SANGFOR

Sangfor NGAF

Ransomware Protection Configuration Guide

Product Version	8.0.35
Document Version	01
Released on	Aug. 11, 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.

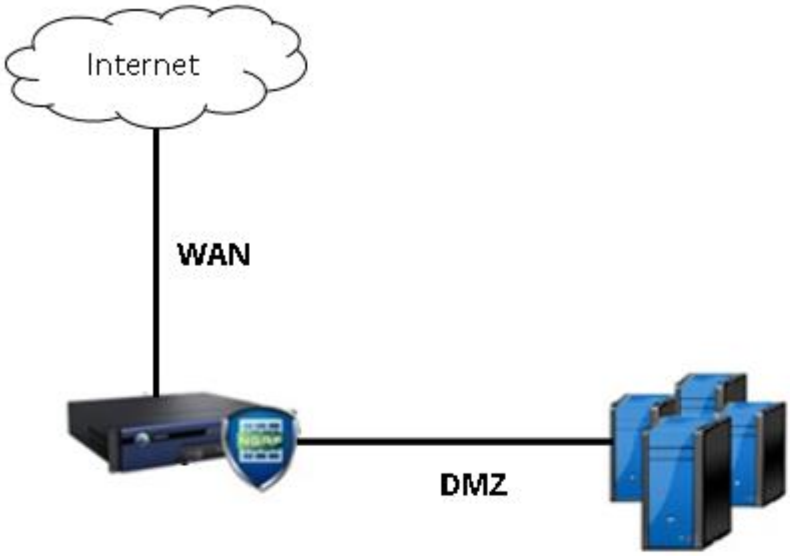
Change Log

Date	Change Description
Aug. 11, 2021	This is the first release of this document.

Contents

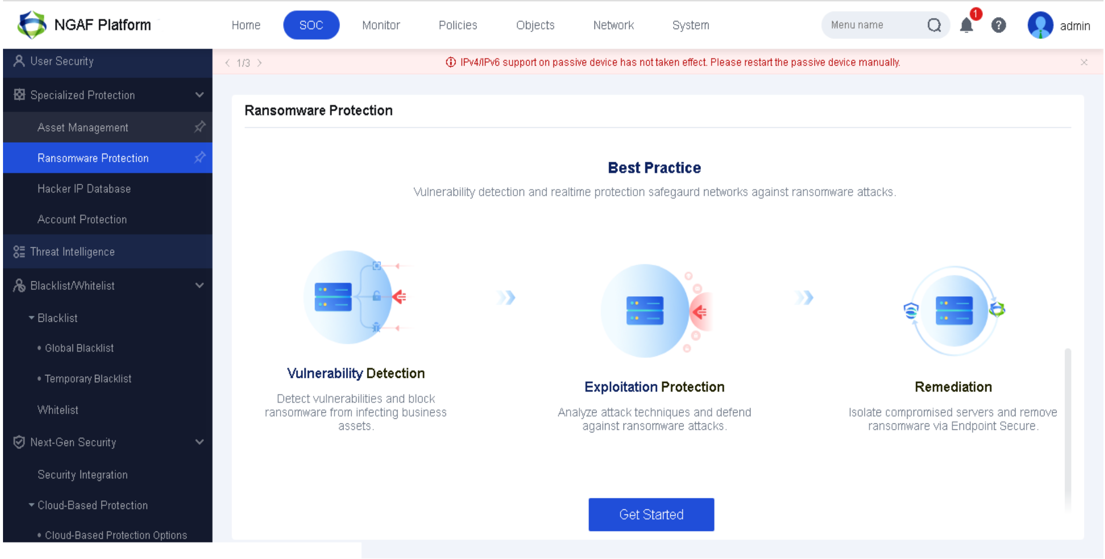
1 Application Scenario

As there is a huge rise in ransomware, ransomware protection is in high demand. Ransomware protection will be protecting servers or business assets from ransomware. Below is an example of topology.



2 Configuration Method

Step 1. To configure ransomware protection, go to **SOC** > **Specialized Protection** > **Ransomware Protection**. Click on **Get Started**.



IPv4/IPv6 support on passive device has not taken effect. Please restart the passive device manually.

Ransomware Protection

Best Practice

Vulnerability detection and realtime protection safegaurd networks against ransomware attacks.

Vulnerability Detection

Detect vulnerabilities and block ransomware from infecting business assets.

Exploitation Protection

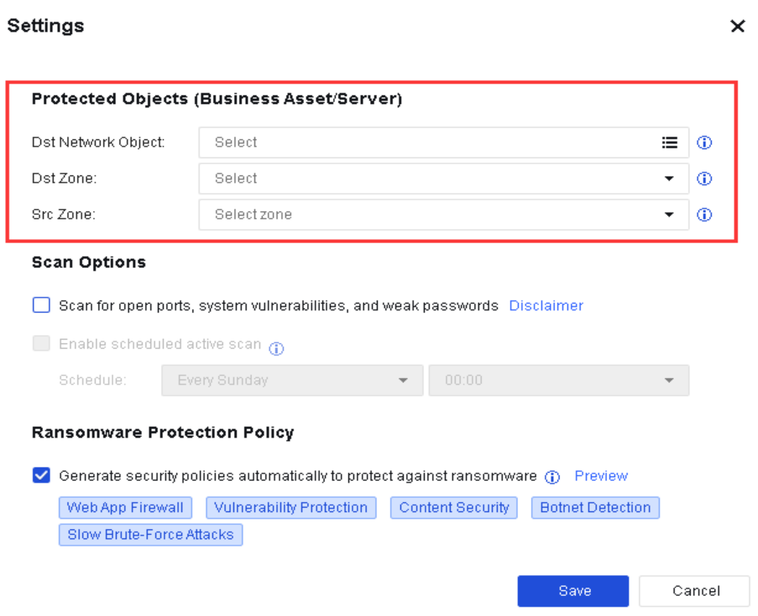
Analyze attack techniques and defend against ransomware attacks.

Remediation

Isolate compromised servers and remove ransomware via Endpoint Secure.

Get Started

Step 2. In this section, you may configure the Destination Network Object, Destination Zone, and Source Zone. For example, in Destination Network Object, you may select the respective destination network object.



Settings

Protected Objects (Business Asset/Server)

Dst Network Object: Select

Dst Zone: Select

Src Zone: Select zone

Scan Options

□ Scan for open ports, system vulnerabilities, and weak passwords Disclaimer

□ Enable scheduled active scan

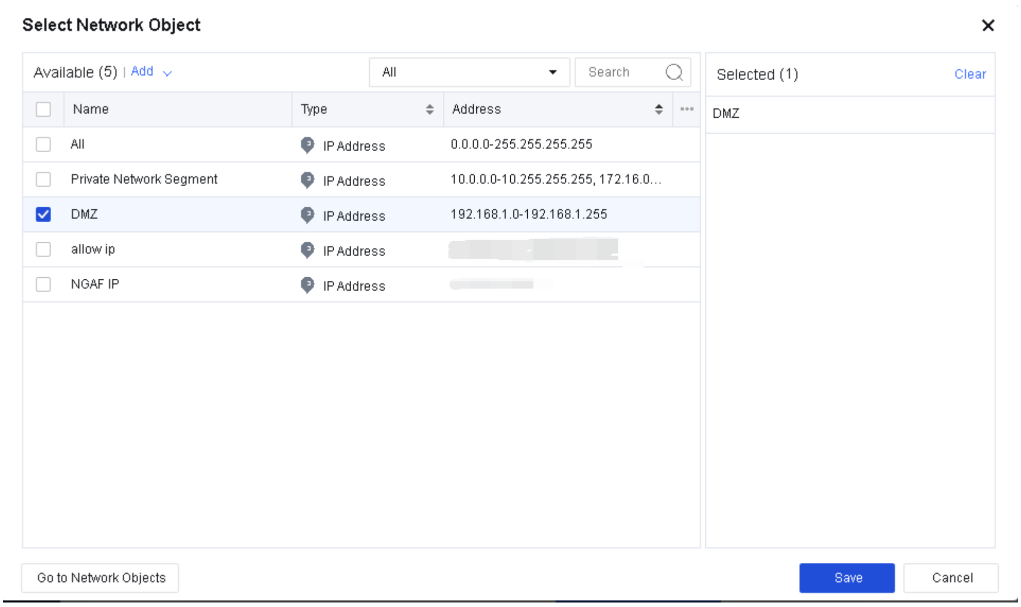
Schedule: Every Sunday 00:00

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



Select Network Object ✕

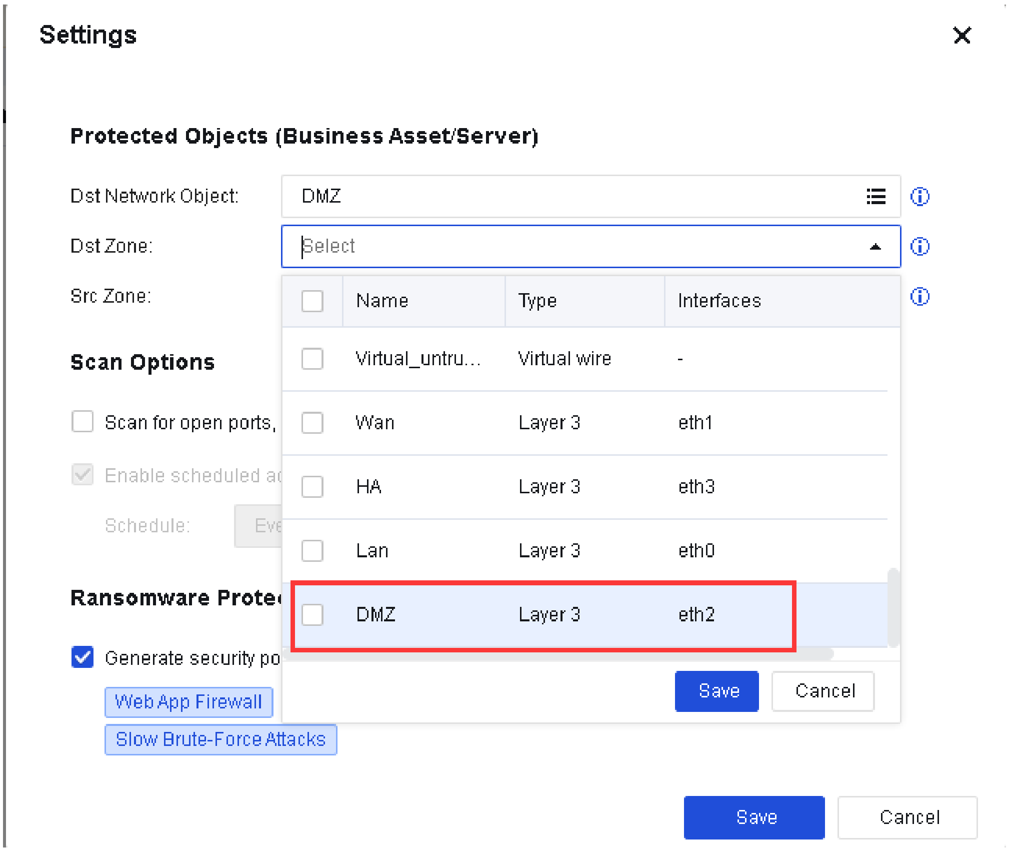
Available (5) | Add ⌄ All ▾ Search

☐	Name	Type	Address
☐	All	IP Address	0.0.0.0-255.255.255.255
☐	Private Network Segment	IP Address	10.0.0.0-10.255.255.255, 172.16.0...
☑	DMZ	IP Address	192.168.1.0-192.168.1.255
☐	allow ip	IP Address	[redacted]
☐	NGAF IP	IP Address	[redacted]

Selected (1) Clear

DMZ

Step 3. After you had selected the Destination Network Object, then you may select the destination zone. In this example, the DMZ was selected.



Settings ✕

Protected Objects (Business Asset/Server)

Dst Network Object: DMZ

Dst Zone: Select ▴

Src Zone:

☐	Name	Type	Interfaces
☐	Virtual_untru...	Virtual wire	-
☐	Wan	Layer 3	eth1
☐	HA	Layer 3	eth3
☐	Lan	Layer 3	eth0
☐	DMZ	Layer 3	eth2

Scan Options

☐ Scan for open ports,

☑ Enable scheduled a

Schedule: Eve

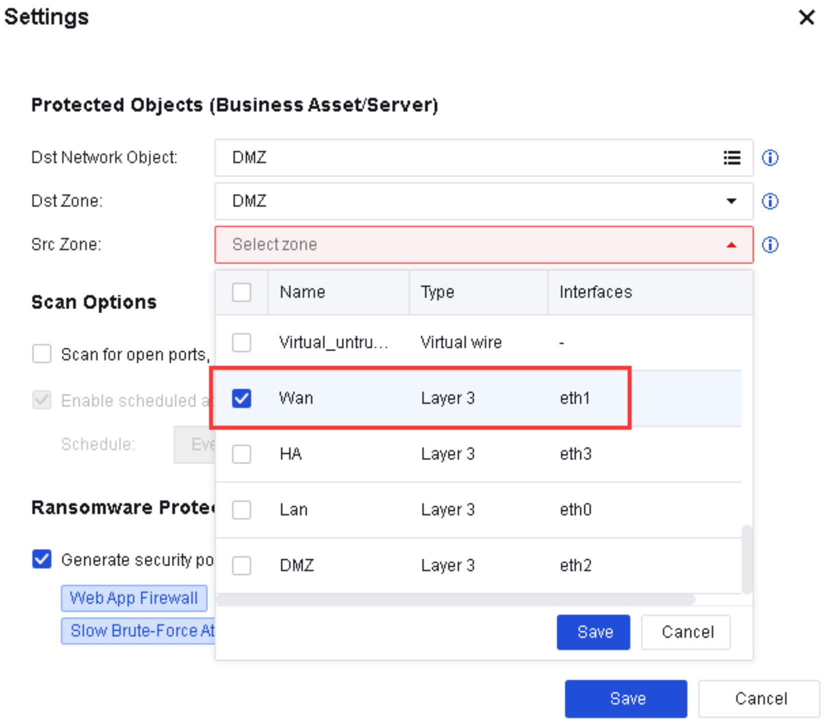
Ransomware Prote

☑ Generate security po

Web App Firewall

Slow Brute-Force Attacks

Step 4. Next, you may select the Source Zone. In this example, the WAN zone will be set as the source zone.



Settings

Protected Objects (Business Asset/Server)

Dst Network Object: DMZ

Dst Zone: DMZ

Src Zone: Select zone

☐	Name	Type	Interfaces
☐	Virtual_untru...	Virtual wire	-
☑	Wan	Layer 3	eth1
☐	HA	Layer 3	eth3
☐	Lan	Layer 3	eth0
☐	DMZ	Layer 3	eth2

Scan Options

☐ Scan for open ports,

☑ Enable scheduled a

Schedule: Eve

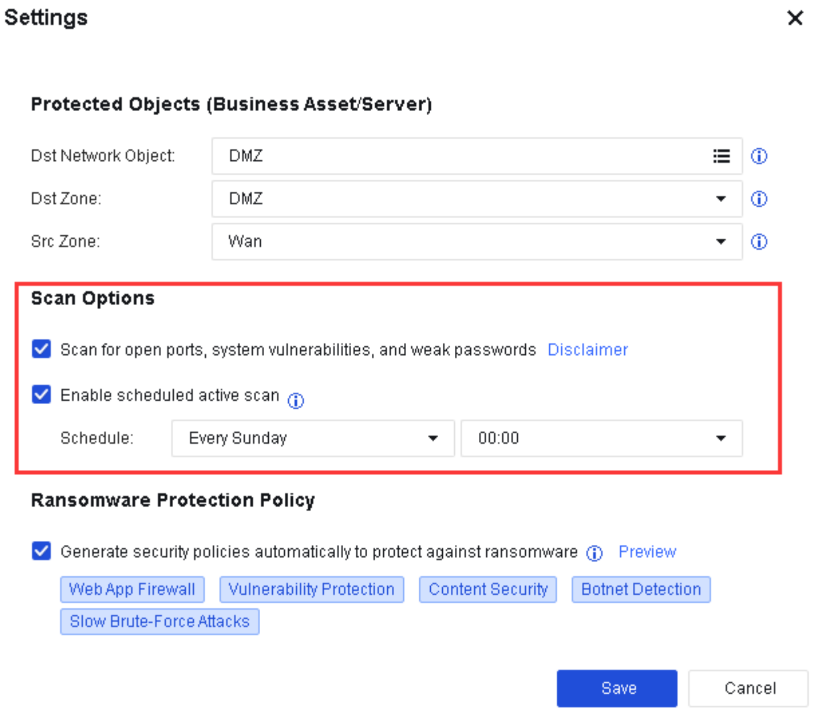
Ransomware Prote

☑ Generate security po

Web App Firewall

Slow Brute-Force At

Step 5. After protected objects were configured, the next step is to enable a scan for open ports, system vulnerabilities, and weak passwords and enable scheduled active scans to have an automated scanning. Then, click 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

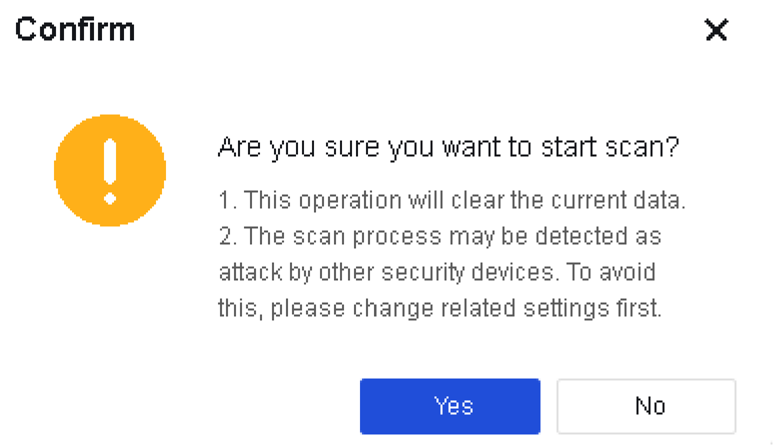
Schedule: Every Sunday 00:00

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

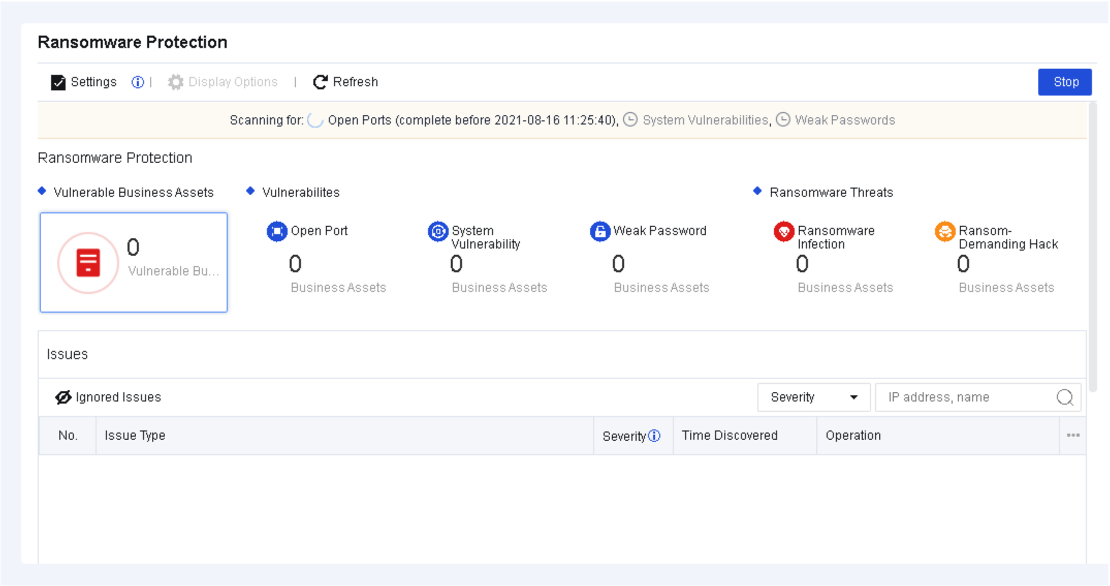
Step 6. Click Save, a confirmation message will prompt. Then, click Yes.



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.

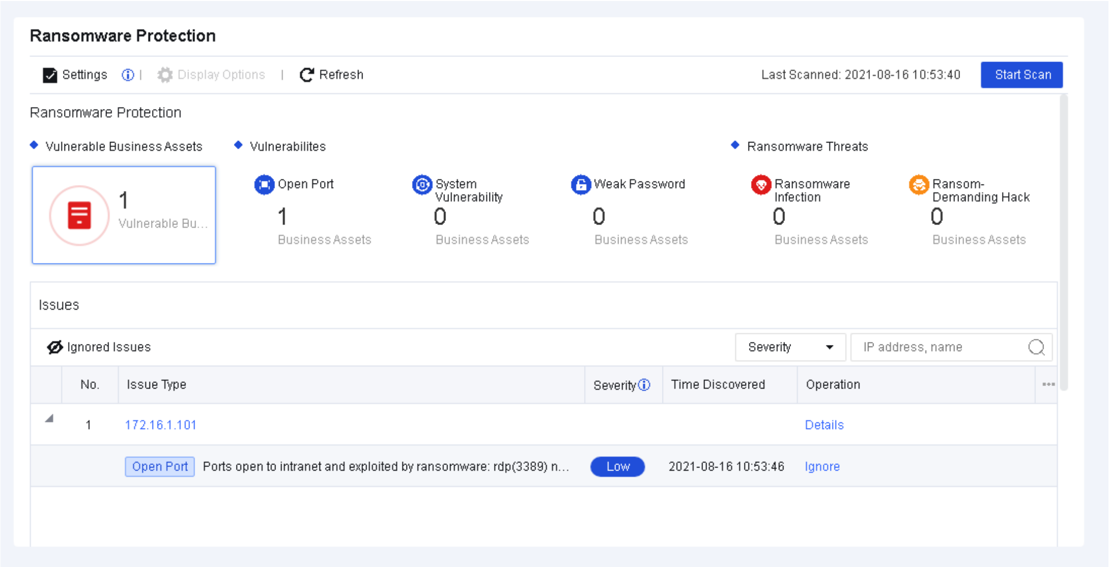


Ransomware Protection

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

No.	Issue Type	Severity	Time Discovered	Operation

Step 7. After the scanning is done, it will show the responding result in **Issue** as shown in the figure below.



Ransomware Protection

Last Scanned: 2021-08-16 10:53:40

No.	Issue Type	Severity	Time Discovered	Operation
1	172.16.1.101			Details
	Open Port Ports open to intranet and exploited by ransomware: rdp(3389) n...	Low	2021-08-16 10:53:46	Ignore

3 Precautions

1. All of the configured destination network objects, destination zone, and source zone must be selected correctly.
2. You may check on the disclaimer as it will perform port scanning in the network.
3. The maximum number of destination IPs in 1024 IPs.

SANGFOR