SANGFOR

Sangfor Correlated Policy Practice Guidance

Document Version	v1.0
Released on	2023-04-24

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.

Intended Audience

This document is intended for:

- Pre-sale
- FAE

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
2023-04-24	This is the first release of this document.

Contents

Technical Support 1
Change Log 2
1 Case 4
1.1 Scene 4
1.1.1 Customer Requirements 4
1.1.2 Implementation Method Analysis 4
1.2 Network Toplogy 6
1.3 Configuration Process 6
1.3.1 Policy Settings 6
1.3.2 Creating playbook policy 7
1.4 Test Validity 9
1.5 Conclusion 10

1 Case

This document aims to carry out high-frequency correlated processing between different self-developed devices(ES/IAG/NGAF/CC) and integrate gateway, terminal, and platform products to achieve continuous threat detection and efficient security operations, bringing value to customers.

According to solutions based on marketing, we provide scenario-based playbook strategies for different customer environments.

No	Solution Type	Main Products Involved	Remark
1	Continuous Threat Detection	NGAF、CC	detection and response in time,improve operation effeciency

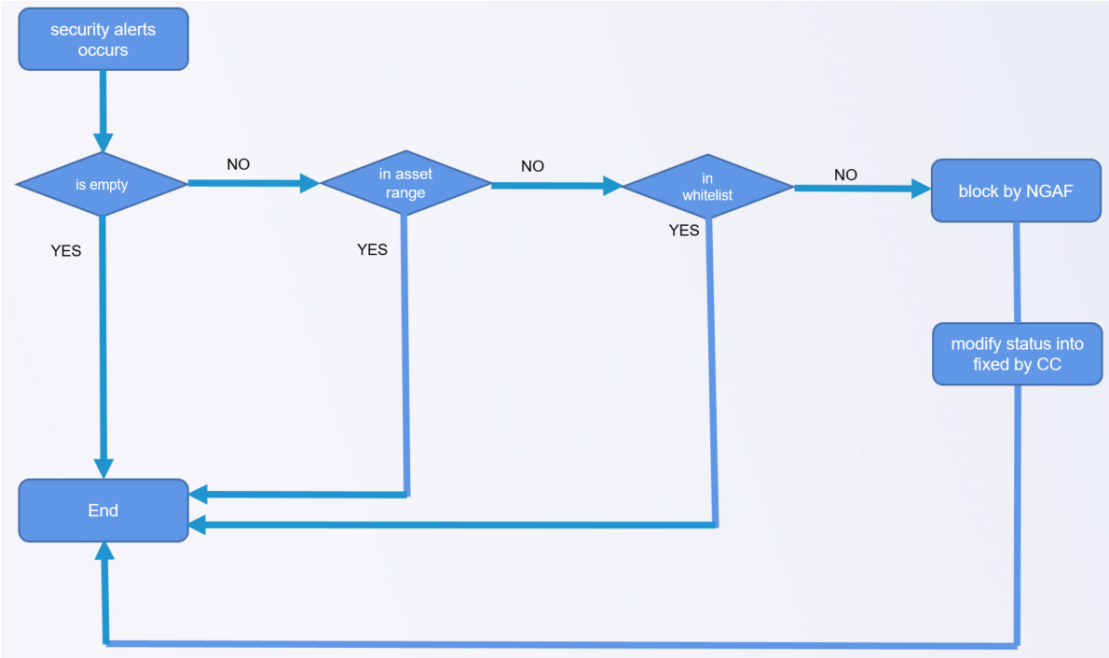
1.1 Scene

1.1.1 Customer Requirements

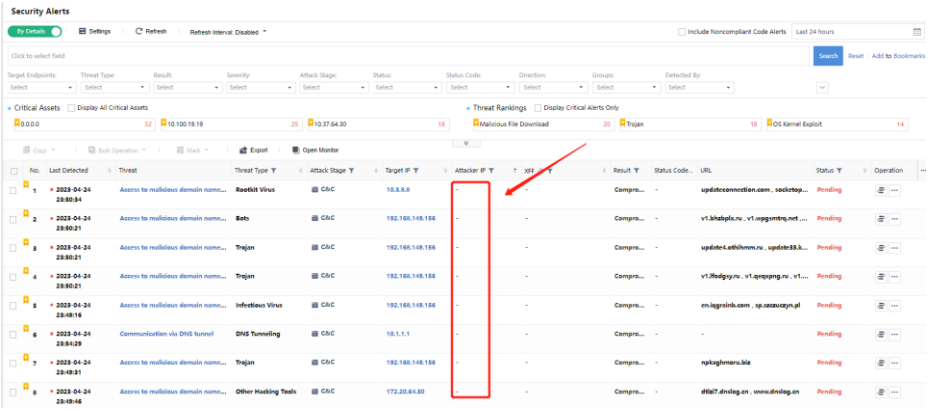
A branch of customer, as a defender, is participating external offensive and defensive drills. There are totally 4 NGAFs which need to be operated and managed in the customer network. Due to the shortage of security analysts, it is necessary to adopt the "black-and-white" mode for blocking attacks from Internet, that is to say, any global ip addresses not in whitelists issued by HQ should be blocked in time when those access to intranet.

1.1.2 Implementation Method Analysis

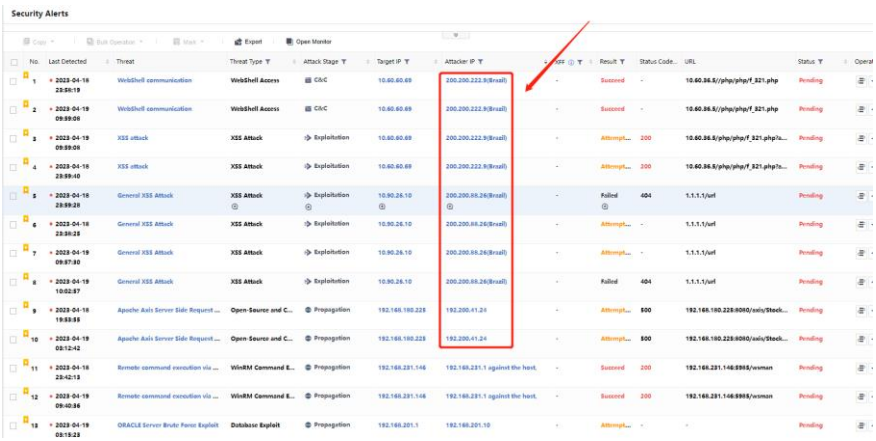
According to the requirement, firstly, we have the common concept that this policy should be oriented to security alerts and be automatic,and then define a constant including all ip addresses. The key action is blocking by NGAF, but we should consider some necessary check before it performs, for example, whether the attacker ip address exists, whether the attacker ip address belongs to whitelists and whether the attacker ip is an intranet asset. After we exclude such conditions it will be appropriate to perform block action in all NGAF devices and change the status of alerts automatically by following action.



- **Step 1：** Once alerts are triggered, they hit the predefined policy settings, initiating the first step in the process of assessing and addressing potential threats.
- **Step2：** If the attacker's IP does not exist, the policy will end directly. If it exists, the system will proceed to make a subsequent judgment regarding whether it is an intranet asset address.



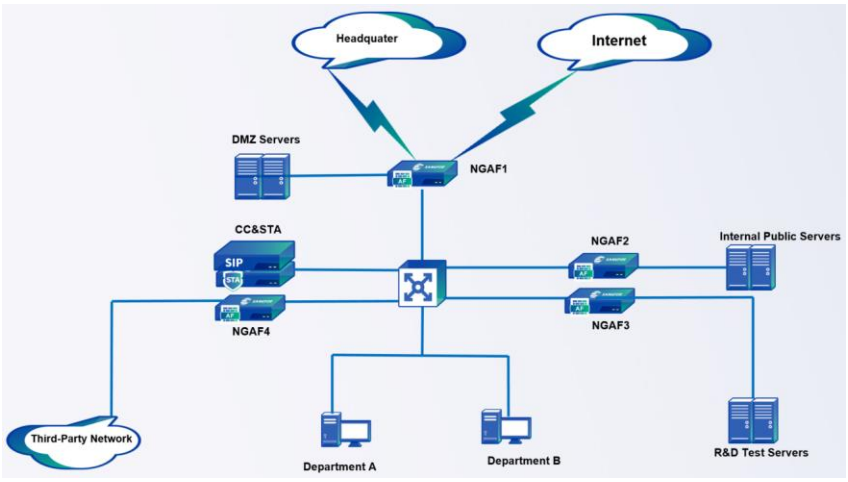
- **Step3：** If the attack's IP is belonged to intranet asset address, the policy will end directly. If not, the system will proceed to make a sub subsequent judgment regarding whether it is belonged whitelist address.
- **Step 4：** If the attacker's IP is belonged to whitelist, the policy will end directly. If not, the system will proceed to push down the block to NGAF.



- **Step 5：** The NGAFs device will block the Internet attacker IP pushed down by CC, and then CC will modify the alerts status into fixed.

1.2 Network Toplogy

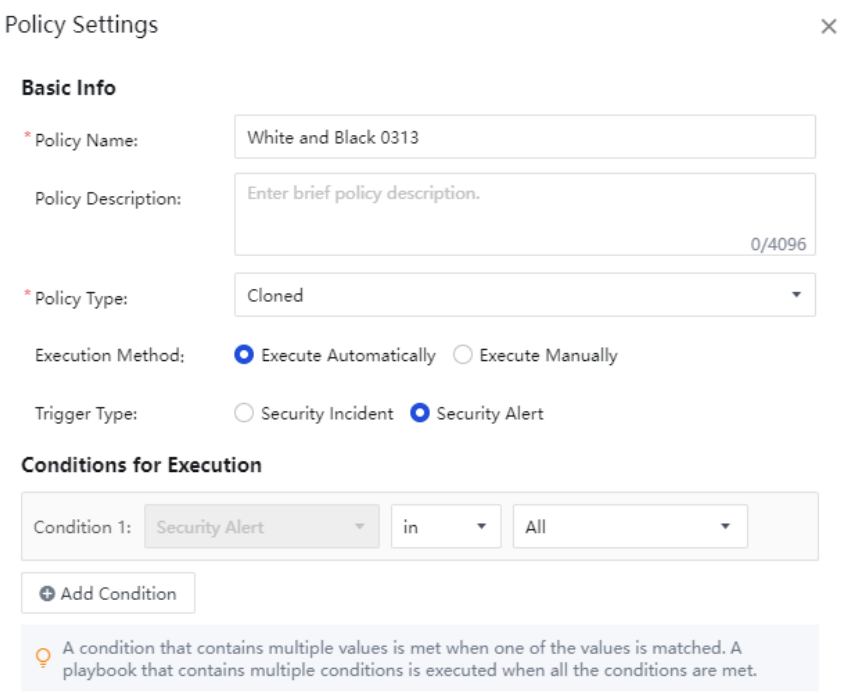
Based on the toplogy provided, the customer has implemented the Security Threat Analytics (STA), Cyber Command (CC), and 4 Next-Generation Application Firewalls (NGAF) for protecting different security zones.



1.3 Configuration Process

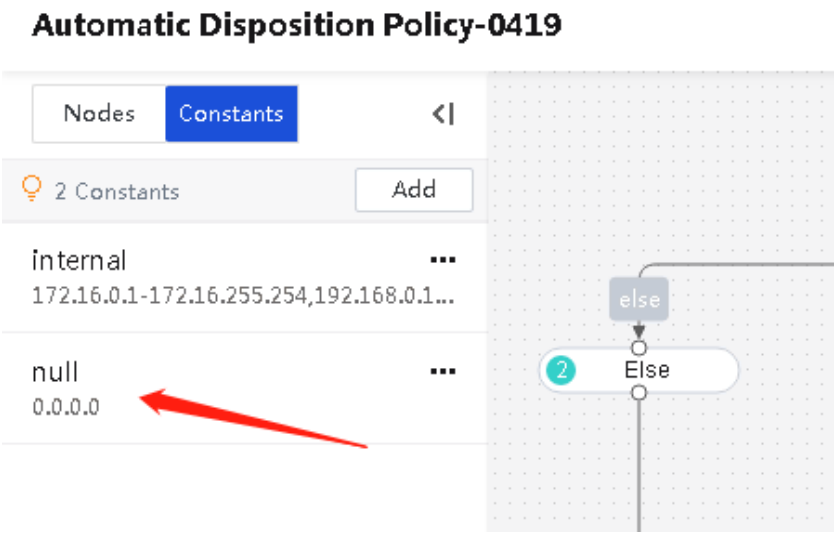
1.3.1 Policy Settings

Select security alert types, execute automatically, security alert, all attack types;

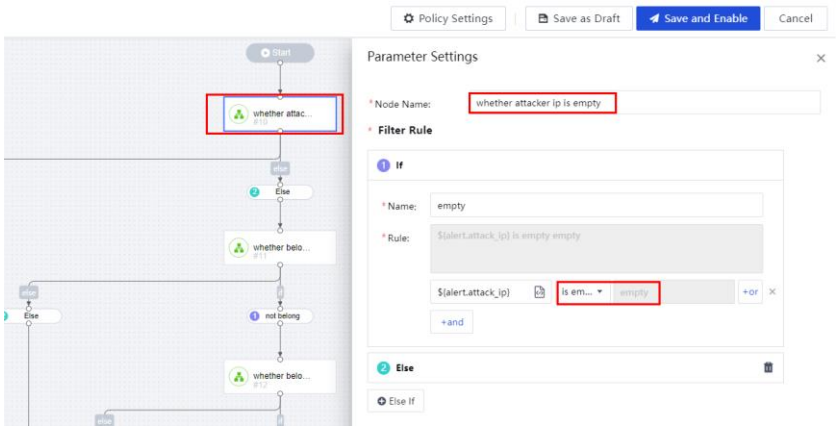


1.3.2 Creating playbook policy

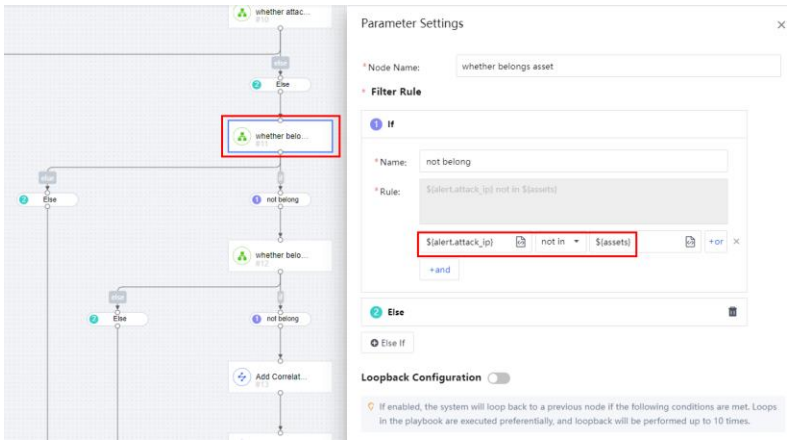
(1)、Create a constant and fill in whitelist ip addresses, create another constant and fill in intranet assets address range.



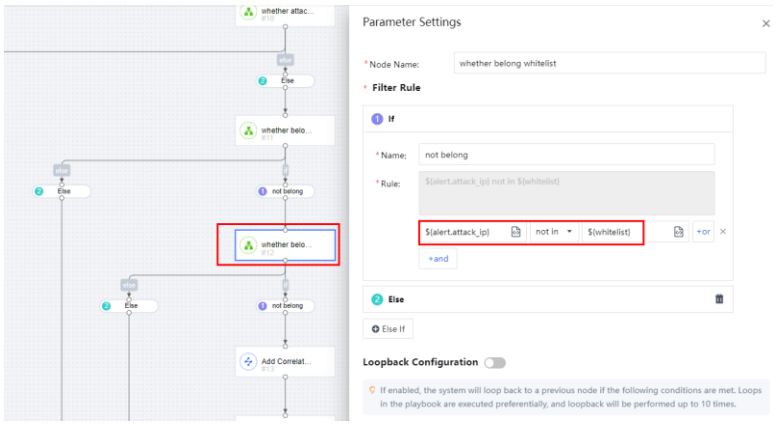
(2)、Decision, excludes the case where the attacker ip is empty.



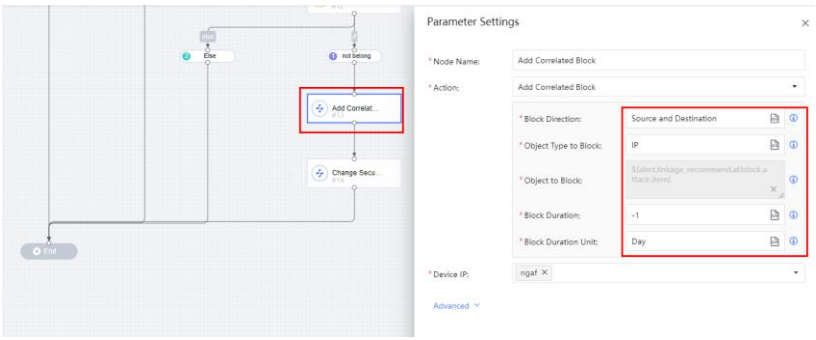
(3)、Define a decision, if the attacker is an intranet address in security alerts;



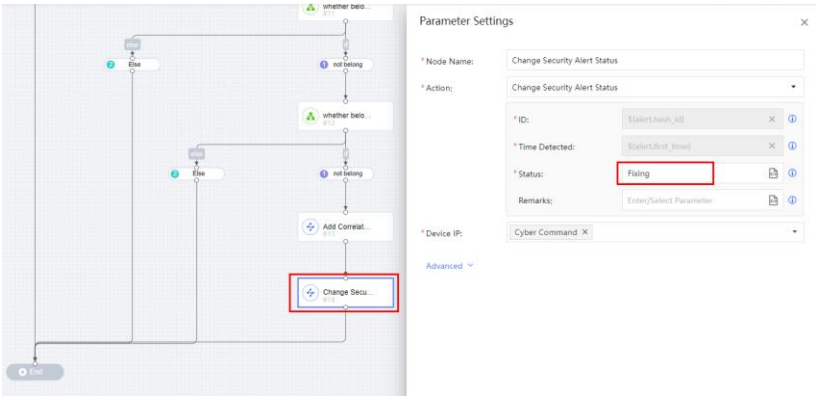
(4)、Decision, excludes the situation that the attacker ip is in the white list address in security alerts.



(5)、Initiate correlated block to NGAF

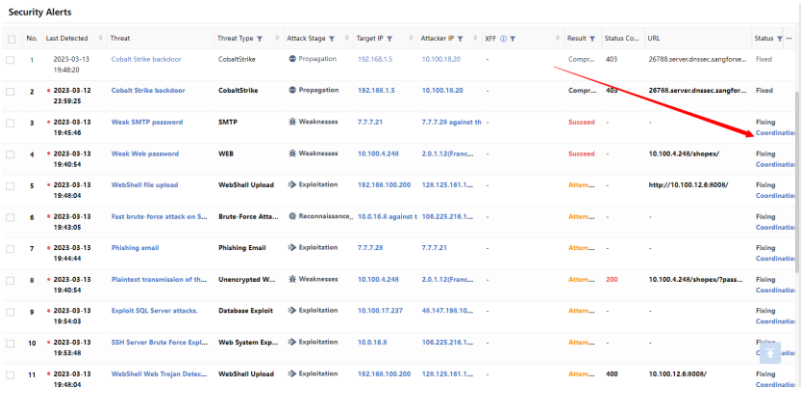


(6)、Action, modify the disposal status of corresponding security alert into fixing.

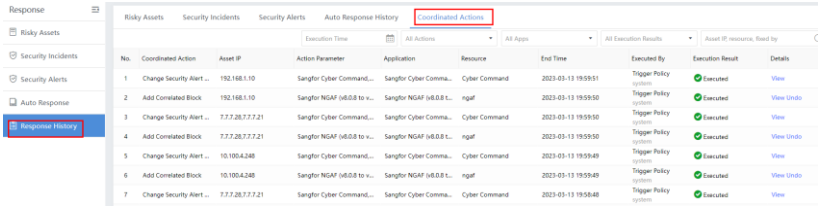


1.4 Test Validity

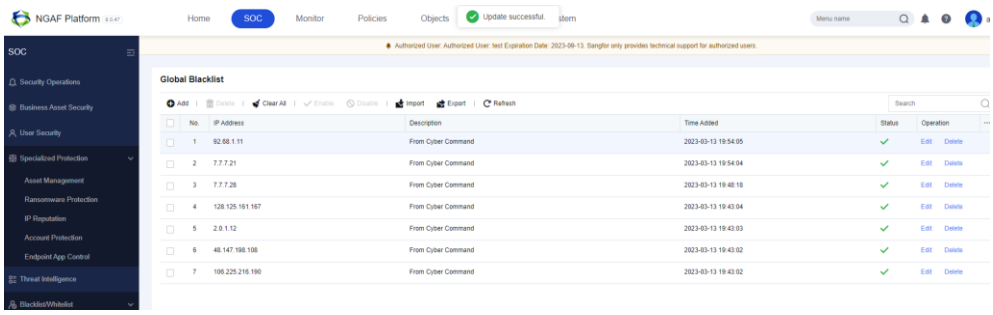
The security alerts flush persistently as usual, when the policy is enabled, new items will hit and executed automatically.



It is available to view the overall coordinated actions in response history page.



Login NGAF devices and blocking internet attacker IP addresses can be viewed.



1.5 Conclusion

From the above example, it is evident that playbook policies of CC can significantly block attacks from internet to intranet with NGAF. The capability can meet the requirement well in some scenarios, such as offensive and defensive, strict inbound access...etc.