iNet Intelligent Operation and Maintenance Management Platform Operation Manual 2024

Catalogue

1. Product overview 1
2. Login to iNet page 2
2.1. How to log in to iNet 2
2.2. Page Introduction 2
3. System settings 3
3.1. Licence 3
3.2. Role management 3
3.2.1. Modify role grouping permissions 4
3.2.2. Create a new role group 5
3.3. User management 5
3.3.1. Create User Group 5
3.3.2. Create User 6
4. Config 6
4.1. New Connection Voucher 6
4.2. Data Center Configuration 7
4.3. Business domain configuration 8
4.4. Add device 8
4.4.1. New Firewall 9
4.4.2. Overview of piping equipment 11
4.4.3. Equipment Configuration Management 12
4.4.4. Installation of piping equipment 26
5. Policy Search 32
6. Policy analysis 34
6.1. Security policy 34
6.1.1. Optimization analysis 35
6.1.2. Compliance analysis 41
6.1.3. Hit analysis 42

6.2. Compliance Rule Library 42
6.2.1. Customize regular rules 43
6.2.2. Custom Rules 43
6.2.3. Zone rules 43
6.3. Analysis Task 45
6.4. Report Configuration 47
6.5. Convergence 47
6.5.1 Create Convergence Task 48

1. Product overview

iNet is an automation platform aimed at solving increasingly complex network operation and maintenance problems, helping enterprises achieve automation and intelligent IT operation and maintenance transformation, and helping users achieve a leap from manual operation and maintenance, tool operation and maintenance to automated operation and maintenance.

iNet parses and models the configuration of mainstream network devices, forming a unified configuration model, providing a comprehensive configuration management interface, and supporting a series of complex network operation and maintenance scenarios through orchestration engines. Through iNet, network administrators can efficiently and compliantly automate the operation and maintenance of network devices.

iNet supports Cisco Juniper、Fortinet、Paloalto、Hillstone、CheckPoint、 Huawei、H3C, Topsec、Sangfor、Chaitin、Dptech、Venus、Leadsec、Tsinghuanovel and other mainstream firewall manufacturers' equipment are configured and managed with relevant policies.

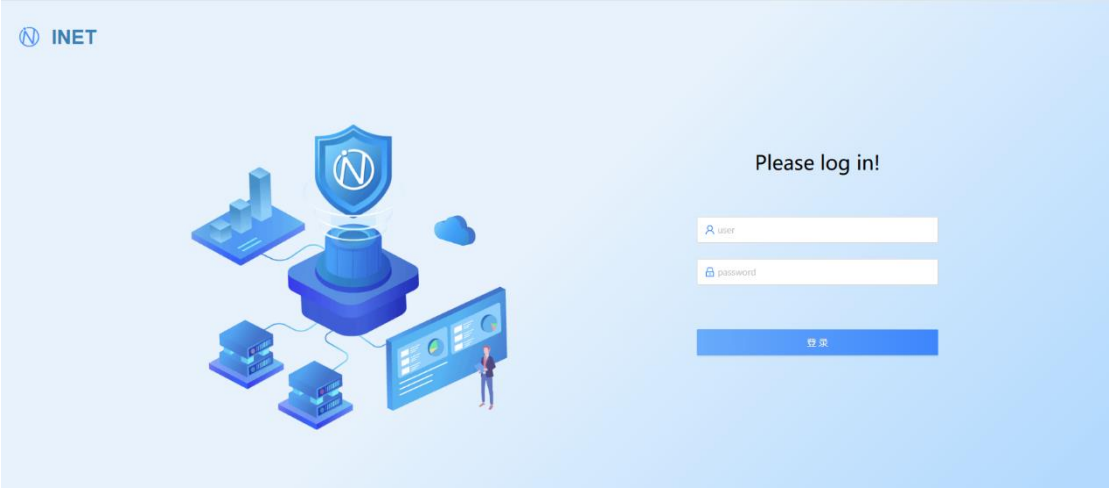
iNet can support the configuration and management of mainstream load balancing devices from manufacturers such as F5, Hillstone, Sangfor, Dptech, Horizon, and Infosec.

2. Login to iNet page

2.1. How to log in to iNet

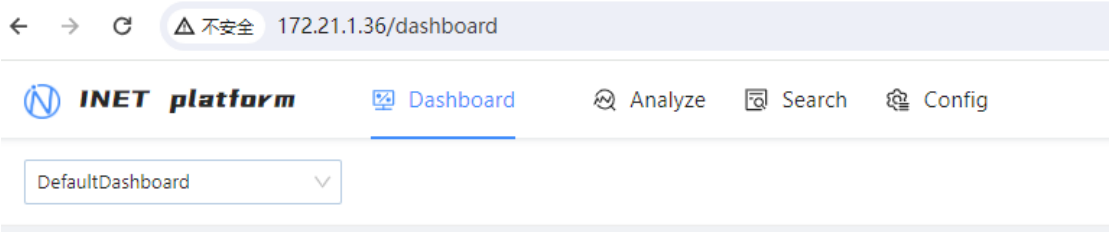
Taking virtual server 172.21.1.36 as an example, open a browser (such as Firefox, Chrome) and enter the address in the address bar http://172.21.1.36/ .

After opening the login page, enter the administrator username and password. The default username and password is **admin/r00tme**, and click "**Login**"



2.2. Page Introduction

After logging in, five main functional components will be displayed. Including **Dashboard**、**Analyze**、**Search and config**。



Dashboard: Platform equipment, configuration, change overview, and quick navigation interface;

Analyze: Firewall security compliance analysis, unified policy management;

Search: Unified search interface for firewall policies across the entire network;

Config: Visual management of network devices and configurations, forming a visual network graph;

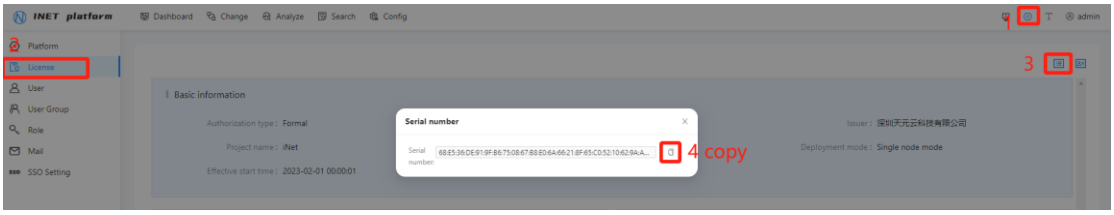
3. System settings

The initial login operation of iNet requires iNet license authorization in the system settings window, and the license authorization code needs to be provided by contacting the manufacturer.

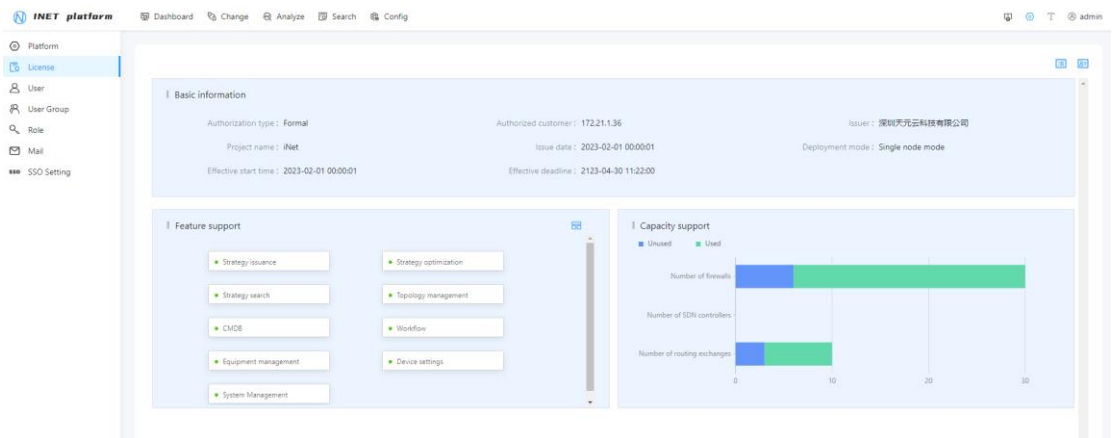
Set the entrance to "Settings - License".

3.1. Licence

The application for iNet license authorization requires obtaining the unique serial number of iNet on the deployed iNet platform in advance and submitting it to the vendor to apply for authorization. As shown below:



According to the customer's testing scenario requirements, provide the iNet serial number to the manufacturer to apply for the corresponding license authorization code. After the authorization operation, you can view the valid start and end times of the license, as well as the list of functional features applied for, from the basic information as follows:



3.2. Role management

In the iNet platform, role management refers to setting the location of user account permissions. The platform initialization defaults to two role names, **ROLE-ADMIN** and **default_role**.

ROLE-ADMIN contains Dashboard, Change, Analyze, Search and config all permissions.

Default_role does not have any permissions.

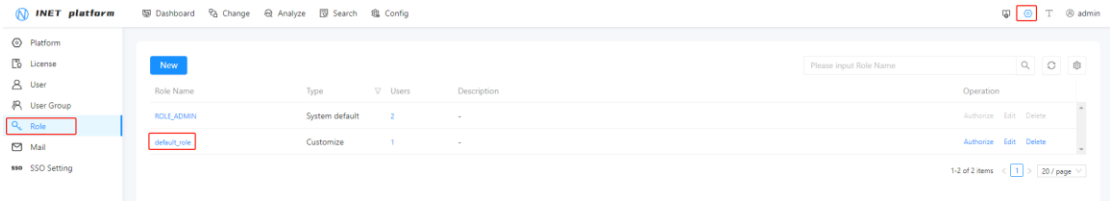
The platform supports modifying existing role grouping permissions and creating new role groups. In the authorization directory, there are module names, submodule names, and functional authorizations.

Module Name: Dashboard, Change, Analyze, Search and config All Permissions.

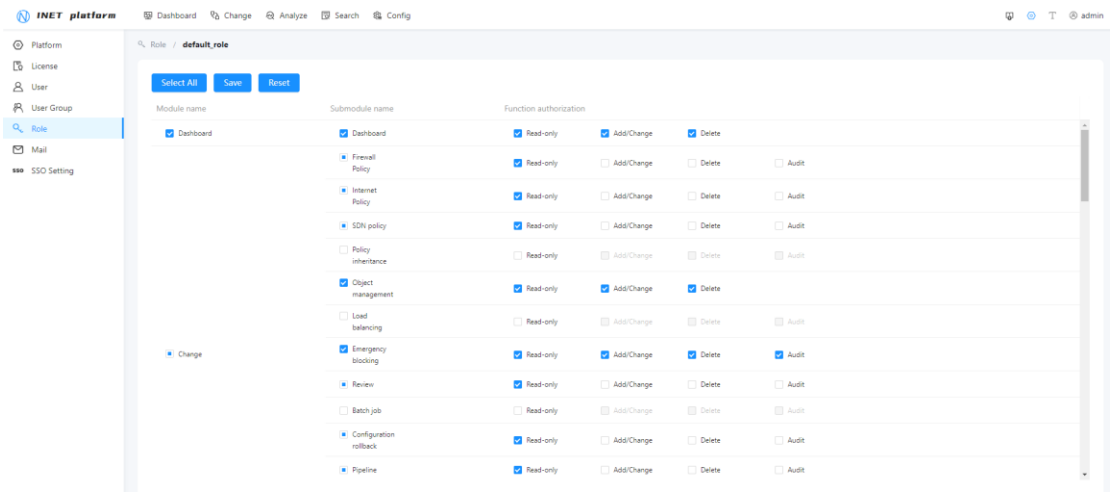
Submodule name: submodules within each module.

Function authorization: For each submodule, there are options for read-only, add/modify, and delete function authorization.

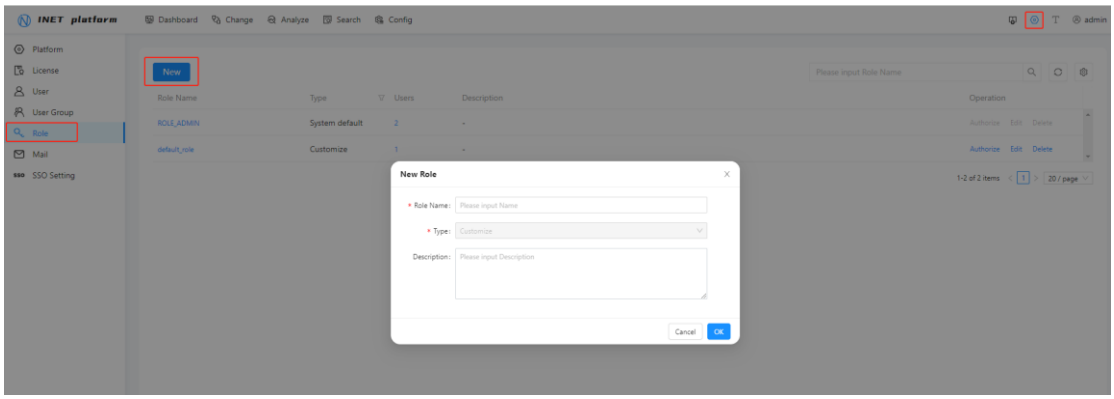
3. 2. 1. Modify role grouping permissions



Click on Settings→ Role, click on User. As shown below, an authorization settings option box will appear, which contains all the functional options supported by the platform. The platform supports selecting as needed, selecting all, and then clicking save to reset.



3. 2. 2. Create a new role group

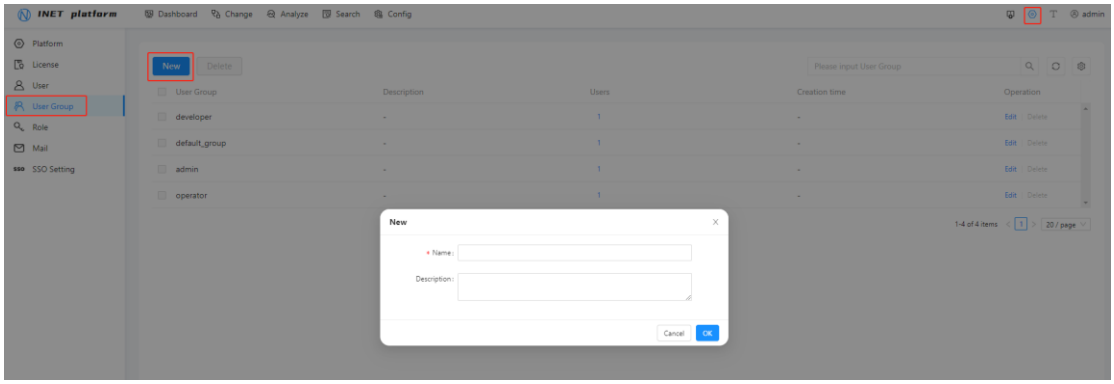


Click "New" in Role, as shown above, a "New Role" dialog box will appear. Enter "Name" and it will be automatically created. By default, there is no permission authorization. Check the function items as needed, and refer to "Modify Role Group Permissions" for authorization settings.

3. 3. User management

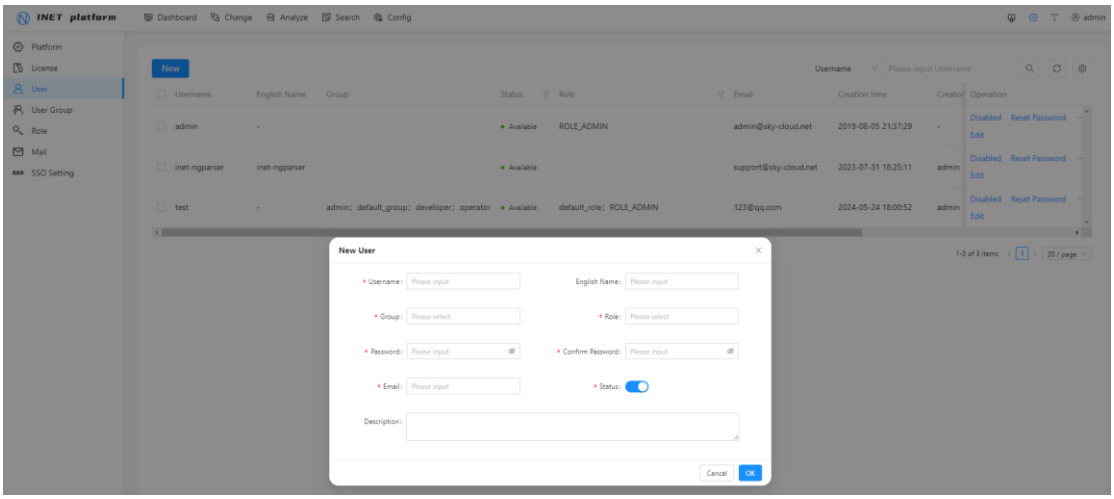
In the iNet platform, user management can be used to create users and user groups, with each user being associated with a user group and user role.

3. 3. 1. Create User Group



Click on Settings → User Group, then click on "New". As shown above, a dialog box for creating a new user group will appear, with red "*" indicating required fields.

3. 3. 2. Create User



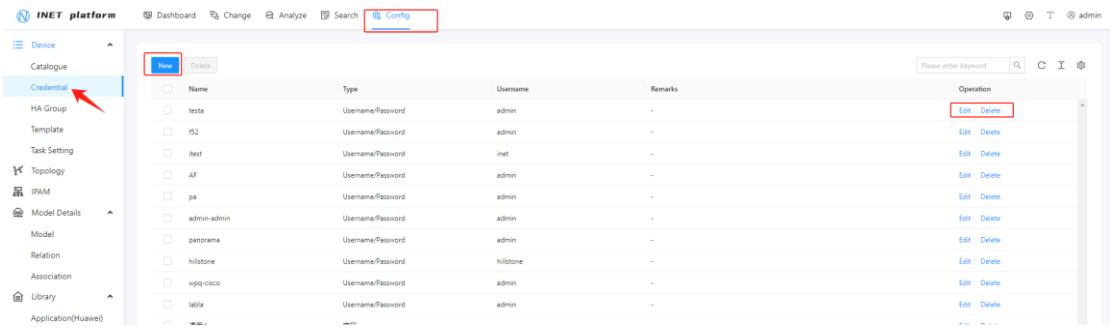
Click on Settings → User, then click on "New". As shown above, a dialog box for creating a new user will appear, with red "*" indicating required fields.

4. Config

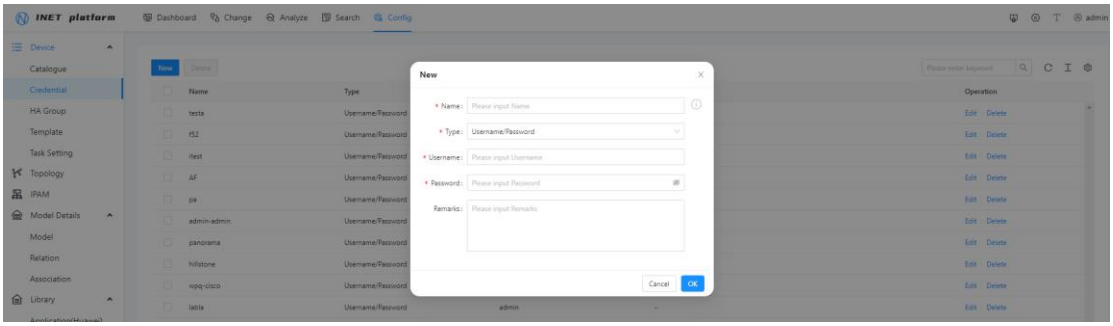
Visual management of network equipment and configuration, semi-automatic topology construction, and unified search and inspection of relational object databases are all completed in network automation.

4. 1. New Connection Voucher

The iNet platform currently supports the management of devices in SSH, HTTPS, and HTTP formats. Before operating the management device, a connection certificate for the device needs to be created, which mainly includes the name and type of the certificate (currently supports username/password and simple password methods). Connection credentials are used when connecting devices. Click on the Config→ Device→ credential (indicated by the red arrow). You can see the corresponding connection credentials. Vouchers can be edited or deleted.



Click New to enter the new interface, as shown below.



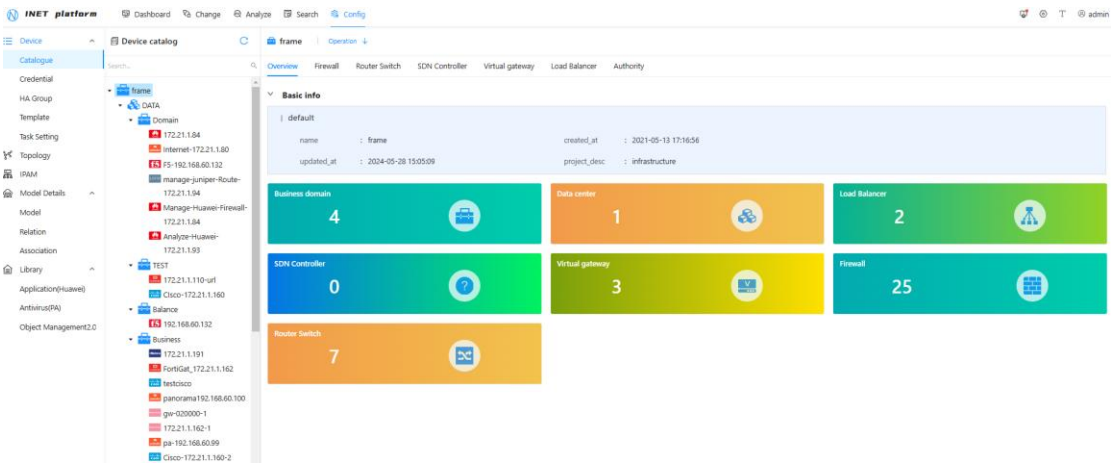
- **Name:** Enter the name of the connection credential;
- **Type:** Connection method, currently supports username/password and simple password methods;
- **Username:** The username used for device login, and the account's permissions require issuing permissions;
- **Password (encrypted):** The password corresponding to the login device username;
- **Remarks (optional):** Enter a note item and description for this connection credential.

The editing interface for connecting credentials is the same as the new interface.

4. 2. Data Center Configuration

After creating a new connection credential, it is necessary to create a new 'Data Center' instance. A data center instance refers to a collection of customers' network devices. Including firewalls, switches, routers, load balancing, and business domains. The newly added network devices are all added at this data center instance level.

Set the entry to "Config - Device - Catalogue".



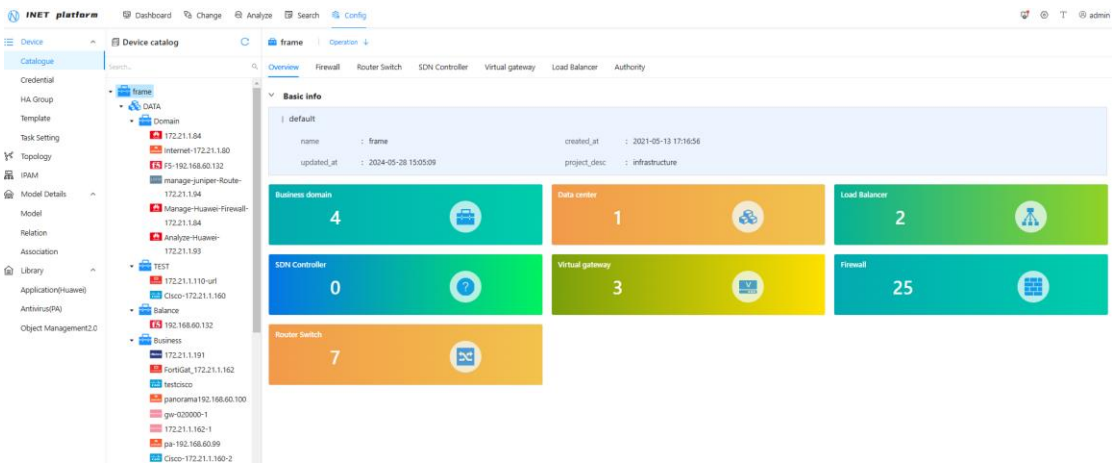
Click on Configure - Device - Catalogue, click on "frame", and then click on

"Operation" (red box). Create a new data center or edit it; Or simply right-click on the frame.

In the new page, enter the instance name (i.e. the name of the data center). Explanation is to annotate the content of this data center (optional). After clicking "OK", complete the addition of a new data center. After creating a new data center, add business domains to this data center instance.

4.3. Business domain configuration

Click on the newly created data center, which is now empty. Click on 'Operation' to display the options for creating a new business domain, editing and deleting, or simply right-click on the newly created data center to create a business domain. (To delete a data center, it is necessary to ensure that there are no related business domains; to delete a business domain, it is necessary to ensure that there are no management devices under that business domain)

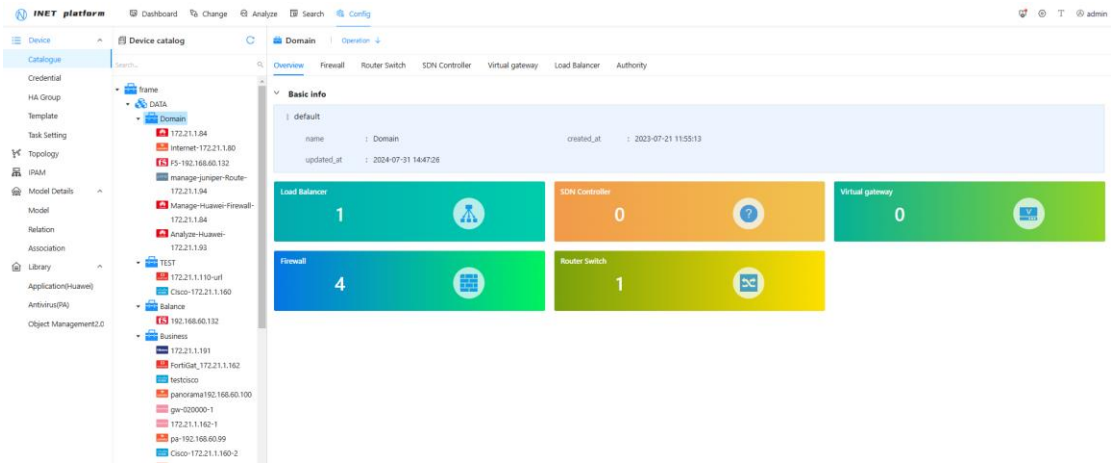


Select the new business domain, enter the instance name of the business domain, click "OK", and complete the creation of the business domain.

4.4. Add device

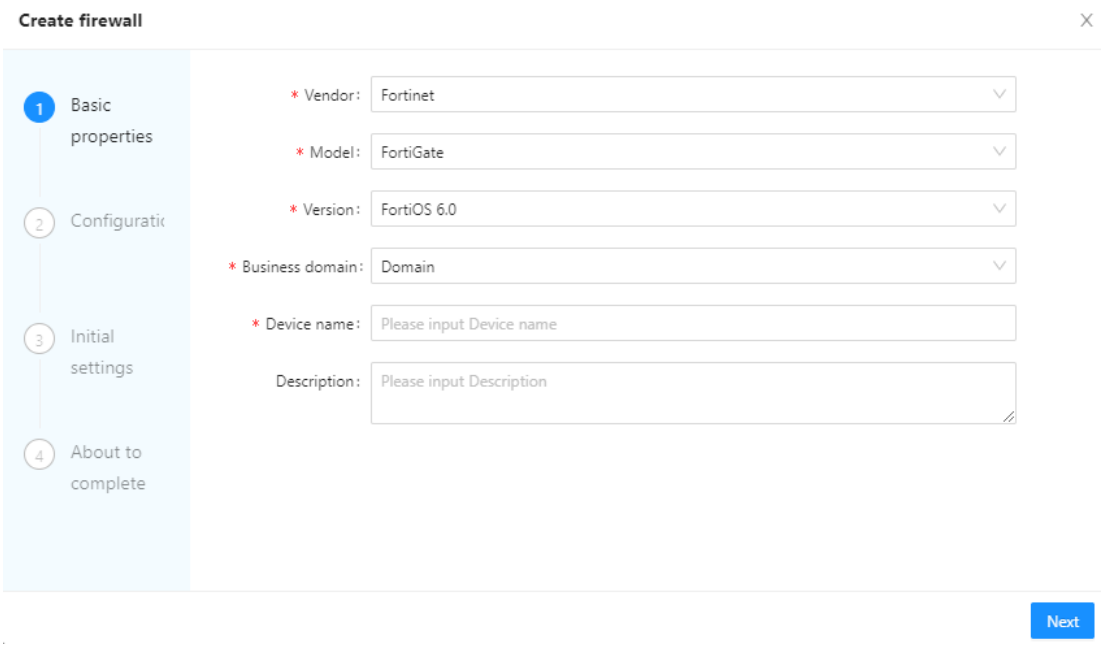
After completing the addition of the business domain, devices can be added to the business domain. Currently, it supports adding firewalls, switches, routers, load balancing, and creating new virtual gateways.

At the business domain level, click on "Operation" and the menu bar will display "New Firewall", "New Virtual Gateway", "New Load Balancing", and "New Routing Switching". Both 'edit' and 'delete' are operations within the business domain.



4. 4. 1. New Firewall

Click on 'Create firewall' and the page for adding a firewall will appear. As shown below.



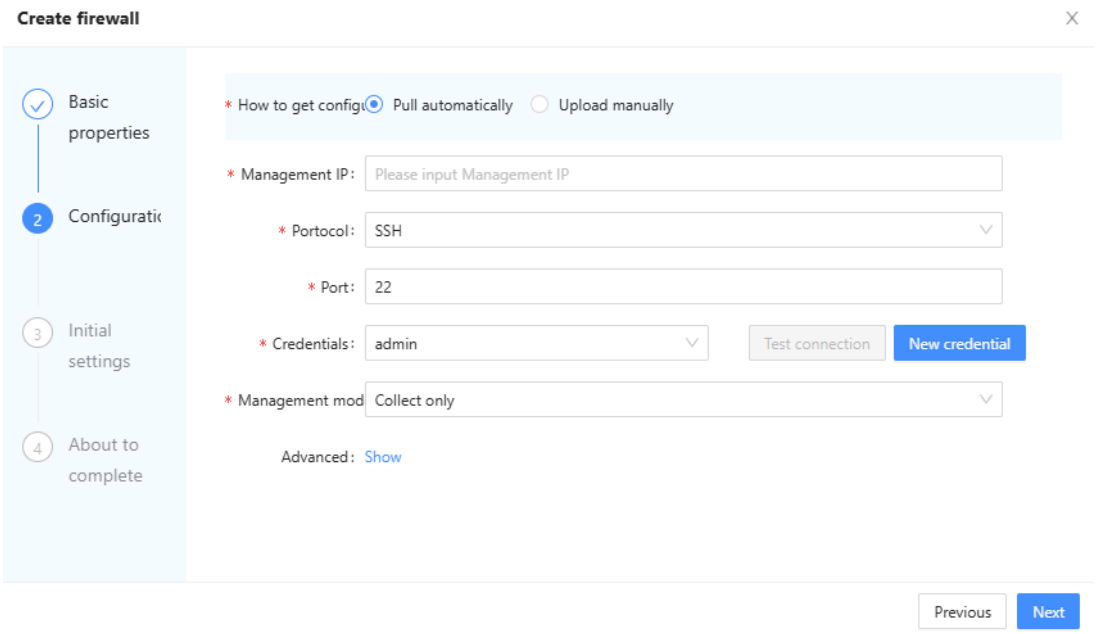
The process of adding a firewall is a configuration wizard. The first page is' Basic Properties'. The 'Basic Attributes' require the following options to be entered:

Manufacturer: Add the manufacturer of the object firewall and select the corresponding manufacturer of the device from the drop-down menu. Currently supports mainstream firewall brands such as FortiNet, Juniper, Cisco, and Hillstone;

- **Model:** The dropdown menu allows you to select the firewall model of the manufacturer, such as Juniper corresponding to SRX and Cisco corresponding to ASA;

- **Version:** OS version of the firewall;
- **Business** Domain: Add the business domain to which the object firewall belongs and automatically associate and generate it;
- **Device Name:** Fill in custom device name.

After selecting the above information, click "Next" to enter the second wizard interface, which is "Configuration Management".



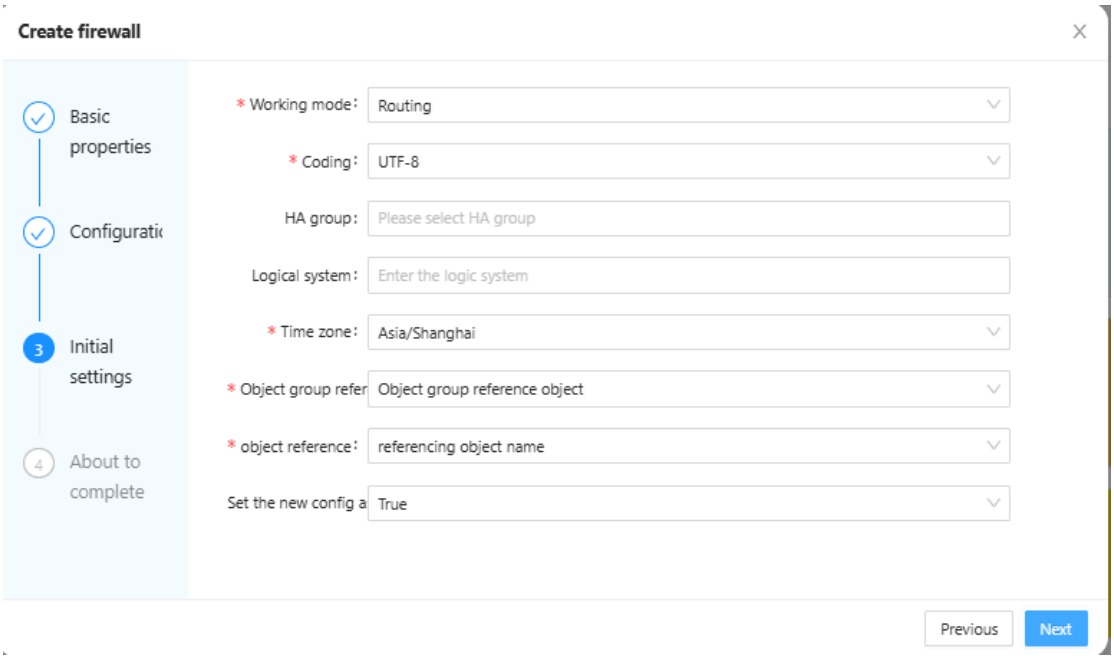
In "Configuration Management", the following options need to be entered:

- **Collection mode:** Select automatic collection, so that the platform regularly performs "connection status check", "configuration collection", "routing collection", etc;
- **Management IP:** Enter the corresponding management IP address for the management firewall;
- **Protocol:** Except for CheckPoint and DeepTrust, other firewalls choose SSH; Checkpoint and DeepTrust choose HTTPS;
- **Port:** Automatically associate port numbers based on the selected protocol, or customize port numbers to be filled in;
- **Connection credentials:** Click on the white option, select the created credential information, or directly create a new credential. After selecting the credential, perform a connection test directly to verify the connectivity of the device and

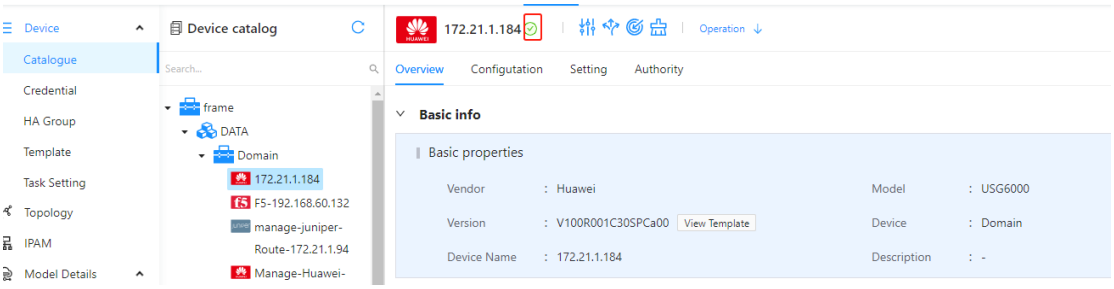
the accuracy of the account password, indicating a normal connection;

- **Management mode:** Select collection+distribution.

After completing the above information selection, click "Next" to enter the third wizard interface, which is "Initial Settings".



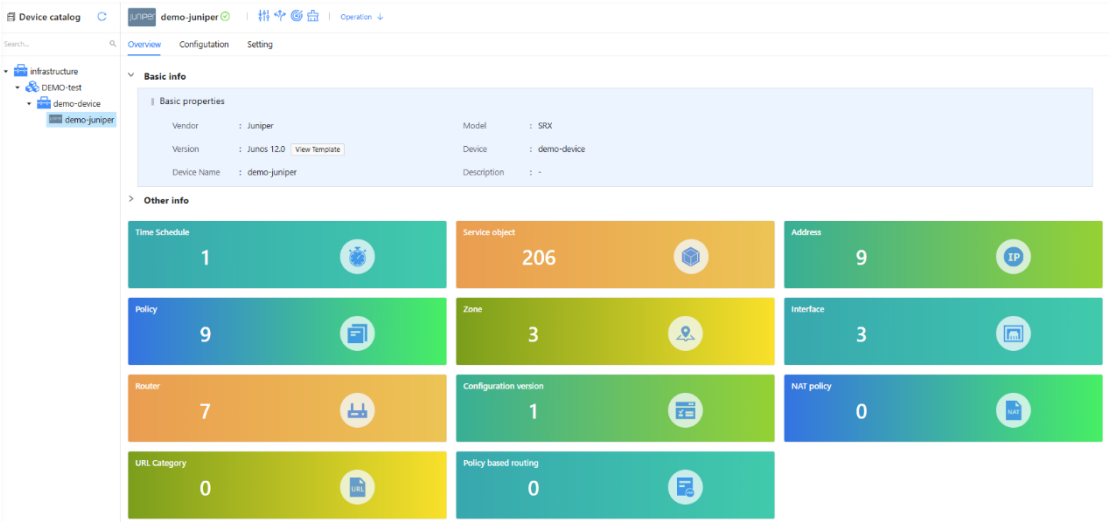
Select the firewall 'working mode', which defaults to 'routing mode'. The rest can be set to default values. Click on 'Next'. Completing the setup indicates successful device management.



4. 4. 2. Overview of piping equipment

At this firewall level, the overview panel, configuration panel, settings panel, and permissions panel of the firewall will be displayed, and by default, the overview panel interface of this firewall will be accessed.

Overview



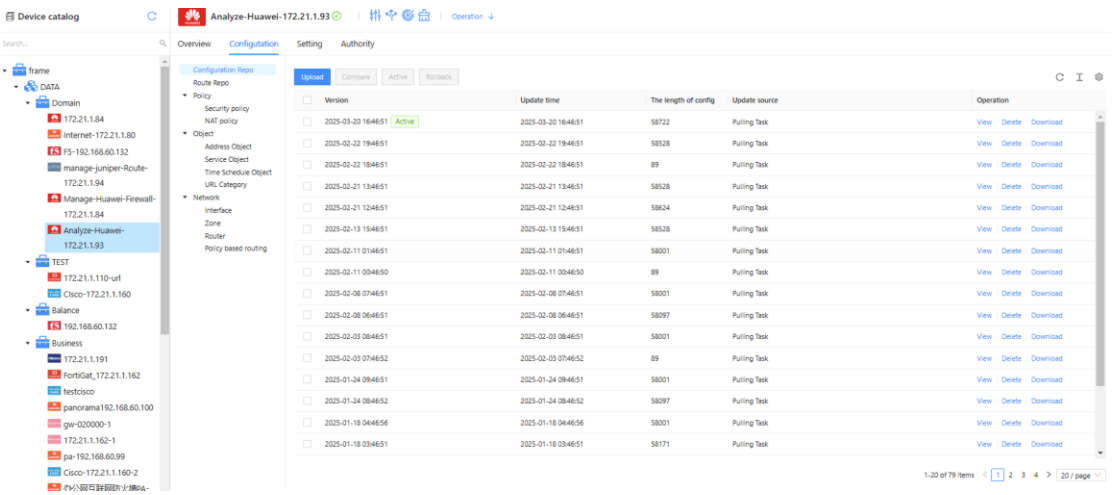
The firewall overview panel interface mainly consists of two parts, one is "Basic Information" and the other is "Other Information"

Basic information: Display the manufacturer, model, version, device group, device name, and description of this firewall

Other information: The platform displays statistical information such as various objects, policies, routes, interfaces, regions, configurations, and URL groups based on the collected information after parsing.

4. 4. 3. Equipment Configuration Management

Click on 'Configuration'. The iNet platform will display detailed information about this firewall. It contains five major items: configuration library, routing library, policy, object, and network.



- **Configuration Repo:** displays current and historical configurations, can view, delete, download, and upload firewall configurations, and can also compare configurations based on different configuration files
- **Routing Repo:** displays collected routing and historical routing information,

supports viewing, downloading, and deleting

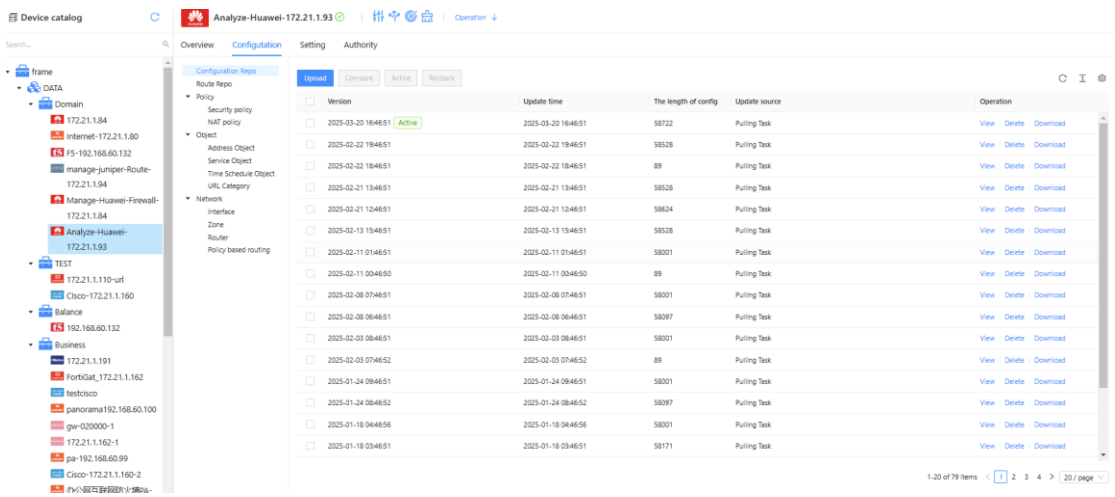
- **policy:** Refers to the current security policy of the firewall, including policy information such as "security policy" and "NAT policy"
- **Object:** including elements of security policies such as "address object", "service object", and "time schedule object"
- **Network:** including network related parameters such as "interfaces", "regions", and "routes"

4.4.3.1. Configuration Repo

The configuration repo stores the current and historical configuration files of the firewall, and updates to the configuration repo are based on two methods: collection tasks and manual uploads.

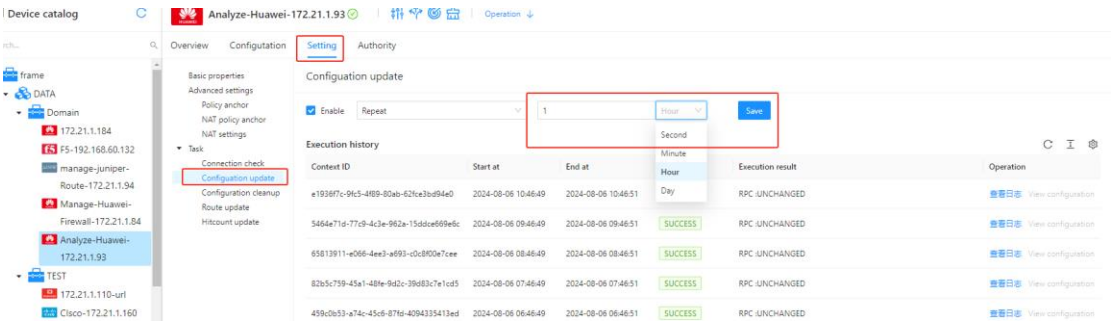
The triggering conditions for the execution of collection tasks can be divided into two types: one is manual triggering of configuration collection updates, and the other is regular collection task execution.

- **Manually triggering configuration updates**



Click on the selected firewall, select "Configuration", click on "Configuration Repo", and then click on "Execute Real time Configuration Collection Task". If there are any changes to the device configuration, the latest current configuration file will be generated. If the configuration has not been updated, no new configuration file will be generated for this collection task.

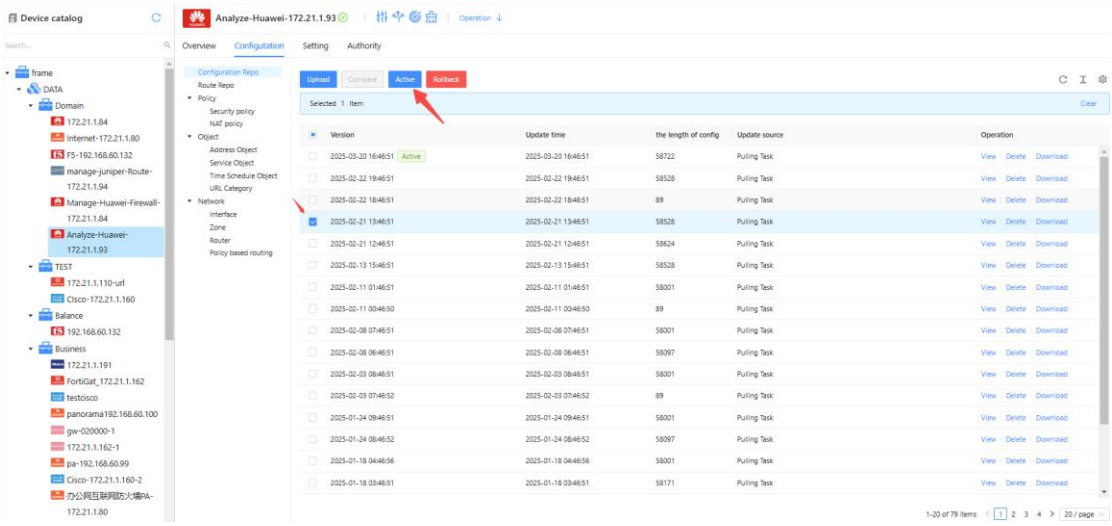
- **Set regular collection tasks**



Click on the selected firewall, select "Setting", click on "Task", and then click on "Configuration Update" to set up regular configuration collection tasks. The default is to collect once every hour. Modify the configuration collection interval as needed. If the collection is successful, the execution information will be displayed SUCCESS.

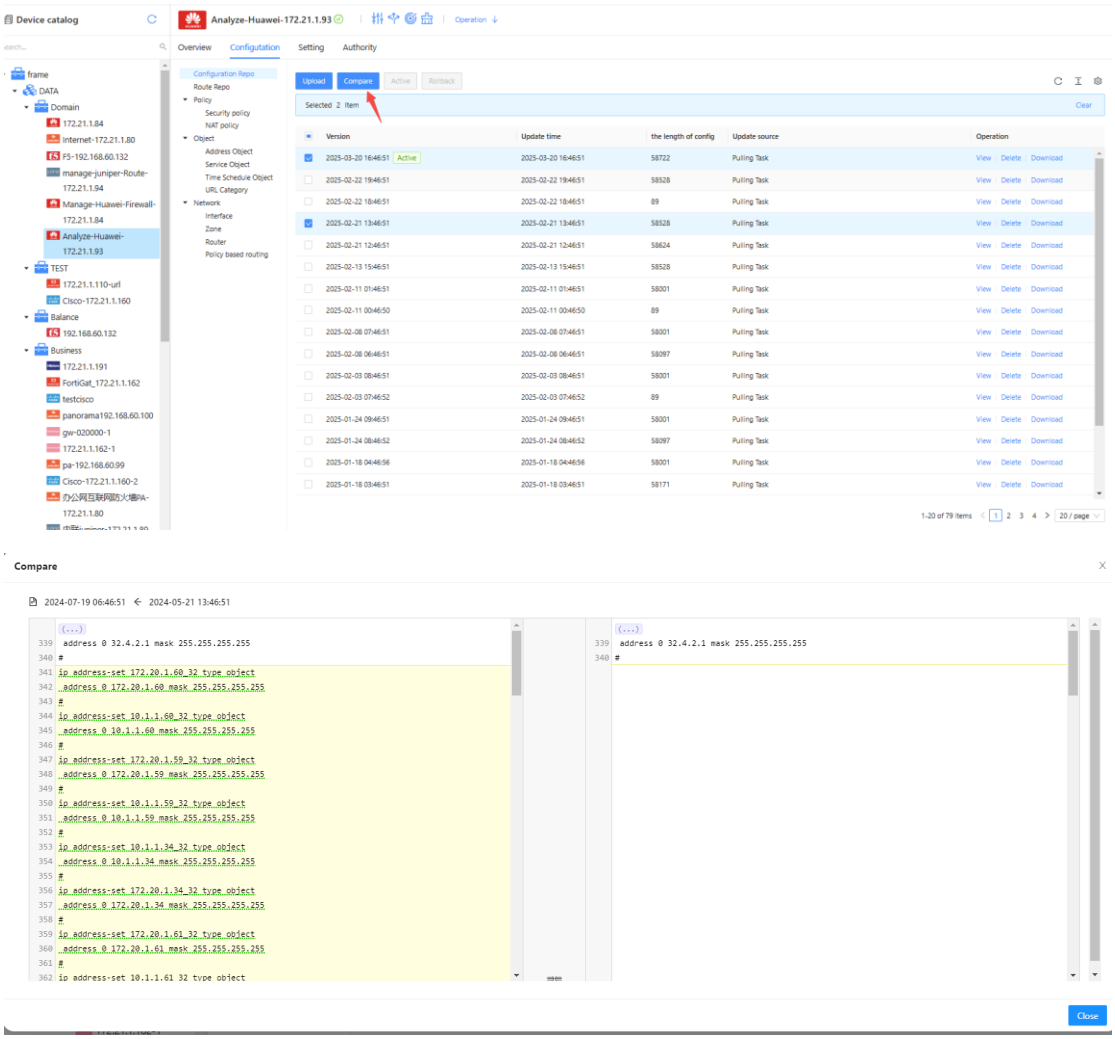
- **Manually upload configuration**

After importing the configuration file into the firewall, it will not be the current configuration file and needs to be manually checked and set to the current version. The 'current configuration' refers to the configuration in which the device is currently running.



Configuration upload "is a manual configuration upload performed by the administrator, but it will not be issued to the device.

'Configuration Comparison' compares two existing configurations. First, check the two configurations that need to be compared. Then click on 'Configuration Comparison', as shown below:



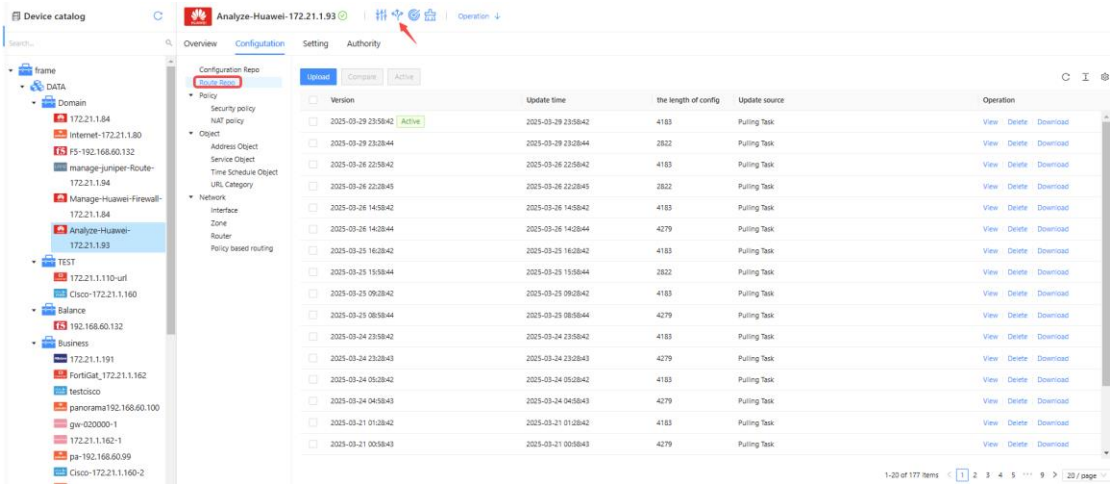
The differences between the two configurations will be displayed in the dialog box shown in the figure above.

4.4.3.2. Routing Repo

The routing repo stores the current routing table and historical routing table files of the firewall. The update of the routing repo is based on two methods: collection tasks and manual uploading.

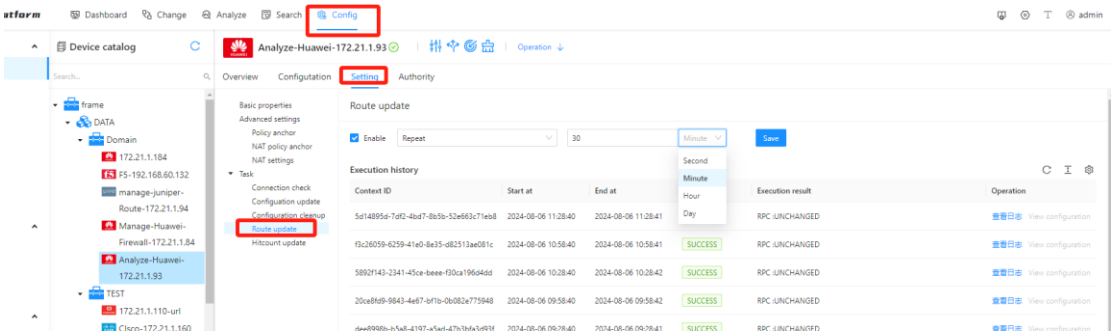
The triggering conditions for the execution of collection tasks can be divided into two types: one is manual triggering of route collection updates, and the other is regular collection task execution.

- **Manually triggering route updates**



Click on the selected firewall, select "Configuration", click on "Routing Repo", and then click on " Execute Real time Routing Collection Task". If there are any changes to the routing entries, the latest current routing file will be generated. If the routing has not been updated, no new routing file will be generated for this collection task. Routing table entries support viewing, deleting, and downloading.

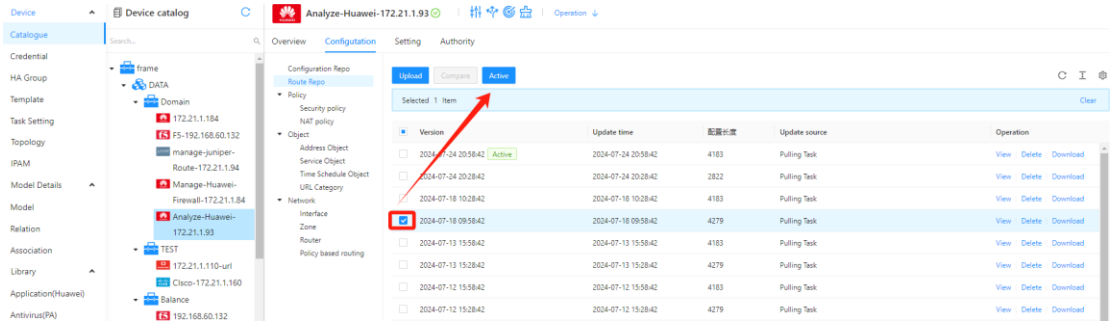
- **Set regular collection tasks**



Click on the selected firewall, select "Settings", click on "Tasks", and then click on "Routing Collection" to set up a regular routing collection task. The default is to collect once every 30 minutes. Modify the routing collection interval as needed. If the collection is successful, the execution information will be displayed SUCCESS.

- **Manually upload routing table entries**

After importing the routing file into the firewall, the routing file will immediately become the current version. The 'current configuration' refers to the routing table entry where the device is currently running.



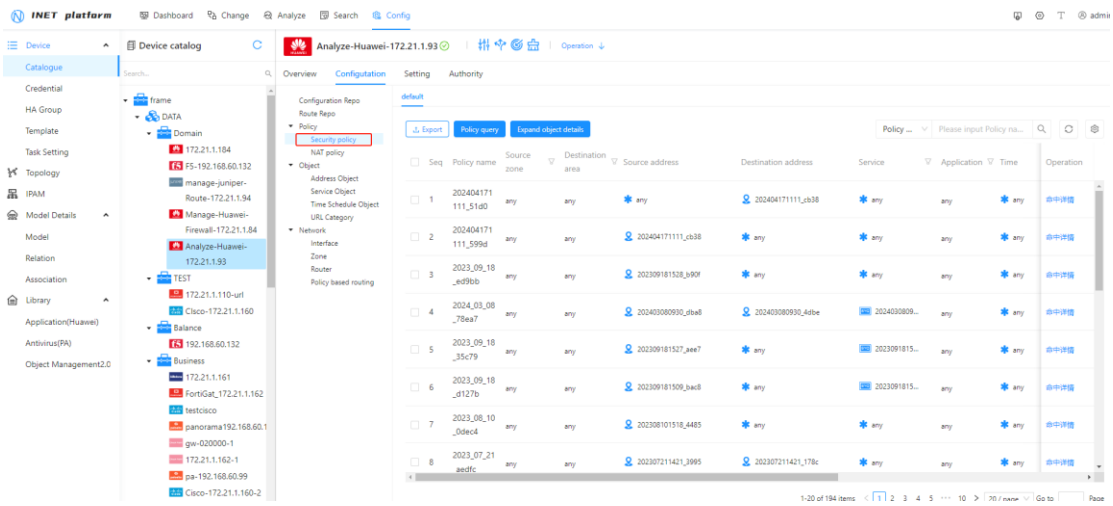
Configuration upload "is a manual routing table item upload by the administrator, but it will not be issued to the device.

'Configuration Comparison' compares two existing configurations. First, check the two configurations that need to be compared. Then click on 'Configuration Comparison', and after comparing the routes, the differences will be highlighted with a color background

4.4.3.3. Policy

- **Security policy**

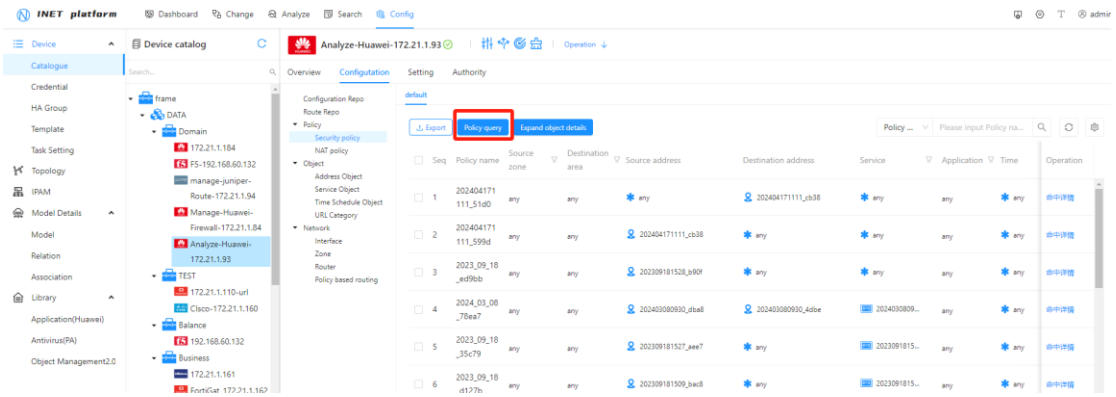
The "Security Policies" section mainly displays the existing security policies of the current firewall. As shown below:



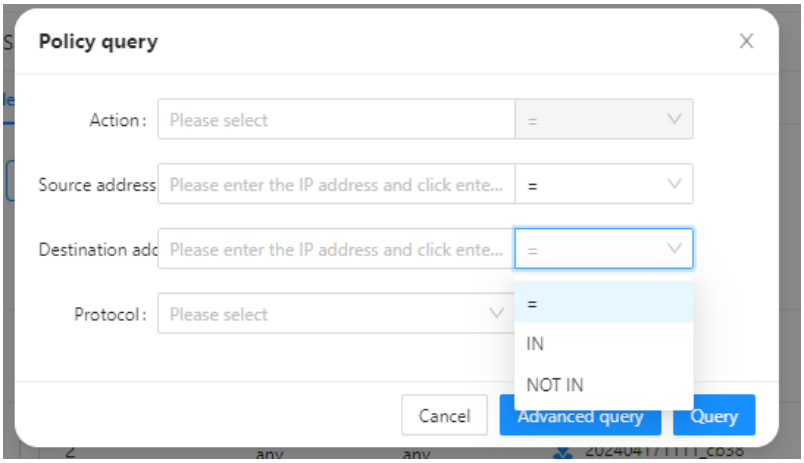
- **policy ID:** The policy IDs are sorted from small to large, corresponding to the order of the policies from top to bottom
- **policy Name:** policy Name
- **Source region:** Zone of policy direction
- **Source interface:** The source port for policy direction
- **Source Address:** The source address matched by the policy

- **Destination zone:** The zone where the policy is directed
- **Destination interface:** Port for policy direction
- **Destination Address:** The destination address matched by the policy
- Time: The effective time point of the policy
- **Service:** Service target
- **Log:** Enable policy session logging function
- **Action:** Represents Permit or Allow, represents Deny or Drop
- **Policy query**

policy query is a precise and fuzzy search for the currently displayed policy. Click on the policy query.

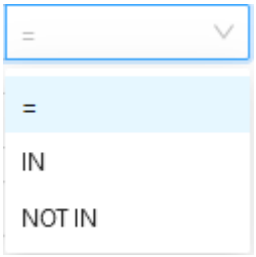


After clicking on 'policy Query', a dialog box will appear



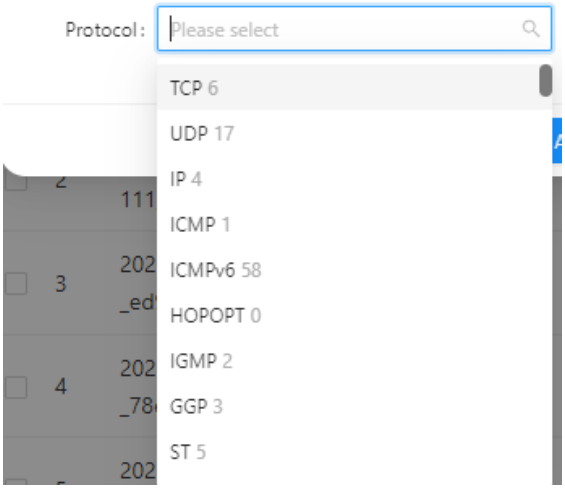
Action: The dropdown menu allows you to select allow or deny;

Source and destination addresses: Enter an IP address (such as 192.168.60.1). The dropdown menu on the right side of the column (red arrow) has options for "=", "IN", and "NOT IN"

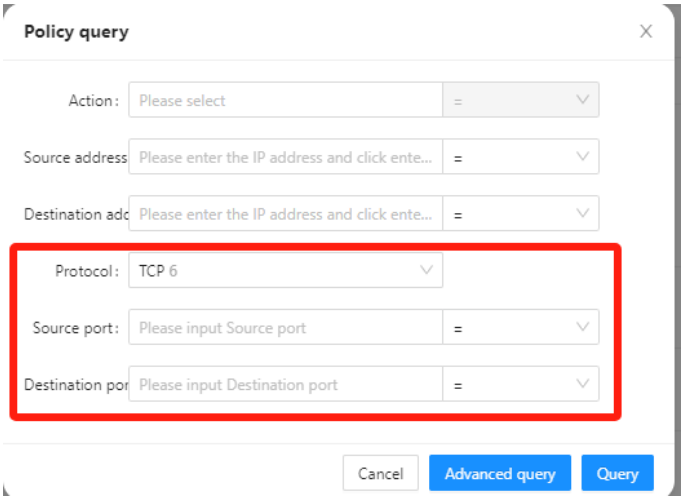


'=' indicates that the IP address needs to match the specific policy exactly. If it is an address segment, it can be written as 10.1.1.0/24 address; 'IN' means that all policies containing the search address will match; 'NOT IN' means that policies that do not include address lookup will be matched.

Protocol: Enter the corresponding protocol number through the drop-down menu, as shown below:

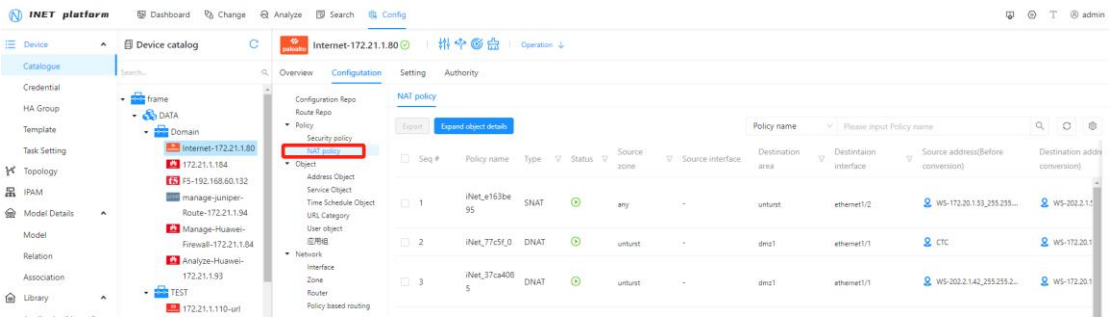


Select the corresponding protocol number. Taking TCP as an example, after selecting TCP, the source and destination ports (red boxes) will appear. The dropdown menu on the right is consistent with the usage of IP addresses, with the addition of ">" and "<". ">" indicates that all values greater than the port number will be queried and displayed; If it is less than the port number value, it will be queried and displayed.



- **NAT Security Policy**

The "NAT Policy" section mainly displays the NAT policies that already exist in the current firewall. The NAT policy is shown below.

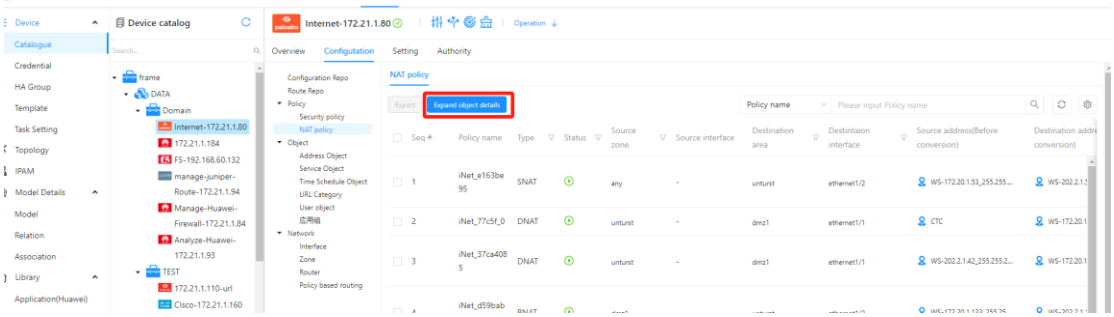


- **Line number: NAT policy IDs are sorted in ascending order, corresponding to policies sorted from top to bottom**
- **policy Name:** policy Name
- **Type:** Types of NAT policies, including SNAT, DNAT, and BNAT
- **Status:** NAT status, indicating enabled, indicating disabled
- **Source region:** Zone of policy direction
- **Source interface:** Interface for policy direction
- **Destination zone:** The zone where the policy is directed
- **Purpose interface:** Interface for policy direction
- **Source address (before conversion):** Address or address segment before source address conversion
- **Destination address (before conversion):** Destination address before conversion
- **Service (before conversion):** Service port before conversion
- **Source Address (Converted):** The address or address segment after source address conversion
- **Destination Address (Converted):** Destination Address Converted Address
- **Service (converted):** converted service port
- **Expand object details**

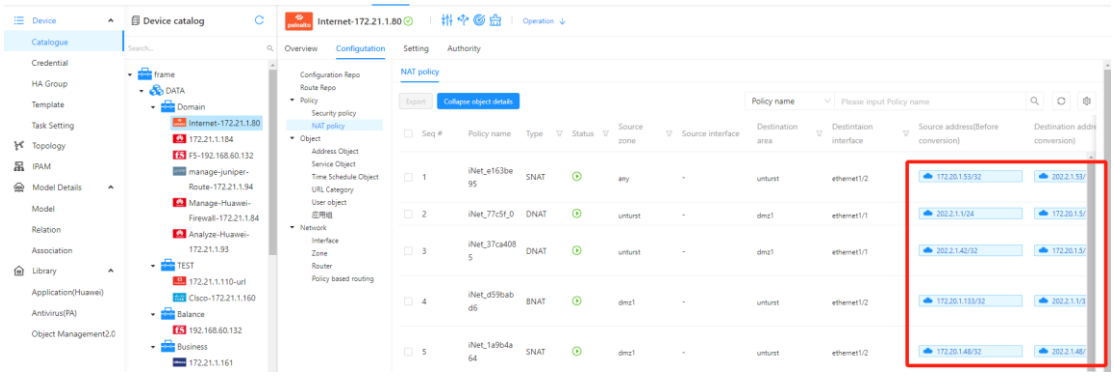
The click policy usually displays the name of the address object rather than the specific address content. You can view the actual address corresponding to the address name through "Expand Object Details". The red box before expanding the

object details shows 192.168.70.0_24 as the address object name. After clicking on 'Expand Object Details', the actual address is 192.168.70.0/24 in the red box after expanding the object details.

- **Before expanding object details**



- **After expanding the object details**



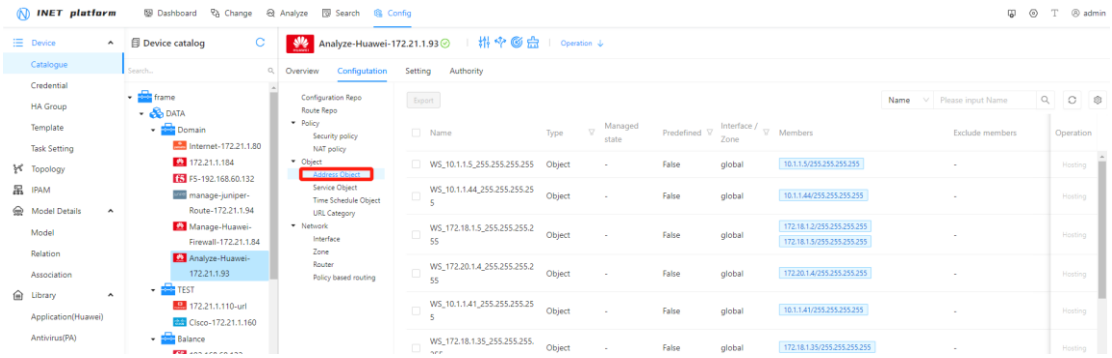
4.4.3.4. Object

The objects include "address objects", "service objects", and "time objects".

- **Address object:** The name of the address object parsed from the firewall configuration;
- **Service object:** Refers to the services or applications defined by the system, mainly used for being referenced by policies. The service targets include both predefined and customized applications of the system, as well as "application groups";
- **Time schedule object:** Refers to the time schedule object referenced by the policy. After referencing, the policy will take effect at the corresponding time and will not take effect at other times.

Address Object :

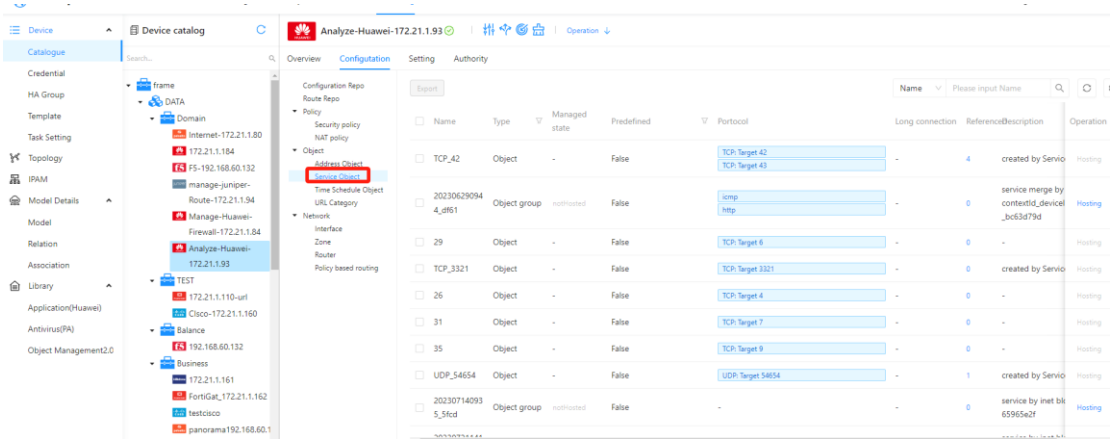
The "Address Objects" section mainly displays the address objects parsed from the firewall configuration. As shown below.



- **Name:** The name of the address object
- **Object type:** divided into "object" and "object group"
- **Predefined:** divided into True and False, True indicates pre-defined, False indicates not pre-defined
- **Interface/Domain:** The interface or domain to which an address belongs. When referenced by a policy, the address will be referred to as the source or destination address based on the direction of the domain
- **Member:** The specific address or address segment included in the address
- Exclude members: In an address member segment, it is allowed to have excluded address members
- **Reference:** Statistics of the number of times referenced by policies

service object

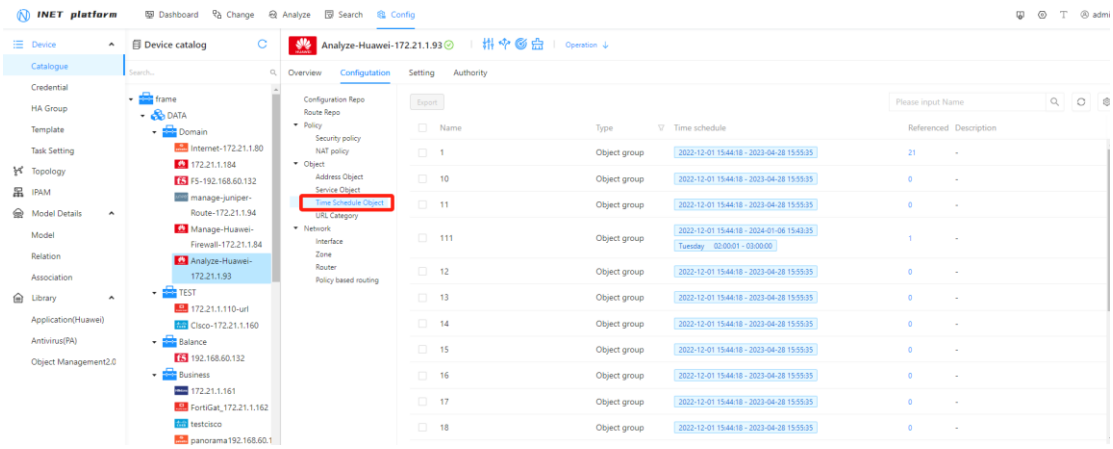
The 'service object' mainly displays the application service objects parsed from the firewall configuration. As shown below



- **Name:** The name of the application service object
- **Object type:** divided into "object" and "object group"
- **Predefined:** There are True and False, True indicates pre-defined, False indicates not pre-defined
- **Protocol:** The actual "protocol type" and "destination port number" of the service object
- **Long link:** The long link time set by the application service
- **Reference:** Statistics of the number of times referenced by policies
- **Hosting:** Service objects can be set as hosting objects

Time Schedule object

The 'time schedule object' mainly displays the time object parsed from the firewall configuration. As shown below



- **Name:** The name of the time object
- **Object type:** usually an "object" of time
- **Time plan:** refers to the specific time setting of the time plan, which includes

two types: "specified time period" and "periodic time period"

- **Reference:** Statistics of the number of times referenced by policies

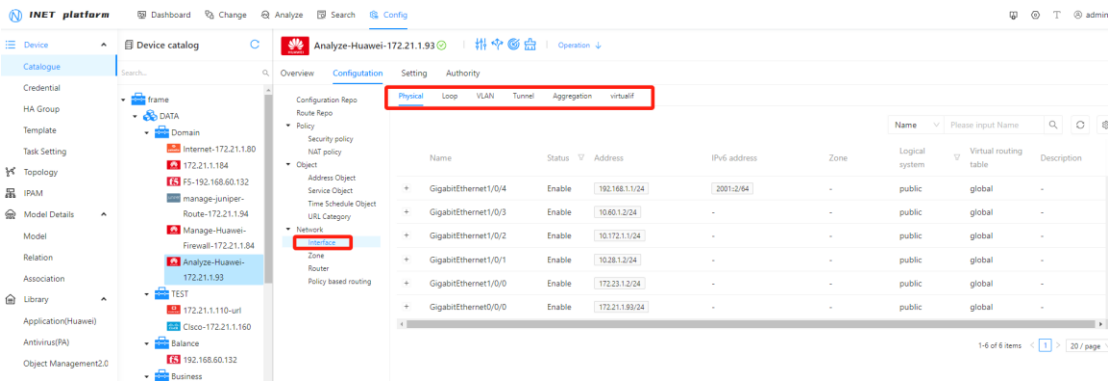
4.4.3.5. Network

Network refers to the network parameters related to firewall devices, including three parameters: "interface", "zone", and "routing".

- **Interface:** Refers to the interface of a firewall, which includes types such as "physical", "loopback", "VLAN", "tunnel", "aggregation", and "virtual", corresponding to different types of interfaces of the firewall;
- **Region:** Some firewalls control traffic exchange based on zones, assigning interfaces to different zones to achieve business isolation;
- **Routing:** The device routing table is obtained by parsing the collected routing table.

Interface

Interface "mainly displays various interface forms parsed from firewall configuration, including" physical "," loopback "," VLAN "," tunnel "," aggregation ", and" virtual ", as shown below. Taking" physical "as an example:

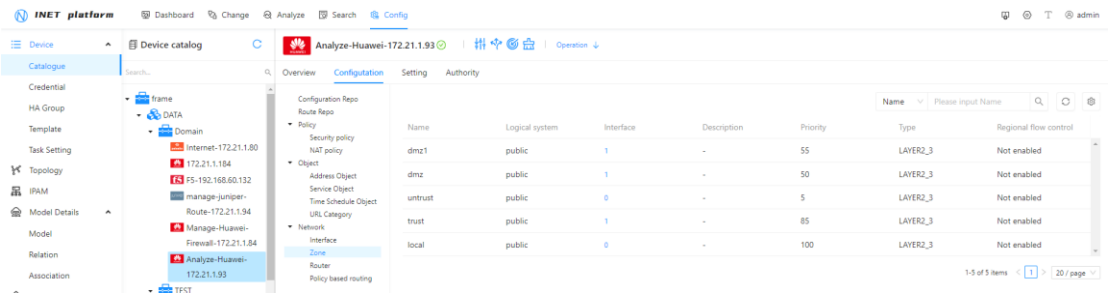


- **Name:** Interface name of firewall
- **Alias:** Alias for interface settings
- **Status:** The current status of the interface, divided into "enabled" and "not enabled"
- **IP address:** The IP address corresponding to the interface. If the interface does not have an IP, it will not be displayed
- **IPv6 address:** The IPv6 address corresponding to the interface. If the interface does not have IPv6, it will not be displayed

- **Zone:** The configuration of the security domain (i.e. zone) currently configured by the firewall, including system predefined and user-defined. Different manufacturers have different predefined security domains
- **Logical system:** The logical system of the firewall where the interface is located will have different displays depending on the firewall manufacturer
- **Virtual routing table:** The virtual router of the firewall where the interface is located. For example, Juniper's corresponding routing table has iNet.0, indicating that the interface is in the default routing instance, and vr. iNet. 0, indicating that the interface is in the routing instance of virtual router vr

Zone

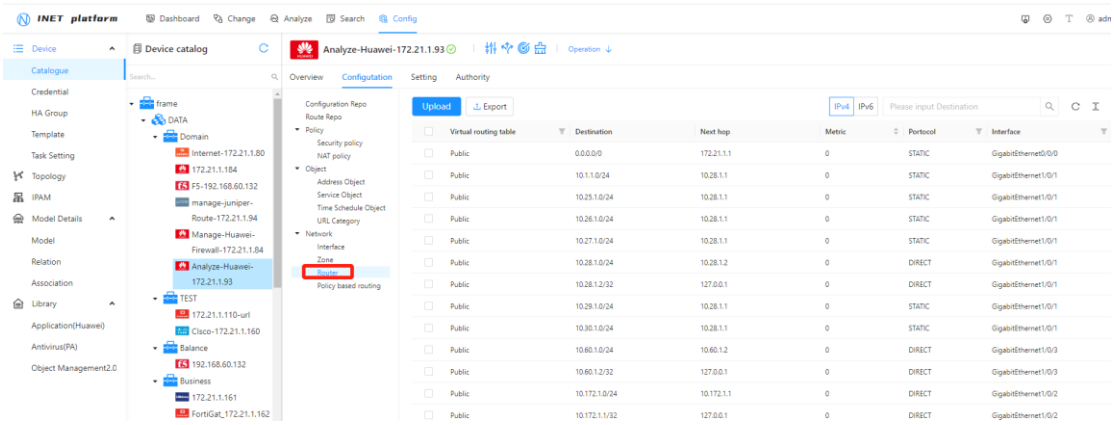
The 'Zone' mainly displays various security zones parsed from the firewall configuration, as shown below:



- **Name:** The name of the security zone
- **Logical System:** Name of the logical system where the security domain is located
- **Interface:** refers to the number of interfaces currently configured to this security domain

Router

Router "mainly displays the results of parsing the routing table collected from the firewall, as shown below:



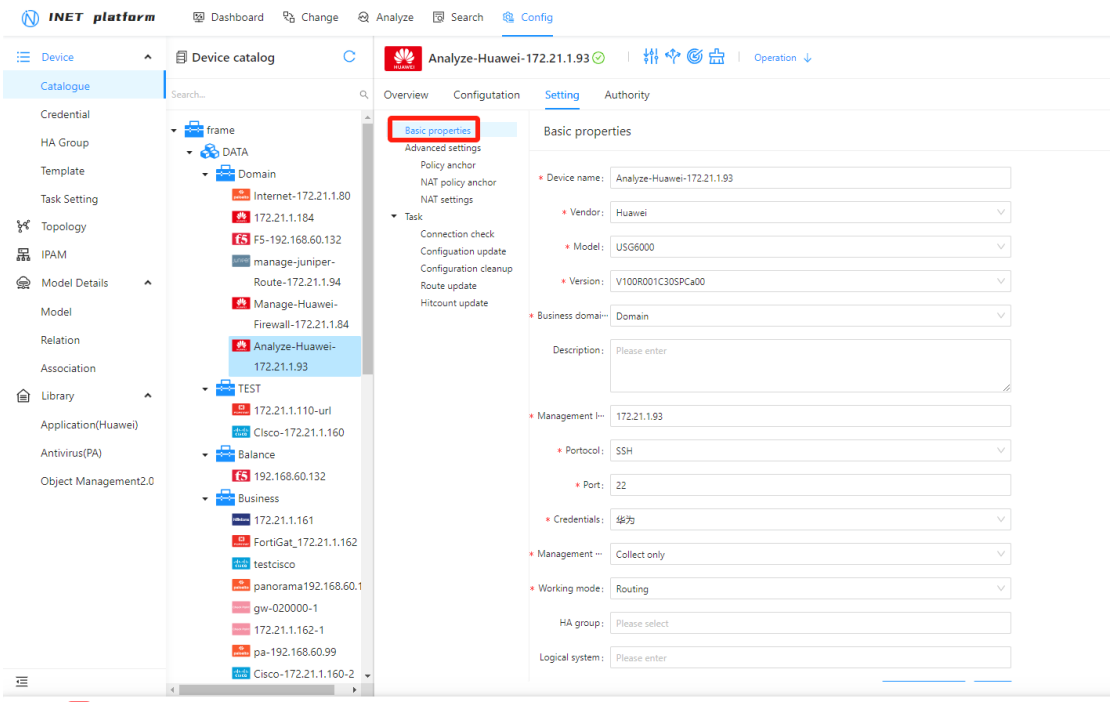
- **Virtual routing table:** The virtual routing table where the route is located
- **Destination IP:** The destination address network segment that the route points to. 0.0.0.0/0 is the default route
- **Next hop:** Refers to the gateway pointed to by the route, 0.0.0.0 is a direct connection route or a local route
- **Weight:** Routing weight value, similar to the distance value of a flying tower firewall
- **Protocol:** Refers to the protocol type corresponding to the routing, such as static for static and direct for direct routing
- **Port:** The port corresponding to the route. If the firewall configured route does not have a corresponding port, it will display "N/A"

4. 4. 4. Installation of piping equipment

It mainly refers to some basic settings related to the current firewall, including management methods, management options, and some basic information about the firewall.

4. 4. 4. 1. Basic attributes

The basic attributes include the manufacturer, device name, model, and other related information of the device.

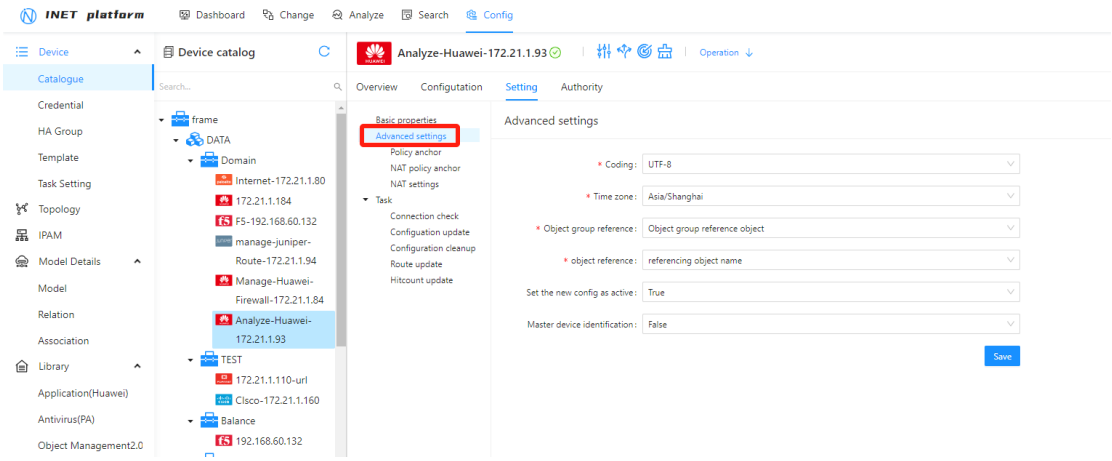


- **Device Name:** The name of the device
- **Manufacturer:** The manufacturer of the firewall, available from the dropdown menu
- **Model:** The model corresponding to this firewall can be selected from the drop-down menu
- **Version:** The version of the firewall that is running, available from the dropdown menu
- **Business domain:** The business domain in iNet corresponding to this firewall
- **Management IP:** The management IP address of the device
- **Protocol:** Manage the remote connection protocol used by this firewall
- **Port number:** The port number corresponding to the remote connection protocol used to manage this firewall
- **Connection credentials:** The "credential configuration" used when joining the device
- **Management mode:** Select "Collect and Distribute" or "Collect Only" from the drop-down menu
- **Working mode:** The mode in which the firewall operates, either in "routing mode" or "transparent mode"

- **Logical system:** If a single physical device creates multiple virtual instances, it is necessary to fill in the corresponding routing instance names, such as Juniper's test. int. 0

4. 4. 4. 2. Advanced setting

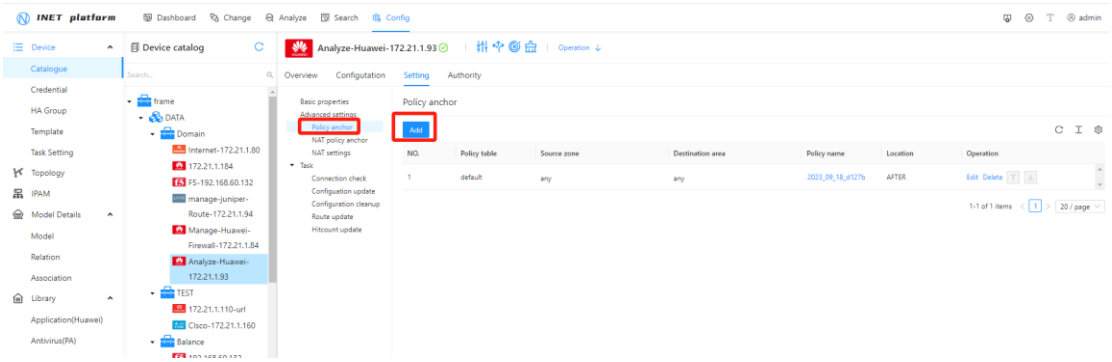
Advanced settings can configure text parsing encoding, time zone, object references, and other related information.



- **Encoding:** You can choose "UTF-8", "GB18030", "ISO-8859-1", and generally choose UTF-8
- **Time Zone:** The time zone where the device is located
- **Object group reference:** When issuing policy reference objects, choose to reference object groups or not to reference object groups

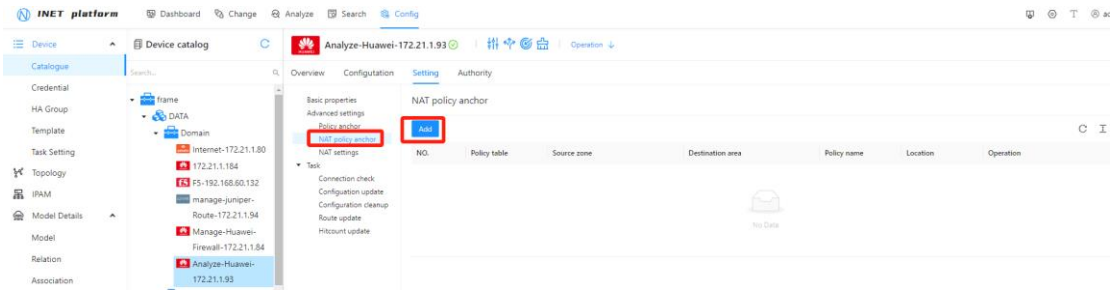
Strategic anchor point

When issuing security policies, sometimes it is necessary to choose to issue them before/after a certain policy. The iNet platform introduces the concept of policy anchors and clicks "Add" to select specific existing policies as policy anchors, defined as being issued before/after that policy anchor. In the policy anchor directory, the display and definition of policy anchors are shown in the following figure:



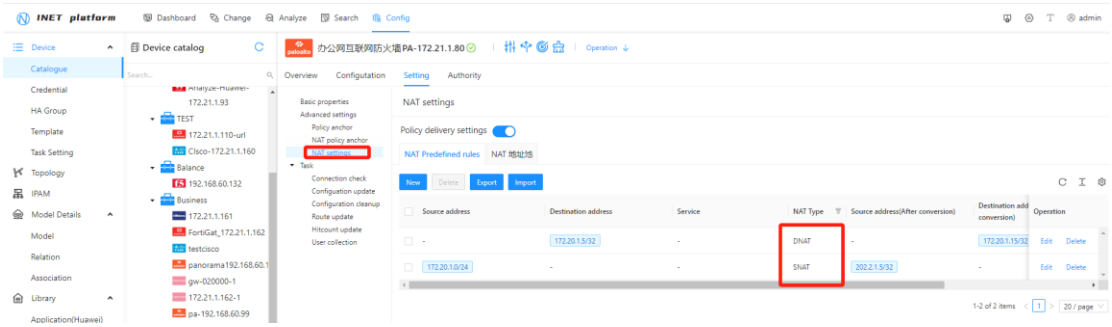
- **NAT Policy Anchor Point**

When issuing NAT policies, sometimes it is necessary to choose to issue them before/after a certain NAT policy. The iNet platform introduces the concept of NAT policy anchors and clicks "Add" to select a specific existing NAT policy as the NAT policy anchor, defined as being issued before/after that NAT policy anchor. In the NAT policy anchor directory, the display and definition of NAT policy anchors are shown in the following figure:



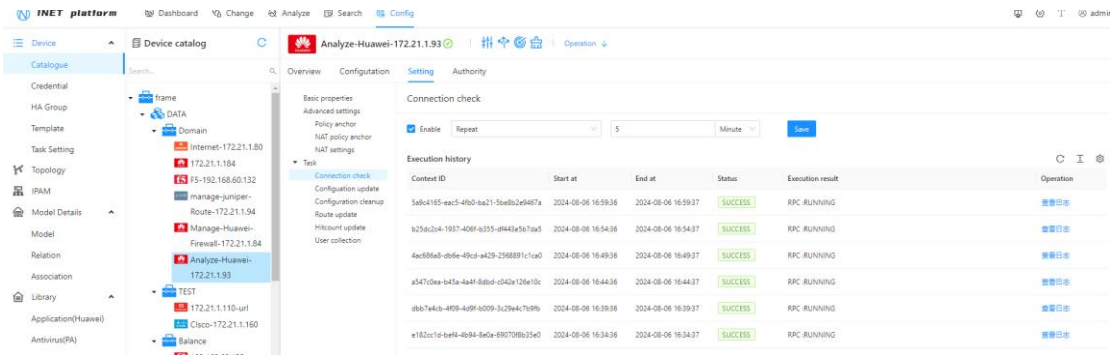
- **NAT settings**

In order to correctly analyze and locate NAT walls in path analysis, iNet platform needs to set NAT rules for NAT walls in advance. This way iNet can search for the corresponding NAT wall based on the NAT address in the work order.



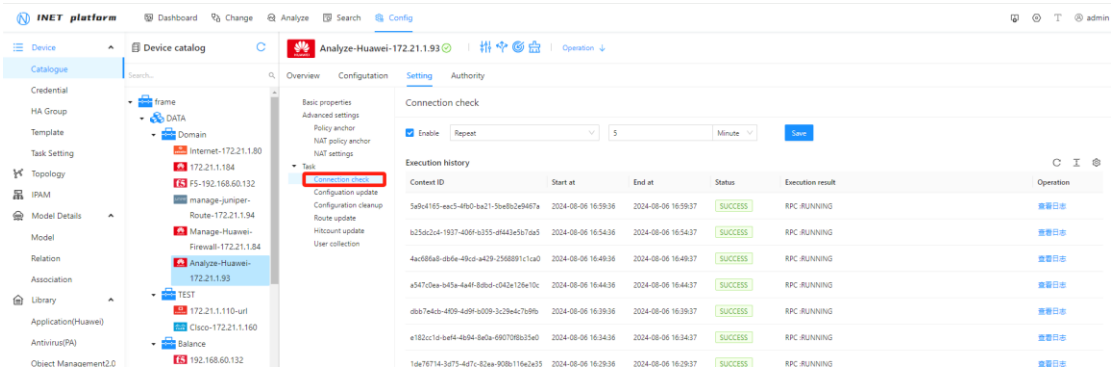
4.4.4.3. Task

The task refers to iNet management and collection of firewall logs and records. You can see the specific execution history and results. There are "connection status check", "configuration collection", "configuration cleanup", "routing collection", and "policy hit count collection".



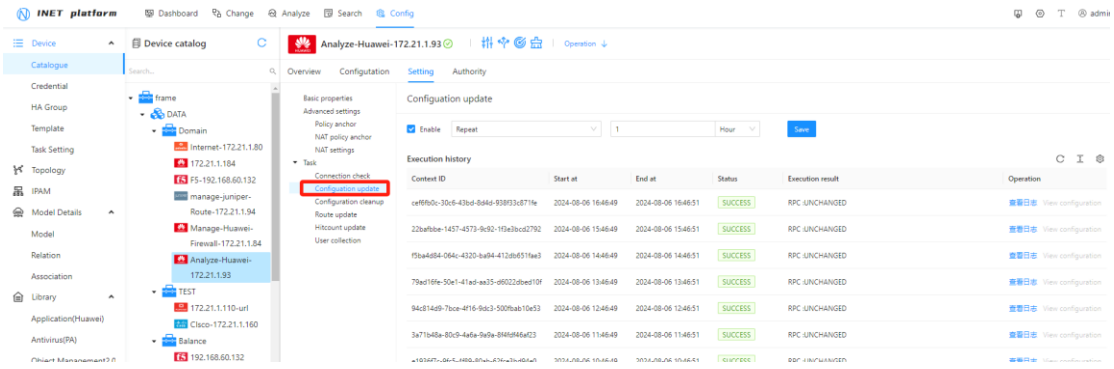
- **Connection status check**

Display the regular connectivity detection status of iNet platform and management equipment, with a default detection time of once every 5 minutes. The detection cycle EXCEPTION can be customized to SUCCESS indicate normal connectivity or connectivity failure. The logs can be viewed to confirm the cause.



- **Configure collection**

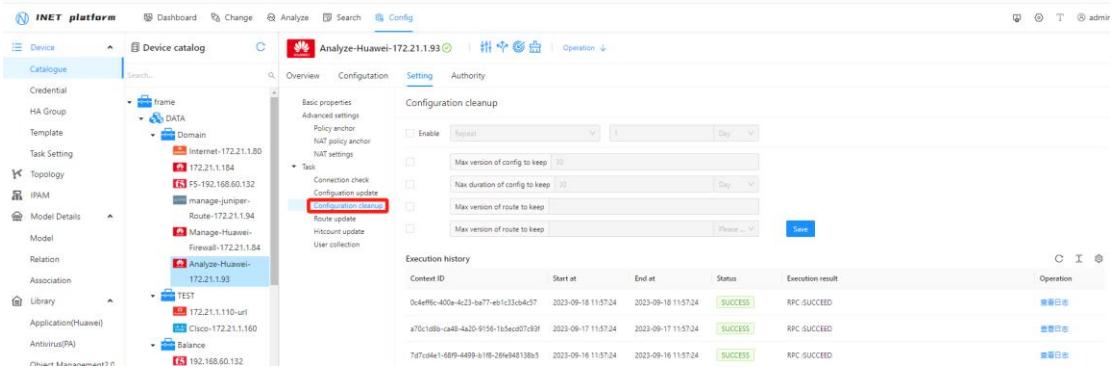
Display the iNet platform's regular collection and management equipment configuration, with a default of once every hour. The SUCCESS collection cycle can be customized and modified to EXCEPTION indicate successful or failed collection. You can check the logs to confirm the reason. Only when there are configuration changes will there be collection updates here. You can click View Configuration to view the current collection configuration file.



- **Configuration Cleanup**

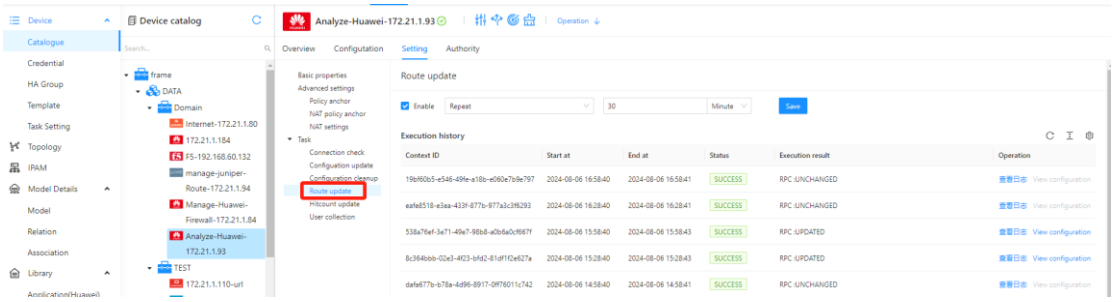
The iNet platform collects device configuration and routing information and stores it in a database. The platform saves 30 copies of configuration and routing files for a period of 30 days. If the number of copies exceeds 30, the earliest configuration/routing file will be deleted, and configuration/routing files that have exceeded 30 days will be automatically cleared. Support custom modification of the

number and time of configurations in the platform.



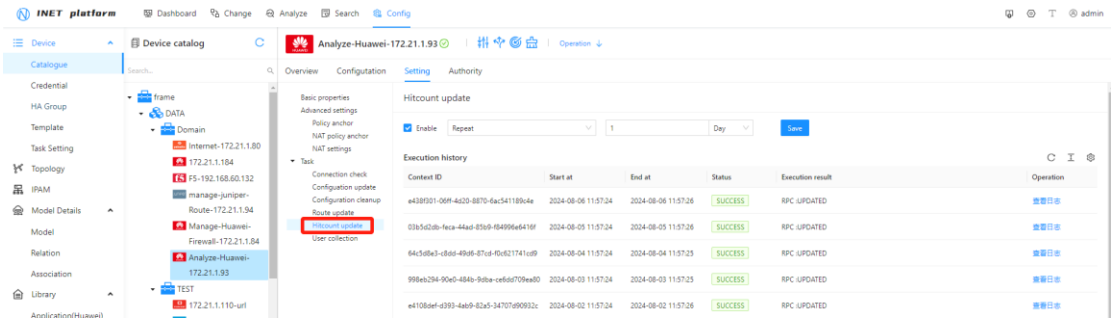
- **Route collection**

Display that the iNet platform regularly collects and manages device routes, with a default of once every 30 minutes. The route collection cycle can be customized to EXCEPTION SUCCESS indicate successful or failed collection. You can check the logs to confirm the reason. Only when there are route changes will there be collection updates here. You can click View Configuration to view the current route information collected.



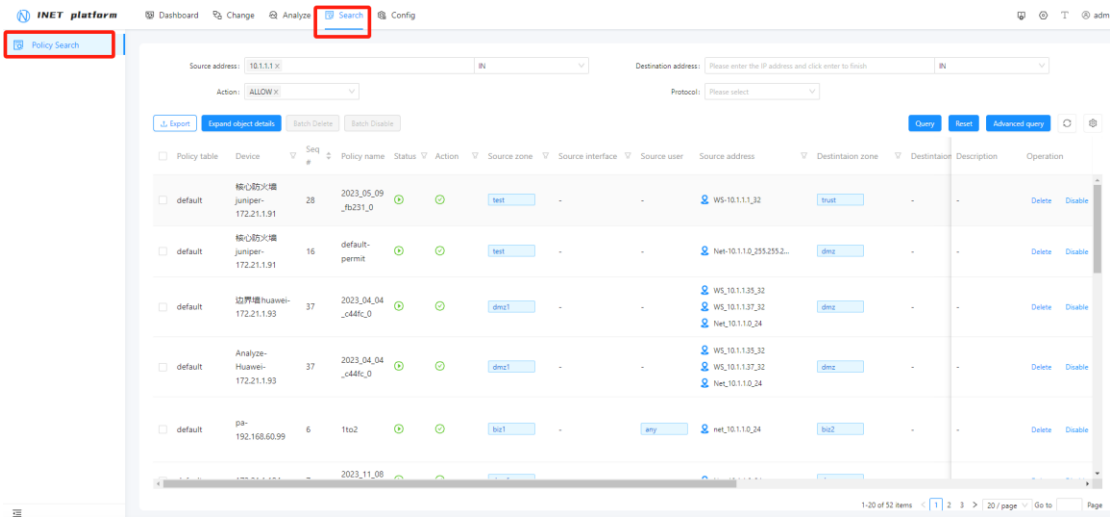
- **Collection of policy hit numbers**

Display the iNet platform's regular collection and management of device policy hit statistics, with a default of once a day. The hit collection cycle EXCEPTION can be customized to SUCCESS indicate successful or failed collection. The logs can be viewed to confirm the reason.



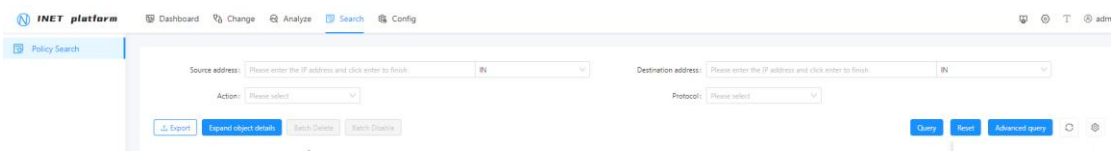
5. Policy Search

policy search is a global search of all managed firewall policies, which can perform policy queries on source addresses, destination addresses, actions, and protocols. It supports fuzzy queries, precise searches, multiple keyword searches, and can export search results in a table format. Search entrance: "Search - Policy Search"

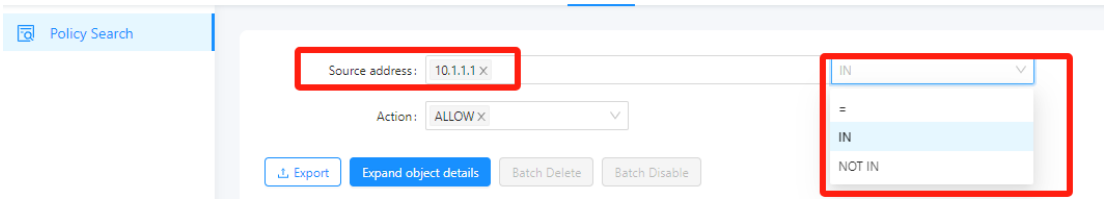


policy Search Method 1

Enter one or more items in the top column to check if there is a corresponding policy;



Source address, destination address: In the input field, enter the corresponding IP address or address range. The drop-down menu has three options: "=", "IN", and "NOT IN".

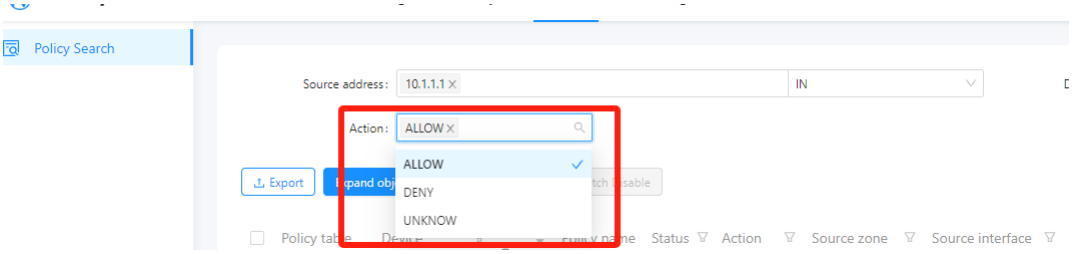


"**=**": Indicates filtering all policy addresses and finding policy addresses that match the input address;

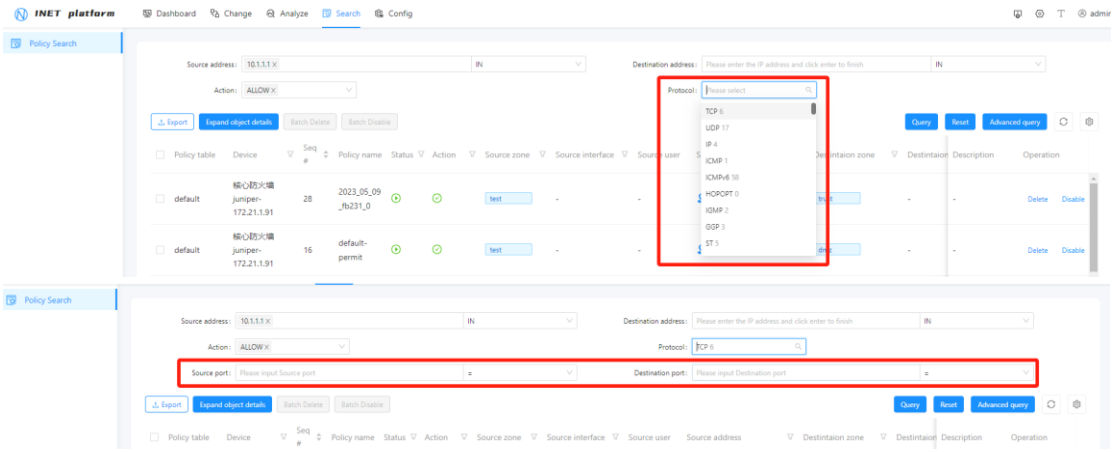
'**IN**': Refers to filtering all policy addresses and finding policy addresses that can contain input addresses, such as 192.168.1.100. Enter the address range of 192.168.1.0/24, and 192.168.1.0/24 addresses will be filtered;

'**NOT IN**': means to filter all policy addresses and find policy addresses that do not contain the input address;

Actions: including allow, deny, and unknown;

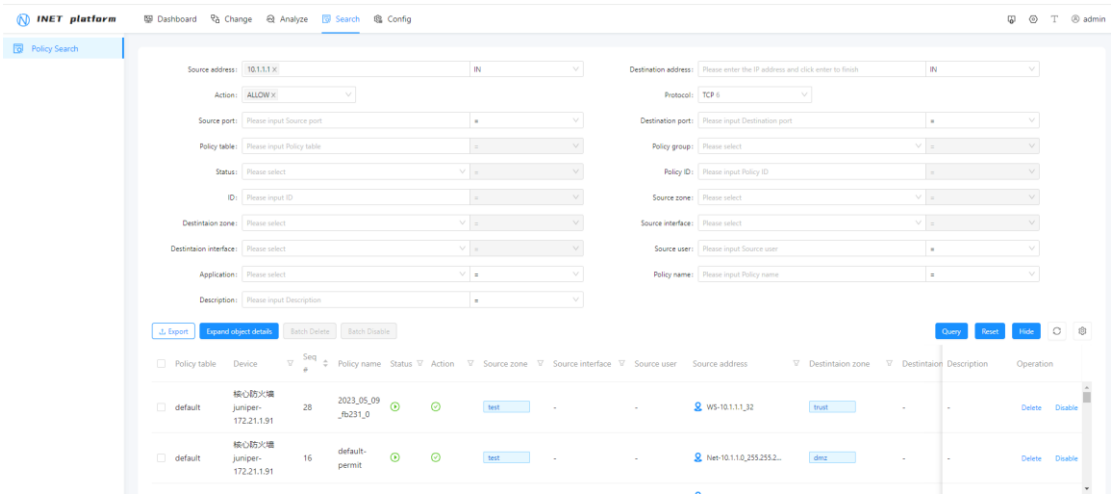


Protocol: including commonly used protocols such as TCP, UDP, and ICMP; After selecting the corresponding protocol, such as TCP, the source port and destination port will appear; The dropdown menu allows you to select "=", "IN", and "NOT IN" (using the same method and address). Choosing ICMP will display two options: type and code;



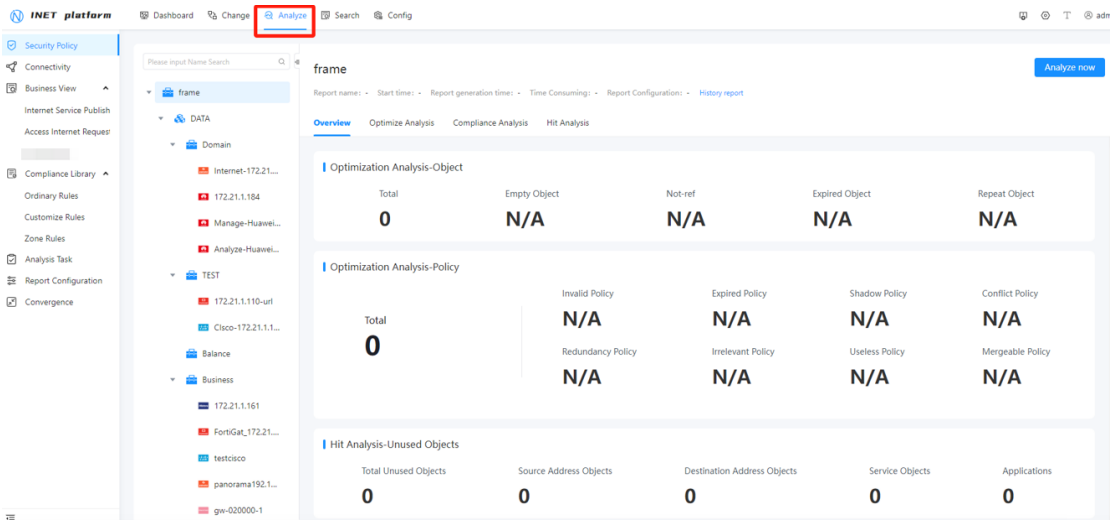
policy Search Method 2

Advanced search, click the advanced search button, so that the matching criteria elements of the search are more refined and the accuracy will be higher.



6. Policy analysis

policy analysis mainly includes "security policy", "connectivity analysis", "security compliance", "analysis tasks", "report configuration", and "policy convergence". The 'security policy' mainly refers to the analysis of the execution object and policy. Connectivity analysis is mainly used to perform policy path analysis, which visualizes whether the devices through which traffic passes have round-trip routes and relevant effective policies. Security compliance "mainly refers to defining a set of rules based on the actual needs of users. When analyzing policies, it is possible to detect whether the policies are compliant according to the rules. 'Policy convergence' mainly refers to the broad policy tightening of firewalls.



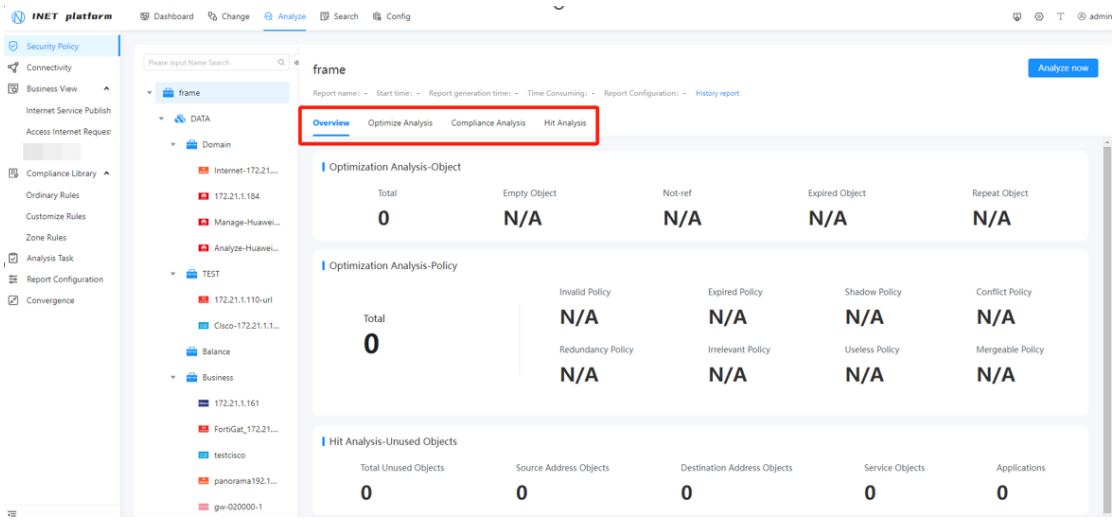
6.1. Security policy

The 'security policy' mainly refers to iNet's analysis of managed firewall objects and policies. After performing policy analysis and object analysis, display whether there are any abnormal or unreasonable configurations, provide suggestions and optimizations. After clicking on the corresponding device, the security policy function will display "Overview", "Optimization Analysis", "Compliance Analysis", "Hit Analysis", etc.

- **Overview:** Indicates some basic information about the current device;
- **Optimization analysis:** Optimization analysis includes object analysis and policy analysis. Object analysis refers to analyzing firewall objects (such as addresses and services) to see if there are empty objects, no reference objects, expired objects, duplicate objects, etc., and providing suggestions or optimization operations for these objects; policy analysis will analyze the phenomena of invalidity, expiration, concealment, conflict, redundancy, and merging in the current policy, and provide suggestions or optimization operations for these

policies;

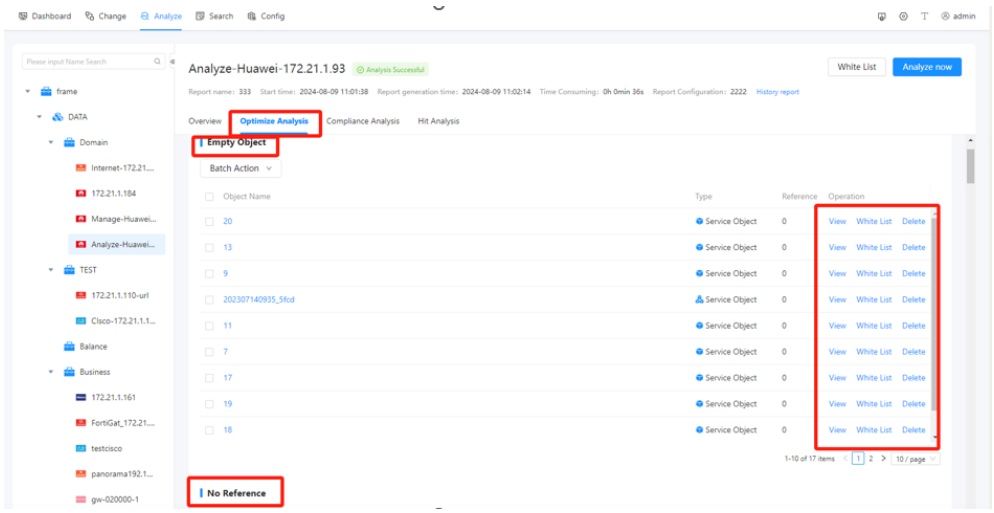
- **Compliance analysis:** It will analyze the statistical information of the high, medium, and low-risk rules defined by the hit platform in the current device policy, and click on the hit policy index to the policy;
- **Hit analysis:** Obtain the Hitcount of the device, collect the device's traffic logs for analysis, and analyze policies with zero hit counts over a period of time.



6. 1. 1. Optimization analysis

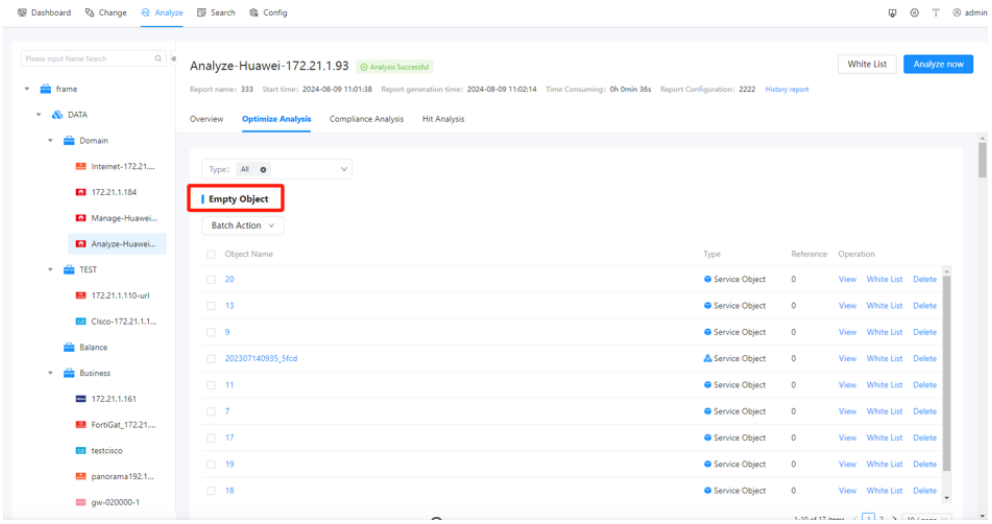
6. 1. 1. 1. Object analysis

Select the device, data center, or business domain that needs to be analyzed, click "Analyze Now", and start object analysis, policy analysis, compliance analysis, and hit analysis on the device. (If selecting a data center or business domain, analyze all devices under that architecture)

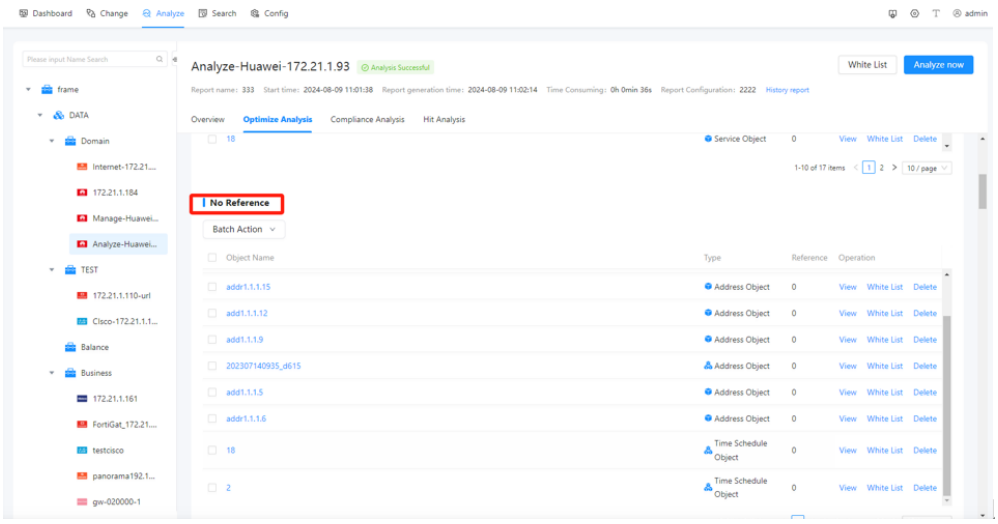


After the analysis is completed, click on "Optimize Analysis" to view the corresponding "Empty Objects", "No References", "Expired Objects", "Duplicate Objects", etc. You can

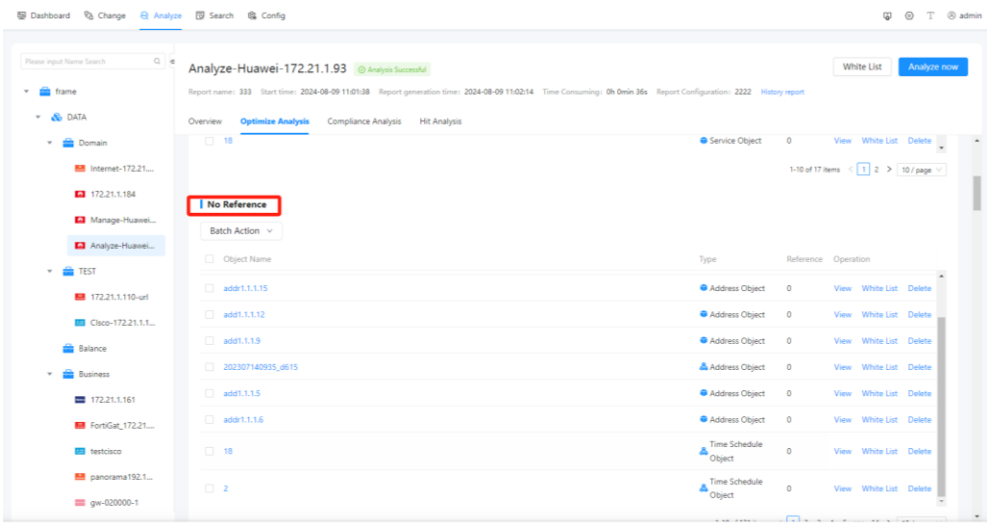
add them to the whitelist or delete them.



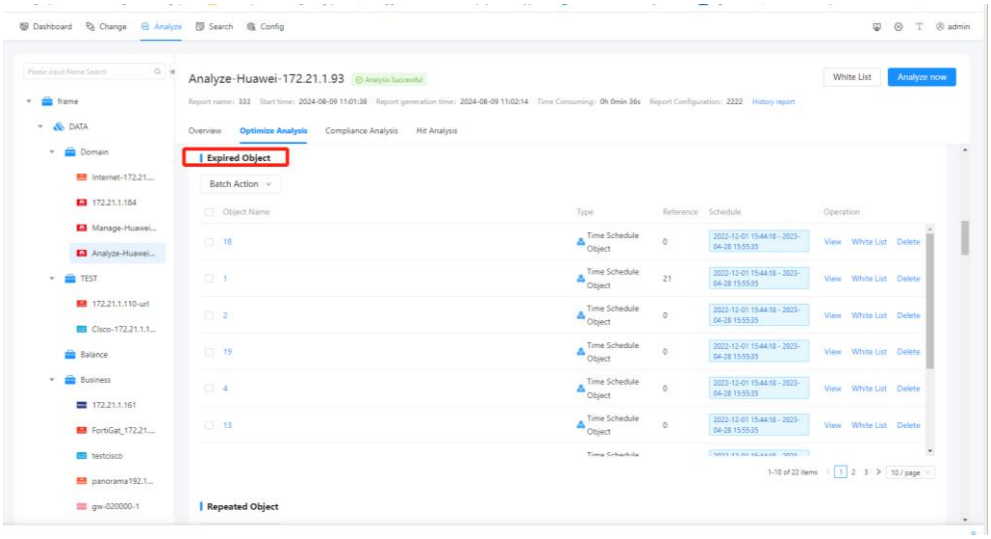
- **Empty object:** Only the object name, without actual address, service, or other object elements. Empty objects can be added to the whitelist (they will not participate in the next object analysis) and deleted;



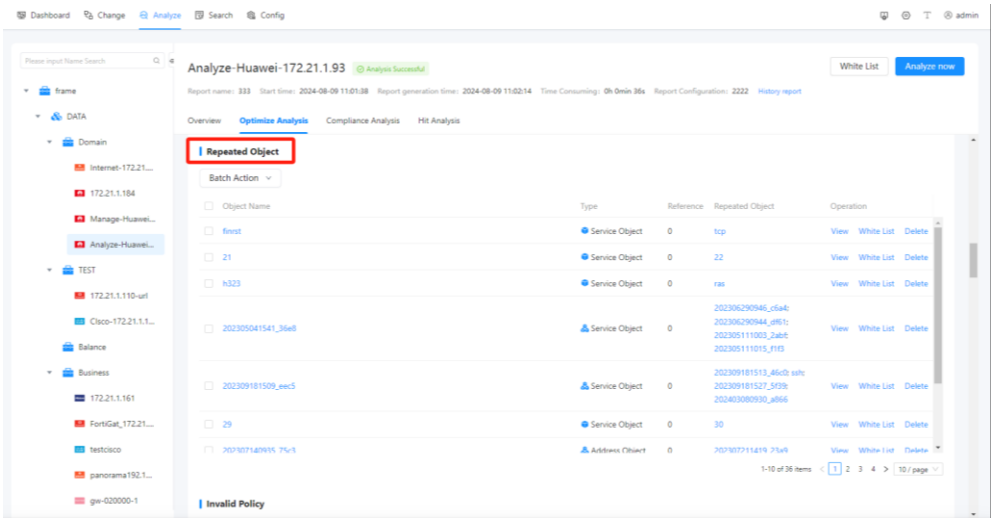
- **No reference:** Objects in the firewall are not referenced. No reference object supports whitelisting (will not participate in the next object analysis) and deletion;



- **Expired objects:** mainly for time objects. Expired objects can be added to the whitelist (they will not participate in the next object analysis) and deleted;

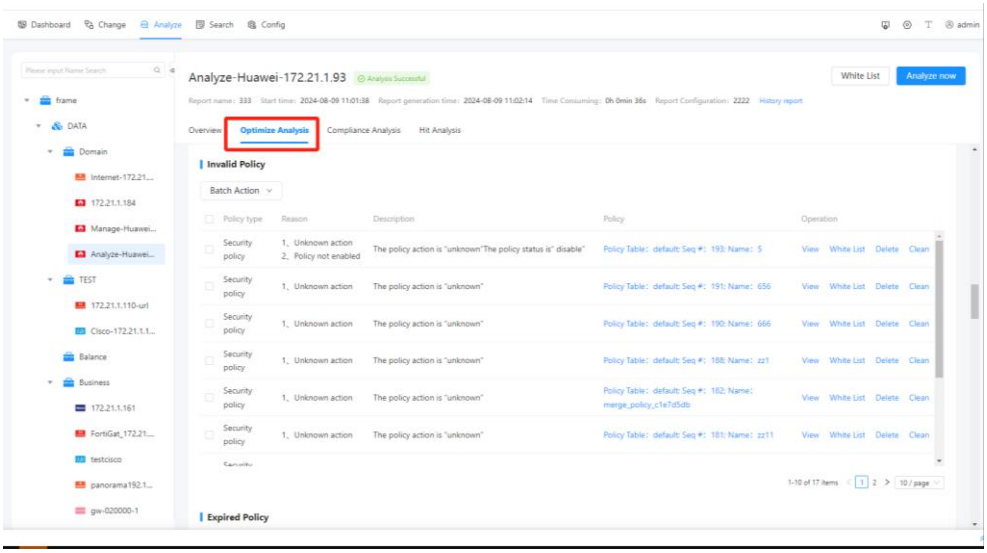


- **Repeated objects:** The names of objects are inconsistent, while the content elements are consistent. If a repeated object is not referenced, it can be deleted or whitelisted. If it is referenced, deletion is not supported, only whitelisting is supported.

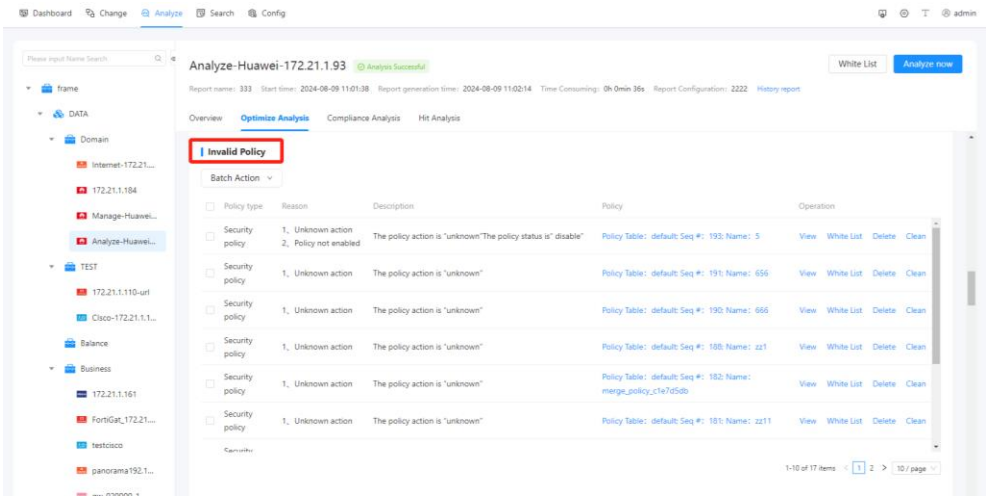


6.1.1.2. Policy analysis

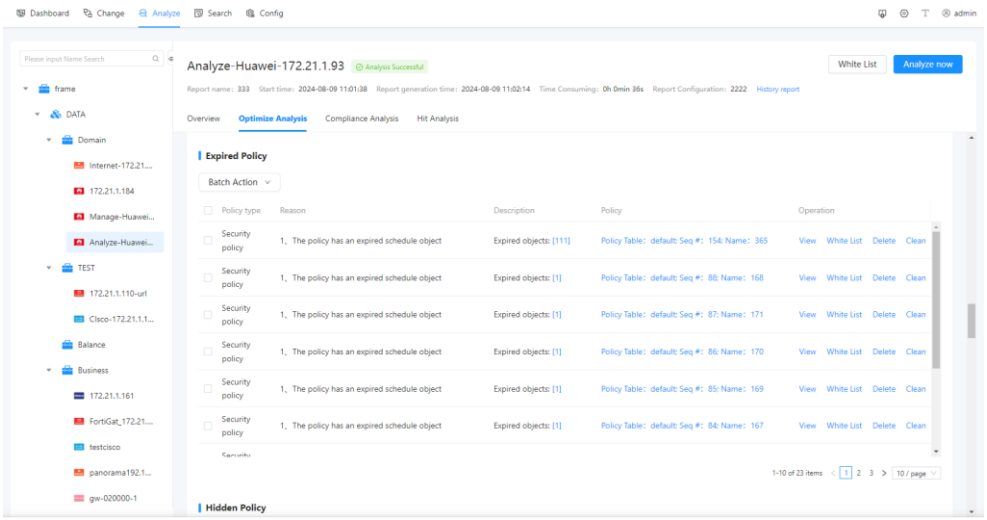
After clicking "Analyze Now", object analysis and policy analysis will be performed. The policy analysis function will analyze whether there are invalid, expired, hidden, conflicting, redundant, and combinable policies in the policy.



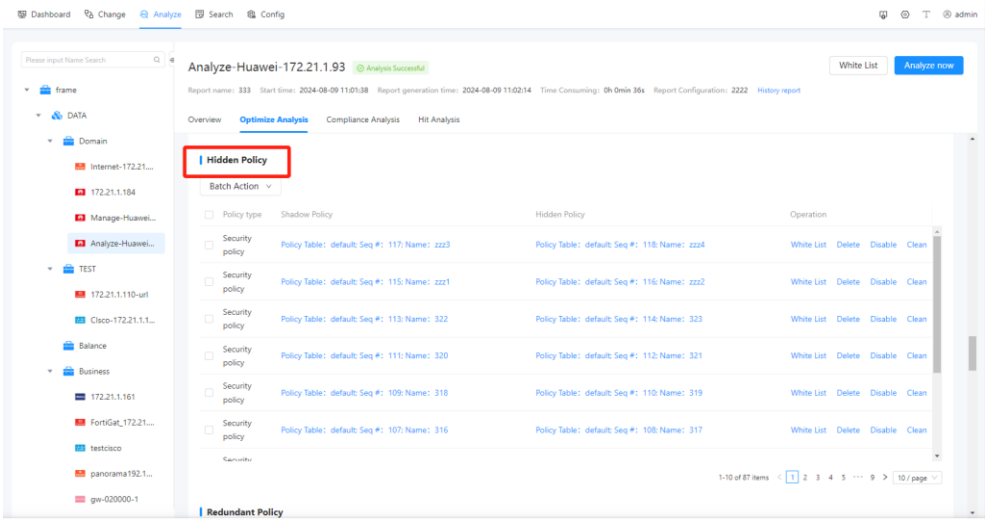
- **Invalid policy:** Refers to policies that are not enabled in the firewall, mainly referring to disabled or disabled policies. The page will prompt the reason and details, and indicate the policy name;



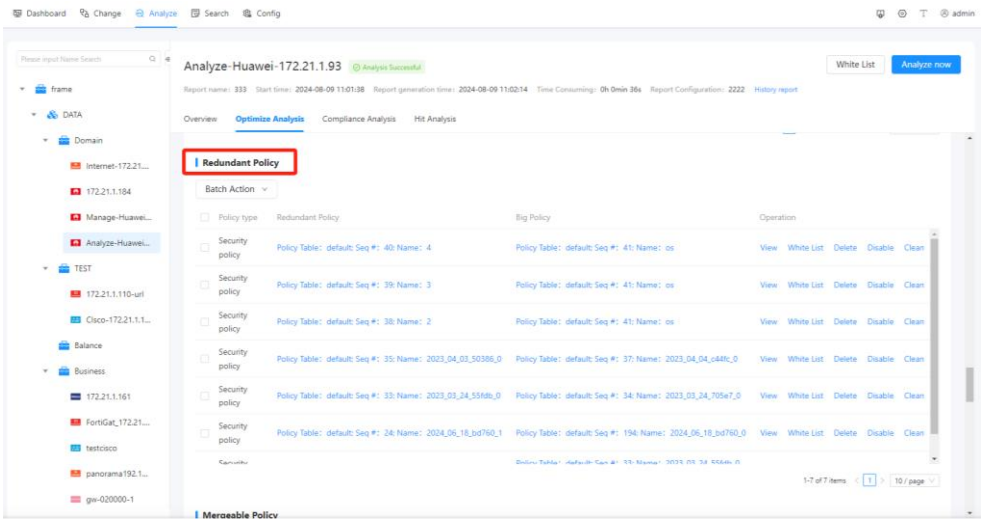
- **Expired policy:** If there is a policy that uses the "policy schedule" and the time has exceeded the schedule, the policy is in a deactivated state;



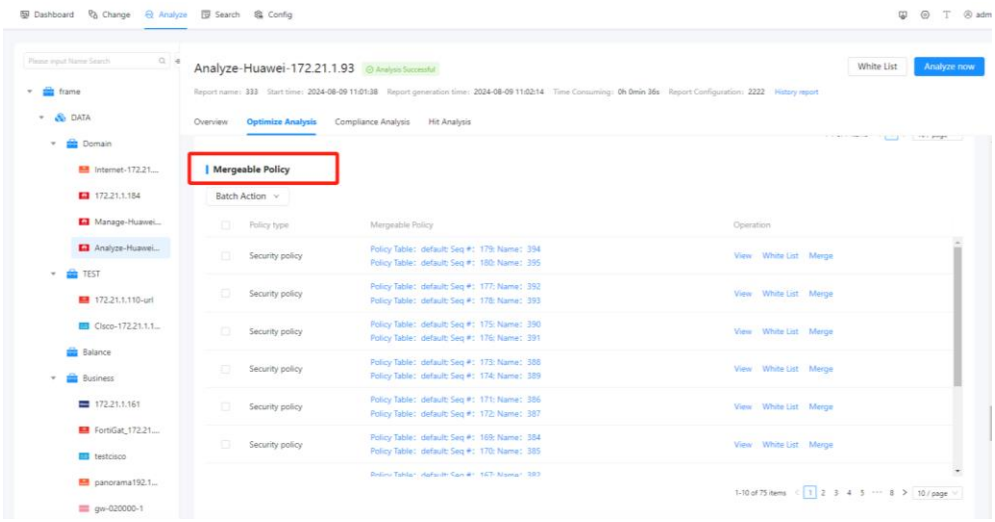
- **Hidden policy:** refers to the situation where there is coverage between policies, and the "big policy" covers the "hidden";



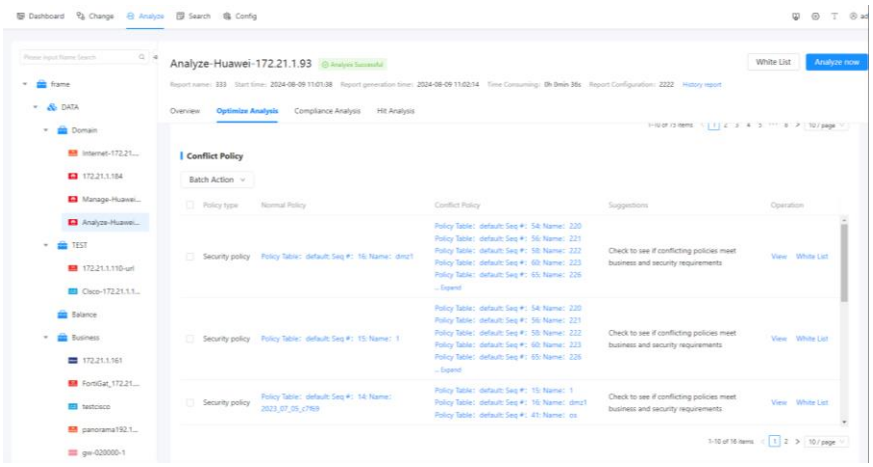
- **Redundant policy:** The previous policy allows some traffic and ports to pass, while the later policy allows for the release of additional traffic. The port number and address of the release are part or subset of the second release policy;



- **Mergeable Policy:** Two policies have only one element that is different, such as address or port. If all other elements are identical, it is considered that the two policies can be merged. As follows, if the addresses of the policies are the same and only the services are different, it can be considered that two policies can be merged into one policy.

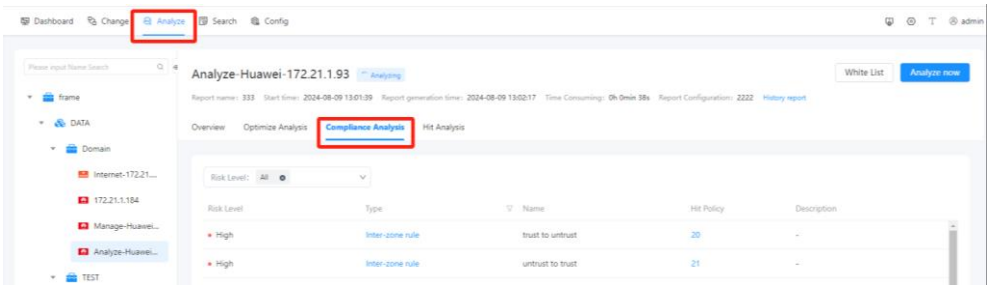


- **Conflict policy: The earlier policy opens up some traffic and ports, while the later policy blocks them. The port number and address for blocking are part or subset of the blocking policy;**



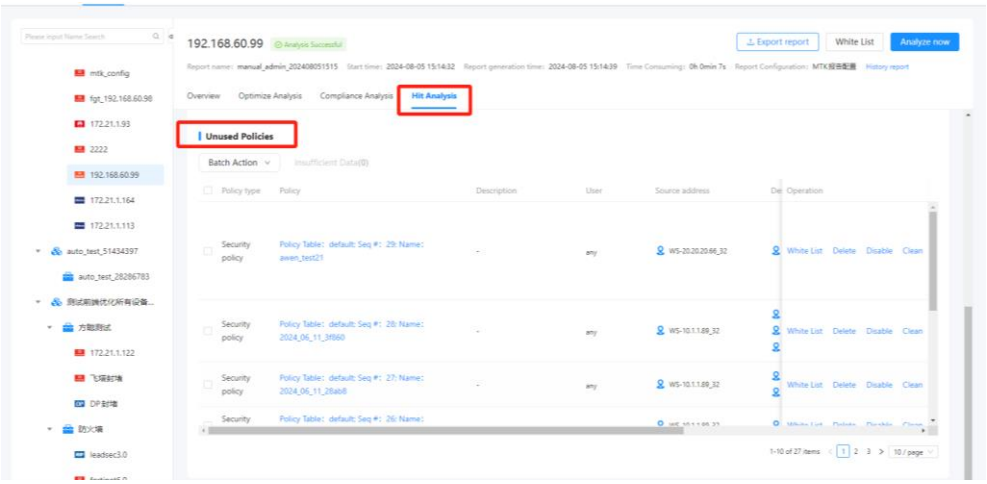
6. 1. 2. Compliance analysis

Compliance analysis is based on the rules of the security compliance library to conduct compliance analysis on new and existing policies, and also to view the policies hit in the compliance rules.



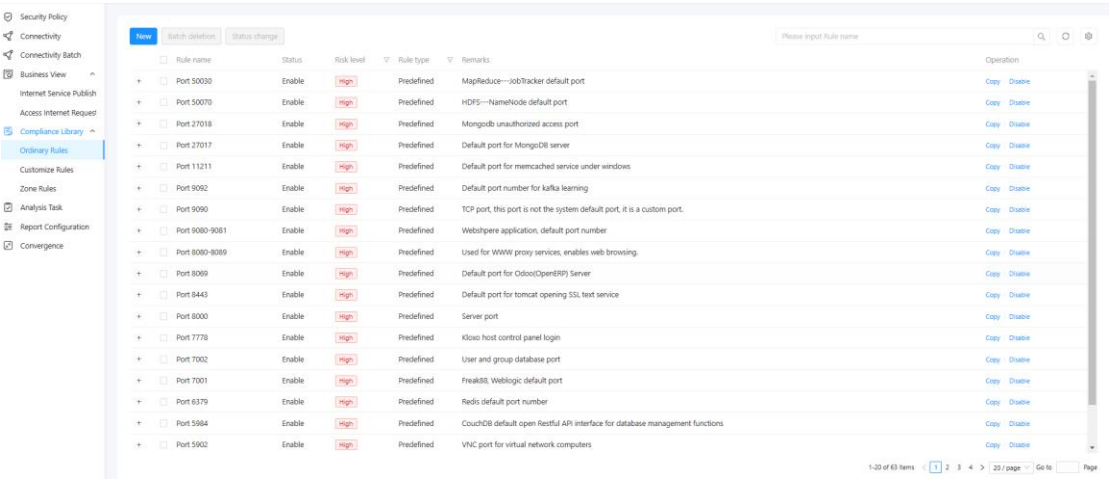
6.1.3. Hit analysis

Obtain the Hitcount of the device, collect the device's traffic logs for analysis, and analyze the policy with 0 hits over a period of time. View the statistics of hit sessions during specific time periods of the device, in order to intuitively understand the use of device security policies.



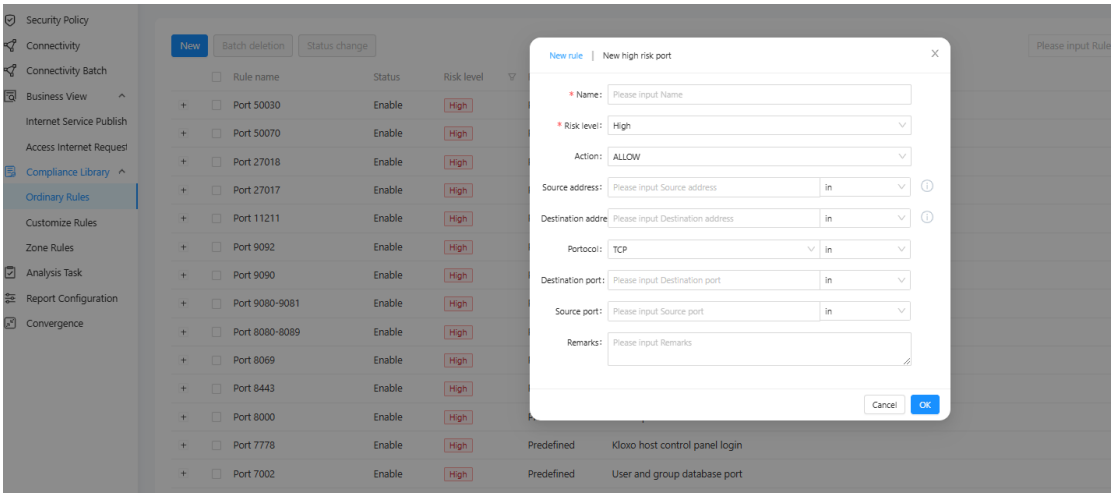
6.2. Compliance Rule Library

The compliance rule library list displays rule names, risk levels, rule types, comments, and operations (new, edit, disable, delete). There are two types of compliance rules: custom and predefined. The predefined ones have system settings and are automatically imported; Custom created by the user. There are already pre-defined high-risk ports in the compliance rule library, and security compliance rules and inter domain compliance rules can be customized based on IP and ports. Subsequently, compliance analysis will be conducted on newly added and existing policies based on the security compliance database, and policies that have been hit in compliance rules can also be viewed.



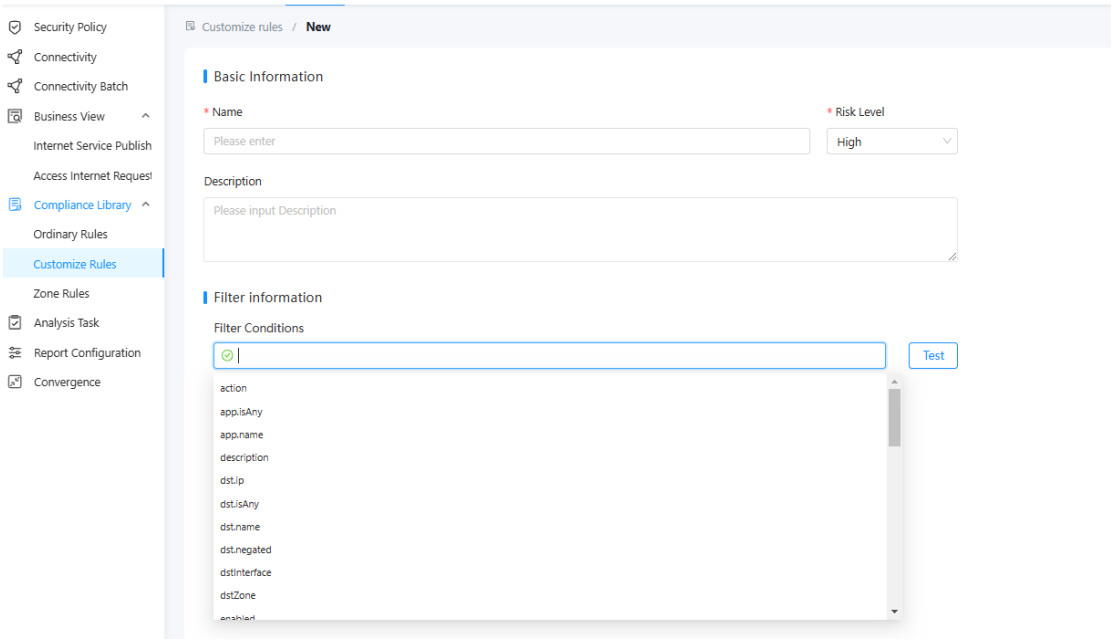
6. 2. 1. Customize regular rules

In Analyze →Compliance Library→ Ordinary Rules, click "New" to select "New Custom Rule" to create high-risk IP and high-risk IP+ports; You can also choose "New Custom High Risk Port" to create a high-risk port.



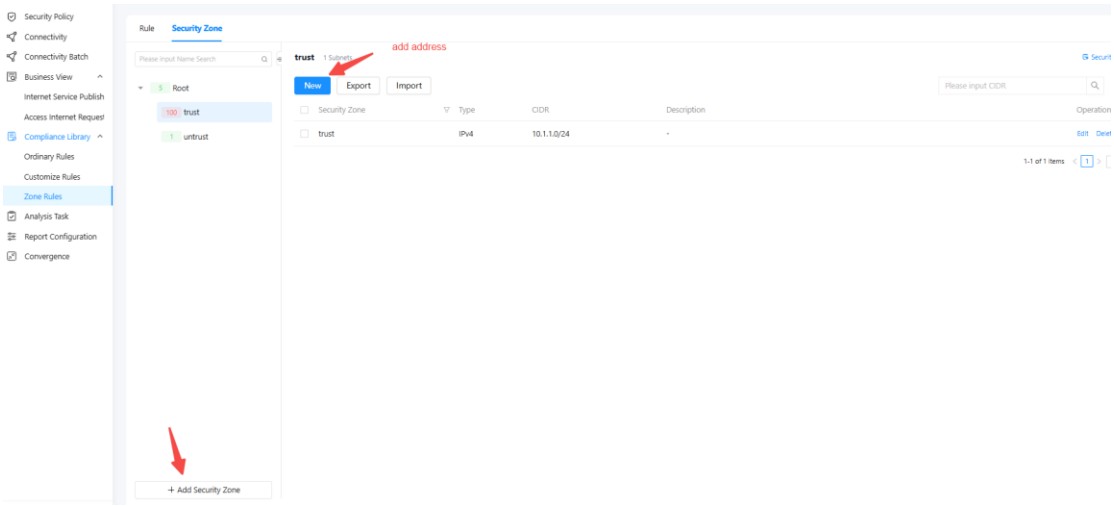
6. 2. 2. Custom Rules

In Analyze →Compliance Library→ Customize Rules, click "New" to customize security compliance rules through XQL statements, supporting perfect matching of multiple keywords.

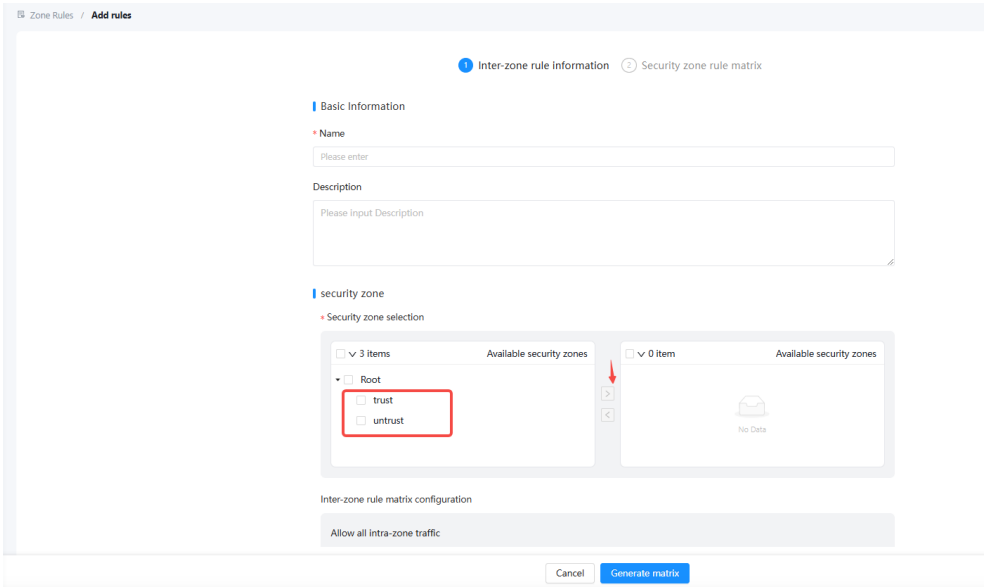


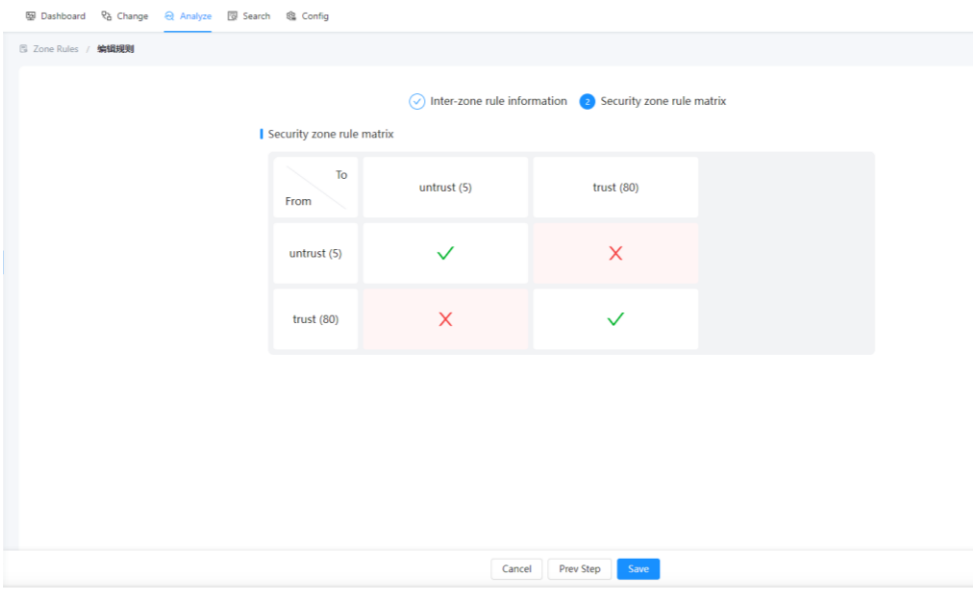
6. 2. 3. Zone rules

In the Analyze → Compliance Library → Zone Rules, click on "Security Zone" to define a security zone. Multiple zones of different levels can be defined, and multiple subnets can be bound to each zone.

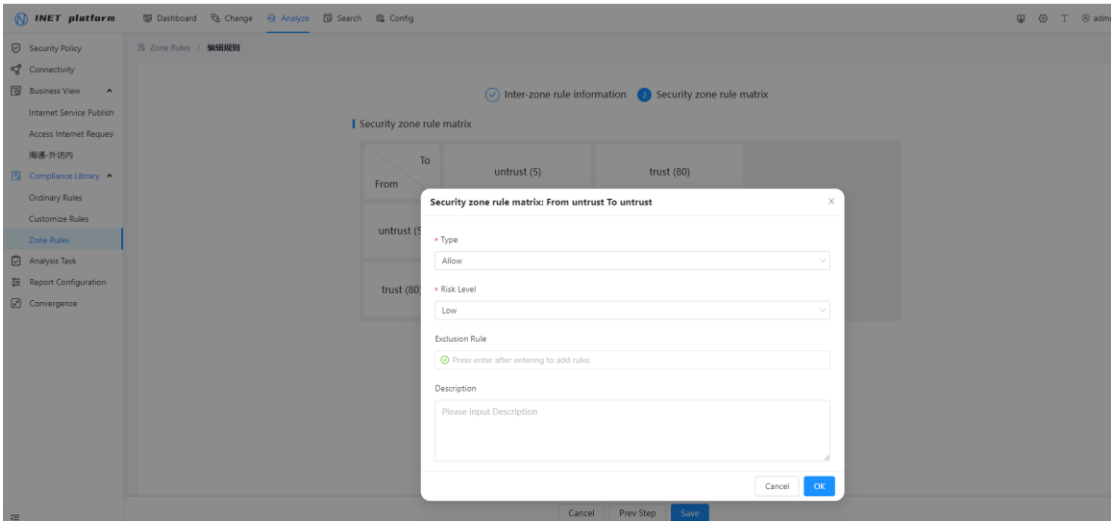


After defining the region, click "Rule" to create inter domain access rules for different regions. Click "New", select multiple regions, enter the allowed inter domain access level difference, and click generate matrix.



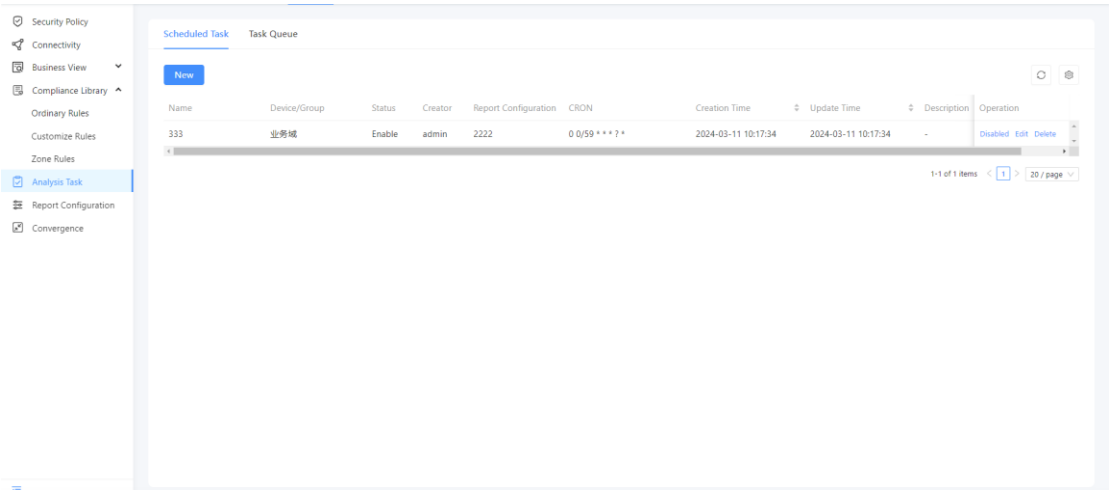


After generating the matrix, it supports clicking the " √ " and "×" symbols to allow or prohibit access modification.

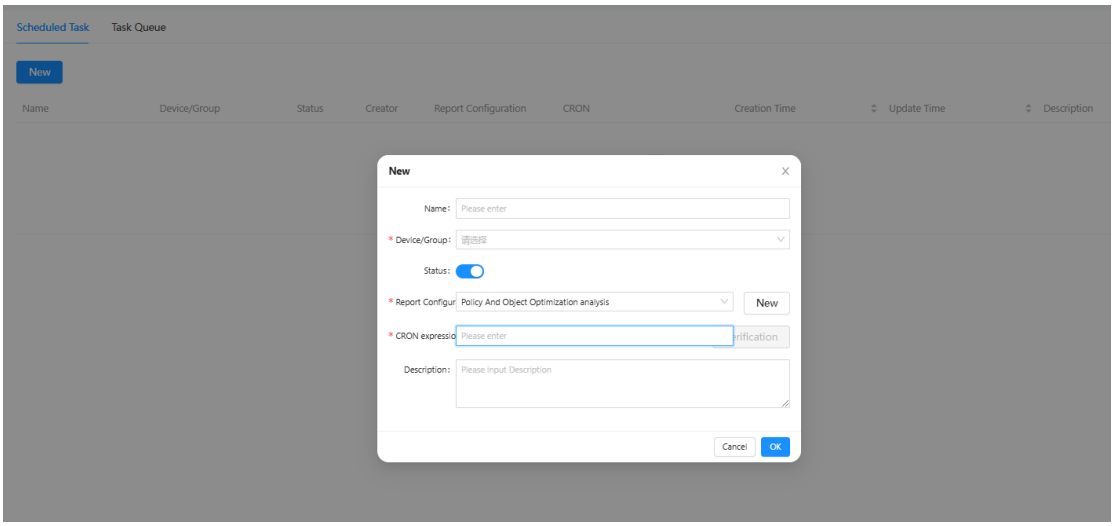


6. 3. Analysis Task

Support for adding new tasks, specifying devices or device groups, and selecting appropriate tasks for regular data analysis.



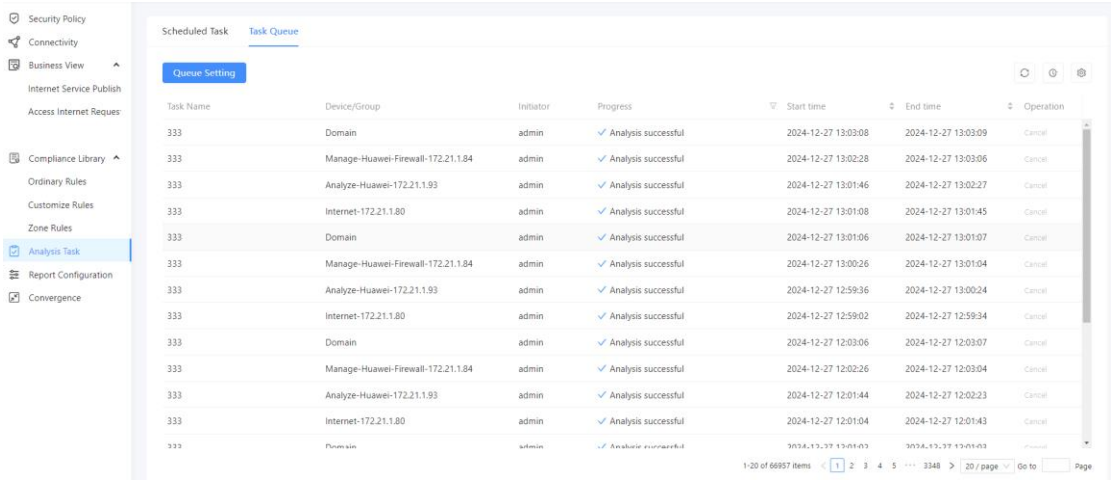
- **NEW:**Add Scheduled Task
- **Device/Group:** Supporting the specification of devices or device groups for analysis tasks.
- **Report Configuration:** Specifying the analysis data for devices/groups, such as policies, objects, compliance, etc., for any combination.
- **Cron Expression**: Used to specify the analysis time for devices/groups.



- **Task Queue：**

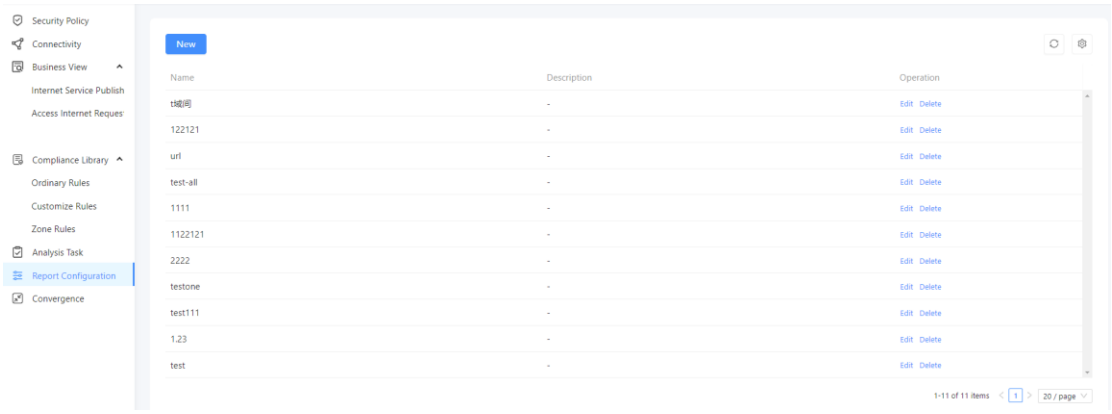
Records of All Executed Analysis Tasks

- **Queue Settings：** Queue concurrency limit settings.

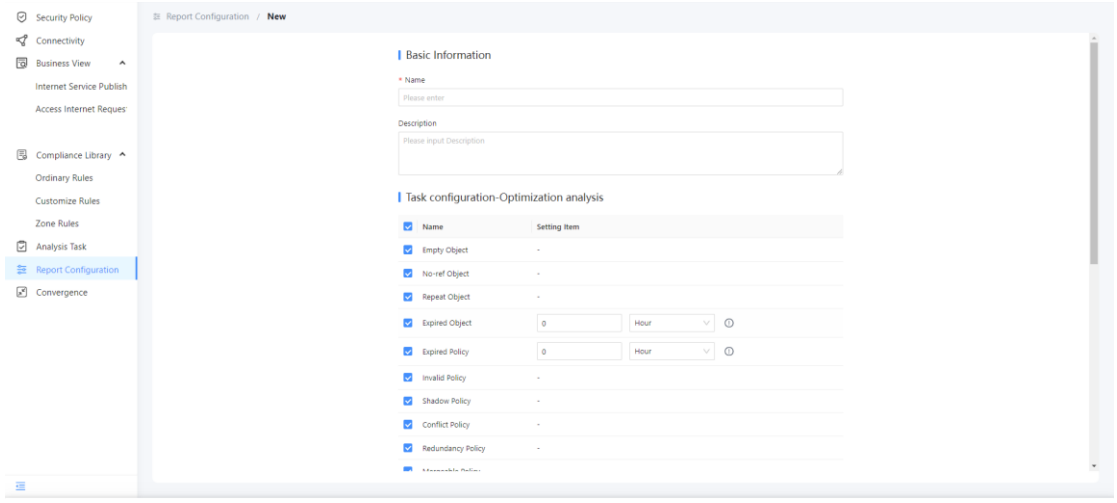


6.4. Report Configuration

For designating analysis projects, and supporting task reuse across multiple firewalls.



- **Add task settings:**Support defining analysis tasks and specifying related analysis projects.



6.5. Convergence

The feature supports traffic-based collection, after a specified analysis period, it

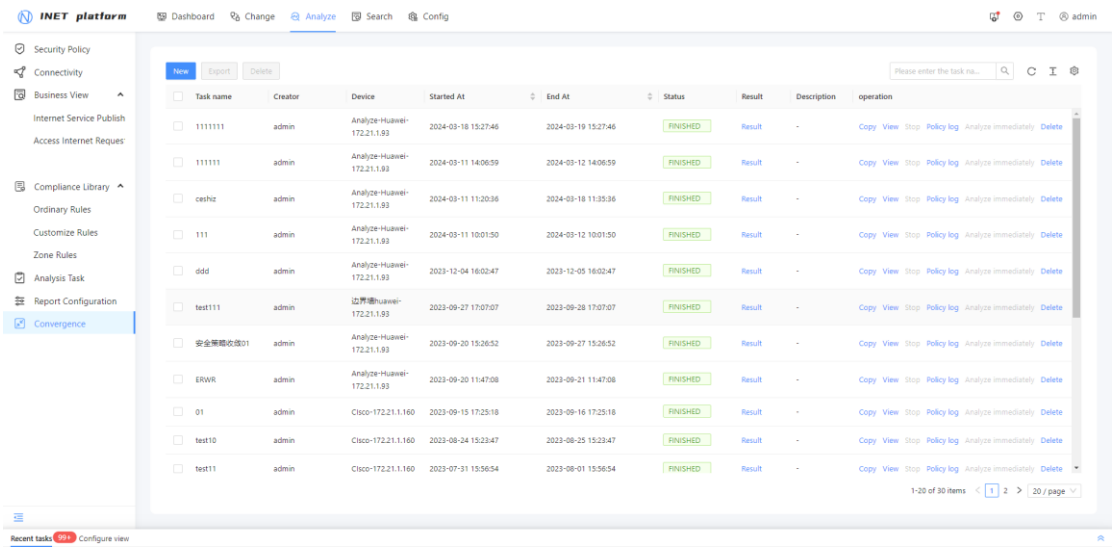
converges large policies into multiple smaller policy data information.

New: Add a convergence task.

Copy: Copy the task

View: View the task's execution time and parameters.

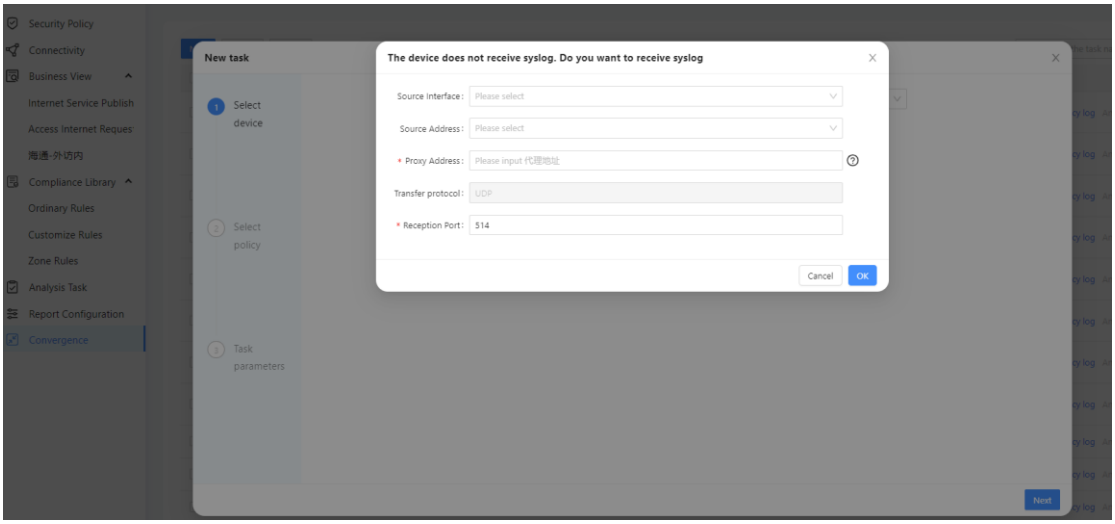
Result: Support for viewing task results.



6.5.1 Create Convergence Task

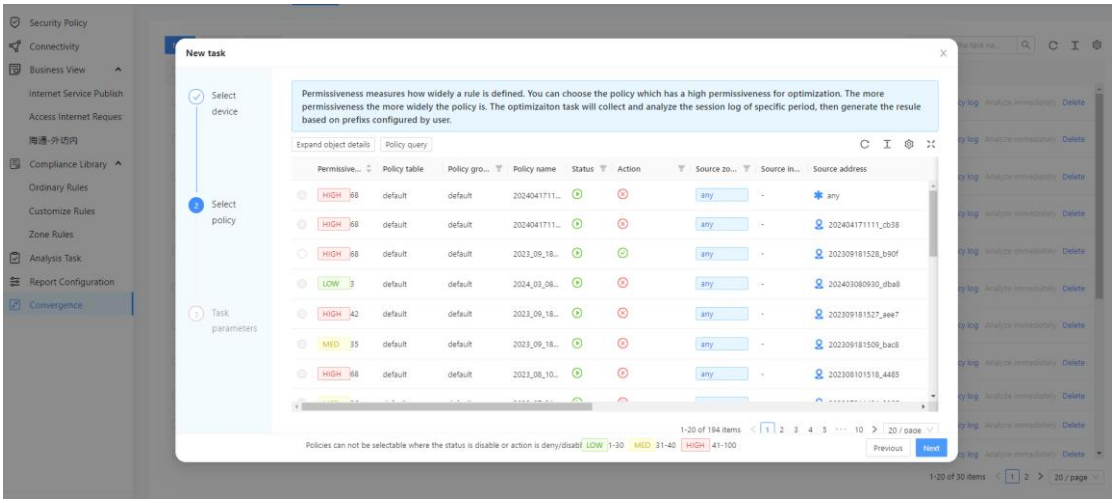
Create Convergence Task,It will check if the device has already enabled syslog reception

- **Source Interface:** The interface through which the device sends syslog
- **Source Address:** The address from which the device sends syslog (must be consistent with the managed address).
- **Proxy Address:** The specified address for accepting syslog (iNet address).
- **Reception Port:** The default port is 514.



Select Policies for Convergence

- **Policy Query:** Supports searching for policies within the device for precise querying of large policies.
- **Scoring Explanation:** Based on the IP range and port range allowed by the policy, the higher the score, the more lenient the policy is.



New Task

- **Task Name:** The information for the execution of this convergence task.
- **Merge Subnet List:** The granularity that needs to be converged, such as wanting to converge a large policy into multiple detailed policies with 24-bit or 28-bit subnets.
- **Analysis Time:** The time required for data to be converged, such as one day, meaning that after enabling this task, all traffic information from the start to

within one day will be analyzed and converged into the corresponding granularity.