SANGFOR

vSTA Mirroring in HCI Practice Guidance

Document Version	v1.0
Released on	2023-04-28

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

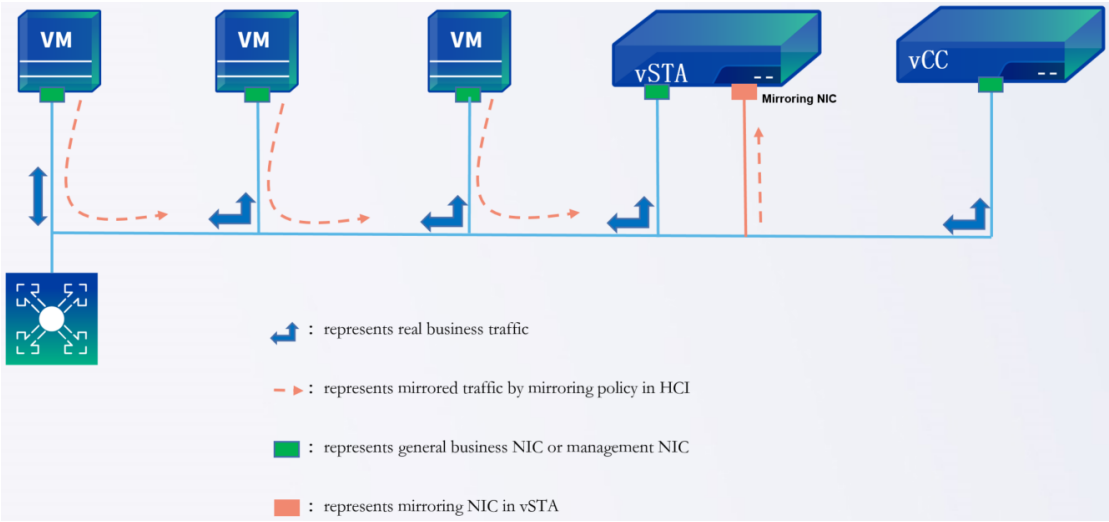
Date	Change Description
2023-04-28	This is the first release of this document.

Contents

1.1 Solution Description

Currently, as many projects have phrchased HCI, vCC and vSTA, compared with opponents, there exists a mature and competitive solution to detect the attacks among VMs in HCI platform. This solution also can be introduced by some POC projects as well.

Based on the technology of mirroring NIC of VMs, you can select any specific VMs flexiblely without affecting business at all. Business VMs communicate with others normally, and create an mirroring policy in HCI. It is necessary confirm the source of mirroring traffic which means specific NICs of VMs in this HCI platform, and the destination port must select mirroring NIC of STA, and you will see the incoming traffic immediately. Theory digarm can be viewed as below.



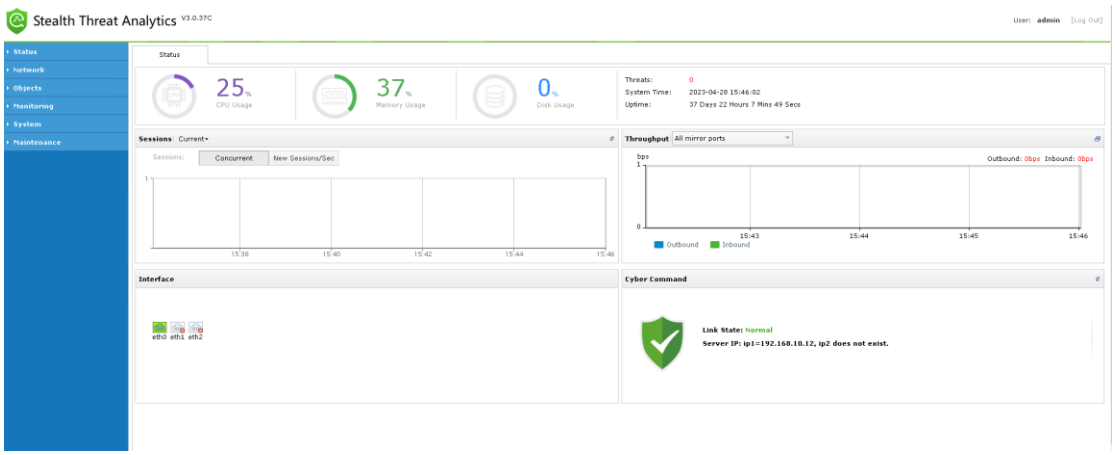
1.2 Supported Version

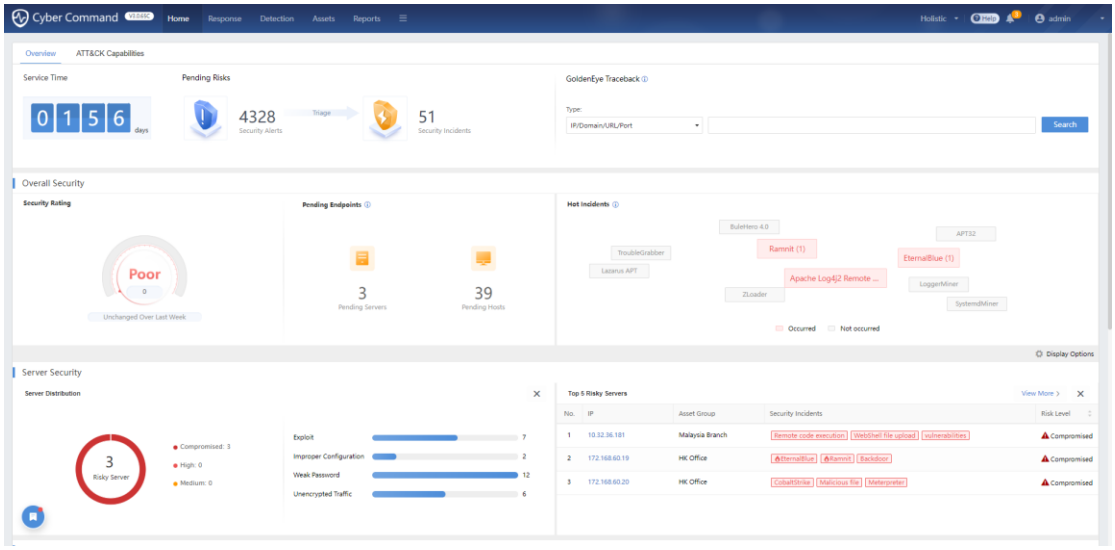
- **HCI：** musu be 6.8.0 and above version;
- **vSTA：** recomme 3.0.37C and above version;
- **vCC：** recommend 3.0.64C and above version;

1.3 Configuration Guidance

- **Preconditions**

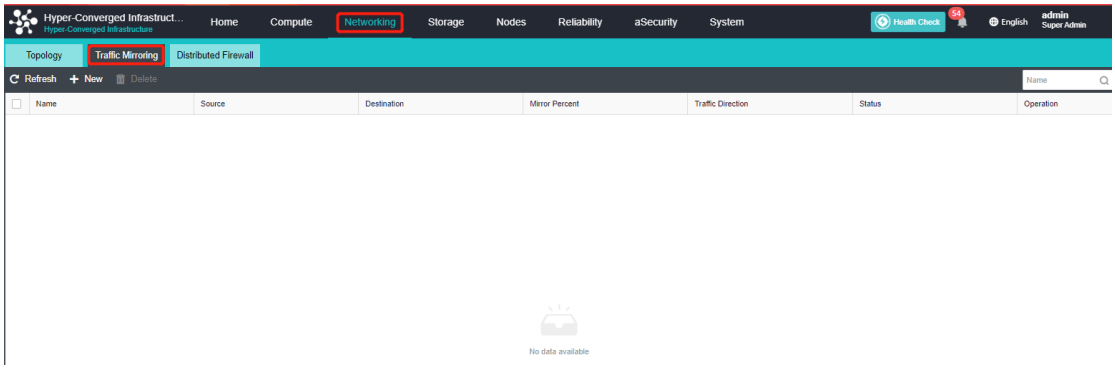
You are required that vSTA and vCC have been installed and configured well (refer to configuration checklist documents)in HCI platform before you create the mirroring policy.



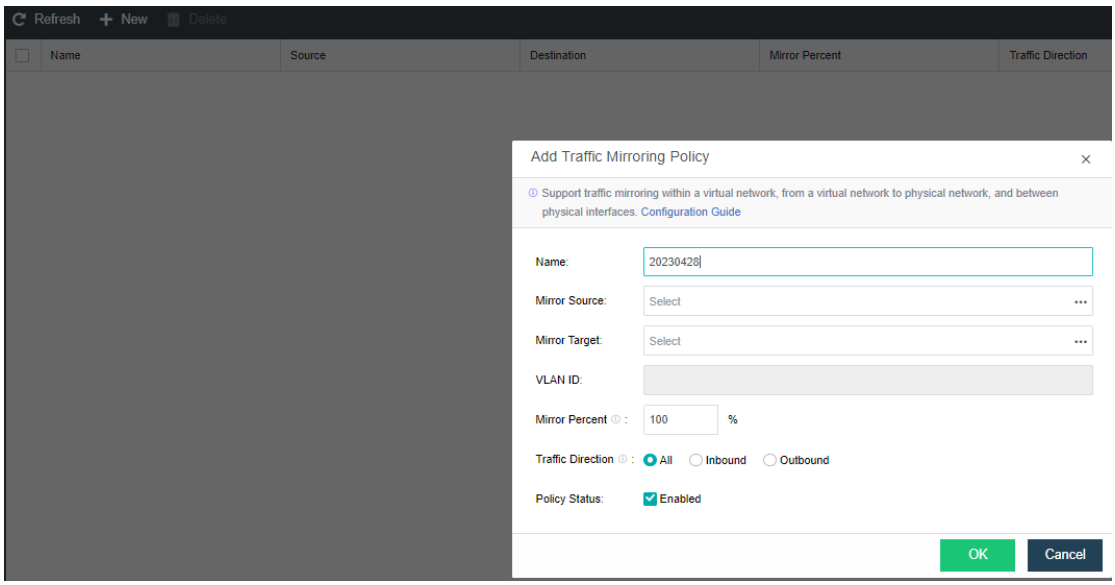


- **Steps**

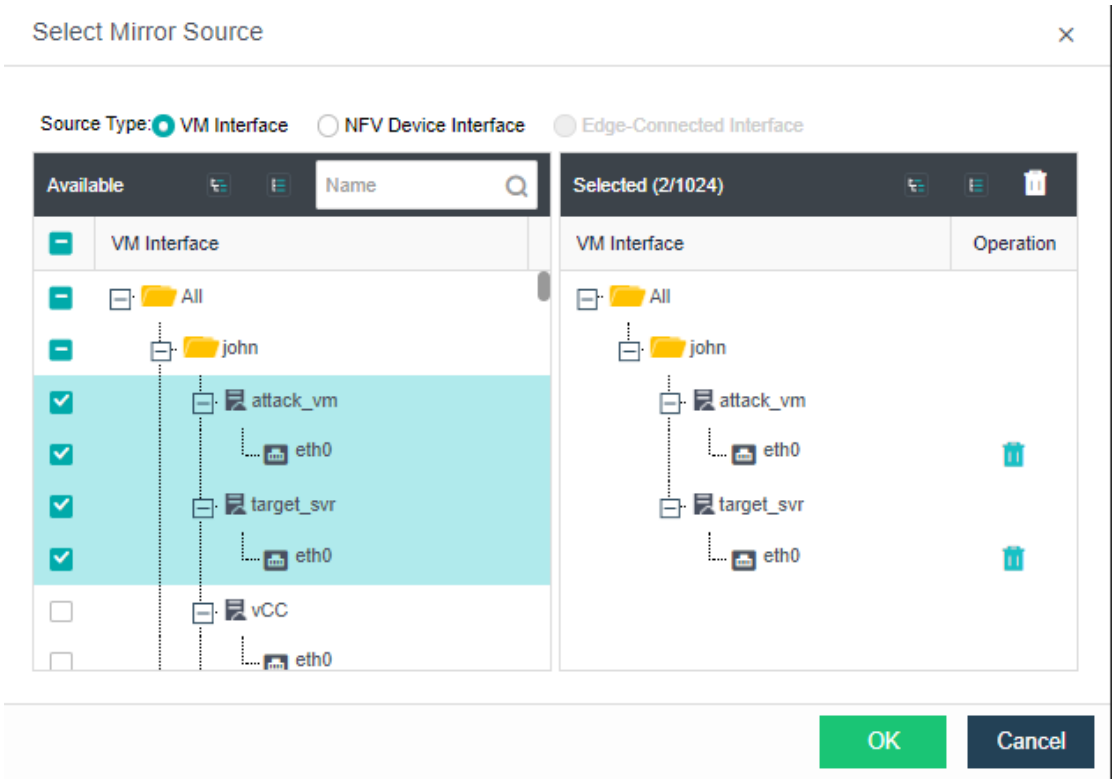
Navigate 【Networking/Traffic Mirroring】



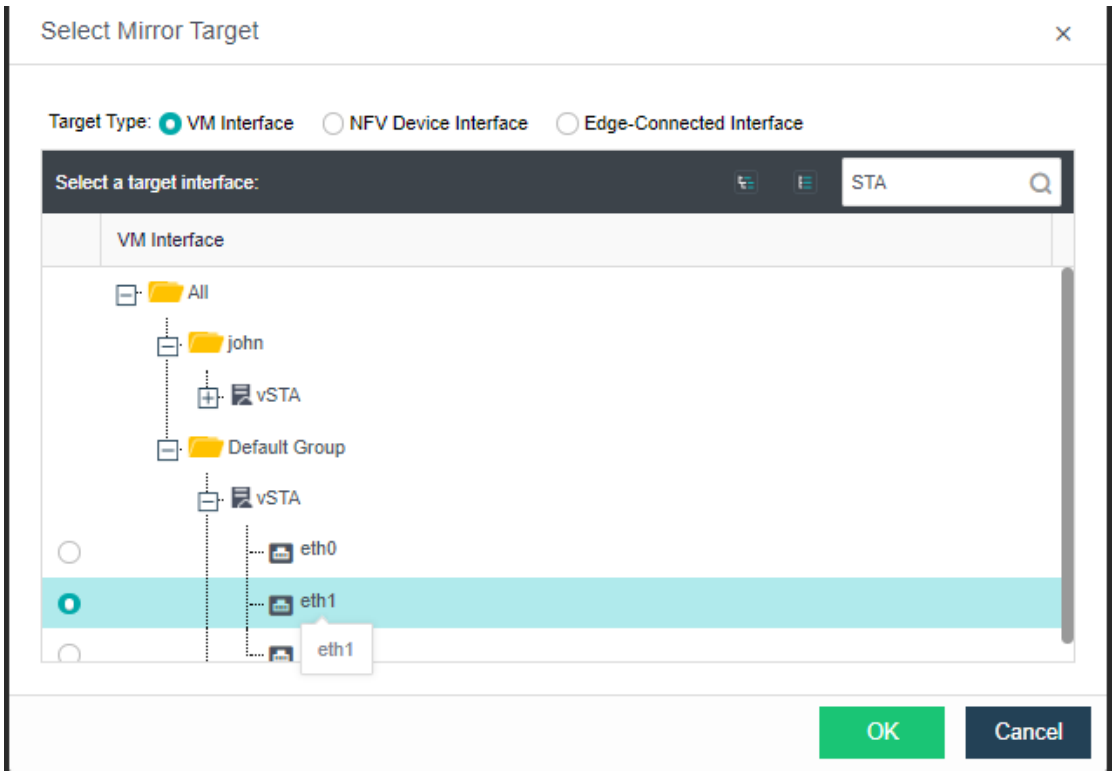
Click "New" to create a traffic mirroring policy. Fill in the necessary information in the pop-up window



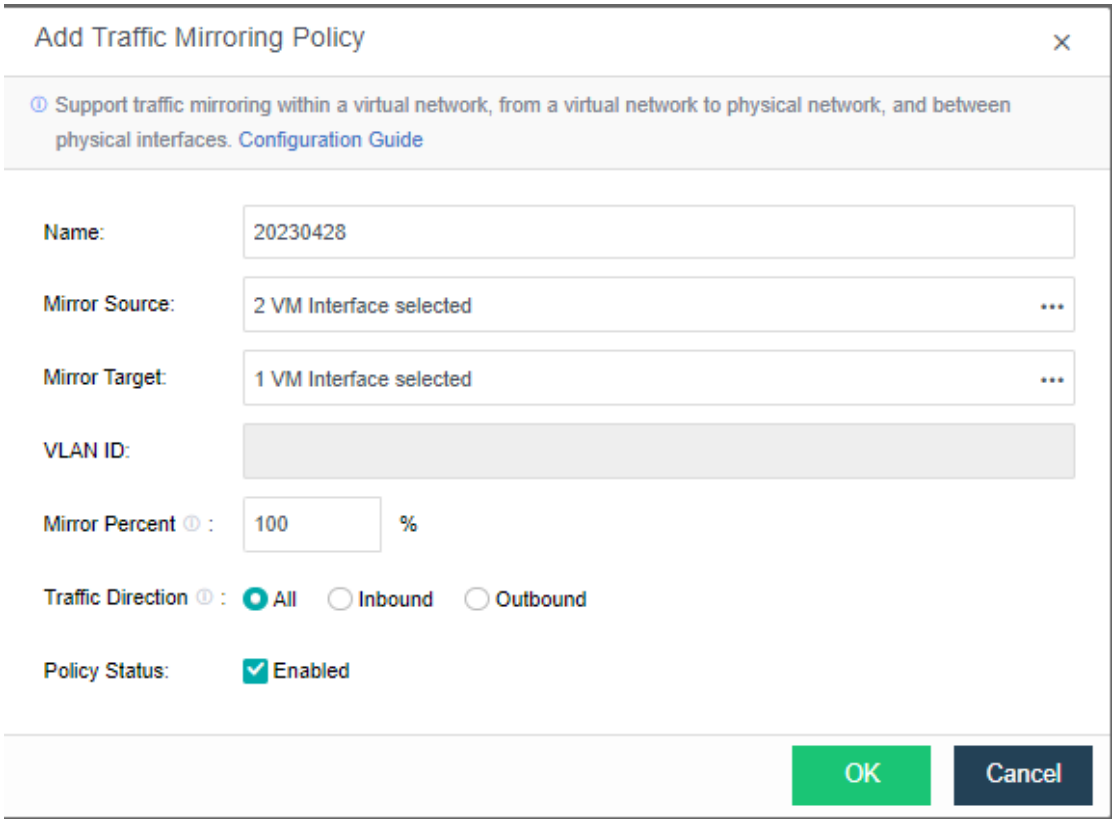
Select the source virtual machine NICs to Mirror Source

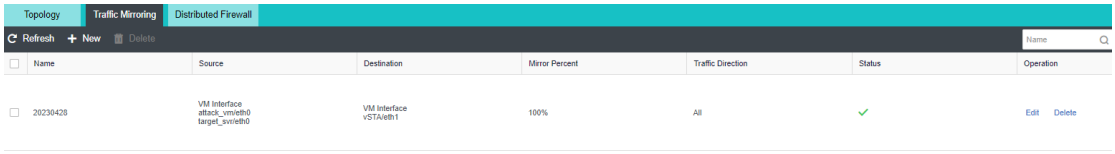


Select mirroring NIC of STA to Mirror Target.



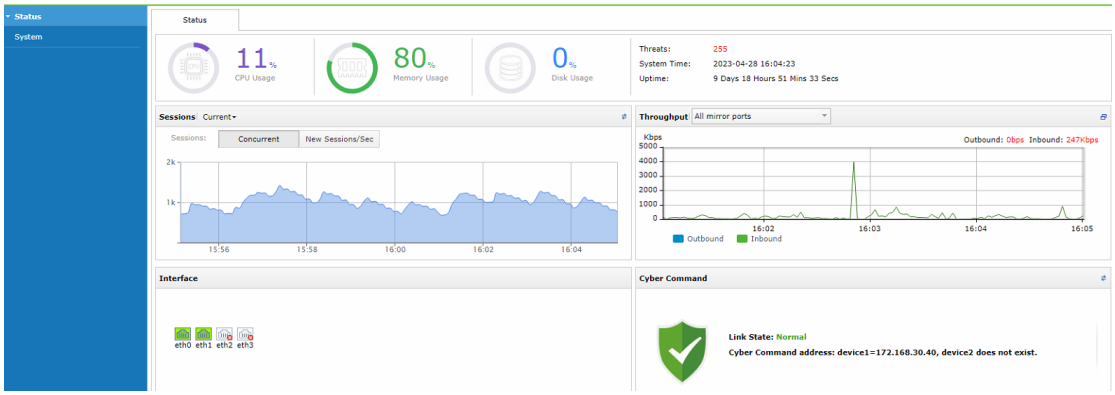
Other settings ca keep the default, click OK to complete the configuration.

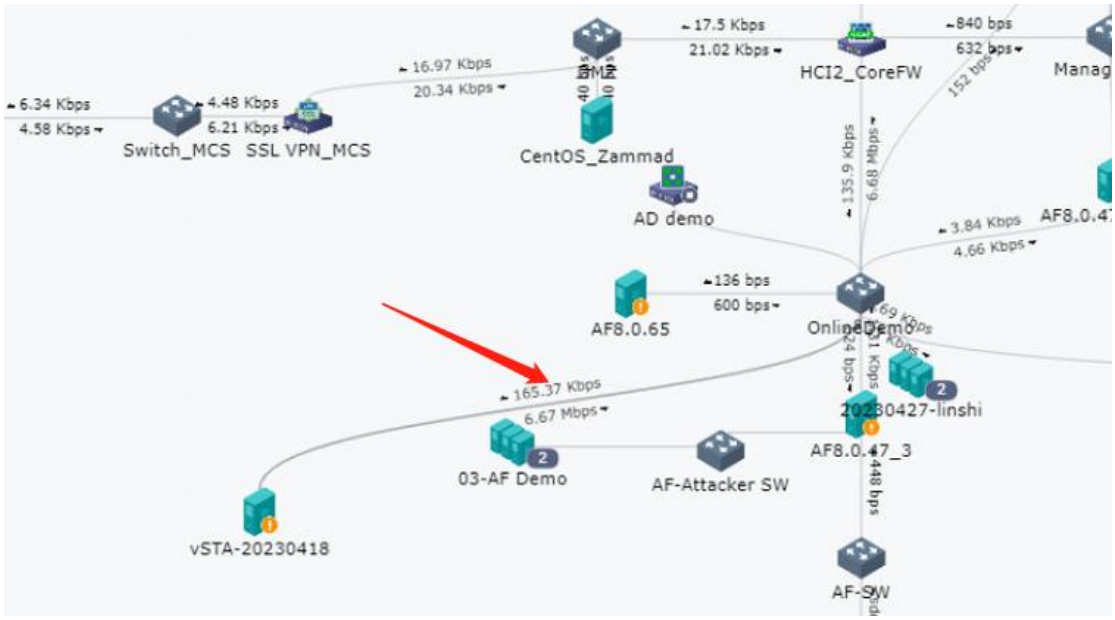


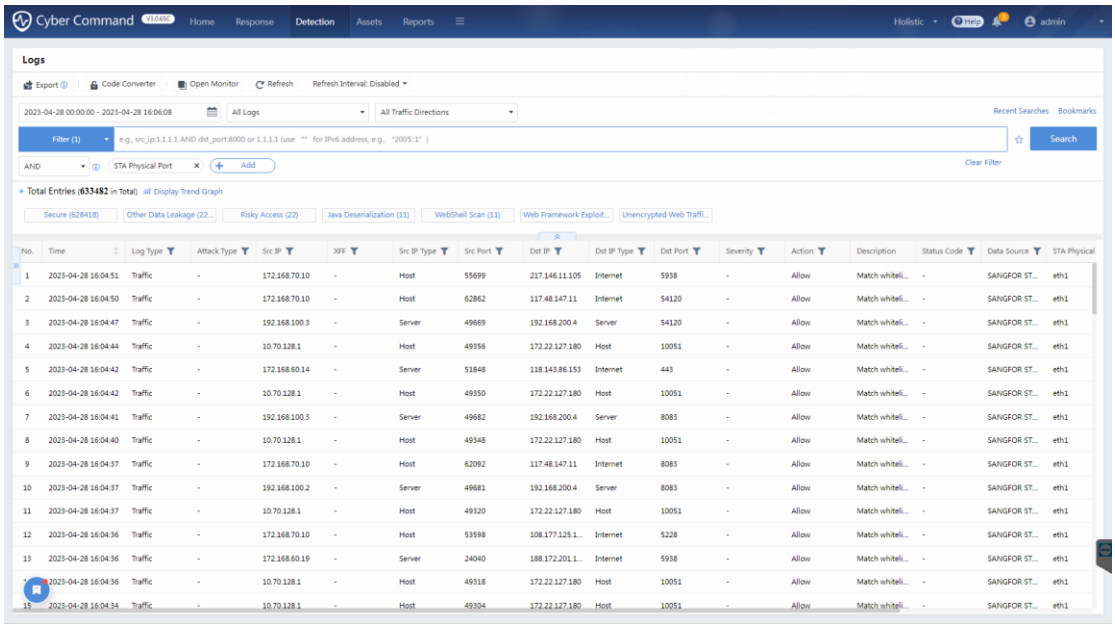


1.4 Validity Verification

You will see the incoming traffic as expected and some analysis in CC platform.






Cyber Command
Home
Response
Detection
Assets
Reports
Logs
Export
Code Converter
Open Monitor
Refresh
Refresh Interval: Disabled
All Logs
All Traffic Directions
Recent Searches
Bookmarks
Filter (1)
Search
Clear Filter
STA Physical Port
Add
Total Entries (633482 in Total)
Display Trend Graph
No.
Time
Log Type
Attack Type
Src IP
XFF
Src IP Type
Src Port
Dst IP
Dst IP Type
Dst Port
Severity
Action
Description
Status Code
Data Source
STA Physical
1 2023-04-28 16:04:51 Traffic 172.168.70.10 Host 55699 217.146.11.105 Internet 5938 Allow SANGFOR ST... eth1
2 2023-04-28 16:04:50 Traffic 172.168.70.10 Host 62862 117.48.147.11 Internet 54120 Allow SANGFOR ST... eth1
3 2023-04-28 16:04:47 Traffic 192.168.100.3 Server 49669 192.168.200.4 Server 54120 Allow SANGFOR ST... eth1
4 2023-04-28 16:04:44 Traffic 10.70.128.1 Host 49356 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1
5 2023-04-28 16:04:42 Traffic 172.168.60.14 Server 51848 118.143.86.153 Internet 443 Allow SANGFOR ST... eth1
6 2023-04-28 16:04:42 Traffic 10.70.128.1 Host 49350 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1
7 2023-04-28 16:04:41 Traffic 192.168.100.3 Server 49682 192.168.200.4 Server 8083 Allow SANGFOR ST... eth1
8 2023-04-28 16:04:40 Traffic 10.70.128.1 Host 49348 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1
9 2023-04-28 16:04:37 Traffic 172.168.70.10 Host 62092 117.48.147.11 Internet 8083 Allow SANGFOR ST... eth1
10 2023-04-28 16:04:37 Traffic 192.168.100.2 Server 49681 192.168.200.4 Server 8083 Allow SANGFOR ST... eth1
11 2023-04-28 16:04:37 Traffic 10.70.128.1 Host 49320 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1
12 2023-04-28 16:04:36 Traffic 172.168.70.10 Host 53598 Internet 5228 Allow SANGFOR ST... eth1
13 2023-04-28 16:04:36 Traffic 172.168.60.19 Server 24040 Internet 5938 Allow SANGFOR ST... eth1
2023-04-28 16:04:36 Traffic 10.70.128.1 Host 49318 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1
15 2023-04-28 16:04:34 Traffic 10.70.128.1 Host 49304 172.22.127.180 Host 10051 Allow SANGFOR ST... eth1