



Sangfor NGAF

Panduan Konfigurasi Proteksi terhadap Ransomware

Produk Versi	8.0.35
Dokumen Versi	01
Rilis pada	Aug. 11, 2021



Copyright © Sangfor Technologies Inc. 2021. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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.

Dukungan Teknikal

Untuk dukungan teknis, harap kunjungi: <https://www.sangfor.com/en/about-us/contact-us/technical-support>

Kirimkan informasi perihal kesalahan atau permasalahan yang berhubungan dengannya ke tech.support@sangfor.com.

Data Perubahan

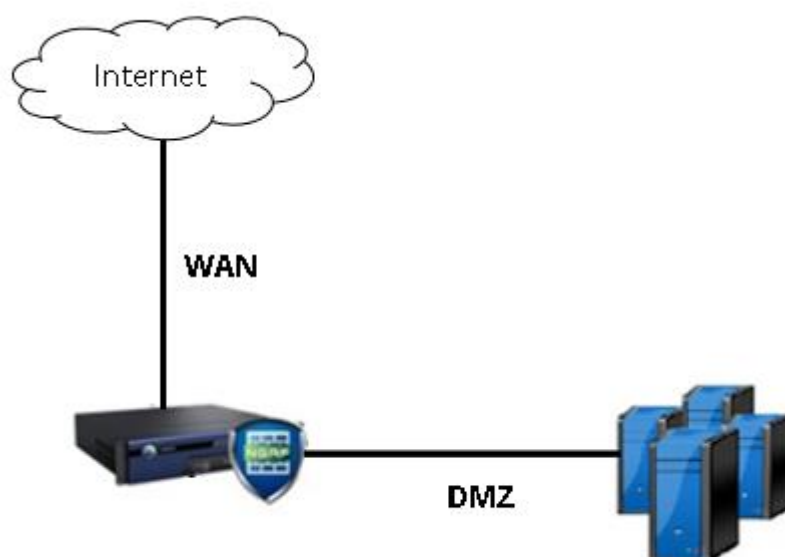
Tanggal	Keterangan Perubahan
Aug. 11, 2021	Ini merupakan dokumen yang dirilis paling pertama

Daftar ini

1 Skenario Penerapan	1
2 Metoda Konfigurasi	2
3 Perhatian.....	6

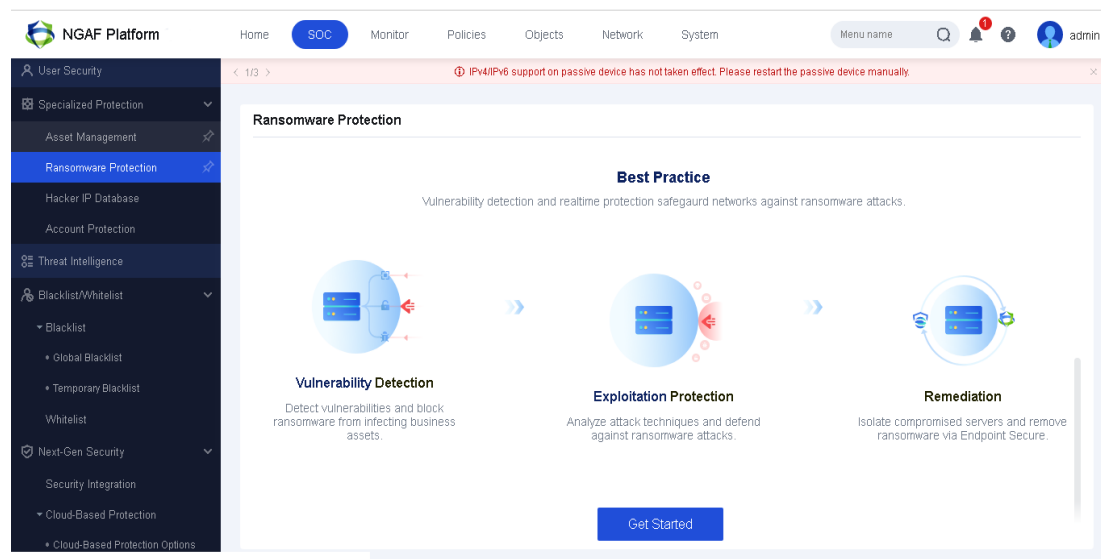
1 Skenario Penerapan

Sehubungan peningkatan besar dalam ransomware, perlindungan ransomware sangat diminati. Perlindungan Ransomware akan melindungi server atau aset bisnis dari ransomware. Berikut di bawah ini adalah contoh topologi.



2 Metoda Konfigurasi

Langkah 1. Untuk konfigurasi perlindungan terhadap ransomware, pada **SOC > Specialized Protection > Ransomware Protection**. Klik pada **Get Started**.



Langkah 2. Pada bagian ini, Anda dapat mengkonfigurasi Destination Network Object, Destination Zone, dan Source Zone. Untuk contoh, dalam Destination Network Object, Anda bisa memilih tujuan dari masing masing network object.

Settings ×

Protected Objects (Business Asset/Server)

Dst Network Object: ⋮ ?

Dst Zone: ▼ ?

Src Zone: ▼ ?

Scan Options

☐ Scan for open ports, system vulnerabilities, and weak passwords [Disclaimer](#)

☐ Enable scheduled active scan ?

Schedule: ▼ ▼

Ransomware Protection Policy

☒ Generate security policies automatically to protect against ransomware ? [Preview](#)

[Web App Firewall](#) [Vulnerability Protection](#) [Content Security](#) [Botnet Detection](#) [Slow Brute-Force Attacks](#)

[Save](#) [Cancel](#)

Select Network Object

Available (5) | [Add](#)

All

Search

<input type="checkbox"/>	Name	Type	Address
<input type="checkbox"/>	All	IP Address	0.0.0.0-255.255.255.255
<input type="checkbox"/>	Private Network Segment	IP Address	10.0.0.0-10.255.255.255, 172.16.0...
<input checked="" type="checkbox"/>	DMZ	IP Address	192.168.1.0-192.168.1.255
<input type="checkbox"/>	allow ip	IP Address	
<input type="checkbox"/>	NGAF IP	IP Address	

Go to Network Objects

Selected (1) | [Clear](#)

DMZ

Save Cancel

Langkah 3. Setelah anda memilih Destination Network Object, lalu anda bisa memilih zone yang dituju. Pada contoh berikut, dipilih zone DMZ.

Settings

Protected Objects (Business Asset/Server)

Dst Network Object: DMZ

Dst Zone: Select

Src Zone:

Scan Options

☐ Scan for open ports,
 ☒ Enable scheduled a

Schedule: Even

Ransomware Protection

☒ Generate security po

Web App Firewall

Slow Brute-Force Attacks

Save Cancel

Virtual_untru...

Virtual wire

-

Wan

Layer 3

eth1

HA

Layer 3

eth3

Lan

Layer 3

eth0

DMZ

Layer 3

eth2

Save Cancel

Langkah 4. Berikutnya, anda dapat memilih Asal dari Source Zone. Pada contoh berikut, zone WAN dipilih sebagai asal dari source zone.

Settings ✕

Protected Objects (Business Asset/Server)

Dst Network Object: DMZ ⓘ

Dst Zone: DMZ ⓘ

Src Zone: Select zone ⓘ

Scan Options

☐ Scan for open ports

☒ Enable scheduled active scan ⓘ

Schedule: Every Sunday

Ransomware Protection Policy

☒ Generate security policies automatically to protect against ransomware ⓘ [Preview](#)

[Web App Firewall](#) [Slow Brute-Force Attacks](#) [Save](#) [Cancel](#)

<input type="checkbox"/>	Name	Type	Interfaces
<input type="checkbox"/>	Virtual_untru...	Virtual wire	-
<input checked="" type="checkbox"/>	Wan	Layer 3	eth1
<input type="checkbox"/>	HA	Layer 3	eth3
<input type="checkbox"/>	Lan	Layer 3	eth0
<input type="checkbox"/>	DMZ	Layer 3	eth2

[Save](#) [Cancel](#)

Langkah 5. Setelah konfigurasi proteksi untuk objek, langkah berikutnya adalah mengaktifkan pemindaian untuk open ports, system vulnerabilities, dan kekuatan kata kunci dan mengaktifkan penjadwalan pemindaian secara otomatis. Lalu klik Save.

Settings ✕

Protected Objects (Business Asset/Server)

Dst Network Object: DMZ ⓘ

Dst Zone: DMZ ⓘ

Src Zone: Wan ⓘ

Scan Options

☒ Scan for open ports, system vulnerabilities, and weak passwords [Disclaimer](#)

☒ Enable scheduled active scan ⓘ

Schedule: Every Sunday 00:00

Ransomware Protection Policy

☒ Generate security policies automatically to protect against ransomware ⓘ [Preview](#)

[Web App Firewall](#) [Vulnerability Protection](#) [Content Security](#) [Botnet Detection](#) [Slow Brute-Force Attacks](#) [Save](#) [Cancel](#)

Langkah 6. Klik Save, akan muncul peringatan konfirmasi. lalu klik Yes.

Confirm



Are you sure you want to start scan?

1. This operation will clear the current data.
2. The scan process may be detected as attack by other security devices. To avoid this, please change related settings first.

Yes

No

Ransomware Protection

☒ Settings
 [?](#)
☐ Display Options
 ☐ Refresh
 Stop

Scanning for: Open Ports (complete before 2021-08-16 11:25:40), System Vulnerabilities, Weak Passwords

Ransomware Protection

Vulnerable Business Assets

0

Vulnerable Bu...

Vulnerabilities

Open Port

0

Business Assets

System Vulnerability

0

Business Assets

Weak Password

0

Business Assets

Ransomware Threats

Ransomware Infection

0

Business Assets

Ransom-Demanding Hack

0

Business Assets

Issues

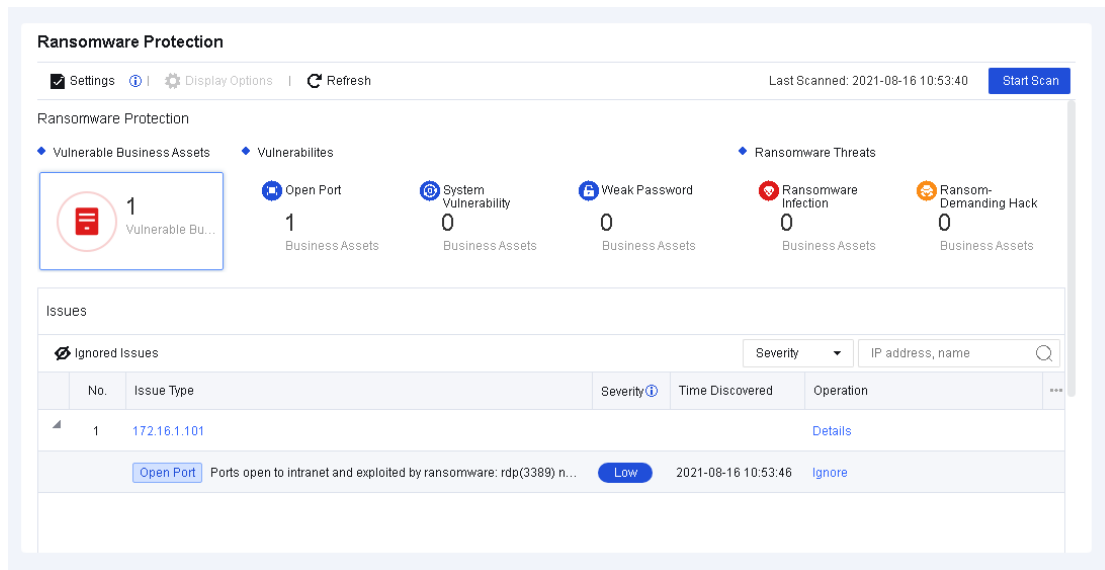
☒ Ignored Issues

Severity
 IP address, name

No.	Issue Type	Severity	Time Discovered	Operation	...

Langkah 7. Setelah pemindaian selesai, akan muncul hasil dan menampilkan **Issue/permasalahan** seperti tampilan dibawah ini.

5



3 Perhatian

1. Pastikan semua yang dikonfigur Destination network objects, destination zone, dan source zone sudah benar.
2. Anda dapat memeriksa disclaimer karena akan melakukan pemindaian port di jaringan.
3. Jumlah IP tujuan maksimum adalah 1024 IP.



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