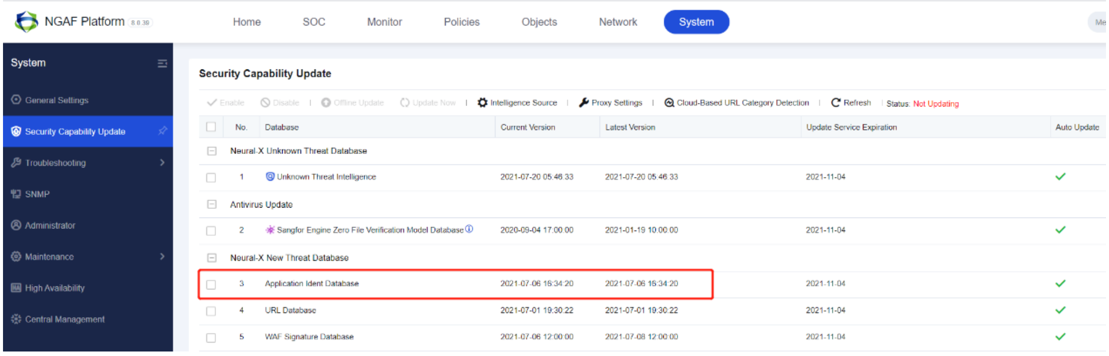
Security Capabilities and Update

- Basic and Advanced Security

Basic Functionality — Activated
Access Control, Intrusion Prevention, Botnet Detection, Content Security and more to ensure gateway security
Expiration Date: Never

Advanced Functionality — Activated
Web App Firewall, Passive Vulnerability Scan, Anti Web Defacement and more to ensure security of business assets
Expiration Date: Never

2. Periksa apakah database telah diperbarui hingga tanggal terbaru. Database terbaru akan membantu pencapaian Anti-Proxy yang lebih baik.

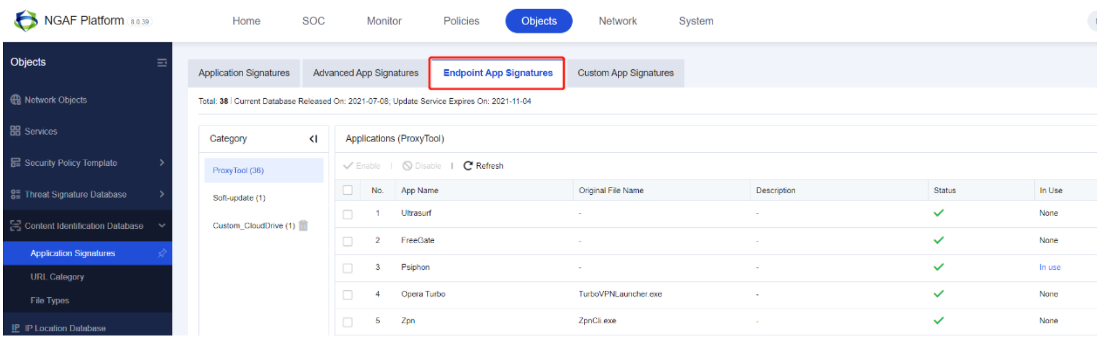


Security Capability Update

Status: Not Updating

No.	Database	Current Version	Latest Version	Update Service Expiration	Auto Update
Neural-X Unknown Threat Database					
1	Unknown Threat Intelligence	2021-07-20 05:46:33	2021-07-20 05:46:33	2021-11-04	✓
Antivirus Update					
2	Sangfor Engine Zero File Verification Model Database	2020-09-04 17:00:00	2021-01-19 10:00:00	2021-11-04	✓
Neural-X New Threat Database					
3	Application Ident Database	2021-07-06 16:34:20	2021-07-06 16:34:20	2021-11-04	✓
4	URL Database	2021-07-01 19:30:22	2021-07-01 19:30:22	2021-11-04	✓
5	WAF Signature Database	2021-07-06 12:00:00	2021-07-08 12:00:00	2021-11-04	✓

3. Periksa fitur Aplikasi dalam daftar pusaka dalam application control. Disini anda dapat melihat alat proxy yang didukung NGAF untuk manajemen dan kontrol.



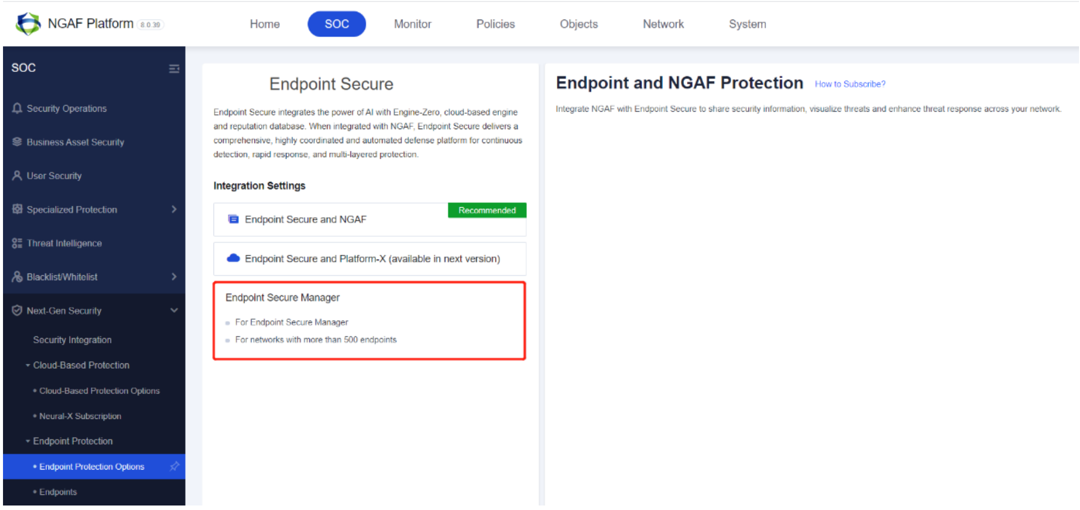
Total: 38 | Current Database Released On: 2021-07-08; Update Service Expires On: 2021-11-04

Applications (ProxyTool)

No.	App Name	Original File Name	Description	Status	In Use
1	Ultrasurf	-	-	✓	None
2	FreeGate	-	-	✓	None
3	Psiphon	-	-	✓	In use
4	Opera Turbo	TurboVPNLauncher.exe	-	✓	None
5	Zpn	ZpnCli.exe	-	✓	None

2.1.2 Korelasi NGAF dengan Endpoint Secure

1. Koneksi NGAF ke Endpoint Secure.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Integration Settings

Endpoint Secure and NGAF

Endpoint Secure and Platform-X (available in next version)

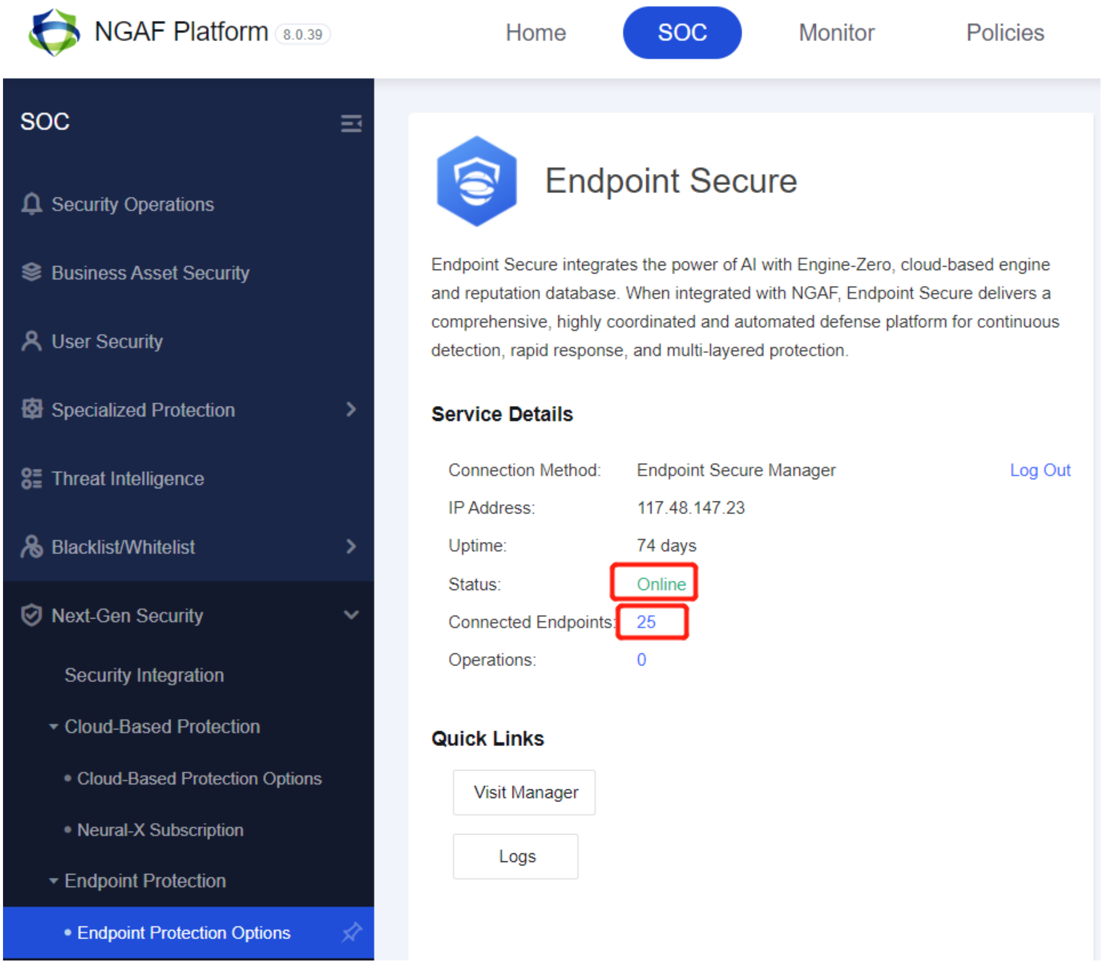
Endpoint Secure Manager

- For Endpoint Secure Manager
- For networks with more than 500 endpoints

Endpoint and NGAF Protection

Integrate NGAF with Endpoint Secure to share security information, visualize threats and enhance threat response across your network.

2. Jika korelasi NGAF dengan Endpoint Security berhasil, anda dapat melihat endpoint dalam NGAF dan status koneksi.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Service Details

Connection Method: Endpoint Secure Manager

IP Address: 117.48.147.23

Uptime: 74 days

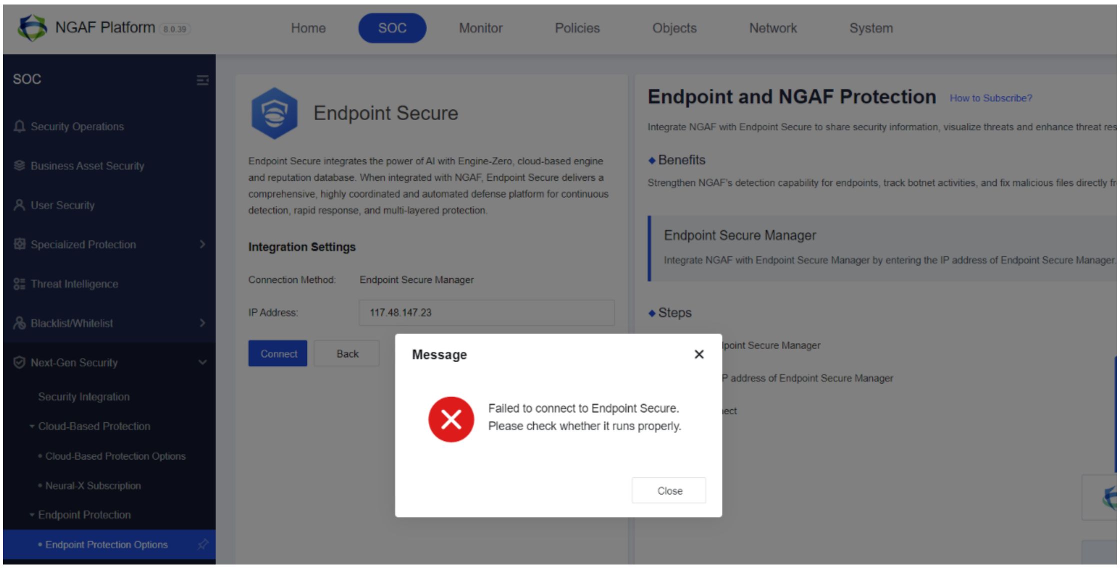
Status: Online

Connected Endpoints: 25

Operations: 0

Catatan:

1. Saat NGAF terhubung ke Endpoint Security, pesan kesalahan berikut akan muncul. Ini disebabkan ijin akses perangkat belum diaktifkan pada Endpoint Security.



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

Integration Settings

Connection Method: Endpoint Secure Manager

IP Address: 117.48.147.23

Message

Failed to connect to Endpoint Secure.
Please check whether it runs properly.

Endpoint and NGAF Protection

Integrate NGAF with Endpoint Secure to share security information, visualize threats and enhance threat res

◆ Benefits

Strengthen NGAF's detection capability for endpoints, track botnet activities, and fix malicious files directly fr

Endpoint Secure Manager

Integrate NGAF with Endpoint Secure Manager by entering the IP address of Endpoint Secure Manager.

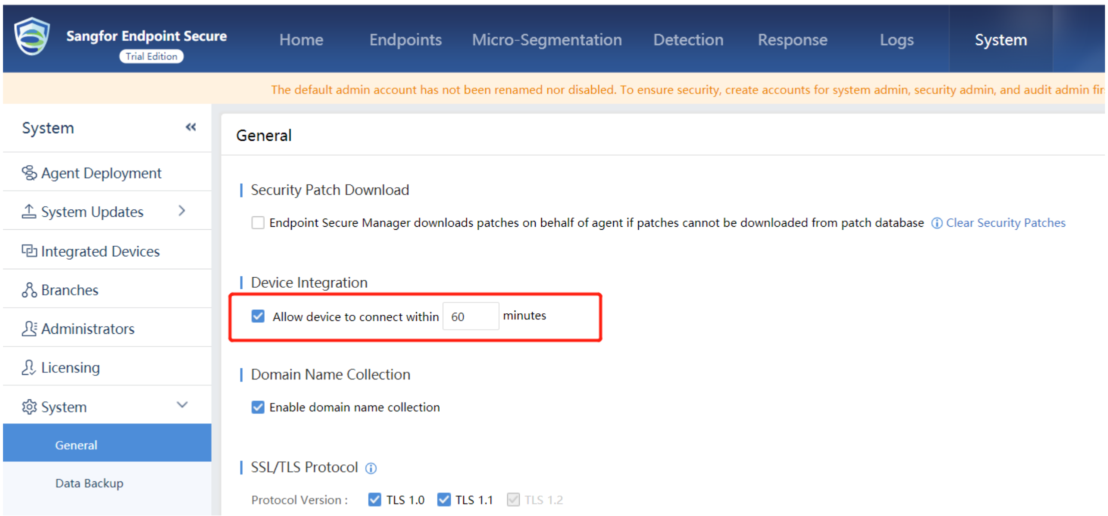
◆ Steps

dpoint Secure Manager

P address of Endpoint Secure Manager

ect

2. Perlu mengaktifkan opsi Device Integration.



The default admin account has not been renamed nor disabled. To ensure security, create accounts for system admin, security admin, and audit admin fir

General

Security Patch Download

□ Endpoint Secure Manager downloads patches on behalf of agent if patches cannot be downloaded from patch database ⓘ Clear Security Patches

Device Integration

☑ Allow device to connect within 60 minutes

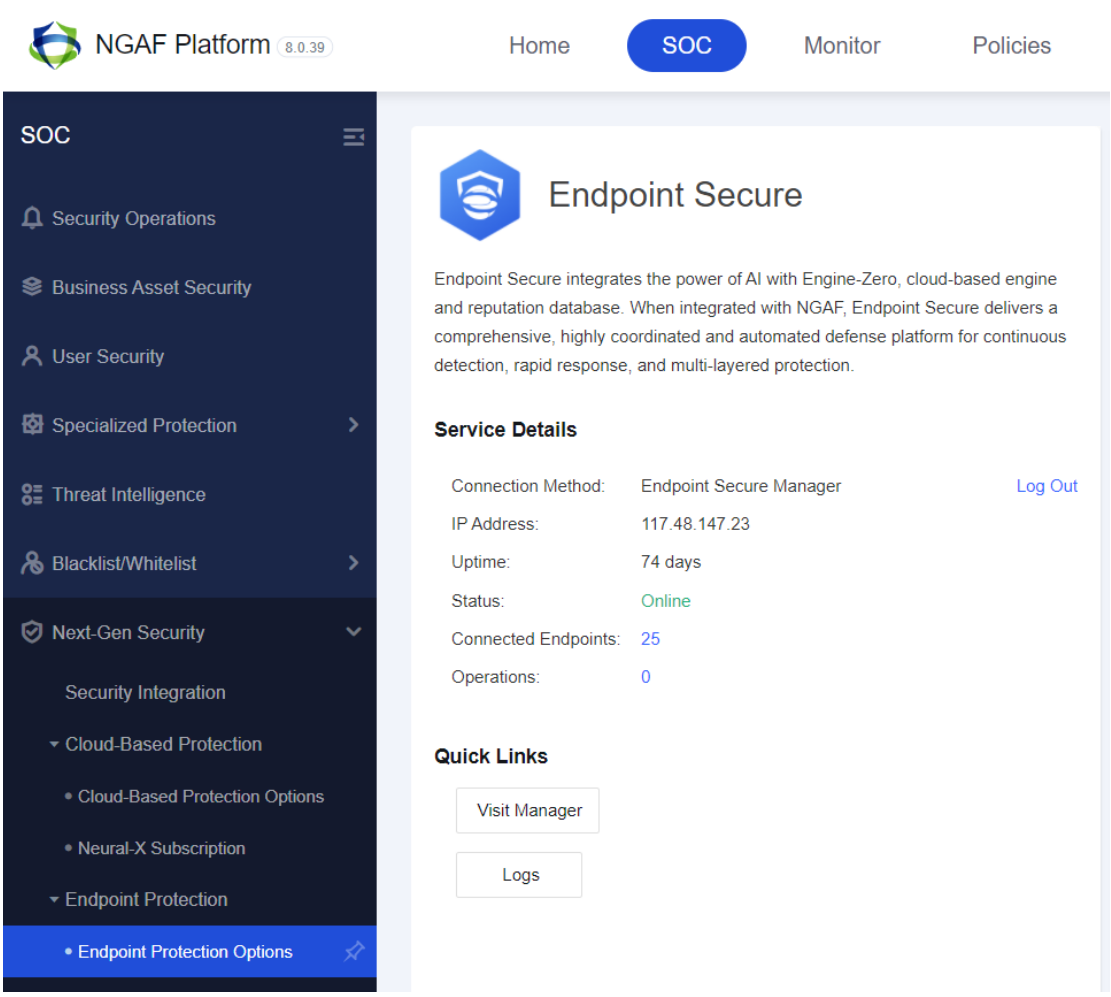
Domain Name Collection

☑ Enable domain name collection

SSL/TLS Protocol ⓘ

Protocol Version : ☑ TLS 1.0 ☑ TLS 1.1 ☑ TLS 1.2

3. Lalu akses Endpoint Secure dari NGAF



Endpoint Secure

Endpoint Secure integrates the power of AI with Engine-Zero, cloud-based engine and reputation database. When integrated with NGAF, Endpoint Secure delivers a comprehensive, highly coordinated and automated defense platform for continuous detection, rapid response, and multi-layered protection.

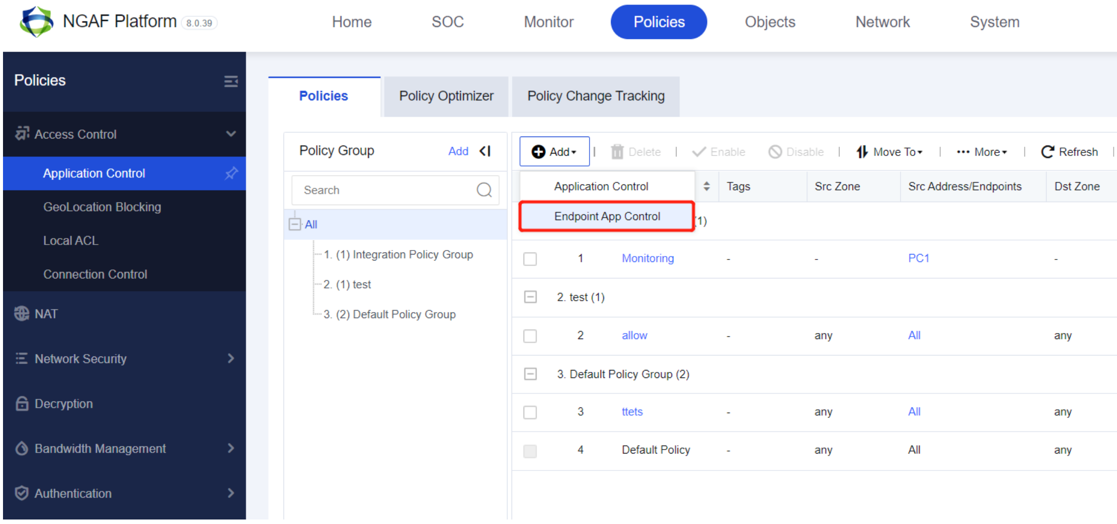
Service Details

Connection Method: Endpoint Secure Manager Log Out
IP Address: 117.48.147.23
Uptime: 74 days
Status: Online
Connected Endpoints: 25
Operations: 0

Quick Links

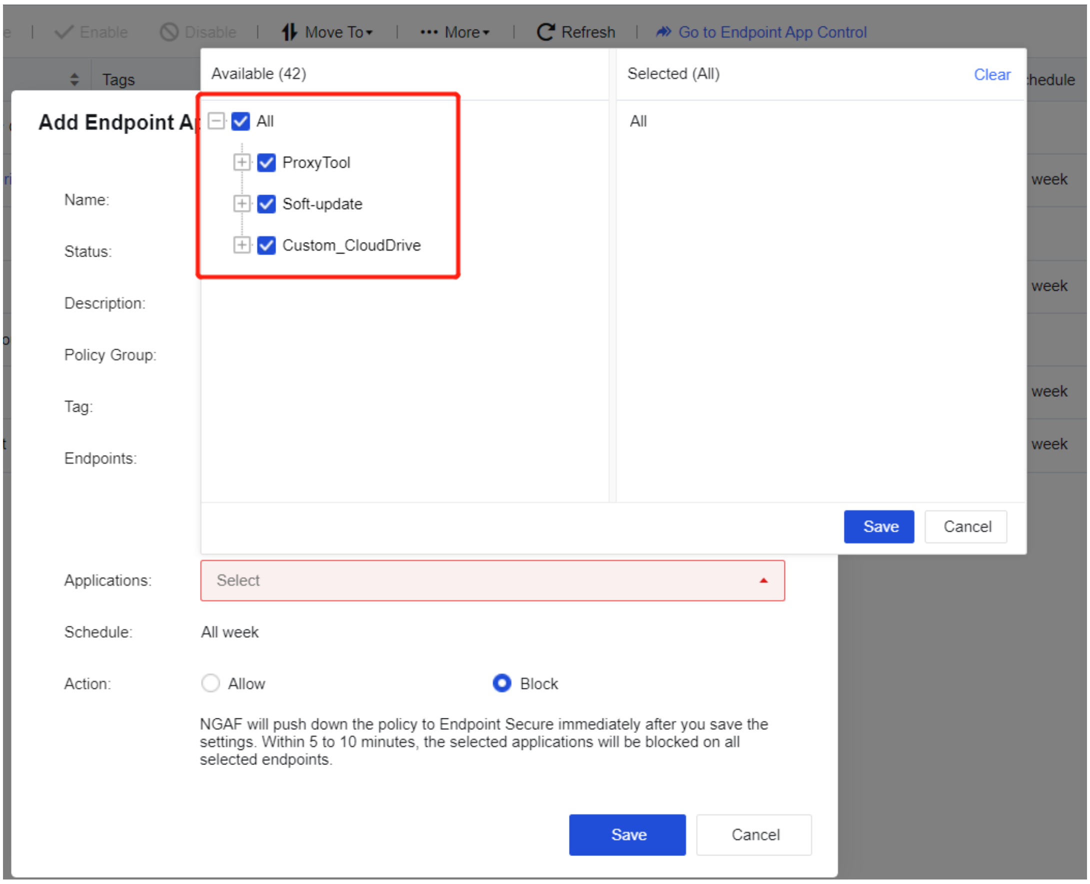
2.1.3 Konfigurasi Endpoint App Control Policy

1. Pada halaman Policies > Access Control > Application Control, Klik Add dan pilih Endpoint App Control



		Tags	Src Zone	Src Address/Endpoints	Dst Zone
1	Monitoring	-	-	PC1	-
2. test (1)					
2	allow	-	any	All	any
3. Default Policy Group (2)					
3	ttets	-	any	All	any
4	Default Policy	-	any	All	any

2. Pilih App yang ingin anda blok.



Add Endpoint A

Available (42)

- ☑ All
  - ☑ ProxyTool
  - ☑ Soft-update
  - ☑ Custom_CloudDrive

Selected (All)

All

Name:

Status:

Description:

Policy Group:

Tag:

Endpoints:

Applications: Select

Schedule: All week

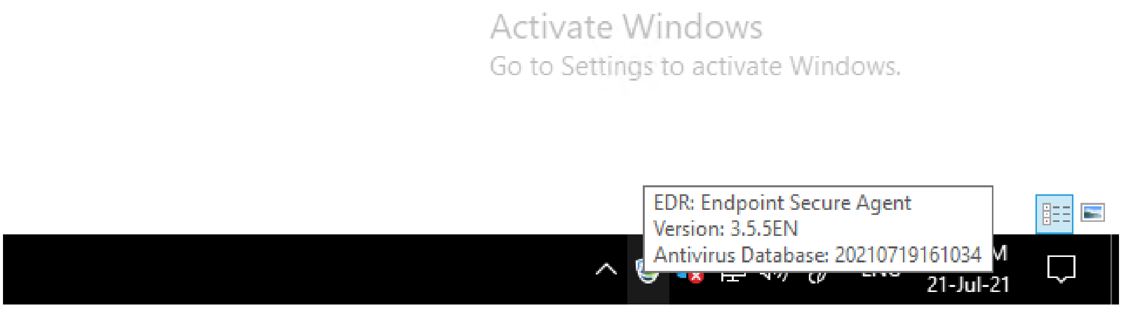
Action: ○ Allow ● Block

NGAF will push down the policy to Endpoint Secure immediately after you save the settings. Within 5 to 10 minutes, the selected applications will be blocked on all selected endpoints.

Save Cancel

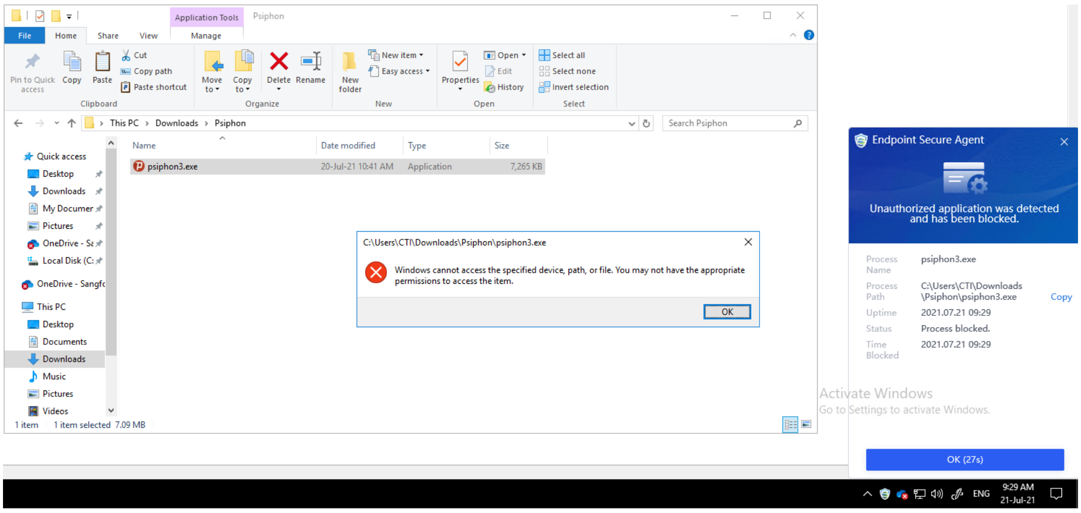
2.2 Jalankan Proxy Tools pada PC

1. Pastikan Endpoint Secure Agent telah jalan.



EDR: Endpoint Secure Agent
Version: 3.5.5EN
Antivirus Database: 20210719161034

2. Jalankan Proxy tool, anda dapat melihat kalau Proxy tool tidak dapat jalan dimana terdapat peringatan dari Endpoint Secure Agent.



Name	Date modified	Type	Size
psiphon3.exe	20-Jul-21 10:41 AM	Application	7,265 KB

C:\Users\CTI\Downloads\Psiphon\psiphon3.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

Endpoint Secure Agent

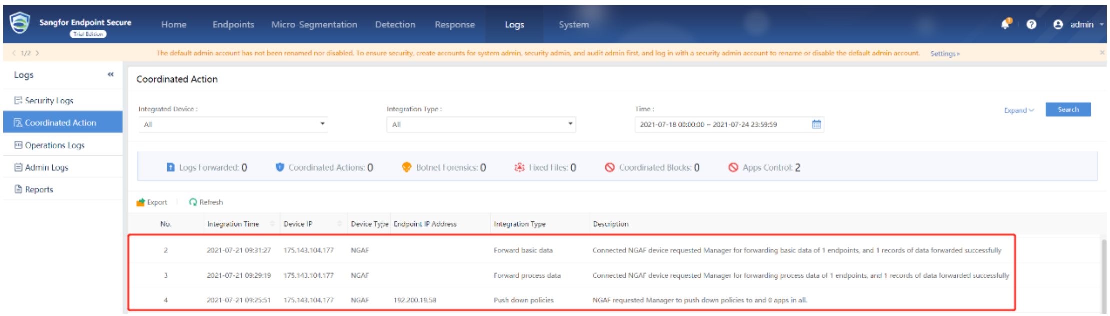
Unauthorized application was detected and has been blocked.

Process Name	psiphon3.exe
Process Path	C:\Users\CTI\Downloads\Psiphon\psiphon3.exe Copy
Uptime	2021.07.21 09:29
Status	Process blocked.
Time Blocked	2021.07.21 09:29

3 Lihat Pencatatan

3.1 Melihat pencatatan Agent dari MGR

1. Anda dapat melihat pencatatan kejadian dari NGAF policy melalui ES MGR log.



The default admin account has not been renamed nor disabled. To ensure security, create accounts for system admin, security admin, and audit admin first, and log in with a security admin account to rename or disable the default admin account. Settings>

Coordinated Action

Integrated Device : All

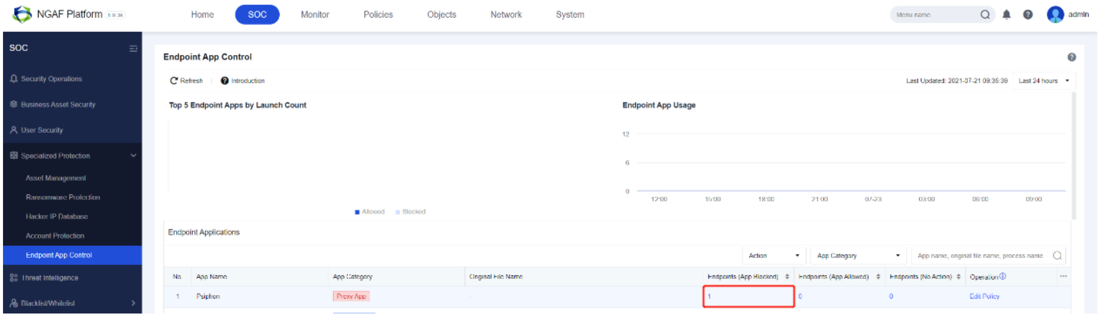
Integration Type : All

Time : 2021-07-18 00:00:00 ~ 2021-07-24 23:59:59

Logs Forwarded: 0 Coordinated Actions: 0 Botnet Forensics: 0 Fixed Files: 0 Coordinated Blocks: 0 Apps Control: 2

No.	Integration Time	Device IP	Device Type	Endpoint IP Address	Integration Type	Description
2	2021-07-21 09:31:27	175.143.104.177	NGAF		Forward basic data	Connected NGAF device requested Manager for forwarding basic data of 1 endpoints, and 1 records of data forwarded successfully
3	2021-07-21 09:29:19	175.143.104.177	NGAF		Forward process data	Connected NGAF device requested Manager for forwarding process data of 1 endpoints, and 1 records of data forwarded successfully
4	2021-07-21 09:25:51	175.143.104.177	NGAF	192.200.19.58	Push down policies	NGAF requested Manager to push down policies to and 0 apps in all.

2. Anda dapat melihat Proxy Tools yang berjalan dari Log dalam NGAF.



Endpoint App Control

Last Updated: 2021-07-21 09:35:39 Last 24 hours

Endpoint Applications

No.	App Name	App Category	Original File Name	Endpoints (App Blocked)	Endpoints (App Allowed)	Endpoints (No Action)	Operation
1	Psiphon	Proxy App	-	1	0	0	Edit Policy

4 Perhatian

1. Jumlah maksimum dari endpoint yang di dukung oleh NGAF dengan memory 4G adalah 1000.

   Jumlah maksimum dari endpoint yang di dukung oleh NGAF dengan memory lebih dari 4G adalah 2000

   Jika jumlah aktual dari endpoint lebih dari 2000, NGAF hanya akan memberlakukan aturan pada 2000 saja. ini akan menyebabkan beberapa endpoint gagal menjalankan aturan tersebut.

2. Ketika policy diberlakukan dalam NGAF, harap pastikan komunikasi antara NGAF dan Endpoint Secure Manager berjalan normal, atau aturan tidak dapat diberlakukan.

3. Data dalam Endpoint App Control pada SOC akan diperbarui per 5-10 menit.

4. NGAF dan Endpoint Secure Manager akan terus berkomunikasi antar kedua pihak untuk mempertahankan komunikasi dengan hearbeat, tetapi mungkin ada beberapa situasi ekstream, seperti NGAF bermasalah untuk berkomunikasi dengan Endpoint Secure Manager karena policy, Endpoint Secure Manager dan Endpoint Secure Agent berkomunikasi tidak normal, menyebabkan kegagalan policy/kebijakan pengiriman ke Endpoint Secure Agent, maka Endpoint Secure Manager akan mengunakan kebijakan yang sudah di cache secara lokal untuk mengkontrol alat VPN.

SANGFOR

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